Topic No 1: What is Information Security?

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **IT Security** is information security applied to technology
- **Information security** also covers physical security, human resource security, legal & compliance, organizational, and process related aspects
- **IT Security functions:**
  - Network security
  - Systems security
  - Application & database security
  - Mobile security
- **InfoSec functions:**
  - Governance
  - Policies & procedures
  - Risk management
  - Performance reviews
- **What is Cyber Security?**
  - Precautions taken to guard against unauthorized access to data (in electronic form) or information systems connected to the internet
  - Prevention of crime related to the internet
- Three Pillars of Information Security:
  - **Confidentiality**: keeping information secret
  - **Integrity**: keeping information in its original form
  - **Availability:** keeping information and information systems available for use

Topic No 02: Why Is Information Security Needed?

- **Bangladesh Bank SWIFT Hack – Feb 2016:** Hackers used SWIFT credentials of Bangladesh Central Bank employees to send more than three dozen fraudulent money transfer requests.
  - Requests sent to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
  - USD 81 million stolen
  - Total impact could have been USD 1 billion

NHS

NHS cyberattack is 'biggest ransomware outbreak in history'

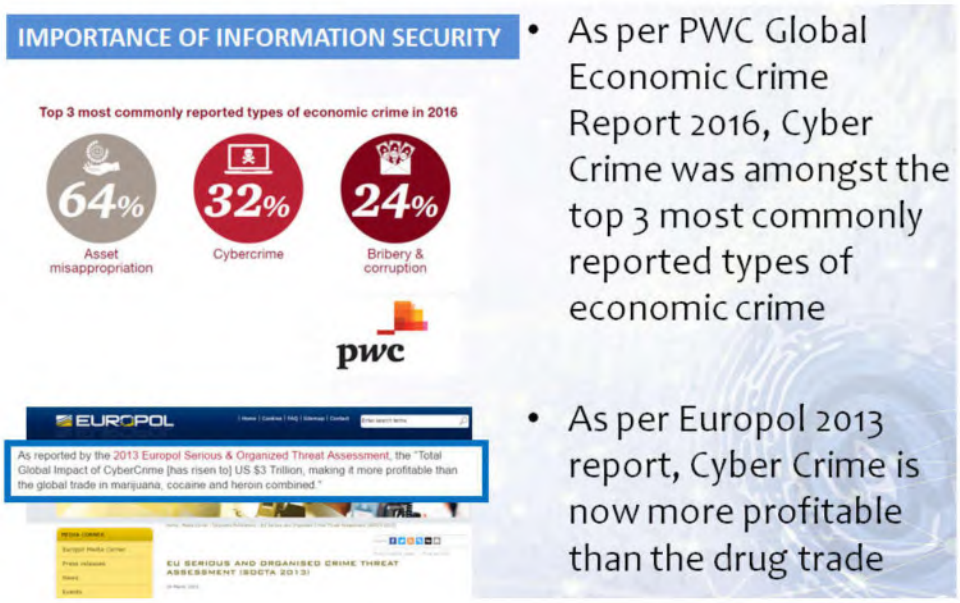
The NHS hack using Wanna Decryptor ransomware has shut down IT systems with 75,000 attacks in 99 countries

Ransomware attack hits 99 countries with UK hospitals among targets – live updates

Screenshot of the suspected ransomware message on a GP's computer in the Greater Preston area CREDIT: PA

- **The Importance Of Information**
  - IT is pervasive in our society & critical to the Ops & Mngmt of all organizations

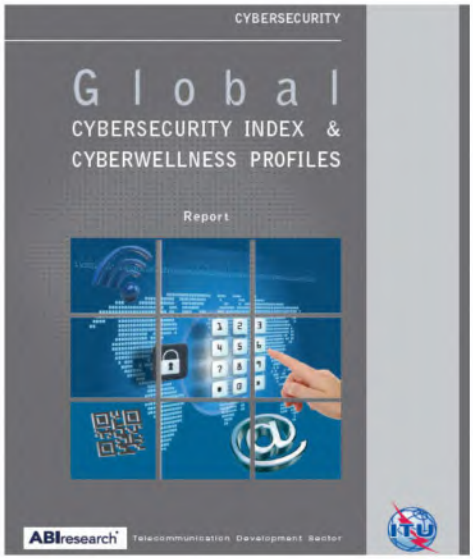
- IT is an enabler for business and govt
- Personal information is vital for individuals to function in society
- Information holds value



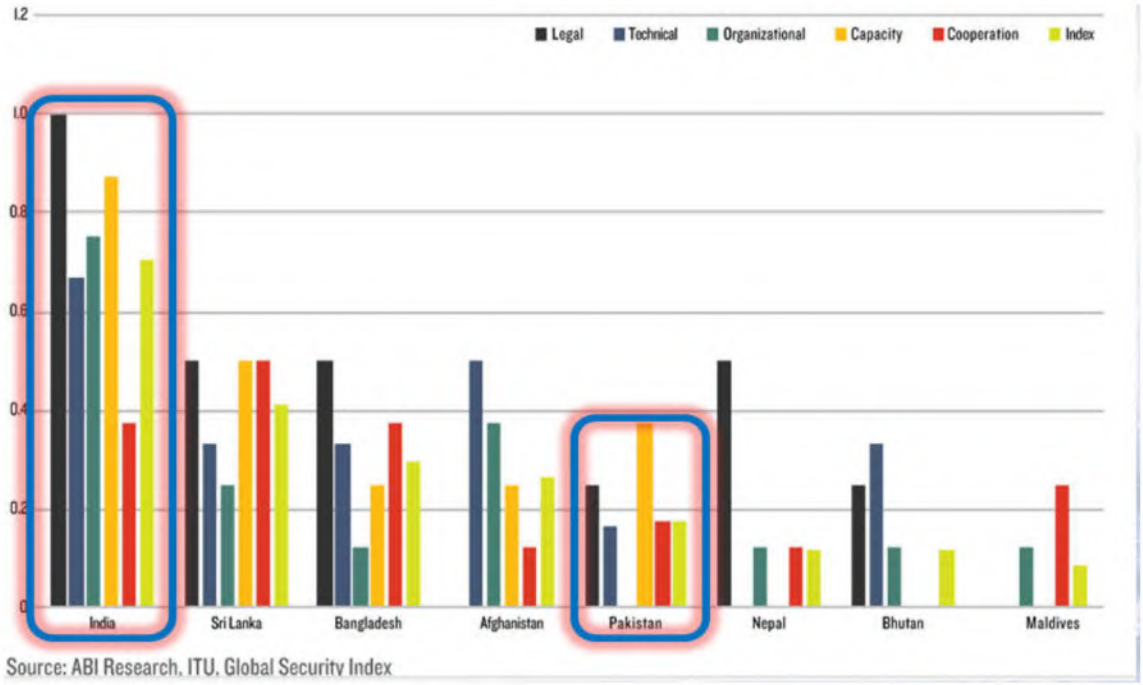
Topic No 03: Who Is Information Security For?

- **Personal:**
  - Social media passwords and safe usage
  - Online banking and email account passwords
  - Home PC/laptop security
  - Mobile security
- **Organizational:**
  - Board and executive leadership (management commitment)
  - CISO (responsible to drive security program)
  - IT staff and business users (following information security policies & procedures)
- **Govt and national:**
  - Law enforcement
  - Legal and policy making

  - National database
  - Critical infrastructure
  - Regulation
  - Standards and certification
  - Capacity-building and coordination



- Legal
- Technical
- Organizational
- Capacity building
- Cooperation



- Pakistan ranked almost at the bottom of the table in International ranking by ITU
- Information security is everyone's responsibility
- Pakistan Cyber Security Association (PCSA) formed to address Pakistan's international ranking

Topic No 04: How Is Information Security Implemented?

- **Three pillars of information security:**
  - People
  - Process
  - Technology

- **Leadership commitment:**
  - "Tone at the top"
  - Information security policy and objectives
  - Assigning responsibility and authority
  - Resource allocation
  - Performance reviews
  - Ensuring accountability
- **Information Security Manager or CISO:**
  - Heads department responsible for implementing information security program

    Directs planning, implementation, measurement, review, and continual improvement of program
- **IT user:**
  - Understand policies
  - Conduct security/risk assessment
  - Design effective security architecture
  - Develop SOPs and checklists
  - Implement controls
  - Report incidents
  - Conduct effective change management
- **Business user:**
  - Security awareness and training
  - Follow information security policy
  - Develop and implement secure business processes

- Role-based access control and periodic reviews
- Reporting incidents

- **Information security program**
  - Assessing security risks and gaps
  - Implementing security controls
  - Monitoring, measurement, & analysis
  - Management reviews and internal audit

    Accreditation/testing

Topic No 05: Who Are The Players In Information Security?

- Government
- Industry & sectors
- International organizations
- Professional associations
- Academia and research organizations
- Vendors and suppliers

- **Government:**
  - Policy making
  - Law enforcement
  - Legal system
  - National cyber security strategy and standards
  - International coordination
  - Computer Incident Response Team (CIRT)

- **Industry & sectors:**
  - Financial institutions
  - Telecoms
  - Armed forces
  - Federal and provincial IT boards

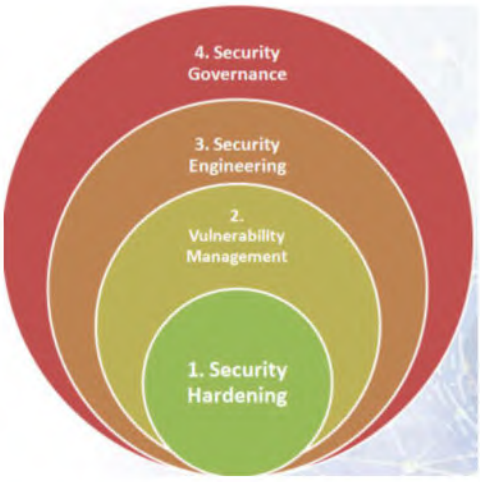
- Enterprises
- Various other sectors (manufacturing, automotive, health, insurance, etc)

- **International organizations:**
  - APCERT (www.apcert.org)
  - European Union Agency for Network & Information Security - ENISA (www.enisa.org)
  - ITU IMPACT (http://www.impact-alliance.org)
- **Professional associations:**
  - ISACA (isaca.org)
  - ISC2 (www.isc2.org)
  - OWASP (www.owasp.org)
  - Cloud Security Alliance
  - Pakistan Cyber Security Association (PCSA)

- **Academia & research organizations:**
  - Universities and research programs
  - SANS (www.sans.org)
  - Center for Internet Security (www.cisecurity.org)

Topic No 06: Infosec Transformation Framework 4 Layers

1. Security hardening
2. Vulnerability management
3. Security engineering
4. Security governance



1: Security hardening:

- Compile IT assets
- Establish minimum security baseline (MSB)
- Research security controls and benchmarks
- Pilot (test)

- Implement controls
- Monitor and update controls

2: Vulnerability management:

- Purchase internal tool (NESSUS, Qualys, etc)
- Conduct vulnerability assessment
- Prioritize and remediate
- Report
- Repeat cycle on quarterly/monthly basis

3: Security engineering:

- Assess risk profile
- Research security solutions
- Design security architecture
- Implement security controls & solutions
- Test and validate security posture

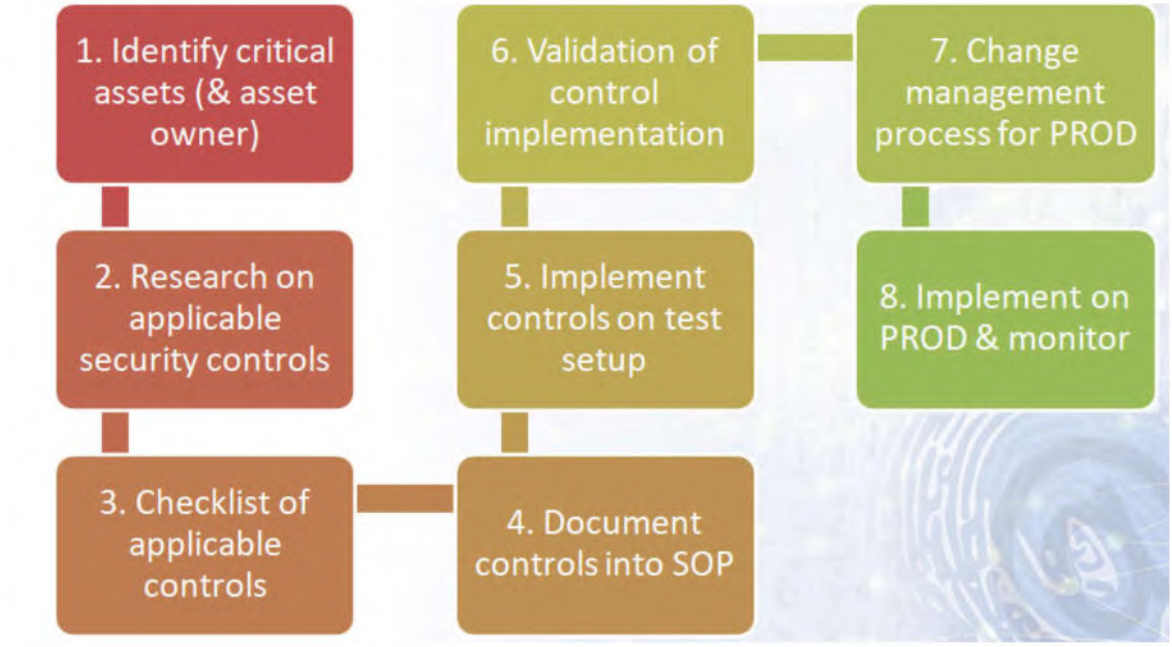
4: Security governance:

- Policies and procedures
- Risk management
- Core governance activities (change management, incident management, internal audit)
- Training & awareness
- Performance reviews

Topic No 07: What Is Information Security Hardening?

- **IT assets** (network, systems, application, databases, mobile, physical security) come with default settings which are not suitable for security
- **Security hardening** is the process of configuring IT assets to maximize security of the IT asset and minimize security risks

- **Security in the "trenches:"**
  - Security at the most fundamental operational layer
  - Security where it matters most
  - Usually (but not always) involves junior staff who need extra guidance, training, and scrutiny



- **Why is security hardening at the first step in the security transformation model?**
  - Most basic security settings
  - If not adequately addressed here, rest of the security measures hardly matter
- **Short example of Cisco router security hardening:**
  - Remote access through SSH and not through telnet
  - Turn of all unused services
  - Session timeout and password retry lockout

Topic No 08: What Is Information Security Governance?

- Information security governance in simpler terms just means effective management of the security program
- Responsibility for governance is associated with the Board and senior management

- **IT Governance Institute Definition:**

"Security governance is the set of responsibilities and practices exercised by the board and executive management, with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

- **ISO27001:2013 – ISMS (Information Security Management System)** is the world's leading and most widely adopted security governance standard
- **ISO27001** "provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."
- Ten short clauses and a long Annex with 114 controls in 14 groups
- 27000+ certifications globally in 2015

Topic No 09: Difference Between Policy, SOP, & Guideline

- **Policy:**
  - Formal and high level requirement for securing the organization and its IT assets (mandatory)

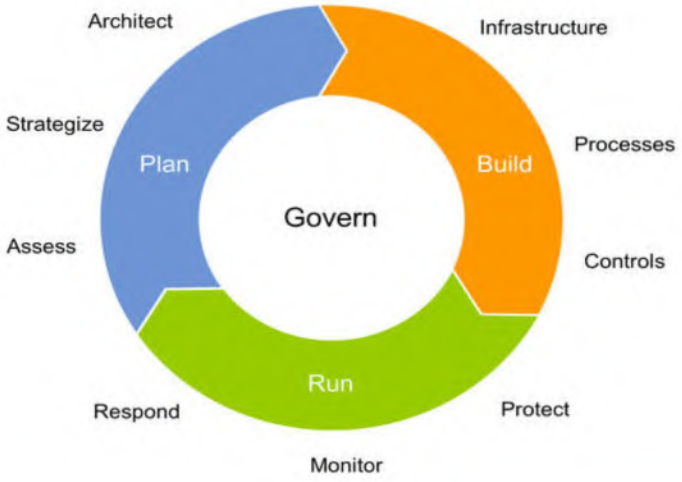
- **Policy:**
  - Scope is across organization so should be brief and focusing on desired results
  - Signed off by senior management
- **Procedure / SOP:**
  - More detailed description of the process; who does what, when, and how
  - Scope is predominantly at a department level having specified audience
  - May be signed off by departmental head

- **Guideline:**
  - General recommendation or statement of best practice
  - Not mandatory
  - Further elaborates the related SOP
- **Standard:**
  - Specific and mandatory action or rule
  - Must include one or more specifications for an IT asset or behavior
  - Yardstick to help achieve the policy goals
- **In practice:**
  - Policy recommended to be a single document applicable at the organizational level (wide audience)
  - Sub-policies may be defined at a departmental level
  - Policies and standards are mandatory (exception approval)
- **Examples:**
  - Information security policy
  - System administrator password sub-policy
  - User ID & Access Management SOP
  - Vulnerability Management standard
  - Social engineering prevention guideline

Topic No 10: What Is An Information Security Program?

- **Project definition:**
  - A project has a defined start and end point and specific objectives that, when attained, signify completion
- **Program definition:**
  - A program is defined as a group of related projects managed in a coordinated way to obtain benefits not available from managing the projects individually

- **Security program:**
  - Sum-total of all activities planned and executed by the organization to meet its security objectives

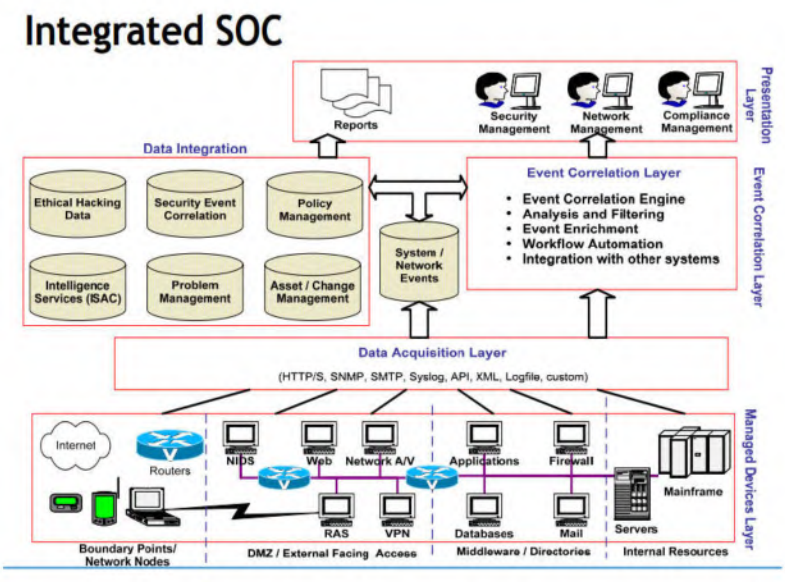


ISO27001:2013 (ISMS) REQUIREMENTS AND CONTROLS

- 4-layer security transformation model may be implemented as an ideal security program
- After establishing a basic policy, the sequence of the program (steps 1 through 4) is paramount in order to achieve constructive results

Topic No 11: Role of People, Process, and Tech In InfoSec

- People, process, and technology are together referred to as the Information Security Triad
- All three aspects help to form a holistic view of Information Security
- All three are important and cannot be overlooked in an Information Security program or activity
- **People:**
    - People must be trained to effectively & correctly follow policies, information security processes, and implement technology
    - Social engineering and phishing are aspects that people must be trained to handle appropriately
- **Processes** are fundamental to effective information security
    - User access management
    - Backups
    - Incident management
    - Change management
    - Vulnerability management
    - Risk management
- **Technology plays a central role in the Information Security program:**
    - Firewalls
    - Antivirus
    - Email anti-spam filtering solution
    - Web filtering solution
    - Data loss prevention (DLP) solution



Topic No 12: Role Of An Information Security Manager

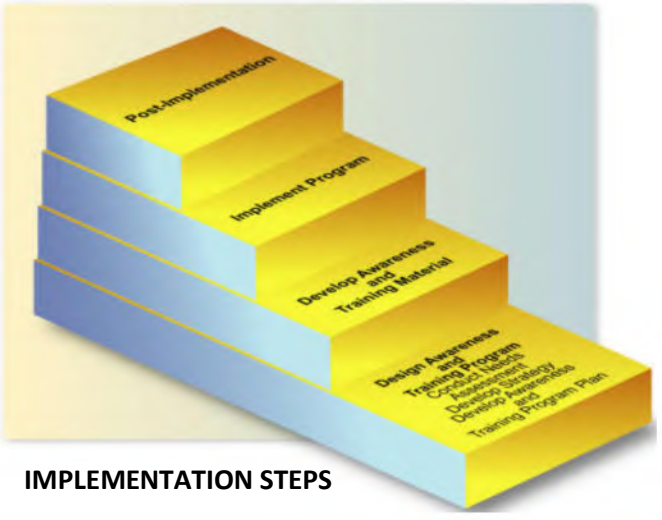
- The Information Security Manager (Head Of Information Security or CISO) is delegated and authorized by senior management to run the Information Security program and meet its objectives
- The Information Security Manager develops a policy to regulate the Information Security program which is signed off by senior management
- Assigned resources and authority to plan, assess, implement, monitor, test, and accredit the Information Security activities

- InfoSec Manager Tasks:
  - Develop policy
  - Training & awareness
  - Design security architecture
  - Design security controls
  - Ensure controls are implemented
  - Conduct risk assessment
  - Conduct security testing
  - Monitor vulnerability management program
  - Facilitate incident management process
  - Sign-off critical change management activities

Topic No 13: What Is Information Security Awareness?

- **Ensure employees are aware of :**
  - The importance of protecting sensitive information
  - What they should do to handle information securely
  - Risks of mishandling information
- **NIST Special Publication 800-50 (Building An IT Security Awareness & Training Program)**
  - Awareness
  - Training
  - Education

- **Awareness:**
  - Awareness is not training
  - Purpose of awareness is simply to focus attention on security
  - Change behavior or reinforce good security practices
- **Training:**
  - "Strives to produce relevant and needed security skills and competencies"
  - Seeks to teach skills
  - E.g. IT Security course for system administrators covering all security aspects
- **Education:**
  - Integrates all of the skills and competencies into a common body of knowledge
  - E.g. a degree program
- **Don'ts:**
  - Share your password
  - Click on suspicious email links
  - Install unlicensed software on your PC
- **Do's:**
  - Logout when getting up from your system
  - Report security incidents



IMPLEMENTATION STEPS

Topic No 14: Leading Security Standards & Frameworks

- A standard or framework is a blueprint or roadmap for achieving Information Security objectives
- Examples are ISO27001:2013 (ISMS), PCI DSS, & COBIT
- ISO27001:2013 (ISMS)

The Payment Card Industry Data Security Standard (PCI DSS)

  - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
  - Ten short clauses
  - Long annex

ISO 27001 ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

ISO 27001 ISO27001:2013 DISCRETIONARY CONTROLS

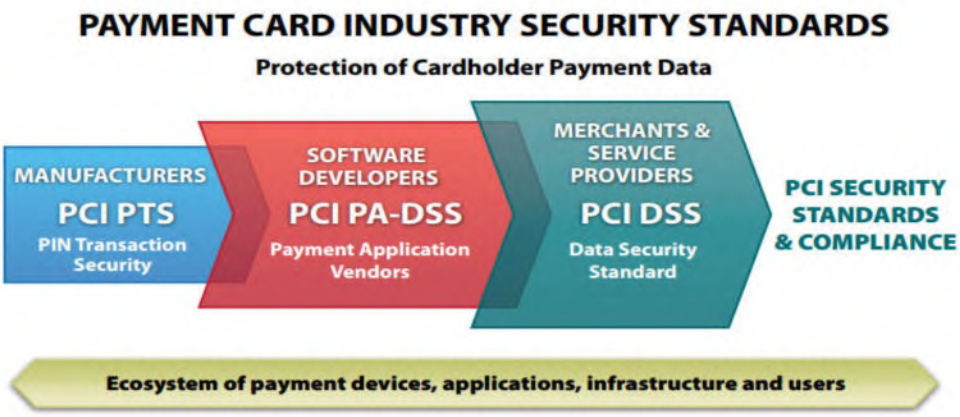
Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

- **PCI Data Security Standard (DSS):**

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

  - Designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment
  - Managed by Security Standards Council

- SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB
- 6 Broad goals and 12 requirements



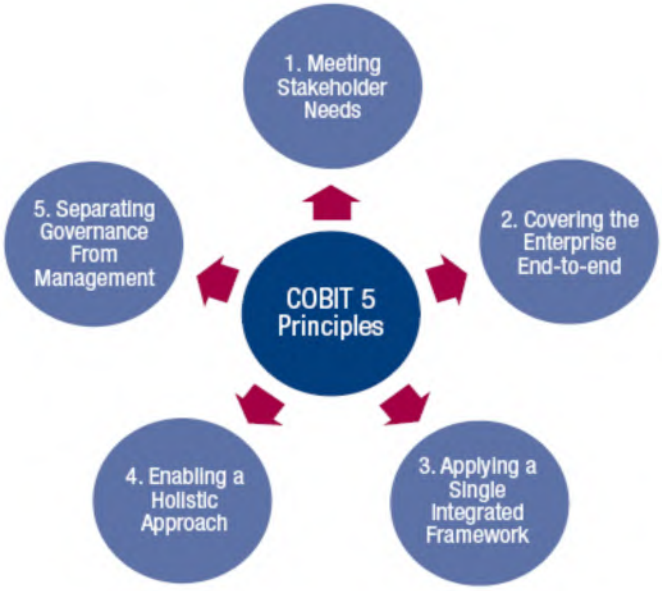
Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

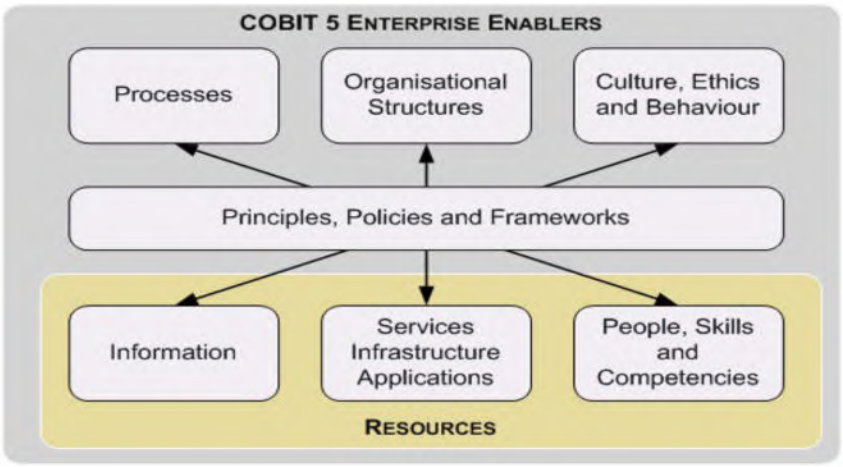
- **COBIT:**
  - ISACA framework for IT Governance

COBIT is the acronym for Control Objectives for Information and Related Technologies. The COBIT framework was created by ISACA to bridge the crucial gap between technical issues, business risks and control requirements.

  - COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

- COBIT 5 brings together five principles that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of seven enablers that optimises IT investment and use for the benefit of stakeholders (ISACA)



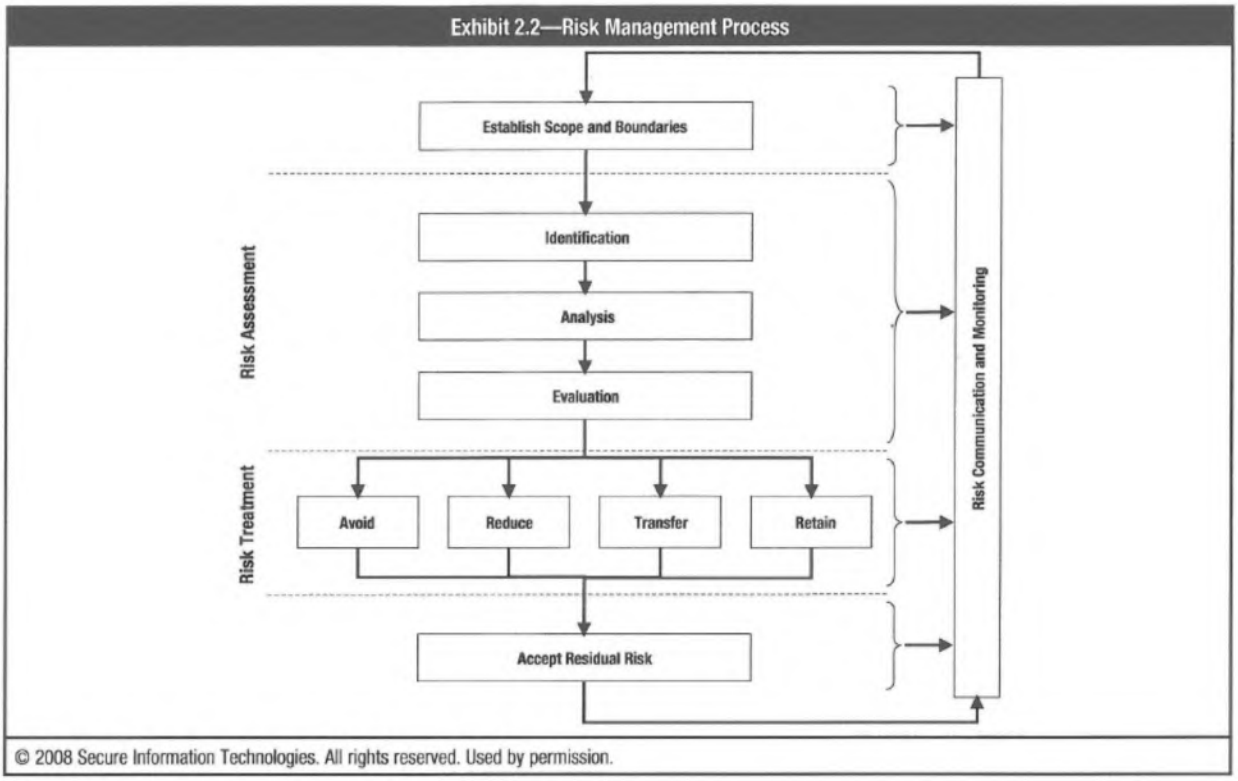


- A standard or framework is a blueprint or roadmap for achieving Information Security objectives
- Examples are ISO27001:2013 (ISMS), PCI DSS, & COBIT

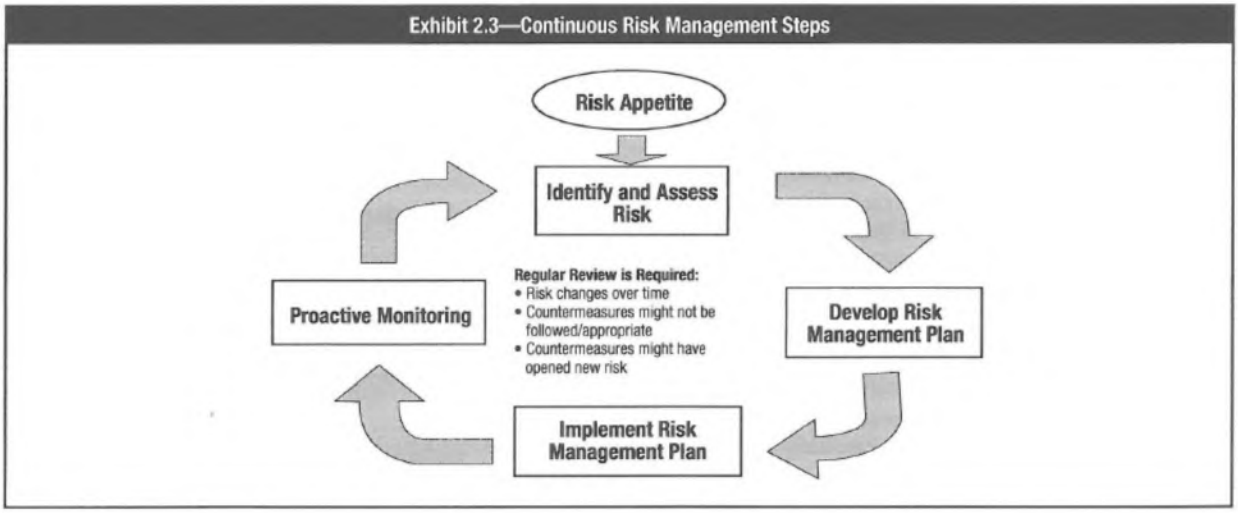
Topic No 15: What Is Information Security Risk?

- Risk is a fundamental concept that drives all security standards, frameworks, and activities
- In simple terms, Information Security Risk refers to the potential damage or loss that may be caused to an organization in the absence of appropriate controls
- A process aimed at achieving an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss
- Usually accomplished by ensuring that impact of threats exploiting vulnerabilities is within acceptable limits at an acceptable cost
- **Risk is managed so that:**

- It does not materially impact the business process in an adverse way
- Acceptable level of assurance and predictability to the desired outcomes of any organizational activity



- **Risk Assessment:**
  - Foundation for effective risk management
  - Solid understanding of the risk universe
  - Nature and extent of risk to IT resources and potential impact on organizations activities



- **Challenges with risk focused approach:**
  - In an environment where controls are absent, a risk based approach may become too academic
  - Effort should focus on 4-Step Security Transformation Framework

Topic No 16: Information Security Lifecycle

- An Information Security lifecycle represents the recommended sequence to adequately address security during any project or activity
- It is a process to ensure that all security projects and activities consistently follow the same sequence and steps
- **Step 1: Requirements**
  - Established by policy, or security program
  - Could also be driven by security transformation program
  - Establish security exposure, determine risk and priority
- **Step 2: Assess Current Security Posture**
  - Conduct gap analysis
  - Could also be a risk assessment and evaluation
- **Step 3: Remediation Plan**
  - Methodology & framework
  - Controls

- Resources
- Approvals and communication
- Timeline
- Project monitoring and review
- Develop SOP

- **Step 4: Implement Controls**
  - Pilot
  - Test/validate in pilot
  - Change management
  - Implement in production/live environment
  - Roll-back if unexpected response
  - Maintain SOP
- **Step 5: Test/Validate**
  - Security team or independent review of correctness and coverage of security control implementation
  - Ensure SOP/checklist developed and followed
- **Step 6: Security Accreditation**
  - Review process has been followed (change management, SOP, sign-offs)
  - Establish monitoring mechanism
  - Awareness training
  - Issue formal accreditation
- **Step 7: Monitor & Audit**
  - Monitoring mechanism (KPIs, reporting, review)
  - Incident management
  - Internal audit

Topic No 17: Management Commitment

- **What is management commitment?**
  - Management commitment is the expression of the intent, relevant actions, and allocation of sufficient resources to ensure the InfoSec program is properly implemented
- **ISO2700:2013 (ISMS) Clause 5.1:**

a) Policy and objectives are established (compatible with strategic direction)

b) Integration of ISMS reqmts into processes

c) Resources

d) Communicating importance

e) Intended outcomes are achieved

f) Directing and supporting persons

g) Promoting continual improvement

h) Supporting other management roles

- **"Tone at the top"**
  - Management closely watches the actions of executive leadership (culture)
  - The importance given to InfoSec by the executive leadership becomes the minimum threshold for rest of the organization
- **In practice:**
  - Security policy
  - Security responsibility delegated to head (CISO) or dept
  - Security steering committee (board level)
  - Quarterly or frequent management reviews of information security program

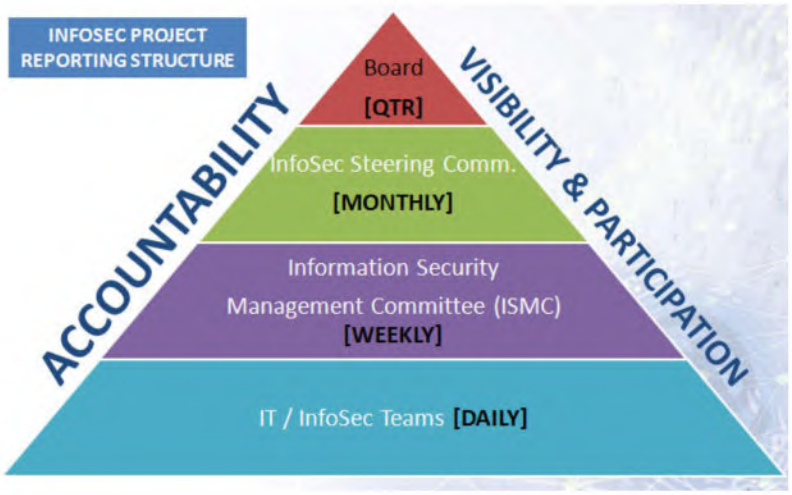
Topic No 18: Information Security Responsibility

- **Default organizational perception:**
  - Security is responsibility of one person or one department
  - Can get away with "security as an after-thought"

- Reactive

- **Security is everyone's responsibility:**
  - Management commitment & tone at the top
  - Security awareness campaigns/program
  - A strong and effective security program
  - Allocation of sufficient resources

- **Security involvement & accountability:**
  - Effective security implementation should be built into the performance KPIs of key team members (management, technical, business)
  - Annual appraisals, security awards and recognition

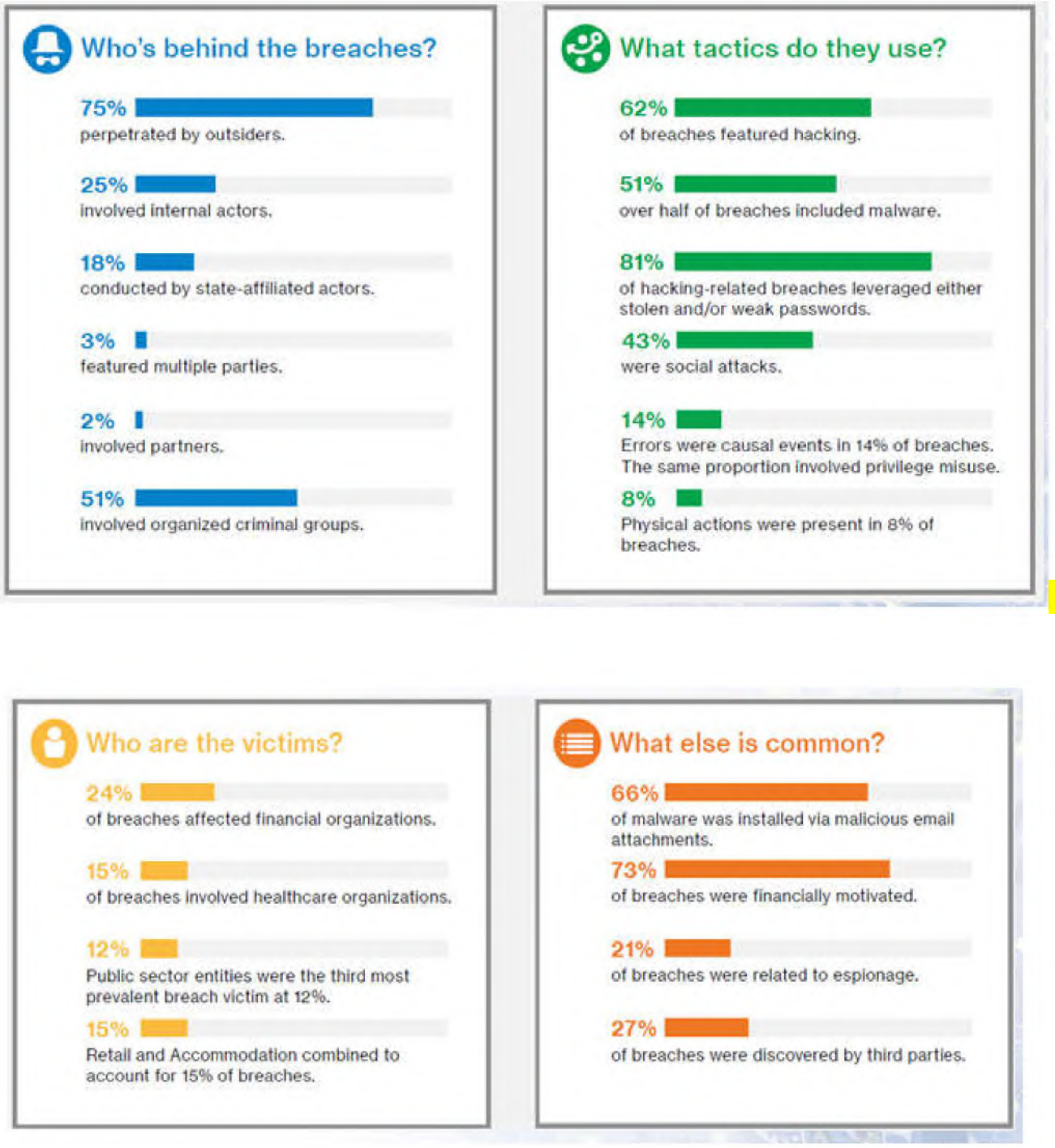


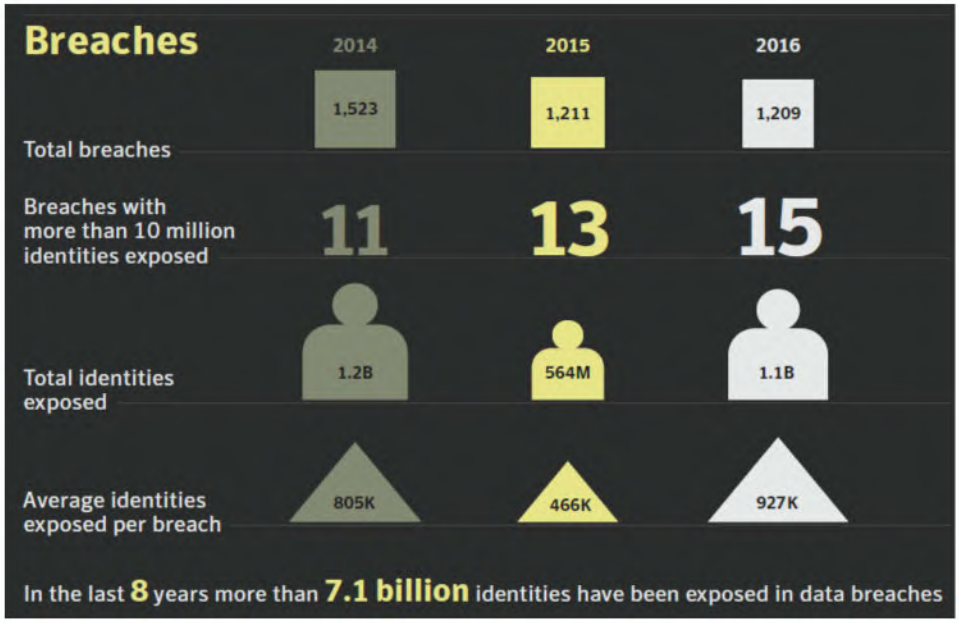
- Security is everyone's responsibility and has to gradually take its place in org culture

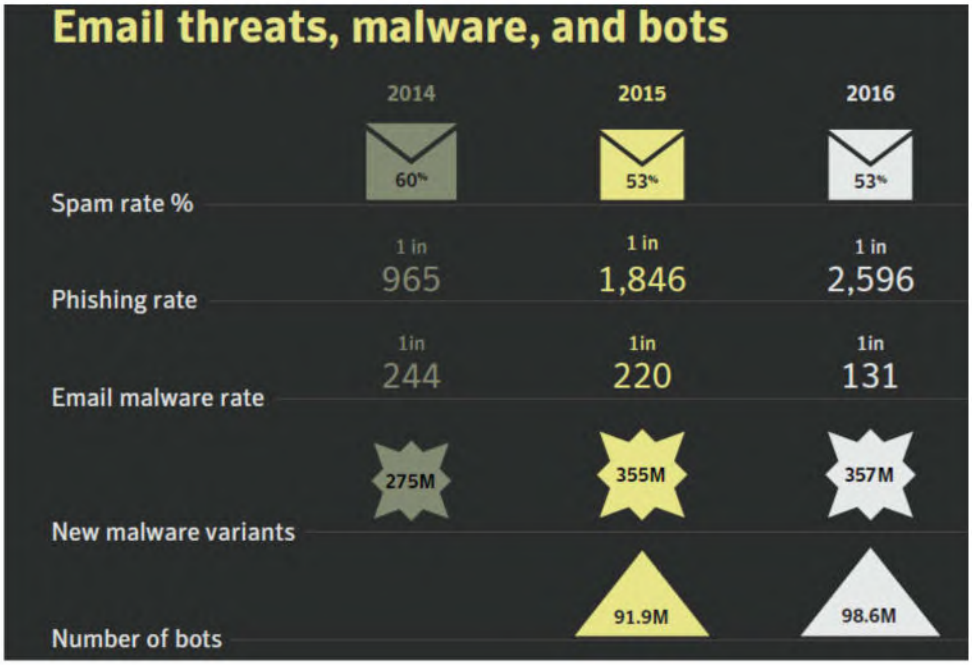
Topic No 19: Cyber Security Breaches

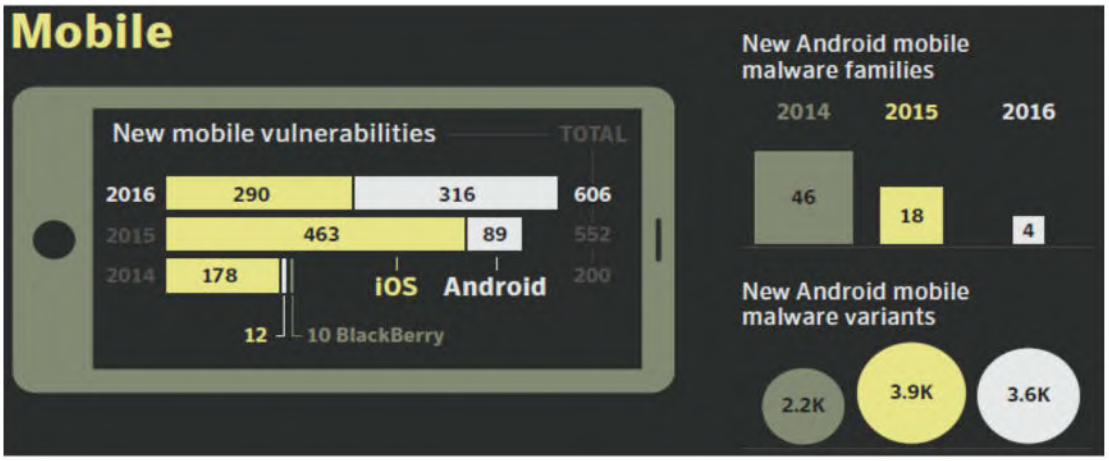
- Fox News Video: "World's Biggest Cyber Attacks"
  - http://video.foxnews.com/v/5435057924001/?#sp=show-clips
- World's Biggest Data Breaches:
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Leading Global Reports:
  - Verizon 2017 Data Breach Investigations Report (DBIR)

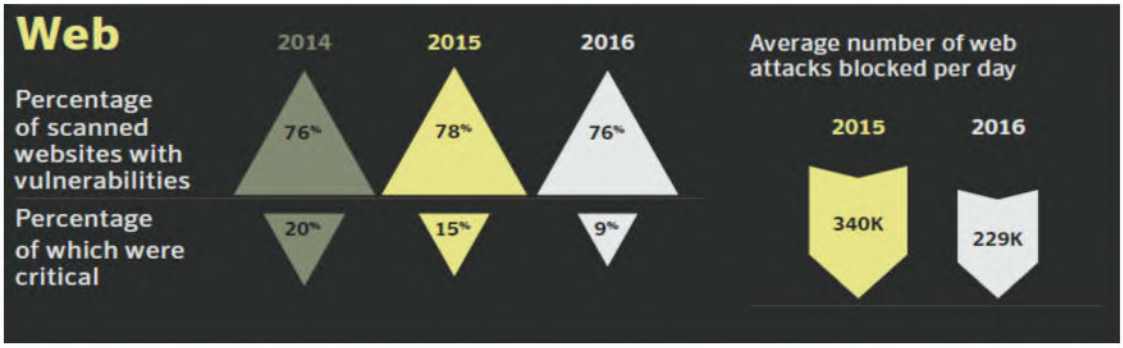
– Symantec 2017 Internet Security Threat Report (ISTR)

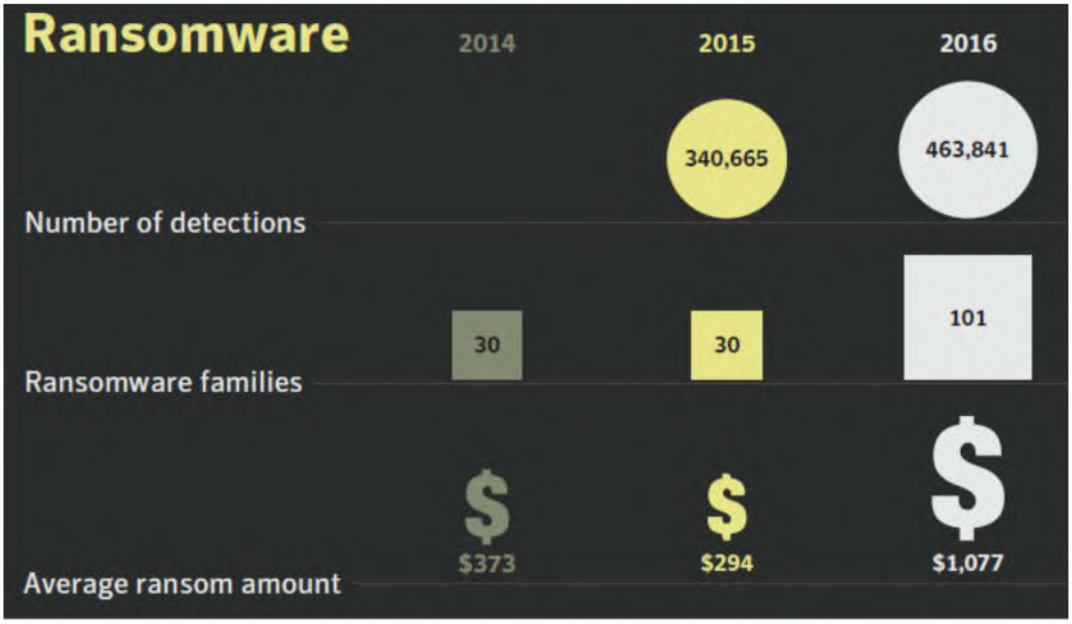



Breaches
2014
2015
2016
Total breaches
1,523
1,211
1,209
Breaches with more than 10 million identities exposed
11
13
15
Total identities exposed
1.2B
564M
1.1B
Average identities exposed per breach
805K
466K
927K
In the last 8 years more than 7.1 billion identities have been exposed in data breaches


Email threats, malware, and bots
2014
2015
2016
Spam rate %
60%
53%
53%
Phishing rate
1 in 965
1 in 1,846
1 in 2,596
Email malware rate
1in 244
1in 220
1in 131
New malware variants
275M
355M
357M
Number of bots
91.9M
98.6M


Mobile
New mobile vulnerabilities
TOTAL
2016
290
316
606
2015
463
89
552
2014
178
200
iOS
Android
12
10 BlackBerry
New Android mobile malware families
2014
2015
2016
46
18
4
New Android mobile malware variants
2.2K
3.9K
3.6K

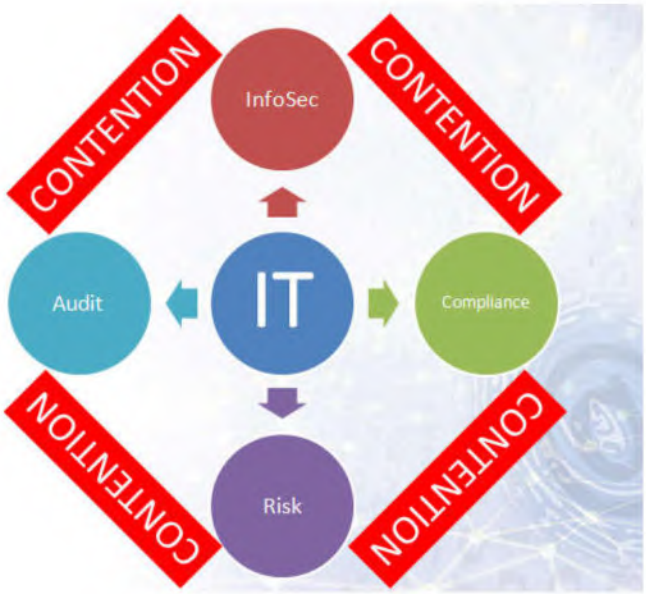




- **Leading Global Reports:**
  - Verizon 2017 Data Breach Investigations Report (DBIR)
  - Symantec 2017 Internet Security Threat Report (ISTR)

Topic No 20: Challenges Of InfoSec Implementation

- **Challenges Of IT:**
  - Complex and difficult to manage
  - Under pressure from business groups
  - Lack of sufficient competent resources
  - Lack of process culture
  - IT not aligned to perform diligent security work



- **Challenges Of InfoSec:**
  - Silos & lack of coherent ownership
  - Lot of time & energy wasted in traversing dept boundaries
  - Enabling environment for tough security work missing
  - Security hardening glaringly absent
- **Pakistan Industry Security Characteristics:**
  - Wavering management commitment
  - Superficial “dressing” security
  - Reactive to regulator audit/compliance mandate
  - Industry in denial

Topic No 21: Role Of A Regulator

- Cyber attack can have devastating consequences causing financial loss and disruption of critical infrastructure
- Cyber security has become a key risk factor putting under threat not only consumer rights protection, but also viability and health of the industry itself
- A **cybersecurity regulation** comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber-attacks (Wikipedia)
- Industry regulators including banking regulators have taken notice of the risk from cybersecurity and have either begun or are planning to begin to include cybersecurity as an aspect of regulatory examinations (Wikipedia)
- **Role Of Regulator In Cyber Security:**

– Regulations, guidelines, and audit

– Engagement of key stakeholders

– Technical and industry expertise

– Regional and international cooperation

- Regionally, the most well developed cyber security strategy and framework developed by Singapore (ITU rank # 1), Malaysia (ITU rank # 3), and Oman (ITU rank # 4)
- **Singapore**:

– Cyber Security Agency (2015); strategy, education, outreach, eco-system development

– National Cyber Security Master Plan 2018 (created 2013)

– Cyber Security Strategy (created 2016)

- **Pakistan; Ministry of IT (MOIT):**

– National IT Policy 2016 (draft)

– Digital Pakistan Policy 2017

- **Pakistan; State Bank Of Pakistan (SBP):**

– Enterprise Technology Governance & Risk Management Framework for Financial Institutions (30 May 2017)

- **Pakistan lacks:**

– National cyber security strategy

- National cyber security master plan
- National cyber security agency
- National certification & accreditation body
- National Computer Emergency Response Team (CERT)

Topic No 22: Status Of InfoSec in Pakistan

- Pakistan Electronic Crimes Act (PECA) enacted as late as 2016
- Cyber security strategy, eco-system still missing
- Research program, capacity building, standardization, & certification bodies absent
- Condition of InfoSec in industry largely dismal

Global Cyber Security Index 2017 (ITU):

Pakistan ranked 67th with a score of 0.44/1

Bangladesh ranked 53rd with a score of 0.524/1

India ranked 23rd with a score of 0.683/1

- **Pakistan cyber security posture (industry):**
  - Superficial security
  - Reactive
  - Emphasis on governance
  - Security hardening of IT assets largely absent
  - Industry has been in denial for last decade
- **Reasons for poor security posture:**
  - Archaic digitalization and commerce
  - Perception that Pakistan is immune

- Lack of awareness and management commitment
- Lack of effective regulations

- **Changing dynamics (PK):**
  - Pakistan financial industry rocked by Bangladesh SWIFT hack 2016
  - Wannacry (May 2017) badly hit several dozen organizations in Pakistan
  - Increasing e-commerce, electronic banking
- **Pakistan needs:**
  - Necessary measures by the Government in line with what Malaysia, Oman have done for cyber security
  - Development of the security eco-system as an enabler in order to drive strong security posture

Topic No 23: Solution For InfoSec Improvement (PK)

- Generally, Pakistan Information Security is one generation behind IT deployment
- Four-layer security transformation model provides the correct sequence and focus in order to address organizational security gaps

1. Security Hardening; Security controls on IT assets & process
2. Vulnerability Management; patching
3. Security Engineering; More complex security design & solutions
4. Security Governance; Managing the information security program

- **Solution for strong security posture:**
  - Management commitment (Board)
  - 4 layer transformation model as security program
  - Allocation of resources
  - Periodic reviews for assessing progress
- **Don't repeat the same mistakes:**
  - Too much governance without the underlying security hardening
  - Reactive rather than intrinsic

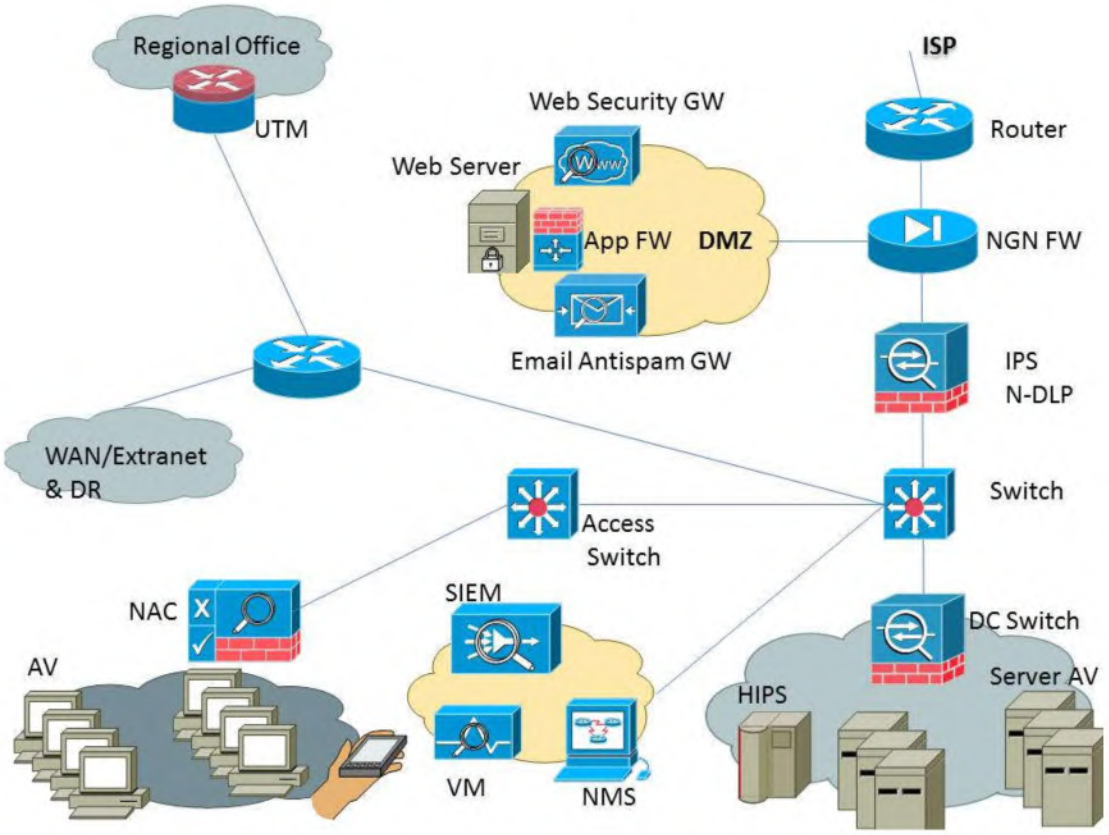
- Lack of resources (10% of what allocated for IT)
- Management interest

Chapter 2:

Typical Enterprise IT Architecture & Security Overlay

Topic No 24: Typical Enterprise IT Network

- What does a typical enterprise IT network look like ?



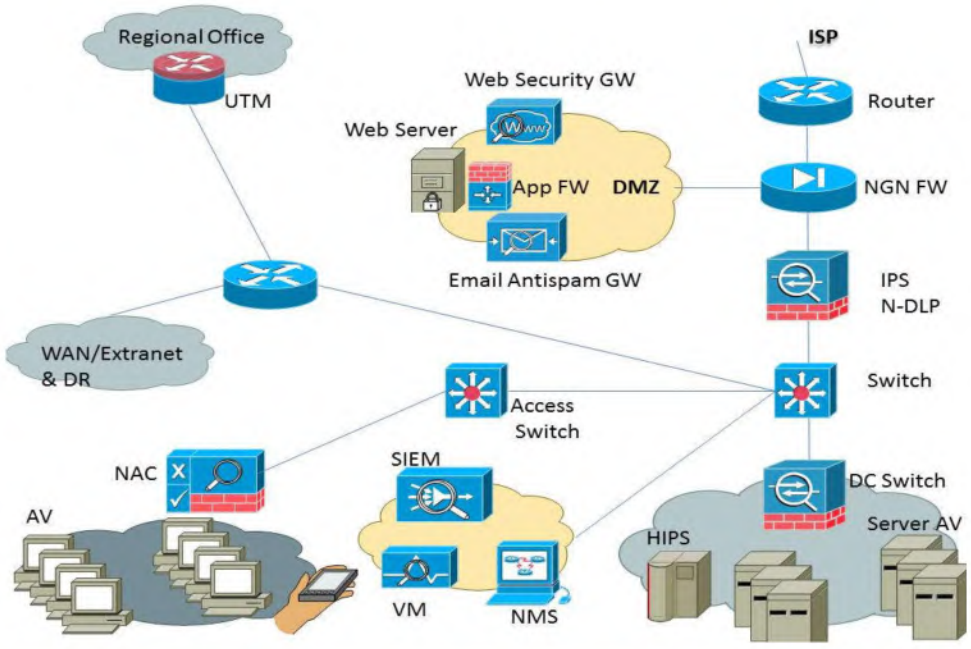
- Edge router
- NGN FW
- DMZ:
  - Web security GW/Proxy
  - Application security FW
  - Web server
  - Email antispam GW
- IPS & N-DLP

- Distribution switch
- Data center switch & FW
- Access switch
- NAC
- SOC:
  - SIEM
  - VM
  - Other SOC tools
- System AV
- Server HIPS
- UTM
- Mobile device - MDM

Topic No 25: Major Components: Enterprise IT Network

- **Edge router**
  - WAN interfaces
  - Edge filtering (access lists)
  - DDOS protection
- **NGN FW**

  Capable of APT attack prevention, malware filtering, web security, email security, application bandwidth filtering



- **DMZ:**
  - Security zone with placement of published web server, web & email security GWs, app security GW
- **IPS:**
  - Intrusion prevention (signature based)
  - May be feature in NGN-FW
- **Distribution switch**
  - Connectivity to access switches, external exit point (WAN), and DC switch
- **Data center switch & FW**
  - Data center filtering (malware & access-lists)
- **Access switch**
  - User connectivity
  - Switchport security & access switch security
- **NAC**
  - Network admission control (IEEE802.1X)
- **SIEM**
  - Logging & dashboard for events, root cause analysis, event correlation
- **Vulnerability Manager**
  - Vulnerability scanning and asset tracking
- **System AV**
  - Signature based malware prevention
- **Server HIPS**
  IPS features for servers, also file integrity checkin
- **UTM**
  - Multi-featured NGN FW device
- **Mobile device – MDM**
  - Security features for mobile devices

Topic No 26: OSI Security Architecture

- ITU-T X.800, Security Architecture For OSI ('91)
- Defines a technique for defining security requirements, and characterizes the approaches to satisfy those requirements
- Defines security attack, mechanism, and service
- Security attack: action that compromises the security of information owned by an organization (or person)
  - Passive: aims to learn or make use of system information only
  - Active: attempts to alter system resources/operation
- Security service is a service that ensures adequate security of the system or data transfer

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation
- Availability

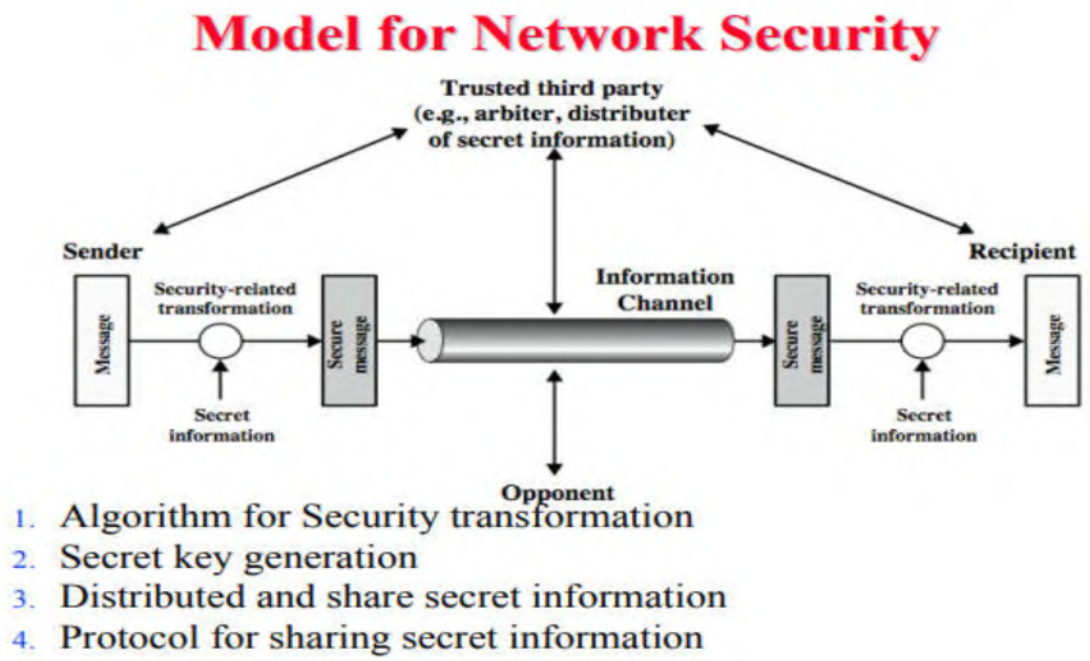
Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

- **Security mechanism:**
  - Feature designed to detect, prevent, or recover from a security attack
  - Cryptography underlies many of the mechanisms

Services and Mechanisms Relationship

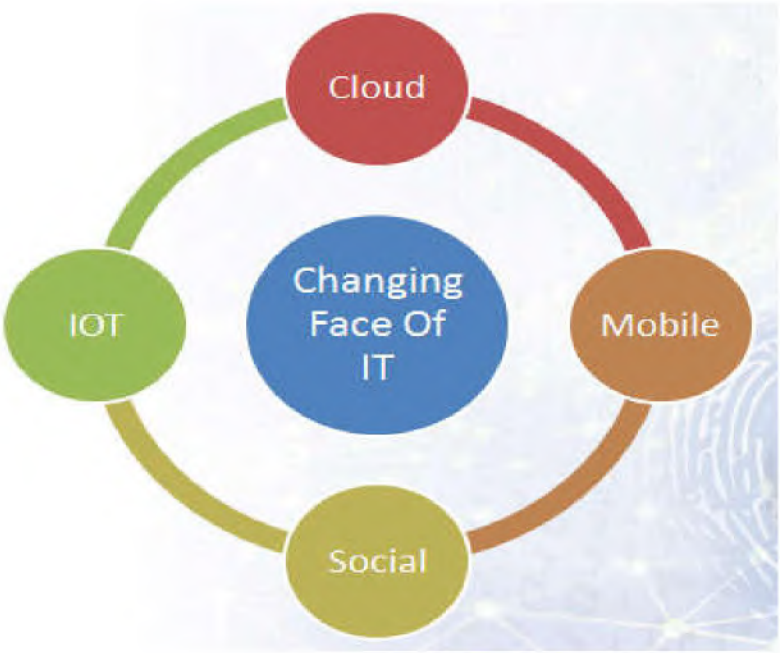
	Mechanism							
Service	**Encipherment**	**Digital signature**	**Access control**	**Data integrity**	**Authentication exchange**	**Traffic padding**	**Routing control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

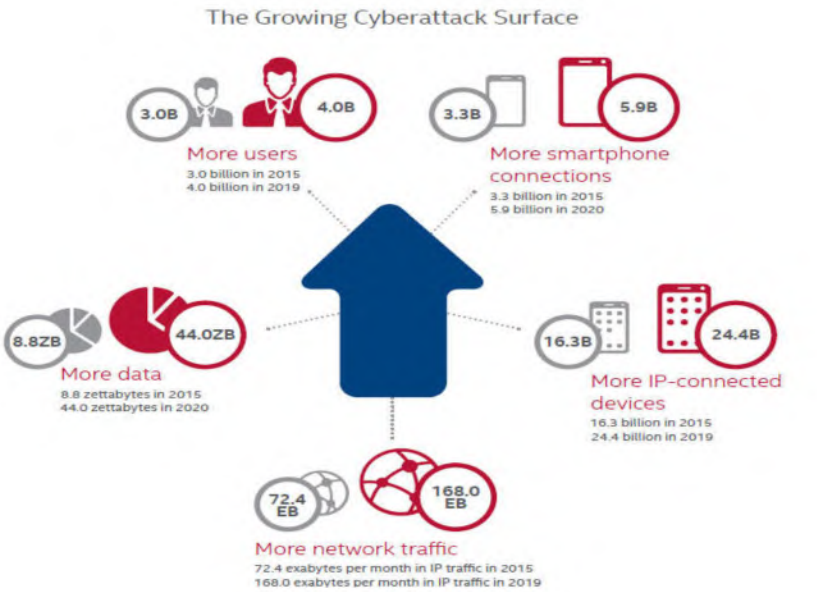


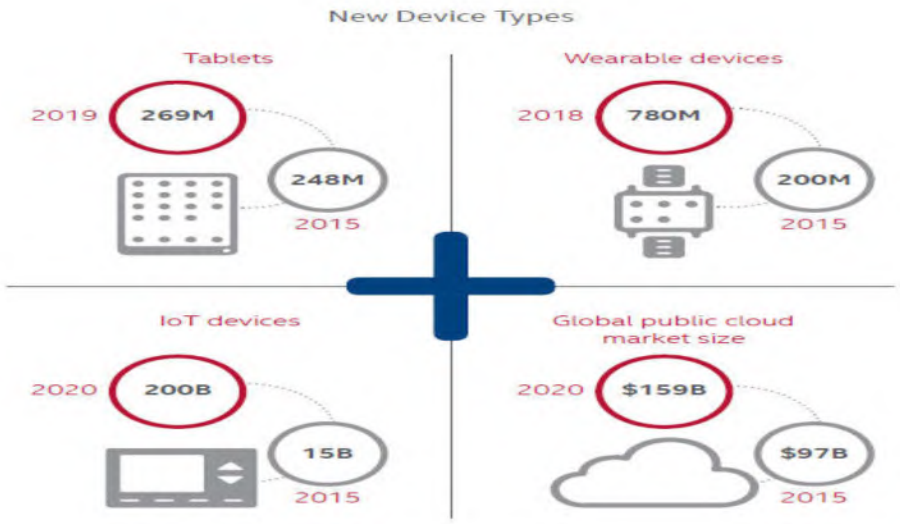
- ITU-T X.800, Security Architecture For OSI is dated from 1991

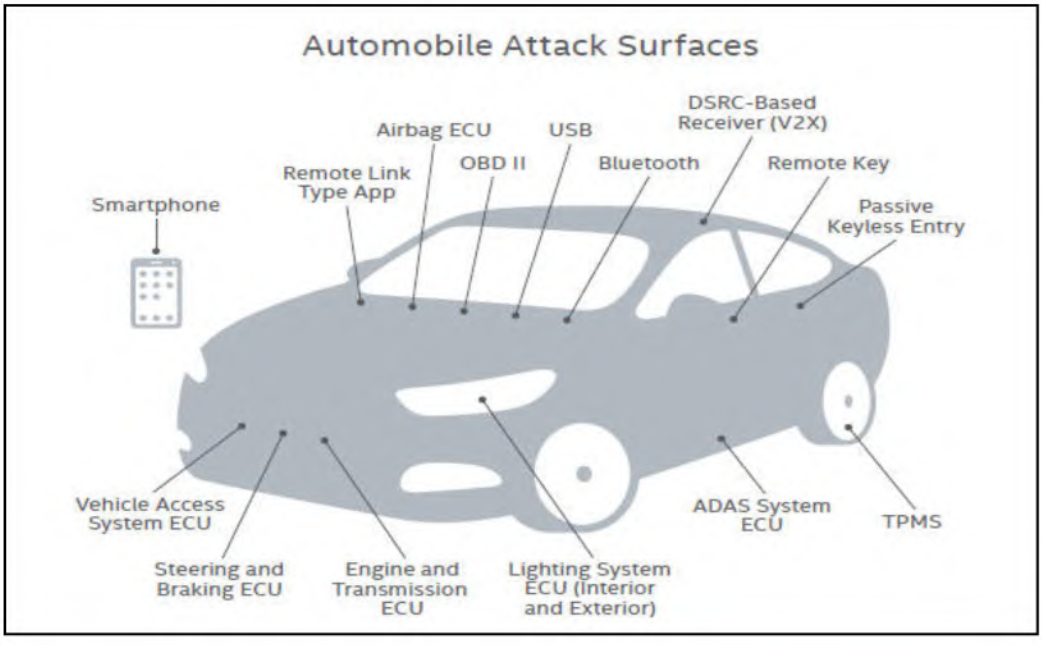
Topic No 27: New IT Frontiers: Cloud, Mobile, Social, IOT

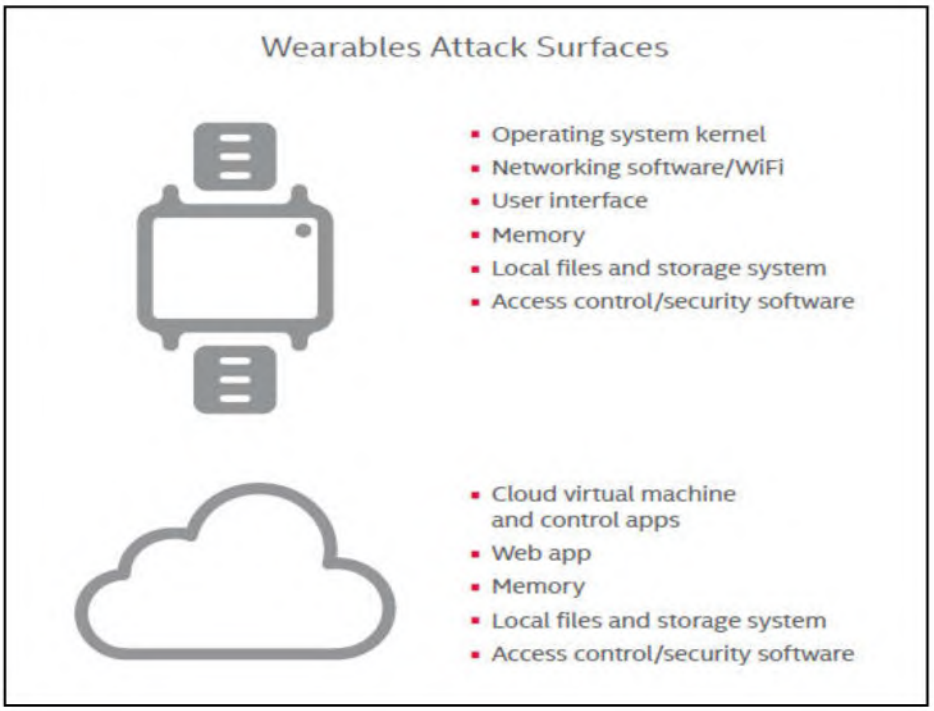
- IT dynamics are changing the way we communicate, work, and live
- These disruptive new IT frontiers have significant security consequences




The Growing Cyberattack Surface
3.0B
4.0B
More users
3.0 billion in 2015
4.0 billion in 2019
3.3B
5.9B
More smartphone connections
3.3 billion in 2015
5.9 billion in 2020
8.8ZB
44.0ZB
More data
8.8 zettabytes in 2015
44.0 zettabytes in 2020
16.3B
24.4B
More IP-connected devices
16.3 billion in 2015
24.4 billion in 2019
72.4 EB
168.0 EB
More network traffic
72.4 exabytes per month in IP traffic in 2015
168.0 exabytes per month in IP traffic in 2019


New Device Types
Tablets
2019
269M
248M
2015
Wearable devices
2018
780M
200M
2015
IoT devices
2020
200B
15B
2015
Global public cloud market size
2020
$159B
$97B
2015


Automobile Attack Surfaces
Smartphone
Remote Link Type App
Airbag ECU
OBD II
USB
Bluetooth
DSRC-Based Receiver (V2X)
Remote Key
Passive Keyless Entry
Vehicle Access System ECU
Steering and Braking ECU
Engine and Transmission ECU
Lighting System ECU (Interior and Exterior)
ADAS System ECU
TPMS



Topic No 28: Virtualization Environment Security

- Cloud Security Alliance: "Best Practices For Mitigating Risks In Virtual Environments" (PDF)
- **Virtualization security classified into three areas:**
  - Architectural
  - Hypervisor software
  - Configuration

1. VM Sprawl
2. Sensitive data within VM
3. Security of offline and dormant VMs
4. Security of Pre-configured (Golden Image) VMs
5. Lack of visibility into virtual networks

- **Risk # 1 (VM Sprawl)**
  - Impact: VMs can be created quickly, self-provisioned, or moved between physical servers, avoiding conventional change management process
  - Proliferation of VMs causing performance and security risks

- **Controls:** Policies, procedures and governance of VM lifecycle management
- Control creation, storage and use of VM images with a formal change management process
- Discover VMs & apply security controls
- **Controls:** keep a small number of identified, good and patched images of a guest operating system separately for fast recovery & restoration of systems

- **Risk # 2 (Sensitive Data Within a VM)**
  - **Impact:** VM images and snapshots can be copied easily via USB or console of hypervisor installed elsewhere
  - **Controls:** Encrypt data stored on virtual and cloud servers
  - Policies to restrict storage of VM images and snapshots
  - Image change management process with approvals
  - Logging & monitoring

Topic No 29: Case Study – Enterprise Network (Small Org)

- **Organizational characteristics:**
  - Location: Karachi
  - 70 total staff
  - 10 IT staff
  - 8 servers
  - 1 main DC, no DR site
  - IT service oriented business delivered to banks, telcos, enterprises
- **Organizational culture:**
  - Small IT oriented profitable business
  - Mostly chaotic culture with no defined or documented processes
  - Organization lacks discipline (execution)
  - Quality of resources: average

- **IT setup:**
  - Windows 2010/2012, Linux server OS
  - ASP.net 4.x, PHP applications (total 10)
  - Windows 8/10 desktops (50+)
  - 1 Cisco ASA FW in DC
  - No DR site or offsite backup
  - Free AV, no AD, no licenses
- **Security posture:**
  - Completely absent
  - No hardening done
  - No vulnerability management
  - No security management or governance
  - No policy or staff dedicated for
  - No management commitment (prior)
- **Security requirement:**
  - Customers are banks and telcos
  - Desired ISO27001:2013 (ISMS) certification for customer RFPs
- **Driving change ?**
  - Executive management facing security questions from top clients
  - COO approaches security consulting company for pen-testing
  - Consultant advises project for security transformation
- **Security transformation project:**
  - Project initiation: 2 Mths
  - Layer 1: security hardening of IT assets (6 Mths)
  - Layer 2: VM (1 Mth)
  - Layer 3: security engineering (1 Mth)
  - Layer 4: Governance & ISO cert.(3 Mths)

- **Conclusion:**
  - Absence of a process oriented, organized culture makes it difficult for security implementation
  - Adhoc culture is difficult to transform
  - Executive management support and commitment was the success factor

Topic No 30: Case Study – Enterprise (Medium Org)

- **Organizational characteristics:**
  - Location: Lahore
  - 350 total staff (group)
  - 15+ IT staff
  - 25 servers
  - 1 main DC, 1 DR site, 1 backup site
  - IT service business in media industry
- **Organizational culture:**
  - Medium sized, profitable IT business
  - Good internal culture (several employees with org since 10 yrs)
  - Organization lacks processes
  - Teams have execution discipline
  - Senior resources are experienced
- **IT setup:**
  - Windows 2010/2012, Linux server OS
  - Oracle & MS-SQL databases
  - ASP.net 4.x applications (total 15)
  - Windows 8/10 desktops (300+)
  - 1 Cisco ASA FW in DC; MicroTik routers as edge routers
  - Asterisk voice server for call center (10 seats, 6-8 lines)
  - 1 DR site (offshore) and 1 backup site (PK)
  - Panda AV, AD, unlicensed windows

- Mdaemon for email server, migrating to MS Exchange

- **Security posture:**
  - Completely absent
  - No hardening done
  - No vulnerability management
  - No security management or governance
  - No policy or staff dedicated for security
  - No management commitment (prior)
- **Security requirement:**
  - Security incident; competitive data leakage to third-party by internal employee
  - License renewal due by regulator; demonstration of security commitment imperative
- **Driving change ?**
  - Executive management concerned about information security & security culture
  - CEO approaches security consulting company
  - Consultant advises project for security transformation
- **Security transformation project:**
  - Project initiation: 15 days
  - Layer 1: security hardening of IT assets (3 Mths)
  - Layer 2: VM (1 Mth)
  - Layer 3: security engineering (4 Mths)
  - Layer 4: Governance & ISO cert.(3 Mths)
- **Conclusion:**
  - Senior resources in the organization were committed
  - Demonstration of security commitment was essential for organizations survival
  - ISO27001:2013 (ISMS) serves as credible credential for customers/regulator

Topic No 31: Case Study – Enterprise (Large Org)

- **Organizational characteristics:**
  - Location: Karachi
  - 10,000+ total staff
  - 150 IT staff
  - 200 servers
  - 1 main DC, 1 DR site
  - Energy & distribution sector
- **Organizational culture:**
  - Large sized privatized org
  - Strong internal culture
  - Organization lacks process culture
  - Teams have high execution discipline
  - Good quality & qualification of IT resources
- **IT setup:**
  - Windows 2010/2012, Linux, AIX OS
  - Oracle & MS-SQL databases
  - Over 100 internal applications (Sharepoint, GIS, ASP.net)

    Windows 7/8/10 desktops (5500+)
  - Asterisk voice server for voice communication
  - 1 DR site (hosted)
  - Licensed AV, AD, & windows
  - Complete SAP ERP suite & internal development
- **Security posture:**
  - Superficial
  - No hardening done

- Weak vulnerability management
- Poor security management/ governance
- Security team exists
- No management commitment (prior)

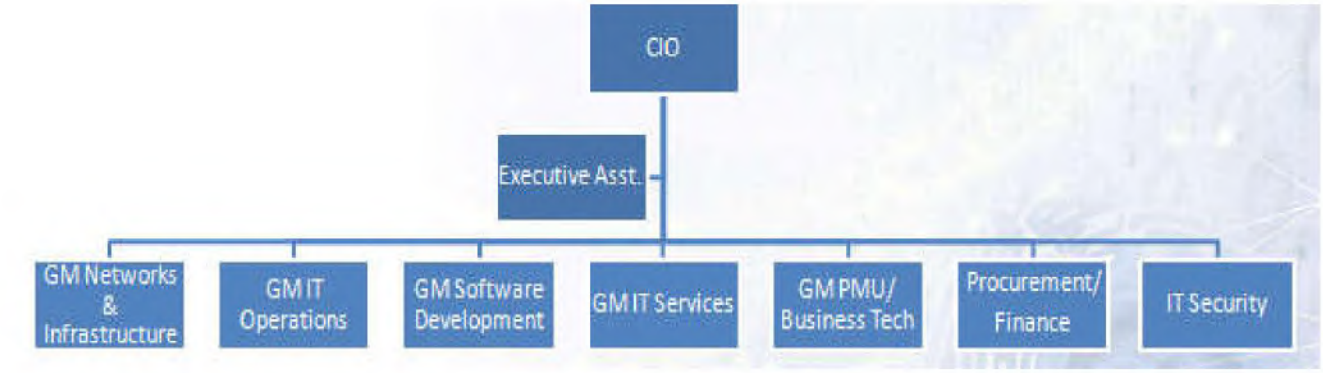
- **Security requirement:**
  - Security incident; servers hacked causing financial loss
- **Driving change ?**
  - Executive management concerned about information security & security culture
  - Board drives IT to hire consultant
  - Consultant convinces IT to go for security transformation
- **Security transformation project:**
  - Project initiation: 15 days
  - Layer 1: security hardening of IT assets (6 Mths)
  - Layer 2: VM (1 Mth)
  - Layer 3: security engineering (1 Mths)
  - Layer 4: Governance & ISO cert.(5 Mths)
- **Conclusion:**
  - Strong commitment of the Board & IT Director drove the implementation of the security transformation project
  - ISO27001:2013 (ISMS) achieved as a security credential

Topic No 32: Structure Of An IT Team

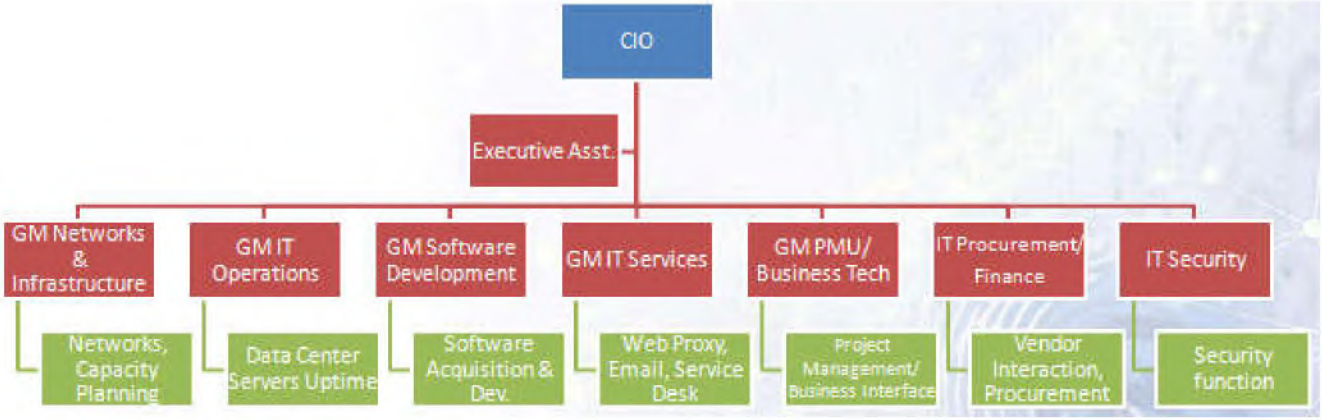
- Typical organogram of an IT team
- Job functions
- Additional tasks
- Large sized org
- Medium sized org

- Small sized org

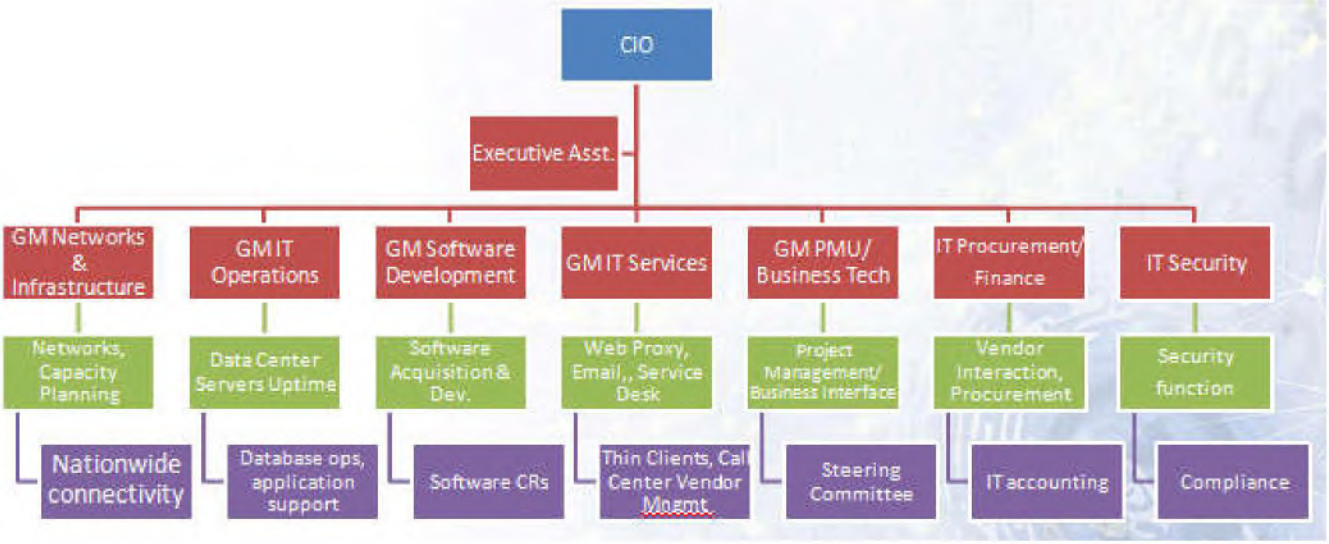
GENERAL STRUCTURE



JOB FUNCTIONS

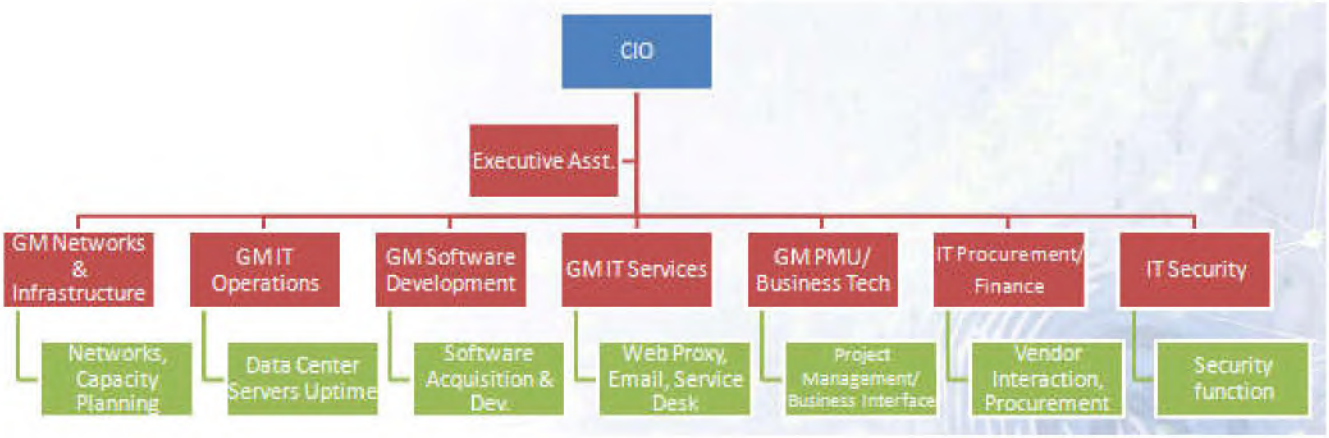


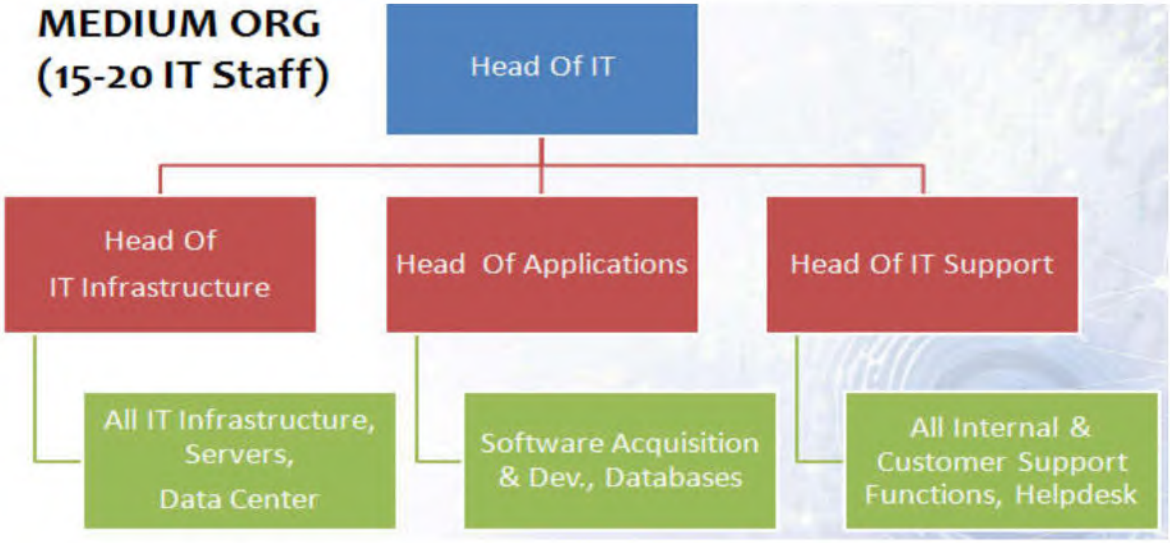
ADDITIONAL TASKS

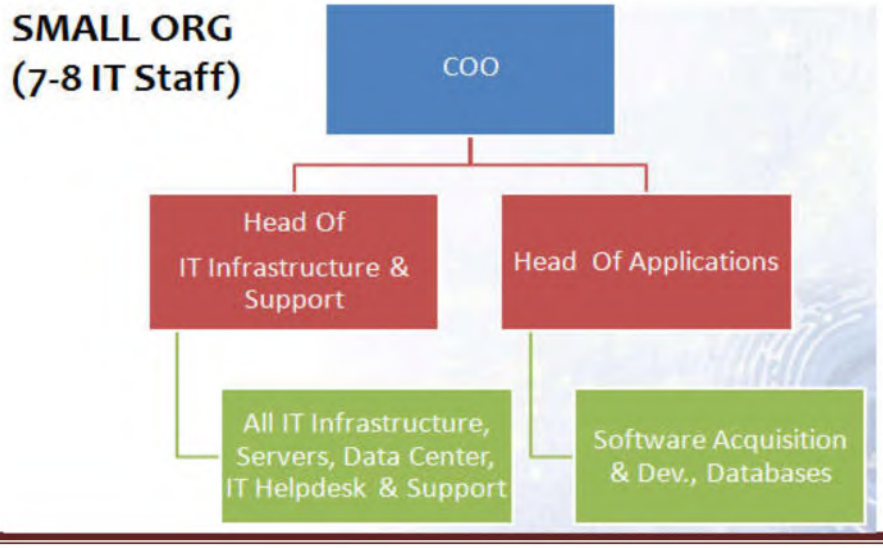


LARGE ORG

(150 IT Staff)







- IT teams come in various structures, however there are set industry best-practices and organizations should follow tried & tested best-practices
- IT is today an enabler forming the engine for business automation, but also carries with it security hazards

Topic No 33: Objectives, Performance KPIs, Priorities Of IT

- IT is a challenging domain which requires skill, experience, structure, and spending to run efficiently
- Business is making steep demands on IT for agile delivery of applications in order to keep up with competition
- Running IT requires a diverse skillset
- Primary objective set for IT by management is to:
  - Setup the infrastructure with least cost in the minimum time
  - To maintain the network with minimum disruption and maximum performance requiring the least resources
- **Performance KPIs:**
  - Minimal network disruption
  - Timely completion of new projects
  - Quick and efficient changes to existing applications (change-requests) to meet business requirements
- **Priorities of IT:**
  - To meet the performance KPIs
  - To meet adhoc and unplanned business requirements
- **General IT teams performance in Banking:**
  - Extremely large number of applications (hundreds) & legacy
  - Heavy-weight business teams and IT seen as a cost-center
  - Technologists generally poor at banking (business)
- **General IT teams performance in Telcos:**
  - More professional and qualified workforce
  - Most telco have been setup in the last 10 years so have clean greenfield networks (no legacy)
  - Fewer applications; IT supports business
- **General IT teams performance in Enterprise:**
  - Competence and professionalism of IT teams matches culture of organization
  - IT efficiency driven by top management commitment and interest
- **Security posture:**
  - Surprisingly in 95% of all orgs in Pakistan (all types and sizes), security posture has been found to be deficient
  - Lack of awareness in the country has contributed to this deficient and poor security posture

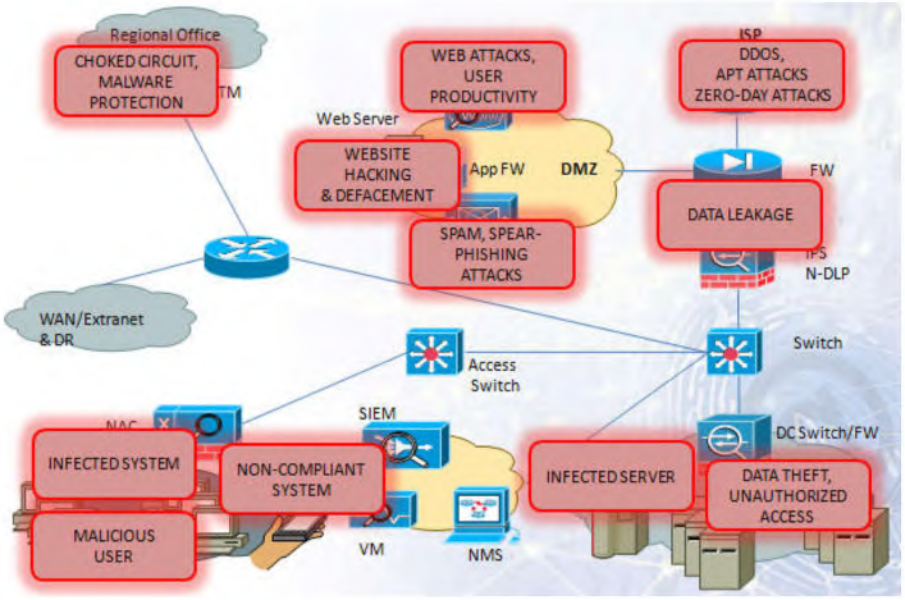
Topic No 34: IT Team Interaction With Other Stakeholders

- IT budget/projects approved by IT Steering Committee (annual)
- Business requirements & new projects
- Audit & compliance requirements
- Expansion (branches) & maintenance
- IT support for computing (helpdesk)
- Business continuity & DR
- IT budget/projects approved by IT Steering Committee (annual):
    - Capex and opex layout
    - Includes new projects & licensing / maintenance of operations
      New hirings

- **Business requirements & new projects:**
    - New upcoming business projects
    - Change requests (CRs) and expansion of existing business projects
    - Vendor management for business solutions
    - UAT (testing) of business applications
- **Audit & compliance requirements:**
    - External audit
    - Internal audit
    - Compliance
    - Information security & risk depts
- **Expansion (branches) & maintenance:**
    - IT requirements for business expansion (new branches, new locations, new territories)
    - Maintenance of existing IT infrastructure (UPS, networking, bandwidth circuits)
- **IT support for computing (helpdesk):**
    - New software and versions rollout (e.g. migration of AV or email program)
    - IT support for business functions (application not working, speed slow, etc)
    - Software bugs
- **Business continuity & DR:**
    - DR is a technology function for which interaction with business functions is required (testing)
    - Business continuity is handled under business operations for which IT also participates

Topic No 35: Security Overlay Of Enterprise (Part 1)

- How is the enterprise secured with the help of various components and security design ?

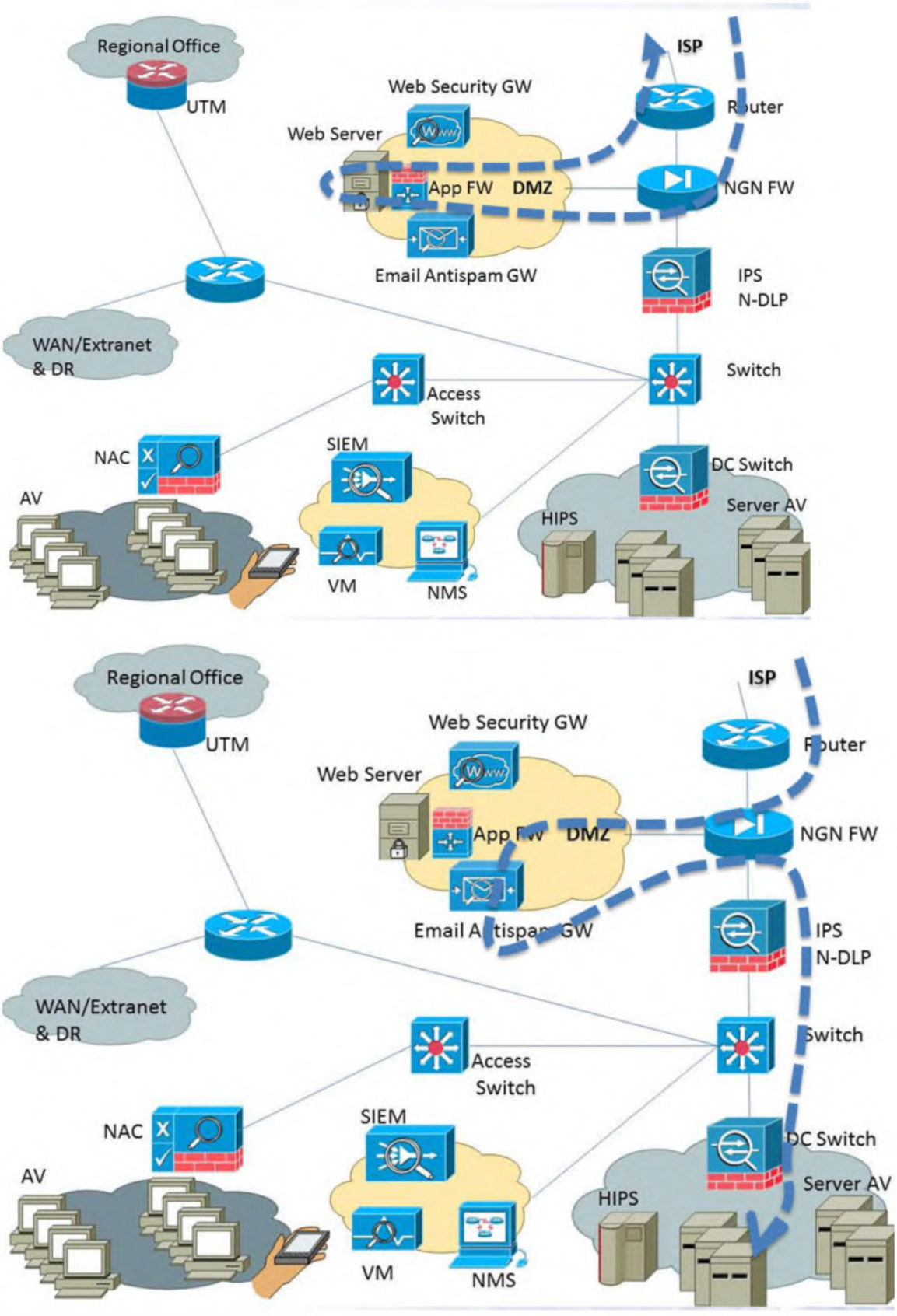


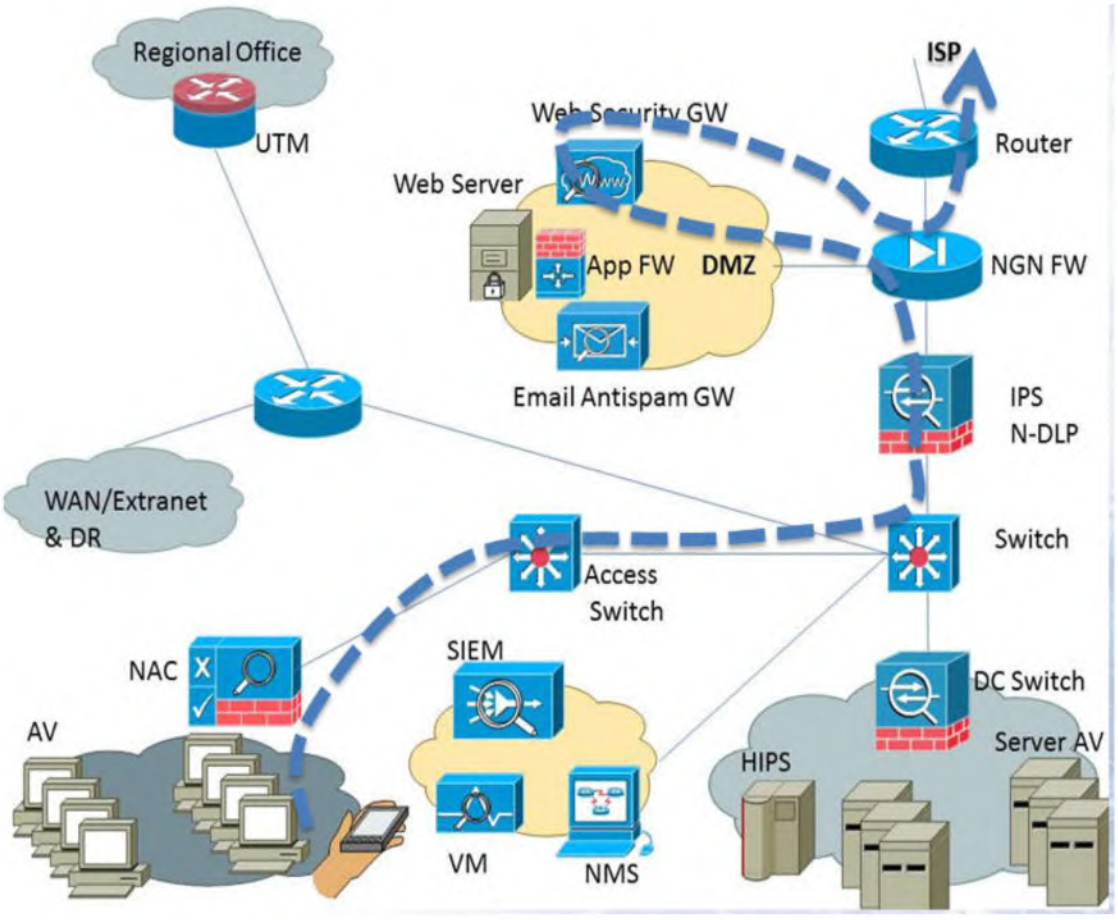
Security Challenge	Location/Device	Security Solution
Perimeter Filtering	Edge Router	Access Lists & Various RFCs
DDOS Attack	Edge Router/DDOS Protection Solution	DDOS Protection
Zero-Day Attack / APT Attack	Edge Device / Edge NGN FW	Zero-Day/APT Attack Prevention
Web Server Attacks	DMZ / Web Application FW	Web Application Attack Prevention
Email SPAM & Malware/Phishing	DMZ / Email Security GW	Email Security

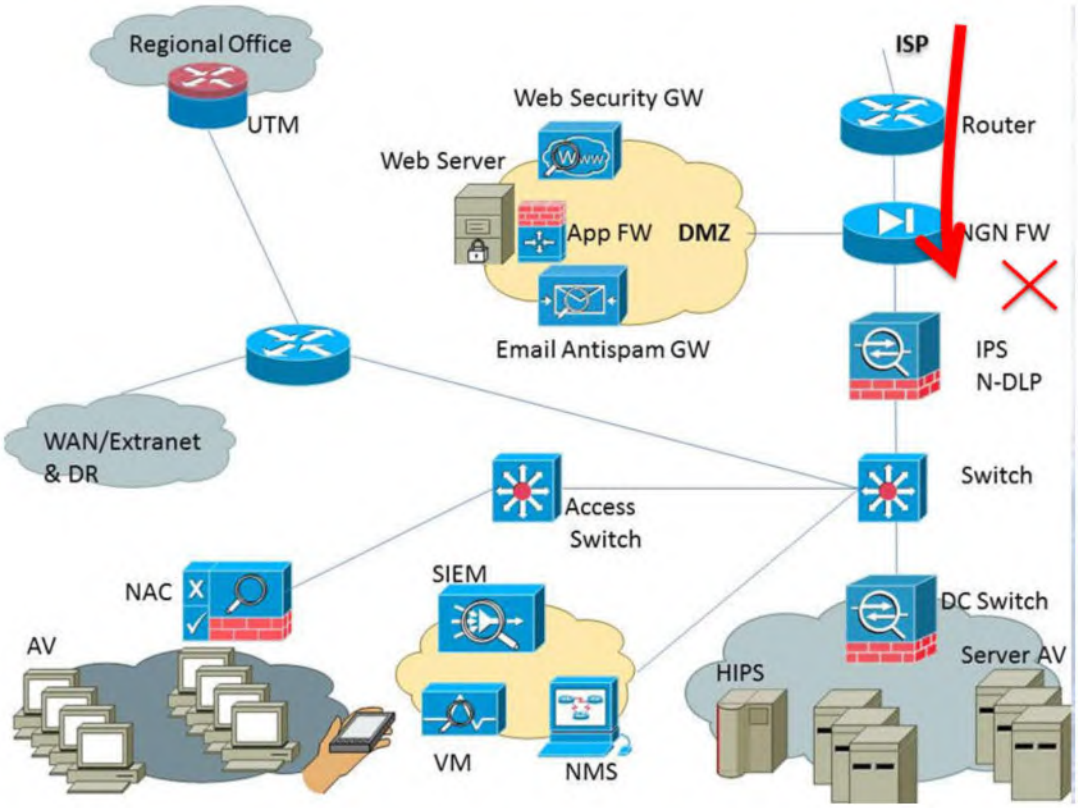
Web-based User Attacks	DMZ / Web Security GW	Web Filtering & Malware Protection
System Malware	System	AV
User Network Access Control	At Aggregation Point Of User Access	Network Admission Control (NAC)
User Controls For USB/Media, HDD Encrypt	System	Data Loss Prevention (DPL) – System Level
Remote Branch Connectivity/ Malware	Intranet-Extranet Edge / UTM	Unified Threat Management (UTM) Solution
Data Center Unauthorized Access / Malware	Data Center FW	Data Center FW Filtering & Malware Protection
Data Exfiltration	Edge / Network DLP	Network DLP Solution
Event Monitoring & Detection	Data Center / SIEM	Security Info. & Event Management
Unpatched Systems	Data Center / VM	Vulnerability Scanner
Server Integrity Monitoring & IPS Filtering	Data Center / HIPS	Host Intrusion Prevention System (HIPS)

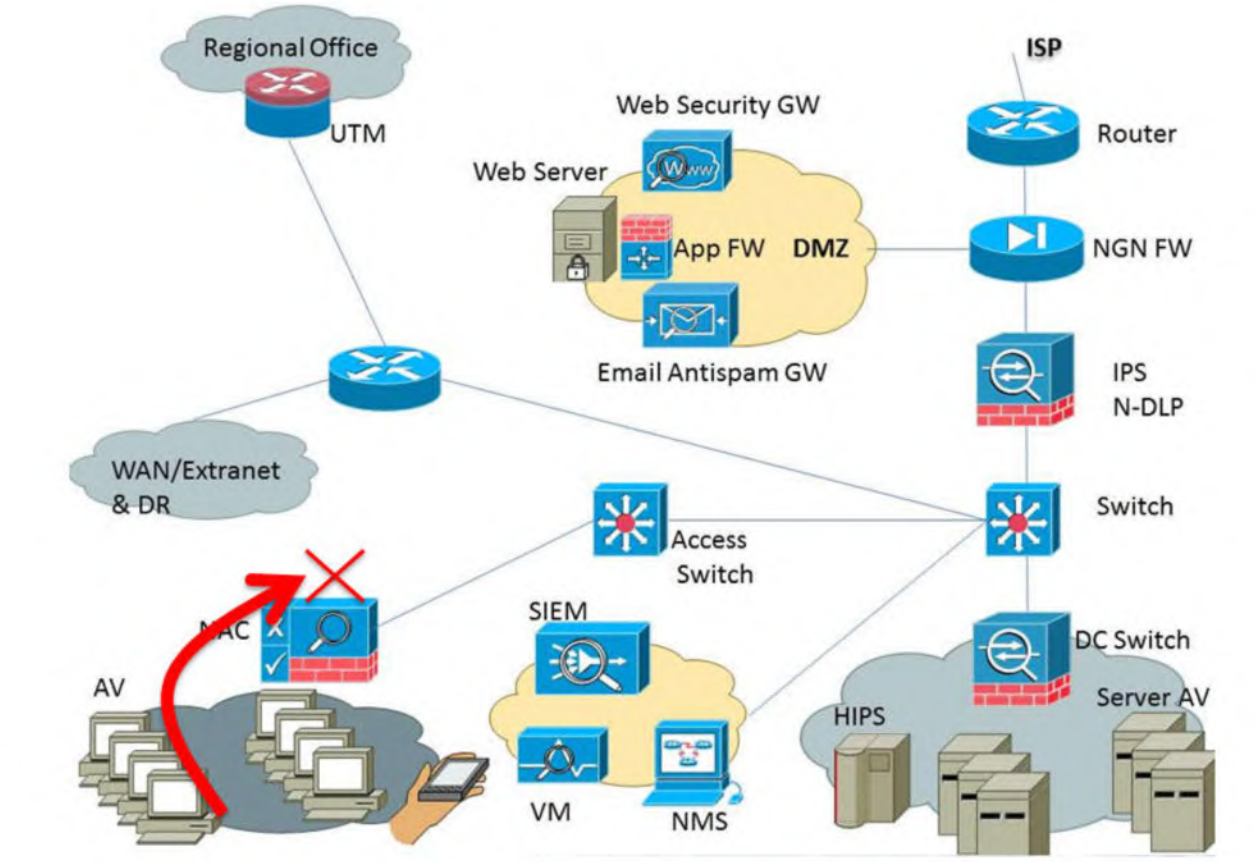
Topic No 36: Security Overlay Of Enterprise (Part 2)

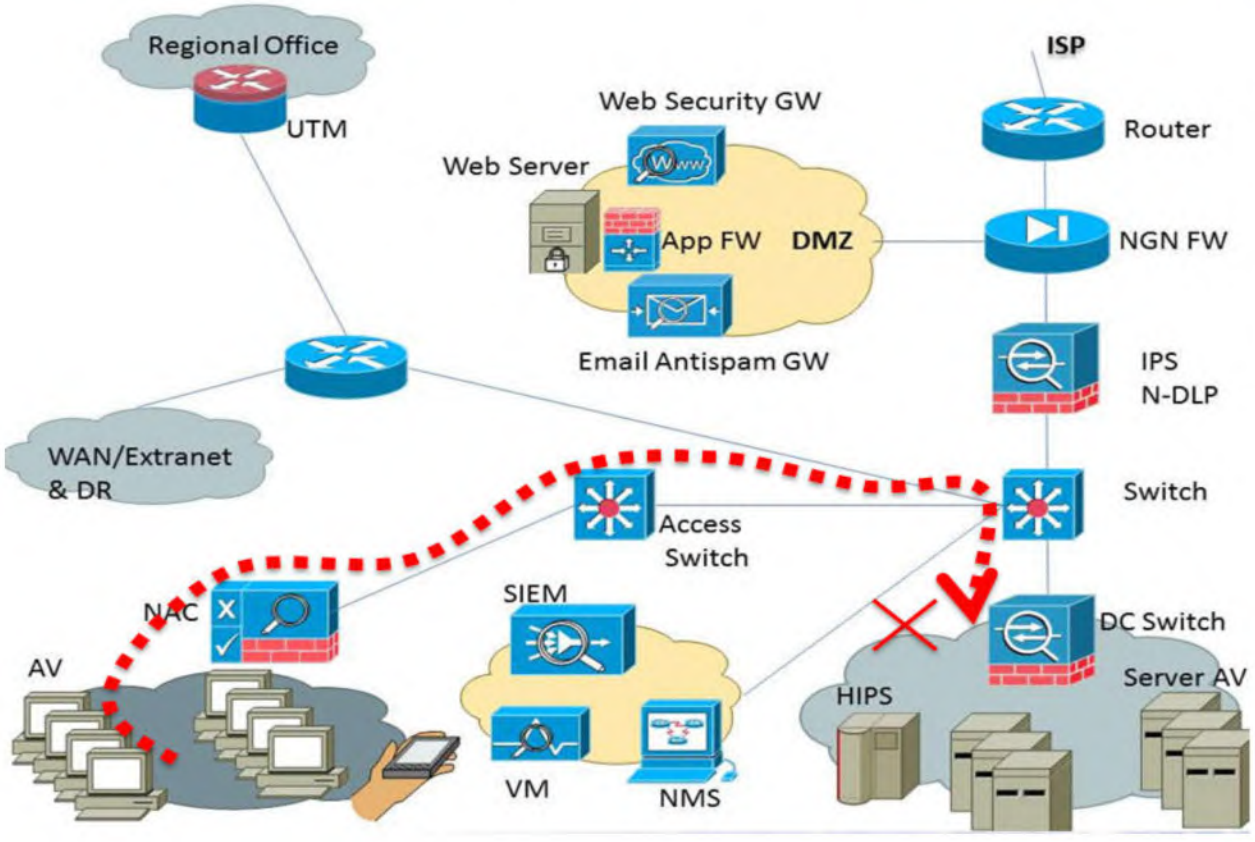
- What are the traffic flows specific to good security design ?

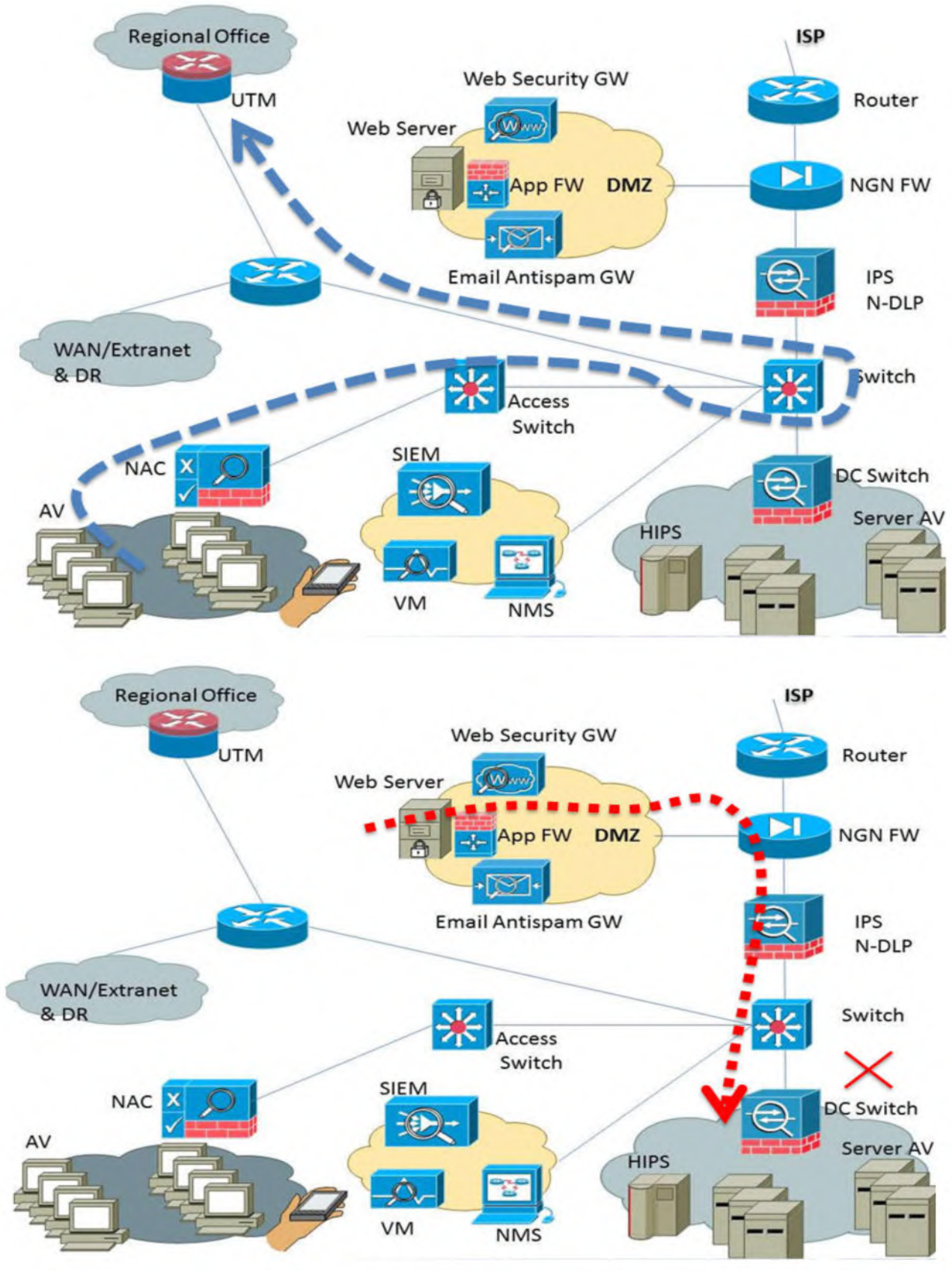



Regional Office
UTM
ISP
Web Security GW
Router
Web Server
App FW
DMZ
NGN FW
Email Antispam GW
IPS
N-DLP
WAN/Extranet
& DR
Switch
Access
Switch
NAC
SIEM
DC Switch
AV
Server AV
HIPS
VM
NMS


Regional Office
UTM
ISP
Web Security GW
Router
Web Server
App FW
DMZ
NGN FW
Email Antispam GW
IPS
N-DLP
WAN/Extranet
& DR
Switch
Access
Switch
NAC
SIEM
DC Switch
AV
Server AV
HIPS
VM
NMS


Regional Office
UTM
ISP
Web Security GW
Web Server
Router
App FW
DMZ
NGN FW
Email Antispam GW
IPS
N-DLP
WAN/Extranet
& DR
Switch
Access
Switch
NAC
SIEM
DC Switch
AV
Server AV
HIPS
VM
NMS

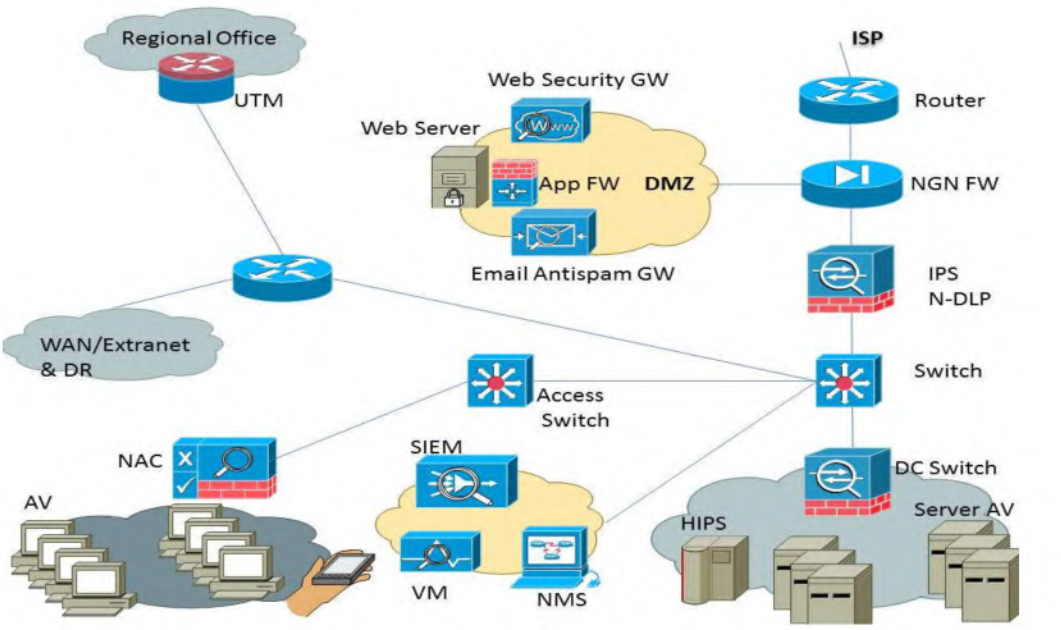

Regional Office
UTM
ISP
Web Security GW
Web Server
Router
App FW
DMZ
NGN FW
Email Antispam GW
IPS
N-DLP
WAN/Extranet
& DR
Switch
Access
Switch
NAC
SIEM
DC Switch
AV
Server AV
HIPS
VM
NMS



- Granular access list filtering and a well planned and tested security design are keys to success

Topic No 37: Security Overlay Of Enterprise (Part 3)

- General security design principles



1. Block unauthorized traffic at edge (direct public www traffic to DMZ web server)
2. Edge malware protection & DMZ
3. Web & email are important vectors to secure against malware and attacks
4. NGN-FW (may be found in a UTM as well)
5. Web security GW and email anti-spam GW solutions
6. Granular access list filtering in edge and data center FWs (source, destination, and traffic type/port)
7. A good AV solution, and keep virus definitions updated
8. Monthly VM scans

More Advanced Security:

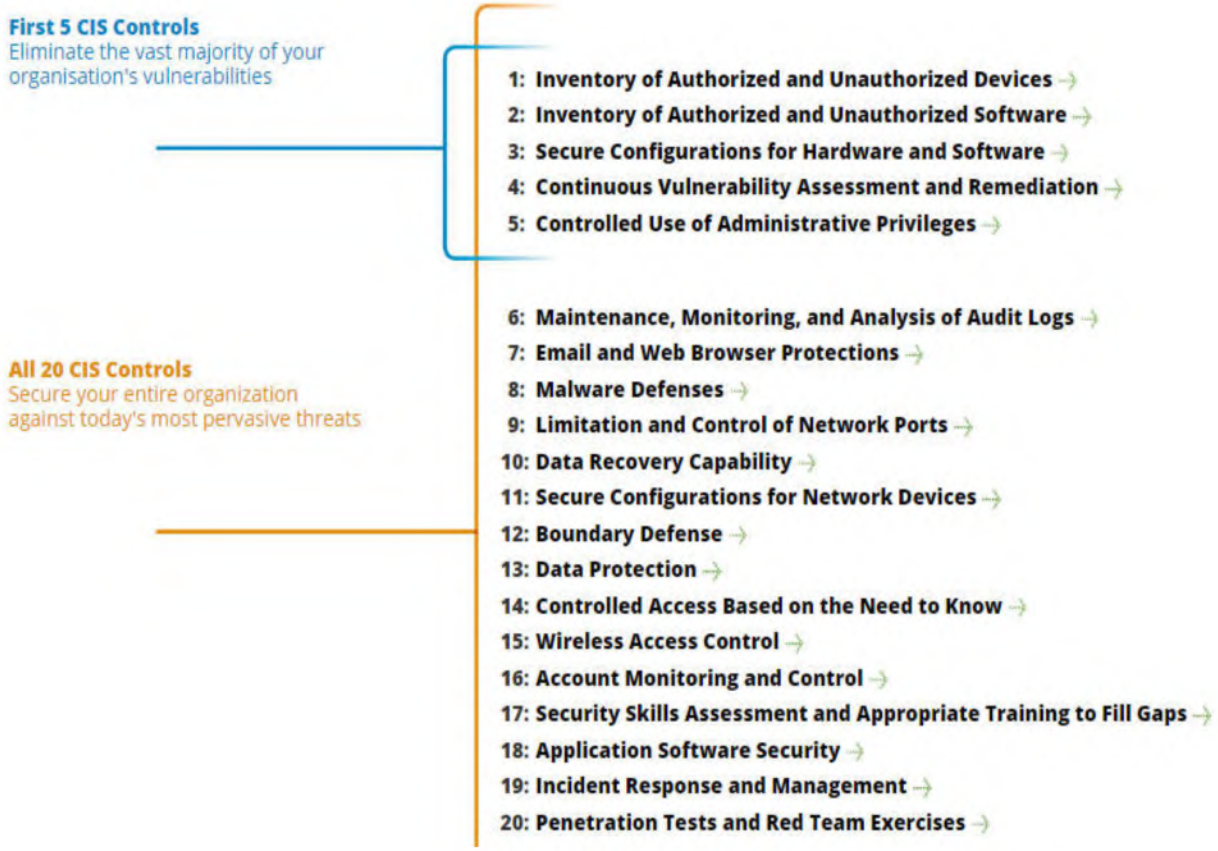
- APT & zero-day attack prevention
- SIEM solution
- Network DLP and system DLP
- Network admission control (NAC)
- Server HIPS
- Web application FW (WAF)

Even More Advanced Security:

- Network forensics
- Host-based APT / IoC solution
- Identity & access management (IAM)
- Privileged identity management (PIM)
- Database security solution

Further guidelines for strong security controls:

- CIS 20 critical security controls



- Further guidelines for strong security controls:
  - CIS 20 critical security controls

Topic No 38: High Availability (HA)

- **What is high availability (HA) ?**
  - High availability of a system or component assures a high level of operational performance (uptime) for a given period of time

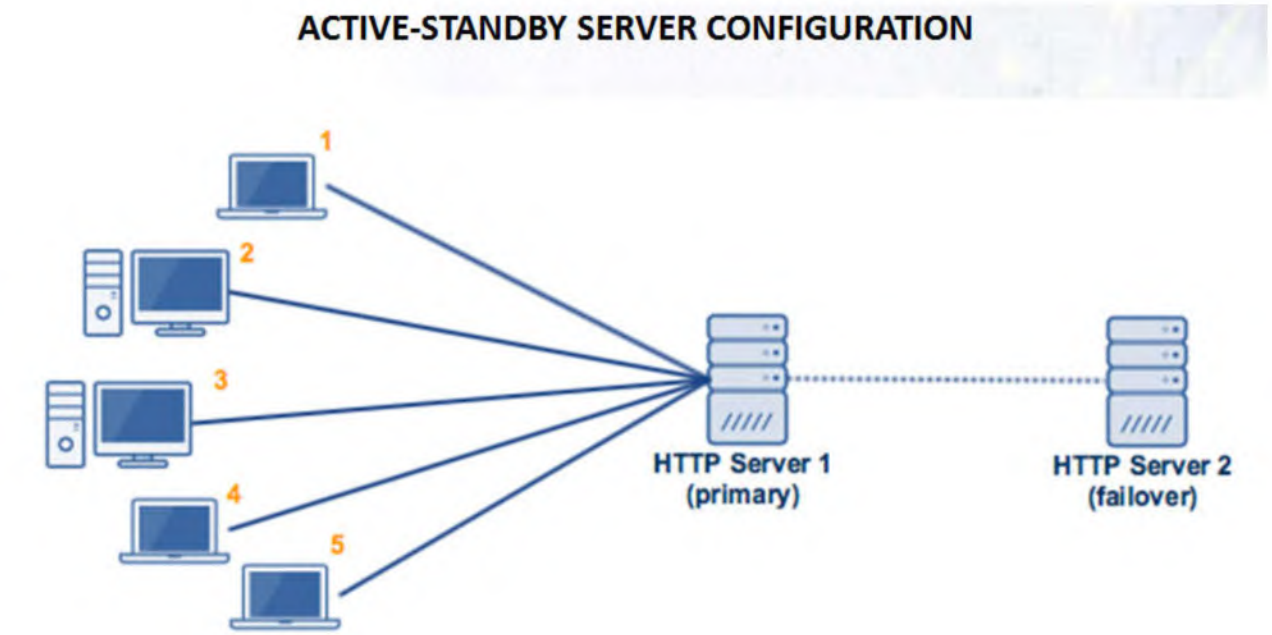
- High availability is a strategy
- Fault tolerance refers to a system designed in such a way that when one component fails, a backup component takes over operations immediately to avoid loss of service

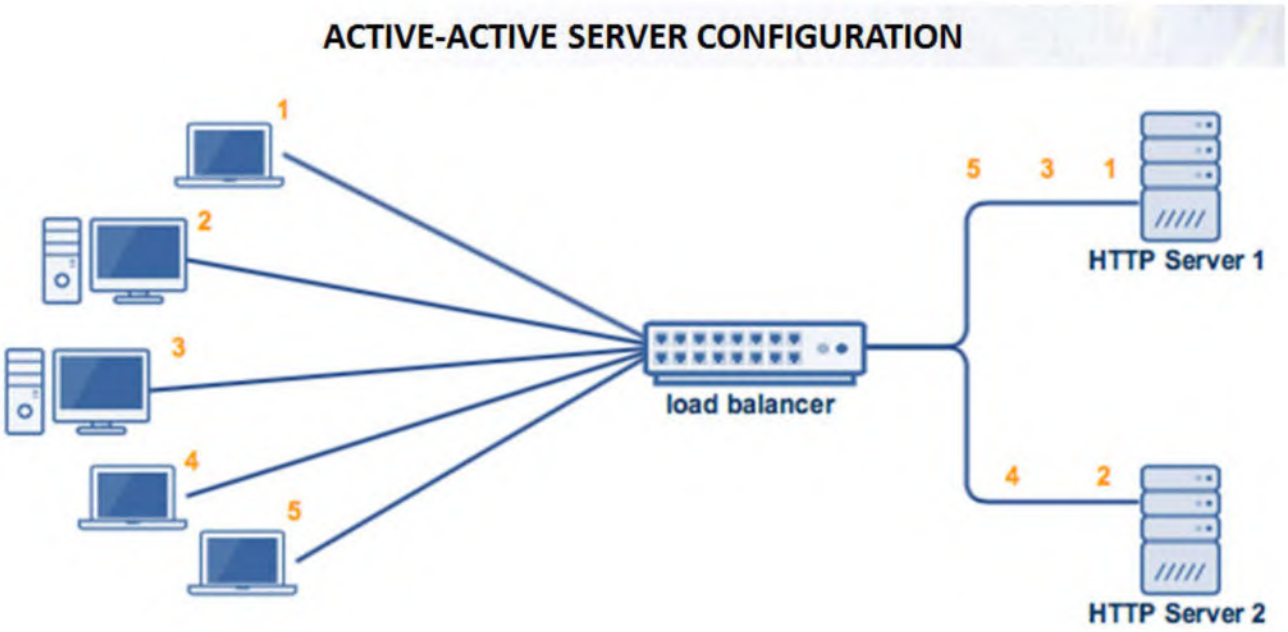
Availability %	Downtime per year	Downtime per month	Downtime per week
90% aka "one nine"	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% aka "two nines"	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% aka "three nines"	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% aka "four nines"	52.56 minutes	4.32 minutes	1.01 minutes
99.999% aka "five nines"	**5.26 minutes**	**25.9 seconds**	**6.05 seconds**
99.9999% aka "six nines"	31.5 seconds	2.59 seconds	0.605 seconds
99.99999% aka "seven nines"	3.15 seconds	0.259 seconds	0.0605 seconds

- High availability is designed in the following manner:
  - System level (data center or service)
  - Device level (within single device)
  - Device level (combination of multiple redundant devices)
  - Alternate site level
- High availability and fault tolerance:
  - Designed to minimize downtime with the help of redundant components
- Disaster Recovery:
  - A pre-planned approach for re-establishing IT functions at an alternate site

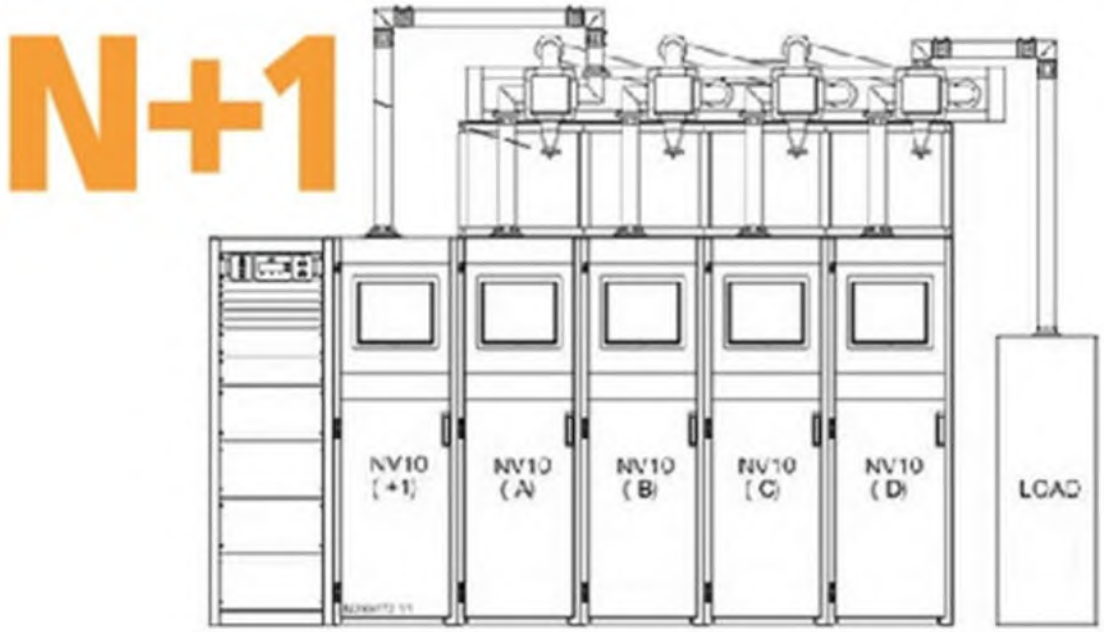
Topic No 39: High Availability Design

- Lets look at various HA designs

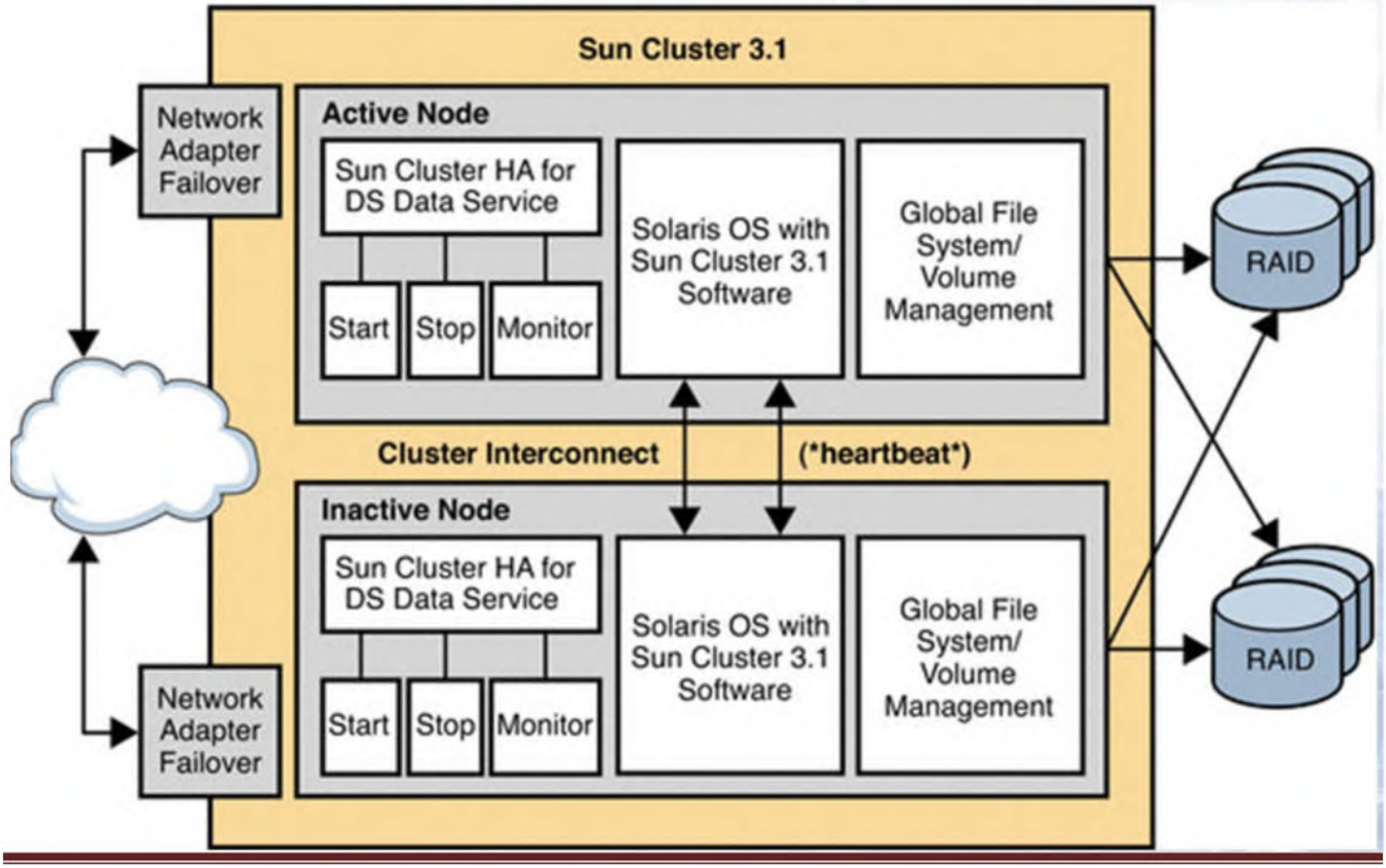


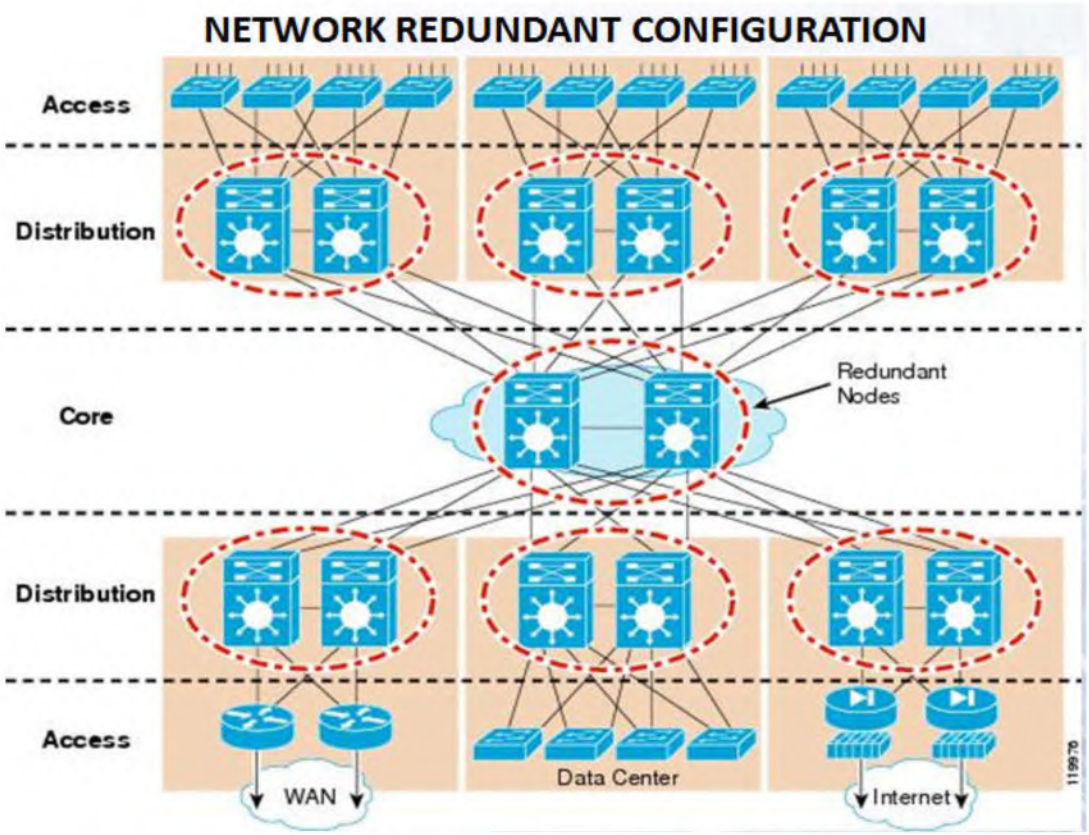


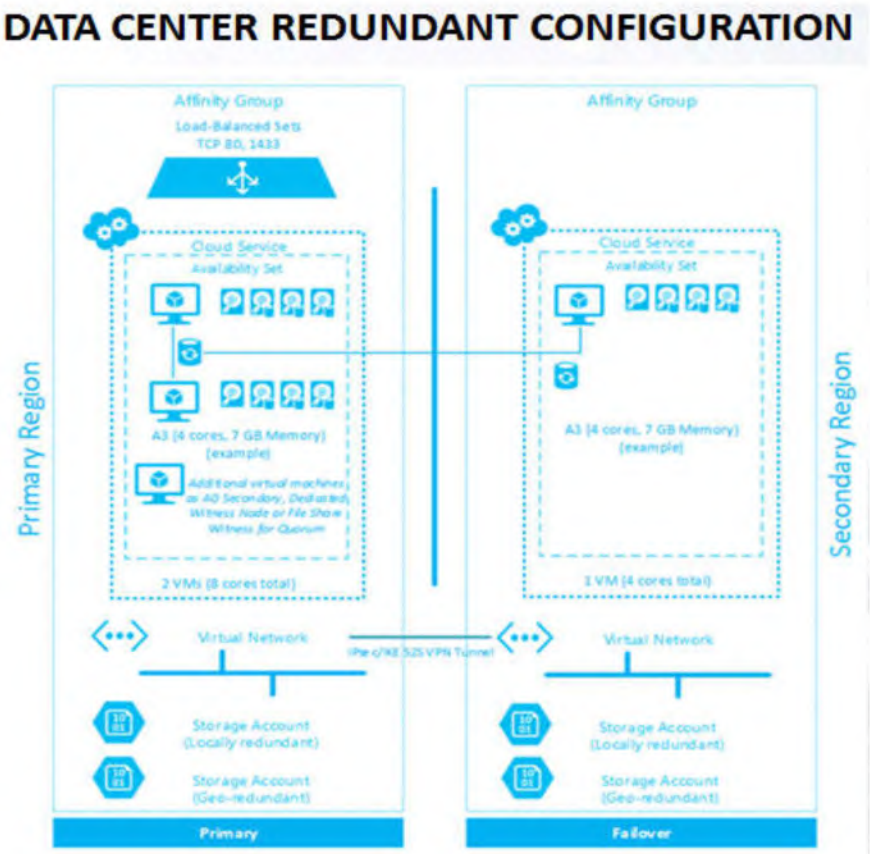
N+1 UPS REDUNDANT CONFIGURATION



ACTIVE-STANDBY SUN SERVER CLUSTER





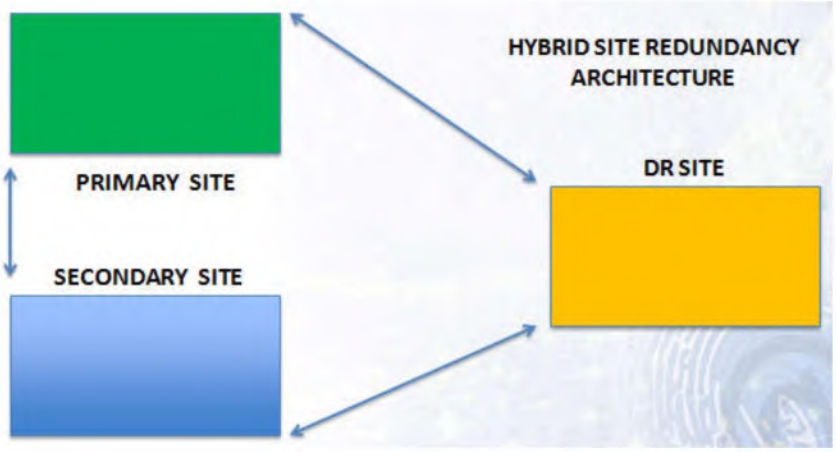


- Don’t forget to test the failover and fault tolerant capabilities of our network

Topic No 40: Site Redundancy

Three types of redundant site models:

- Hot site
- Cold site
- Warm site
- **Hot site (expensive):**
  - Mirror of primary data center
  - Populated with servers, cooling, power, and office space
  - Running concurrently with main/primary data center (synching)
  - Minimal impact
- **Cold site (cheapest):**
  - Office or data center space without any server related equipment installed
  - Power, cooling and office space
  - Servers/equipment migrated in event of primary site failure
- **Warm site (middle ground):**
  - Middle ground between hot site and cold site
  - Some pre-installed server hardware (ready for installation of production environments)
  - Requires engineering support to activate



- **RTO:**
  - Max amount of time, following a disaster, for an organization to recover files from backup storage and resume normal operations (max amount of downtime an organization can handle)
- **RPO:**
  - Max age of files that an organization must recover from backup storage for normal operations to resume after a disaster (minimum frequency of backups)
- **Example:**
  - If an organization has an RTO of two hours, it cannot be down for longer than that.
  - if an organization has an RPO of four hours, the system must back up at least every four hours.

Topic no 41: High Availability & Redundancy Case Study

- Mid-sized enterprise
- 3000 total staff
- 2000 IT users
- 30 IT team
- One DC, one secondary (regional) data center (warm site & backup site), and one DR site 99.9 % uptime designed.

IT setup:

- Oracle ERP system
- Share point portal for workflow automation
- Head office in Karachi
- Primary DC in Karachi (hosted with 3rd party)
- DR site in Lahore (hosted with 3rd party)
- Secondary DC in ISB

Primary DC:

- Fully redundant (HA) design for network, systems, and storage
- Cisco HA (active-standby)
- Oracle cluster technology for servers and DBs (active-active)

Secondary DC (ISB):

- All network, systems, and storage backups maintained here (also mirrored in DR)
- Regional servers (AD, file servers, etc)
- Test & staging environment here (segregated from main DC)
- Office working space

DR site

- Bare minimum HA (as DR site) for network, systems, and storage
- Mirror of all backups from secondary site maintained here
- Office working space
- Some additional computing capacity (minimum for unforeseen events)
- All critical systems and devices maintained in active mode (hot) for immediate DR failover
- Data maintained as per org RTO/RPO for immediate utility
- Monthly DR testing/drill

Backup strategy:

- Primary backup at secondary DR site
- Mirror at DR site
- For critical systems: monthly full backup, daily incremental backup
- For critical network devices: weekly full backup; backups based on change

Topic no 42: Backup Strategies

- **Backup considerations:**
  - What to backup?
  - Backup location?
  - Freq of backup?
  - Backup operator?
  - Backup checker (verification)?
  - Backup test & security methods?
  - Technology & tools used for backup?

- **What to backup?**
  - Network configuration files
  - OS backups
  - Database & application data
  - Other critical data
- **Backup location?**
  - Onsite for faster recovery
  - Offsite for DR purposes
  - Intermediate site (secondary site) as a middle-ground
- **Backup frequency?**
  - Depends entirely on criticality of data, nature of the information being backed up (how frequently does info change?), storage space available, and overall backup plan.
- **Backup operator and checker?**
  - Backups should ideally be automated
  - Operator should ensure that backups have taken place
  - Verifier should sign-off that check has been made
- **Backup testing & security considerations:**
  - Backup testing should be performed on a periodic basis and greater than the frequency of the DR drill (e.g. DR drill once a QTR, & testing once a month)
  - Encryption & compression
- **Backup tools and technology:**
  - Consider NAS, SAN, SCSI/IDE/SATA drives
  - Various tools and technology to perform full, differential, and incremental backups
  - Encryption
  - Access control
  - Alerts & reporting

Topic no 43: Security Tools Used In An Enterprise

- **Typical security tools used in an enterprise:**
  - Enterprise antivirus
  - MS Active Directory (AD)
  - Vulnerability manager
  - Logs management
  - Network & performance monitoring

    Automated backups
- **Typical security tools used in an enterprise:**
  - Microsoft Windows Server Update (WSUS) & SCM/SCCM
  - Asset management software
  - Trouble-ticket system
  - SIEM
  - DLP
  - Encryption software
  - 2FA

Tool	Function	Complexity level	Examples
Enterprise Antivirus	System antivirus and malware protection	Low	Sophos, Avast, Kaspersky, Symantec, McAfee
MS AD (GP)	Pushing out security policies through AD GPO	Low	Pushing out windows password settings
VM	Vulnerability scanning	Medium	OpenVAS, Nessus, Qualys
Log Management	Logs collection & analysis	Medium	OSSEC
Network & Performance Management	NOC	Low	CACTI, ORION
Automated Backups	Backups	Medium	Veritas
Windows Updates	Windows Updates & Configs	Low	WSUS, SCCM, SCM
Asset Management	Dtect, Track, Manage Assets	Medium	Asset Explorer, PulseWay
Trouble Ticket System	TT Workflow	Medium	BMC Track-IT, SysAid
SIEM	Event Management	High	OSSEC, Splunk, Q-Radar
DLP	Data Loss Prevention	High	Symantec,
Encryption Software	Encryption	High	TrueCrypt

Topic no 44: Security Tools – Typical Enterprise (Part 1)

- Gartner Magic Quadrant reports
- List of some other industry reports

Endpoint Protection Jan, 2017 Gartner

Trend Micro
Sophos
Kaspersky
Symantec

Secure Web GW June, 2017 Gartner

Symantec
Zscaler

UTM
(SMB Multi-function FW)
June, 2017
Gartner

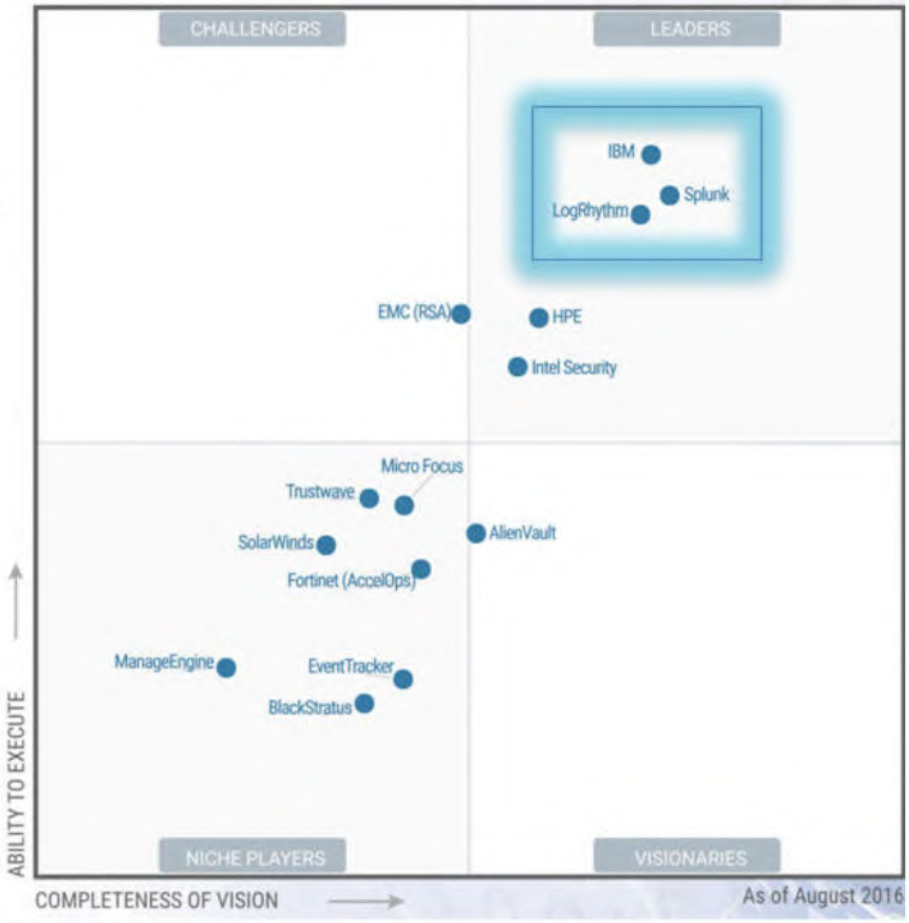
Fortinet
Checkpoint

Enterprise Network FWs
May 2016
Gartner

Palo Alto Networks

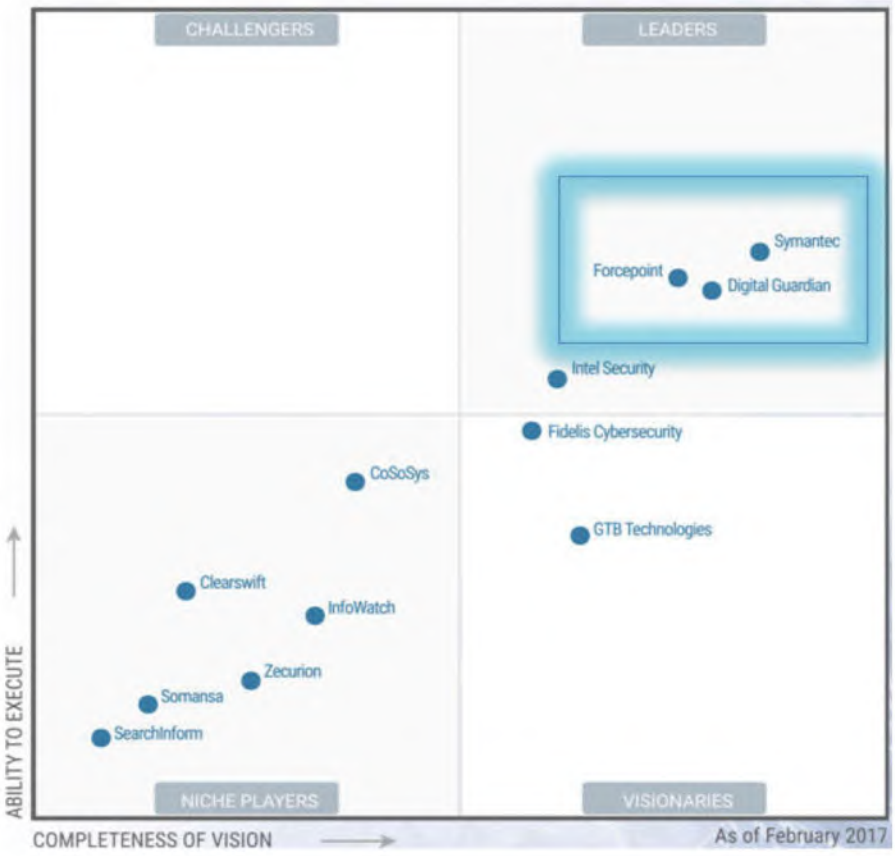
SIEM
AUGUST 2016
GARTNER

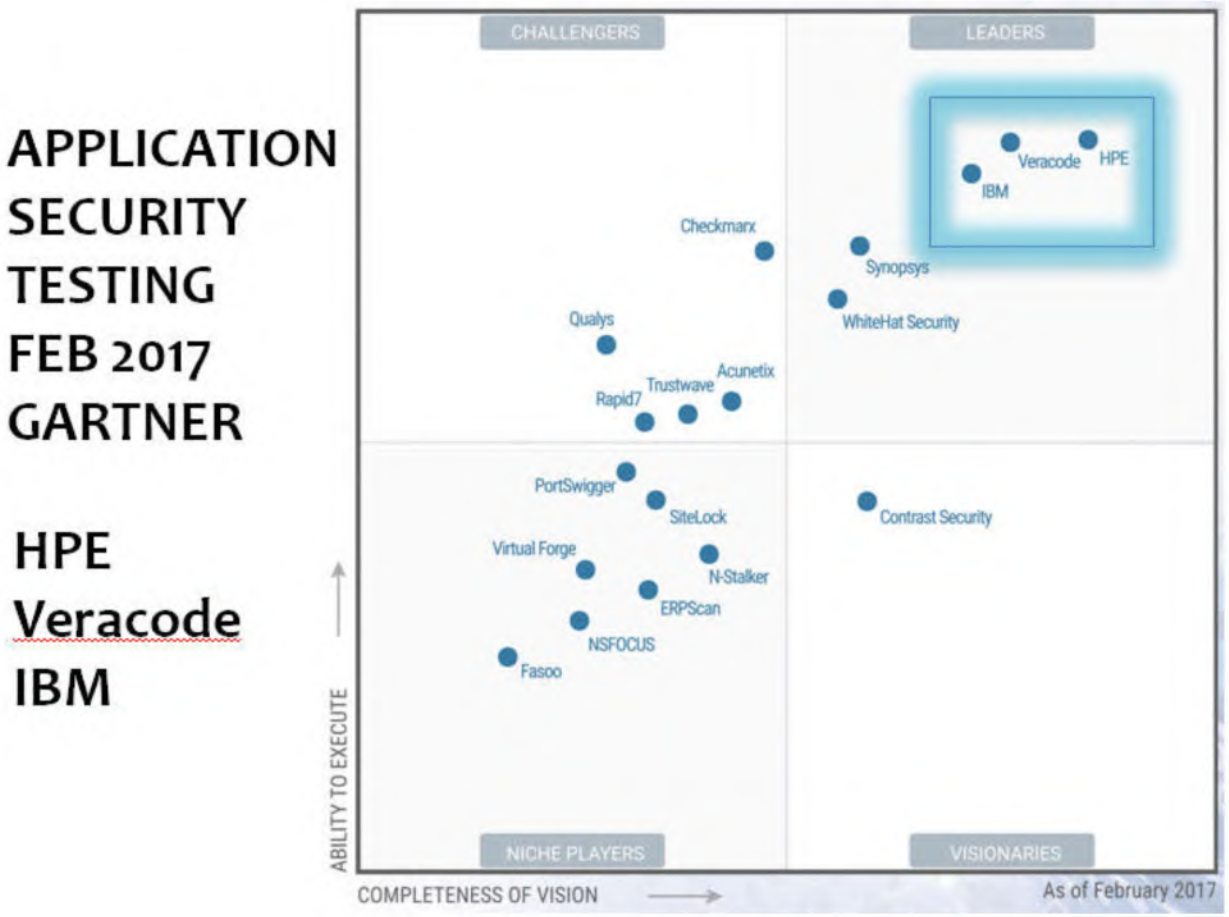
IBM
Splunk
LogRhythm



DLP
FEB 2017
GARTNER

-Symantec
-Digital
Guardian
-Forcepoint





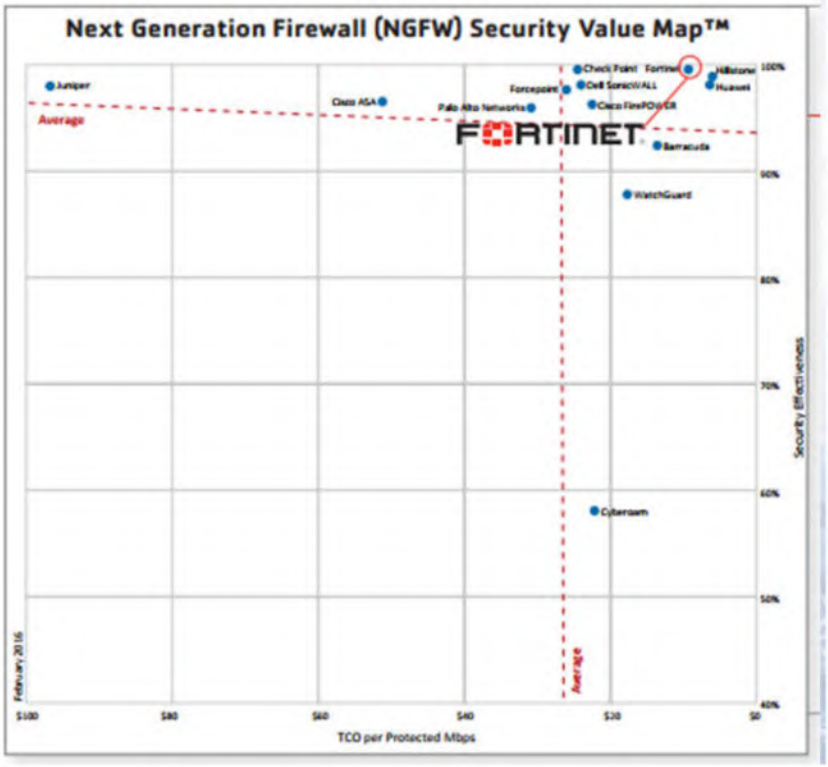
- View and read various industry reports for security tools comparisons:
  - Gartner
  - Forrestor
  - Security Awards
  - Lab reports: ICSA, NSS

Topic no 45: Security Tools – Typical Enterprise (Part 2)

- NSS Labs Security Value Map (SVM)
- Some additional Gartner Magic Quadrant reports

NGFW
NSS Labs
2016

Hillstone
Huawei
Fortinet



Enterprise
Mobility
Management
(EMM)
June 2017

VMWARE
MobileIron
IBM
Blackberry

DC Backup
& Recovery
June 2016

Commvault
IBM
EMC
Veritas

Figure 1. Magic Quadrant for Identity Governance and Administration

Identity,
Governance
Feb 2017

Sailpoint
Oracle
CA
IBM

Source: Gartner (February 2017)

Network Perf Monitoring & Diagnostics Feb 2017

NetScout
Viavi
Riverbed

Web App FW July 2016

Imperva

- **Gartner**
- **Forrestor**
- **NSS labs**
- **ICSA Labs**

Topic no 46: What Does "Box Security" Mean?

- "Box Security" refers to a prevalent approach in the industry, especially in larger organizations in which the solution for every security challenge is in the form of a "box" or device
- **Box for :**
  - Email security
  - Web security
  - FW
  - IPS
  - APT attack prevention
  - DDOS prevention
  - Network DLP
  - Network Forensics
  - Others
- Security is a combination of people, process, and technology
- Industry observation: most of the devices are not used to full capability or capacity after purchase
- Case in point: SIEM solution or DB security solution
- "Box security" is not the silver bullet
- Although many devices and boxes are required, they do not ensure a good security posture
- This approach is unfortunately promoted by many vendors who have equipment to sell
- Consider organizational maturity & readiness

Other challenges with "box security" approach:

- Shortage of staff (IT & security)
- Training and skill required to operate the sophisticated devices and features

- Device objectives, and high-level-design (HLD) should be planned prior to commissioning
- Min operational baseline and configuration should be documented in SOP
- Device feature set and configuration audits should be conducted on a periodic basis (annual)

Topic no 47: Best Approach: IT Enterprise Security

- The 4-layer security transformation model is the only way to effectively and practically address security posture
- 4-layer security transformation model is tried & tested for geographies where the overall security awareness & posture is weak

1. **Security hardening:** address security configuration of all IT assets which security "boxes" won't do for you
2. **Vulnerability management:** scanning to inspect patching of IT assets (essential)

- Security engineering
- Security governance

3. **Security engineering:** this is where more serious investments may be made once layers 1 & 2 have been completed satisfactorily (or are being addressed).
4. **Security governance**: ensure the proper utilization (as intended), ROI, and audits of purchased devices & solutions. Also ensure configs are as per design, and SOPs.

Topic no 48: What Is Disaster Recovery (DR)?

- **What is a disaster?**
  - Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business
- **What is disaster recovery (DR)?**
  - DR is an area of security that allows an organization to maintain or quickly resume mission-critical (IT) functions following a disaster
- **What could cause the invocation of a DR fail over to DR site?**
  - Natural disasters such as flood, earthquake, lightning, storm
  - Disaster caused by human actions such as riot, fire, terrorist act, etc
- **What is the difference between DR and business continuity (BC)?**
  - DR is an IT function, whereas business continuity addresses keeping all essential aspects of a business functioning despite disruptive events (DR is a part of BC)

- **Three step process:**
  - Failover to the DR site (DR invocation)
  - Restoration of the services/facilities on primary site
  - Recovery (switchover back to primary site)
- **What is a DR plan?**
  - A documented, structured approach to dealing with unplanned incidents

- **DR plan checklist:**

- Scope of the activity
- Gathering relevant network infrastructure documents
- Identifying the most serious threats and vulnerabilities, and the most critical assets
- Identifying current DR strategies
- Identifying emergency response team
- Management review & approval of DR plan
- Testing the plan (drill)
- Updating the plan
- Implementing a DR plan audit

Topic no 49: What is Business Continuity (BC)?

- **What is business continuity?**

  - Business Continuity (BC) is the capability of the org to continue delivery of products or services at acceptable predefined levels following a disruptive incident *(Source: ISO 22301:2012)*

- **What is business continuity management?**

- Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building org resilience with an effective response that safeguards interests of key stakeholders, reputation, brand and value-creating activities. *(Source: ISO 22301:2012)*

The BCM Lifecycle
- improving organizational resilience

- **What is a BC plan?**
  - A document that consists of critical information an organization needs to continue operating during an unplanned event
  - The BCP should state essential functions of the business, identify which systems and processes must be sustained, & detail how to maintain them.
  - It should take into account any possible business disruption

Topic no 50: DR In Enterprise Architecture – Part 1

- **DR considerations:**
  - DR plan
  - RTO & RPO
- **DR plan:**
  - A disaster recovery policy statement, plan overview and main goals of the plan
  - Key personnel and DR team contact information
  - Description of emergency response actions immediately following an incident.
  - A diagram of the entire network and recovery site.
  - Directions for how to reach the recovery site.
  - A list of software and systems that will be used in the recovery.
  - Sample templates for a variety of technology recoveries, including technical documentation from vendors.
  - Summary of insurance coverage.
  - Proposed actions for dealing with financial and legal issues.
  - Ready-to-use forms to help complete the plan.

- **RTO:**
  - Max amount of time, following a disaster, for an org to recover files from backup storage and resume normal operations; max amount of downtime an org can handle.
  - If an organization has an RTO of two hours, it cannot be down for longer than that
- **RPO:**
  - RPO is the max age of files that an organization must recover from backup storage for normal operations to resume after a disaster; determines the minimum frequency of backups.
  - For example, if an organization has an RPO of four hours, the system must back up at least every four hours

Topic no 51: DR In Enterprise Architecture – Part 2

- DR considerations:
  - DR facility
  - DR drills & testing
  - DR testing checklist
  - BC plan alignment
- **DR facility:**
  - Location
  - Media circuits and backup circuits
  - Power and environment

  - IT data center design
  - Based on DR plan
  - Operations & maintenance

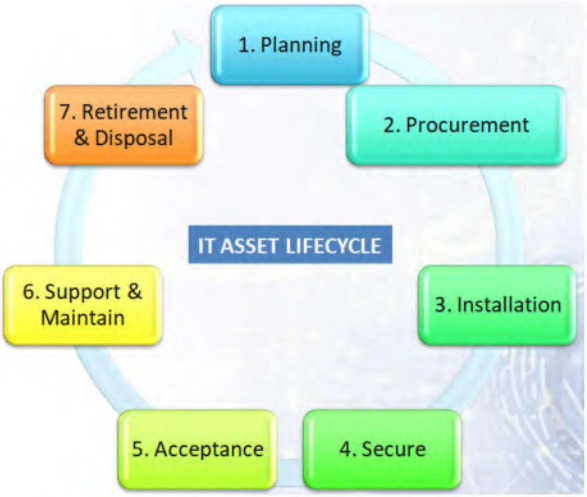
- **DR drills & testing:**
  - Frequency and execution of DR drills as per IT policy of the org
  - Min twice a year and preferable quarterly for critical business reqmts
  - Backup testing

- **DR testing checklist:**
  - Secure management approval and funding for the test.
  - Provide detailed information about the test.
  - Make sure the entire test team is available on the planned test date.
  - Ensure your test does not conflict with other scheduled tests or activities.
  - Confirm test scripts are correct.
  - Verify that the test environment is ready.
  - Schedule a dry run of the test.
  - Be ready to halt the test if needed.
  - Have a scribe take notes.
  - Complete an after-action report about what worked and what failed.
  - Use the test results to update DR plan

- **BC plan alignment:**
  - DR is under IT ownership, whereas BC is under business operations ownership
  - DR is part of overall BC
  - Both plans must integrate and align seamlessly

Topic no 52: Role Of An IT Asset In Enterprise Security

- **What is an IT asset?**
  - An IT asset is any resource such as hardware, software, information, human resource, or facility owned or utilized by the organization for IT processing



1. PLANNING
- Requirements
- Owner & Risk Owner
- High Level Design
- Budget Approvals
- Project Planning

2. PROCUREMENT
- RFP
- Vendor Selection
- PO
- Contract & SLA
- Kick-Off Meeting

3. INSTALLATION
- Site Preparation
- Delivery
- Configuration
- Testing
- Commissioning

4. SECURE
- Security Controls
- Security Checklist
- Security SOP
- Security Testing

5. ACCEPTANCE
- Test Scripts
- UAT
- Security Accreditation
- Commissioning Sign-off
- Change Management

6. SUPPORT/MAINTAIN
- Vendor Support
- Maintenance/Repair
- Change Requests
- Renewals & Upgrades
- Regular Updates
- Monitoring & Audits

7. RETIRE/DISPOSE
- Decommission
- Dispose/Salvage
- Update Inventory

- Asset Owner: a person in the org responsible for managing an asset (e.g. for laptop)

- Risk owner: manages risks associated with the IT asset. Authorized to make decisions associated with managing risks, and in a management position
- **Acceptable Use (Of IT Assets):**
  - Laptops
  - Mobiles
  - Web browsing
  - Email usage
  - Servers
  - Company data

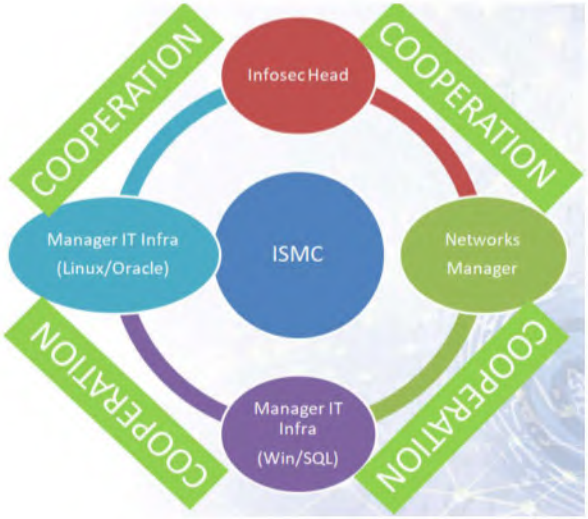
Topic no 53: How To Determine Security Posture?

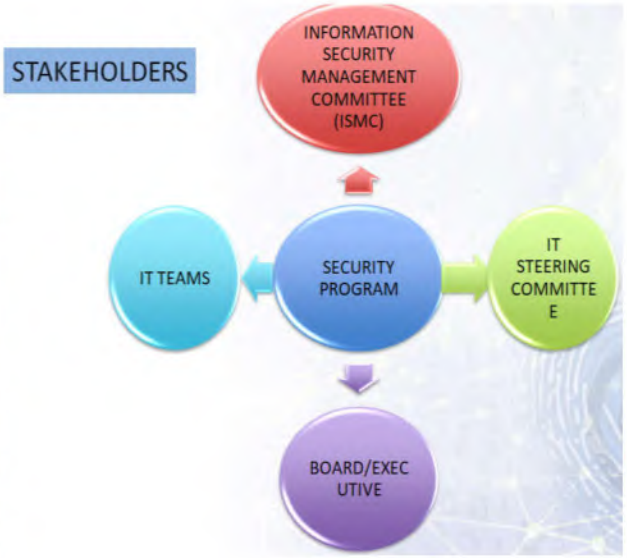
- Questions to ask:
  - Information security policy?
  - Organization security culture and tone at the top?
  - Clearly designated responsibility for security?
  - How many staff in security team [10%] and their roles?
  - Security hardening done on IT assets?
  - Which standard used for hardening?
  - Internal VM program?
  - Frequency of VM scanning?
  - Licensed software for OS/DB/Programs?
  - Last time penetration test was conducted by 3rd party?
  - Maturity of system security policies pushed through AD/GP
  - DR and/or backup site?
  - When was the last time a DR drill was performed?

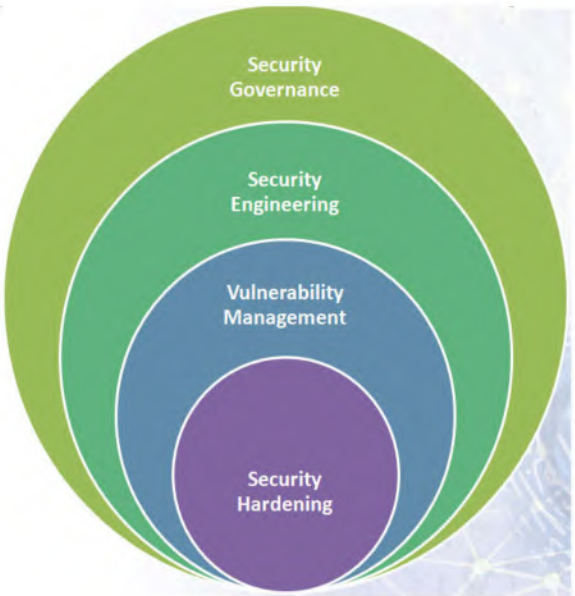
Topic no 54: Driving Successful Security Transformation

- Critical factors for successful security transformation projects:
  - Board-level buy-in and sponsorship
  - Regular Board or Executive management project reviews and decisions
  - Allocation of sufficient priority & resources

- Projects either fail or succeed before they begin!







- Successful security transformation projects can be made successful with correct sponsorship, structure, strategy, and strong project management

Chapter 3

Security Transformation Stage

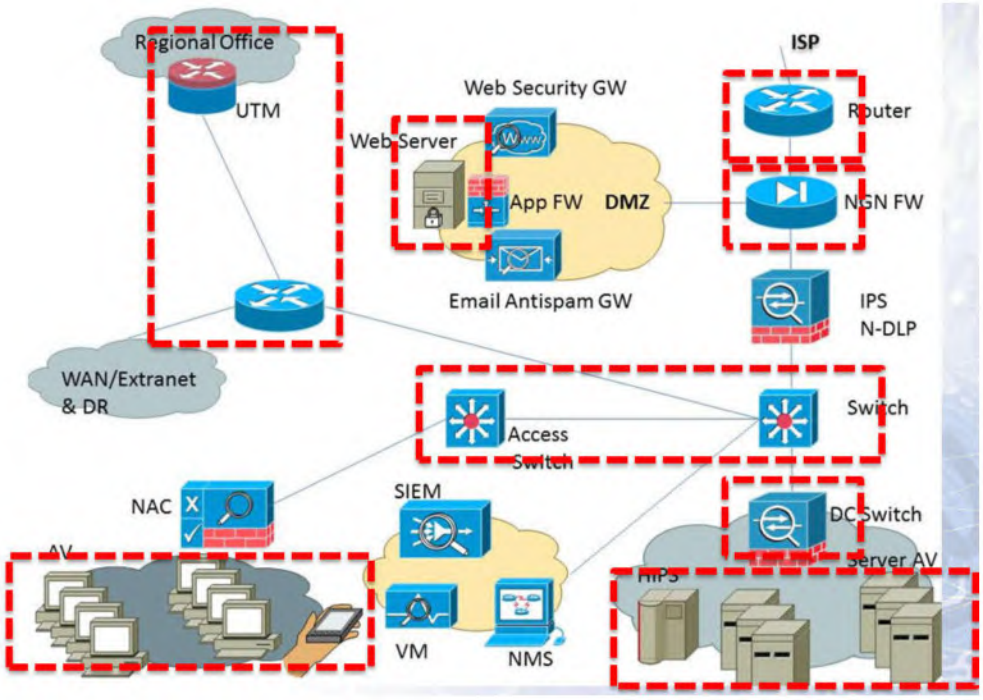
Topic no 55: Revisit Of Security Transformation Model

- **Security hardening:**
  - IT assets such as hardware and software come with default (insecure) configurations which become the basis for attacks
  - Typical case in point: username and password: "admin, admin"
  - System by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one.
- **Patching:**
- Fixing vulnerabilities (which may be exploited by malware or attackers) in software or firmware with vendor released patches (auto or manual updates)
- Patches are also called fixes
- **Patching considerations:**
  - Vendors release patch when they become aware of a vulnerability
  - Patches may be rolled up into a release
  - Off-the shelf software works well but testing reqd for customized instances
- **Hardening:** includes additional steps beyond patching to limit the ways a hacker or malware could gain entry.

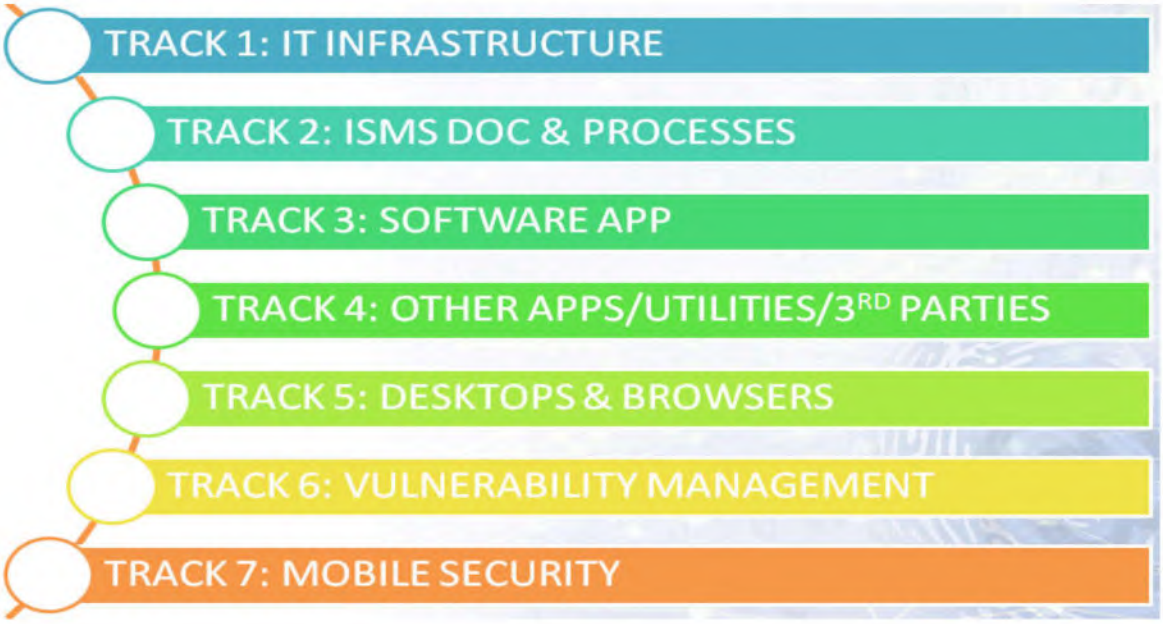
  Accomplished by turning on only the ports and services required, secure configuration of services & additional steps to limit system access
- **Note that both hardening & patching are required**
  - Hardening prevents existing and future vulnerabilities by tightening configuration
  - Patching is more of a vendor driven process but essential nonetheless

Topic no 56: Security Hardening Strategy

- Depending upon the size and type of the organization, there will be dozens, hundreds, or even thousands of IT assets to secure
- Priority is a key factor in all security undertakings
- Prioritize what is most important and needs to be done first
- Cascade as we go along



- Separate security engineering (Step 3) from security hardening (step 1)
- Security engineering requires more thorough working so will slow down the security implementation
- Do the low hanging fruit first (security hardening)
- Minimum security baseline (MSB) refers to the obvious assets which need to be secured and the threshold which is the minimum expectation from the security program



- For a successful security transformation project, good planning, organization, and effective project management is essential.

Topic no 57: Pre-requisites For Security Hardening

1. Security program approved
2. Consultant on board
3. Project kick-off meeting held
4. ISMC team identified and their loading for this project communicated
5. Appraisal linkage of core resources announced by CIO

1. Security program approved

- Project director
- Timeline
- General project sequence and strategy
- Understanding of main players and roles
- Understanding of project structure

2. Consultant on board

- Expert consultants in security transformation can facilitate the project success
- Third party & independent

- Bring a focus on delivering results
- Strong domain knowledge

3. **Project kick-off meeting held**
    - Project goals & mission
    - All key stakeholders made aware of their roles
    - Responsibilities & authority
    - Success criteria & reporting mechanism
4. **ISMC team identified and their loading for this project communicated**
    - ISMC plays a critical role
    - Cooperation & teamwork
    - Security leadership culture
    - Clarity on goals
5. **Appraisal linkage of core resources announced by CIO**
    - Broader team
    - Announcement by CIO
    - Clarity on evaluation mechanism

Topic no 58: Who Will Conduct The Security Hardening?

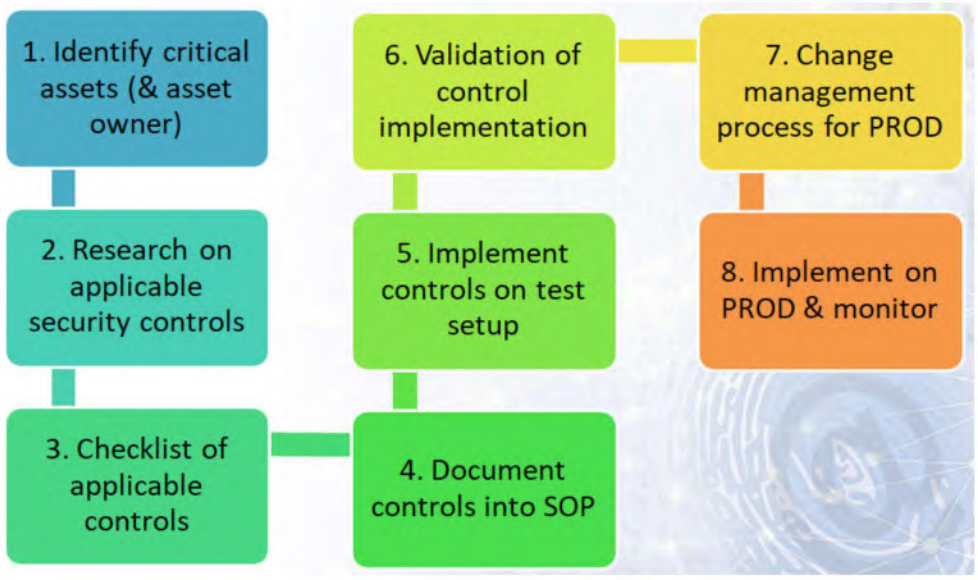
- **Involvement of various stakeholders for security hardening**
    - Operations teams
    - Security team
    - IT management
    - Consultant
    - Business

- **IT Operations teams:**
  - Study the security controls (CIS/DISA)
  - Apply the security controls in pilot/test environment
  - Report the completion of control implementation to ISMC
  - Assist InfoSec team with validation
- **InfoSec team:**
  - Conduct validation of security controls implementation
  - Acquire checklist of controls from relevant IT team
  - Document the status of controls in the form of a checklist
  - Forward validation report to ISMC
- **IT management:**
  - Ensure IT operations teams receive required guidance and support
  - Sign-off on change management requests
  - Assist with planning down-time and business related downtime
- **Consultant or project director:**
  - Drives the security program
  - Ensures that strategy is aligned with project objectives
  - Ensures process and activities are moving at good momentum as per timeline

- **Business stakeholders:**
  - Provide downtime approvals if required
  - Help to engage other vendors if applicable

Topic no 59: 8 Step Methodology – Security Hardening (1)

- What is the 8 step security hardening methodology?



- **Purpose:**
  - Many assets need to be hardened at various times, by various teams, for various requirements and projects
  - Standardize and follow a consistent approach
- **Benefits:**
  - Process for security hardening
  - Discipline to always follow the same steps
  - Helps avoid missing any steps in the process
  - Gives team clarity on what to do and what sequence to follow
- **If You Skip This Process:**
  - Will follow a new approach every time
  - Every resource has their own method

- Dependence on resource rather than the process
- Complicate rather than simplify
- Divergence in security activities

STEP	DESCRIPTION	PERFORMED BY	FACILITATED BY
1	IDENTIFY CRITICAL ASSETS (& ASSET OWNER)	ISMC	HEAD OF IT SECTION
2	RESEARCH APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	ISMC
3	CHECLIST OF APPLICABLE SECURITY CONTROLS	INFOSEC TEAM	TEAM LEAD
4	DOCUMENT CONTROLS INTO SOP	TEAM LEAD	INFOSEC TEAM
5	IMPLEMENT CONTROLS ON TEST SETUP	IT OPERATIONS TEAM	TEAM LEAD
6	VALIDATION OF CONTROL IMPLEMENTATION	INFOSEC TEAM	IT OPERATIONS TEAM
7	CHANGE MANAGEMENT PROCESS FOR PRODUCTION	TEAM LEAD	ISMC
8	PRODUCTION & MONITOR	IT OPERATIONS TEAM	TEAM LEAD

Topic no 60: 8 Step Methodology – Security Hardening (2)

- **Step 1: Identify Critical Assets & Asset Owner:**
  - Asset inventory & infrastructure diagram
  - Examine risks
  - Analyze assets at a high level and prioritize
  - Minimum security baseline (MSB)
  - Break into phases
- **Step 2: Research on applicable security controls**
  - CIS, DISA
  - Search on google
  - Review standards/frameworks (ISO27001, PCI, etc)
  - Look at OWASP, CSA, NIST, CIS Top 20
  - Selection of controls
- **Step 3: Checklist of applicable security controls**
  - Checklist for progress tracking
  - Share with appropriate IT team
  - Forms record for controls trail
- **Step 4: Document controls into SOP**
  - Enter controls set into draft SOP
  - Who will do what when, (and briefly how)
  - Get Dept Head agreement and sign-off on checklist and SOP

Topic no 61: 8 Step Methodology – Security Hardening (3)

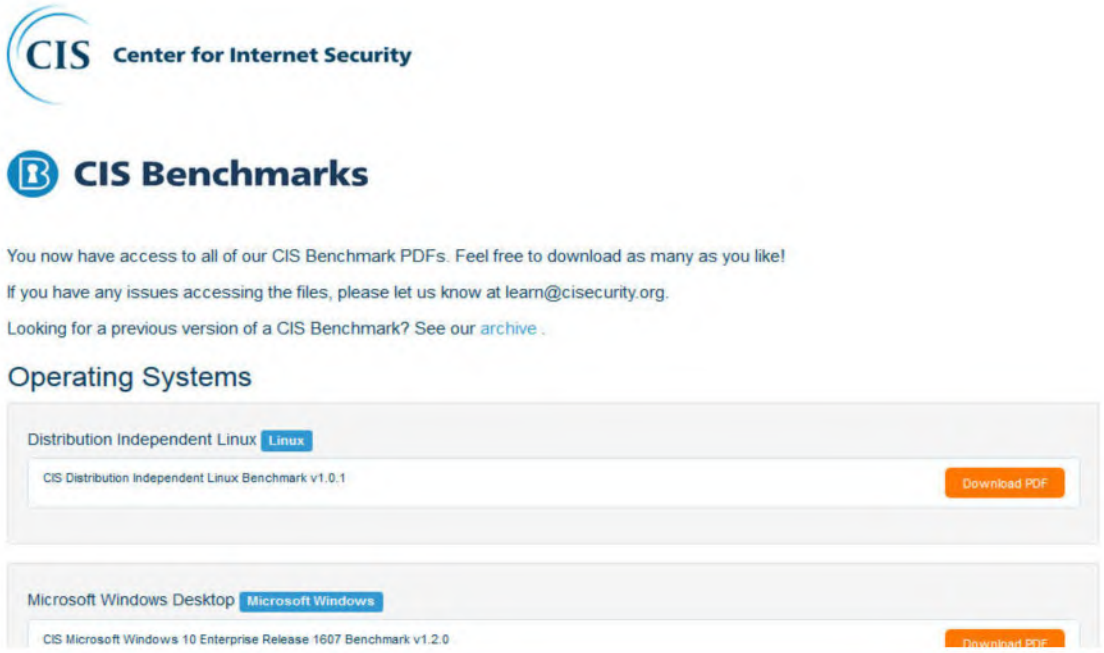
- **Step 5: Implement controls on test setup**
  - Relevant IT team to implement controls on test setup
  - Update checklist
  - Update SOP (if necessary)

- Send checklist back to InfoSec team

- **Step 6: Validation of control implementation (by InfoSec team)**
  - InfoSec resource with relevant domain knowledge
  - Conduct preparation before actual validation (study controls)
  - Update checklist with status column
- **Step 7: Change management process for PRODUCTION:**
  - ISMC receives validation status from InfoSec team
  - Relevant dept head takes up change management process and prepares for shifting to PROD
  - Rollback, impact etc
- **Step 8: Implement on PROD & monitor:**
  - Monitor closely for 24-48 hours after moving to PROD
  - Rollback in case of unforeseen circumstances
  - IT team SOP finalized and now ops task

Topic no 62-65: A Look At CIS Security Benchmarks (1)

- Center for Internet Security (CIS)
  - https://www.cisecurity.org/cis-benchmarks/
  - Fill out your details and will receive an email with link



#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

#	OPERATING SYSTEMS	TOTAL
1	DISTRIBUTION INDEPENDENT LINUX	1
2	MICROSOFT WINDOWS DESKTOP	5
3	DEBIAN LINUX	2
4	UBUNTU LINUX	3
5	AMAZON LINUX	1
6	CENTOS LINUX	2
7	ORACLE LINUX	2

#	OPERATING SYSTEMS (CONTD)...	TOTAL
8	REDHAT LINUX	3
9	SUSE LINUX	2
10	APPLE OS (UNIX)	5
11	IBM AIX (UNIX)	1
12	ORACLE SOLARIS (UNIX)	3
13	MS WINDOWS SERVER	6
	TOTAL BENCH MARKS OPERATING SYSTEMS	**36**

#	CLOUD PROVIDERS	TOTAL
1	AMAZON WEB SERVICES	2
	TOTAL CLOUD PROVIDERS	**2**

#	SERVER SOFTWARE	TOTAL
1	MICROSOFT IIS (WEB SERVER)	3
2	VMWARE (VIRTUALIZATION)	2
3	MONGODB (DATABASE SERVER)	3
4	IBM DB2 (DATABASE SERVER)	3
5	BIND (DNS SERVER)	1
6	APACHE TOMCAT (WEB SERVER)	2
7	MICROSOFT SQL SERVER (DB SERVER)	3
8	APACHE (HTTP SERVER)	2
9	DOCKER (VIRTUALIZATION)	5
10	ORACLE (DATABASE SERVER)	3
11	KUBERNETES (VIRTUALIZATION)	1
12	MIT KERBEROS (AUTHENTICATION)	1
13	ORACLE MySQL (DB SERVER)	4
	TOTAL BENCH MARKS SERVER SOFTWARE	**33**

- Mobile devices, network devices, desktop software, multifunction print devices

#	MOBILE DEVICES	TOTAL
1	APPLE IOS	5
2	GOOGLE ANDROID	3
	TOTAL BENCH MARKS MOBILE DEVICES	**8**

#	NETWORK DEVICES	TOTAL
1	CISCO	4
2	PALO ALTO NETWORKS	2
	TOTAL BENCH MARKS NETWORK DEVICES	**6**

#	DESKTOP SOFTWARE	TOTAL
1	MICROSOFT OFFICE	13
2	GOOGLE CHROME (WEB BROWSER)	1
3	MS EXCHANGE SERVER	3
4	MS INTERNET EXPLORER	2
5	MOZILLA FIREFOX	2
	TOTAL BENCH MARKS DESKTOP SOFTWARE	**21**

#	MULTIFUNCTION PRINT DEVICES	TOTAL
1	MULTIFUNCTION DEVICE	1
	TOTAL BENCH MARKS MULTIFUNCTION PRINT DEVICES	**1**

- CIS Benchmarks example (Network Devices)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

- June 29, 2016
- 174 pages PDF doc

- **Control content:**
  - Profile applicability (ASA 8.X, ASA 9.X)
  - Description
  - Rationale
  - Audit
  - Remediation
  - Default value
  - References
- **1.8 (page 88); Session Timeout**
  - Profile applicability: Level 1, Cisco ASA9.X
  - Description: Sets the idle timeout for a console session before the security appliance terminates it.
  - Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

- CIS Benchmarks example (Operating Systems)
  - MS Windows Server 2012-R2

- January 31, 2017
- 760 pages PDF doc
- Profile applicability:
  - Level 1 domain controller
  - Level 1 member server
  - Level 2 domain controller
  - Level 2 member server
- **Level 1:** Items in this profile intend to:
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means
- **Level 2:** extends the Level 1 - profile
  - intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology
- **Control content:**
  - Profile applicability (ASA 8.X, ASA 9.X)
  - Description
  - Rationale
  - Audit

- Remediation
- Impact
- Default value
- References

- **1.1.2 [L1]:** *Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)*
  - *Profile applicability: Level 1 Domain Controller, Level 1 Member Server*
- **1.1.2 [L1] Description:**
  - This policy setting defines how long a user can use their password before it expires.
  - Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.
- **1.1.2 [L1] Audit:**
  - Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

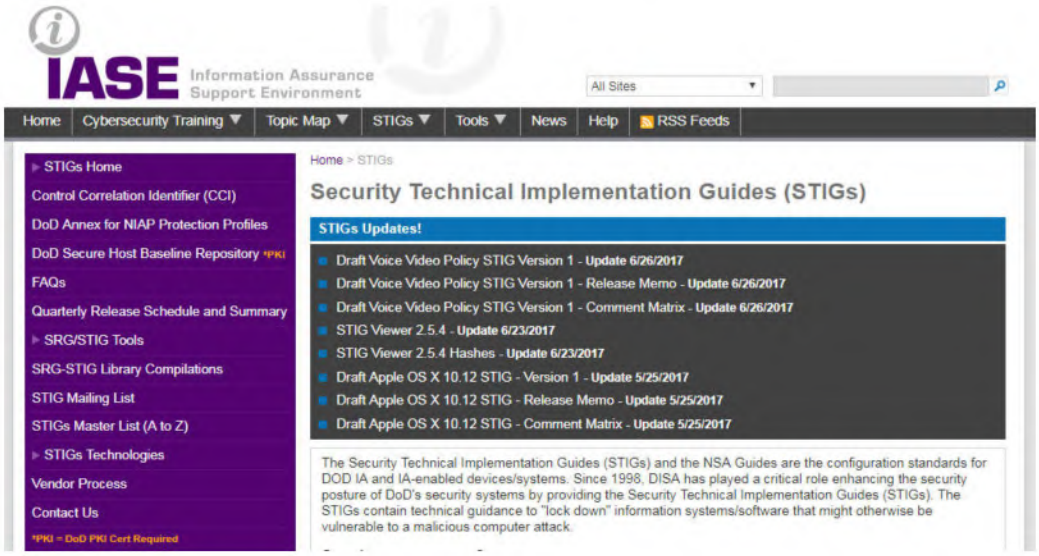
- 1.1.2 [L1] Default Value: 42 days
- 1.1.2 [L1] Reference: CCE-37167-4
  - Common Configuration Enumeration (Unique identifiers for common system config issues)

Topic no 66: A Look At DISA STIGs (1)

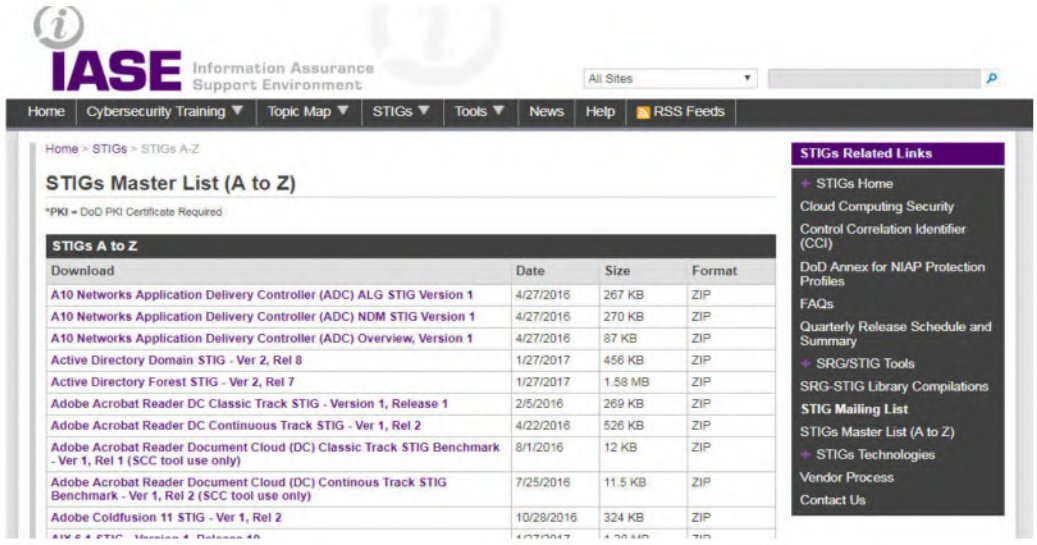
- USA DoD
- Security Technical Implementation Guides (STIGs)
- Most expansive security benchmarks available
- Most regularly updated
- Unclassified version

- http://iase.disa.mil/stigs/Pages/index.aspx
- 425 STIGs available
- STIGs master list (A-Z):
  - http://iase.disa.mil/stigs/Pages/a-z.aspx
- STIG viewer:
  - http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

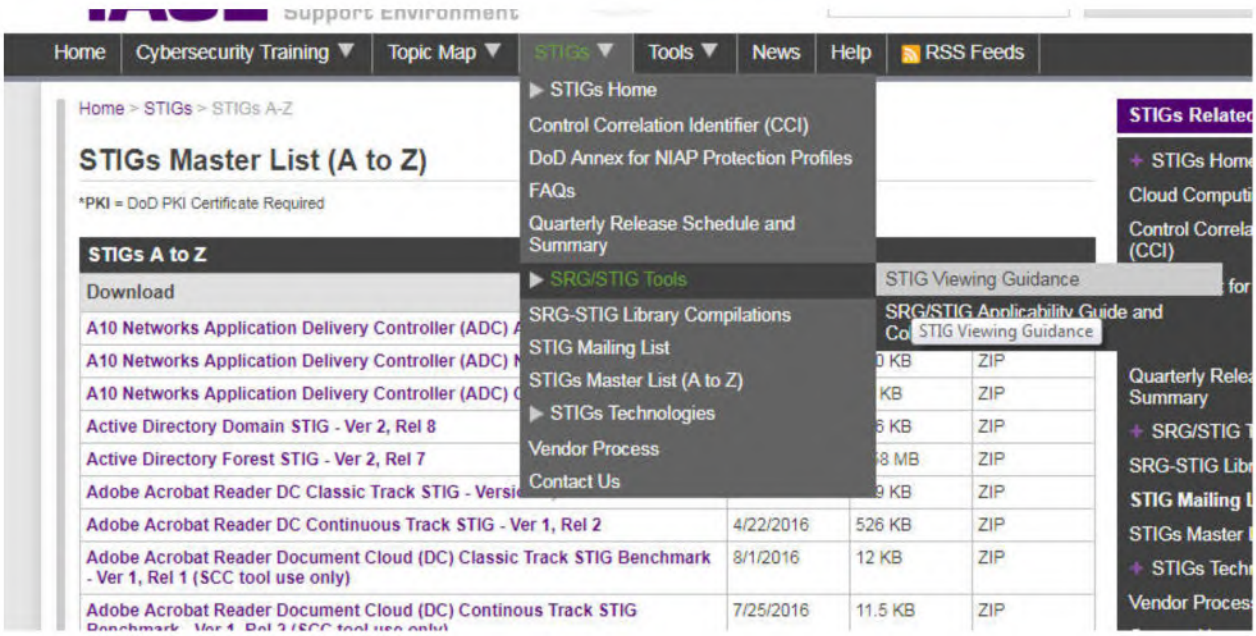
STIGs HOME



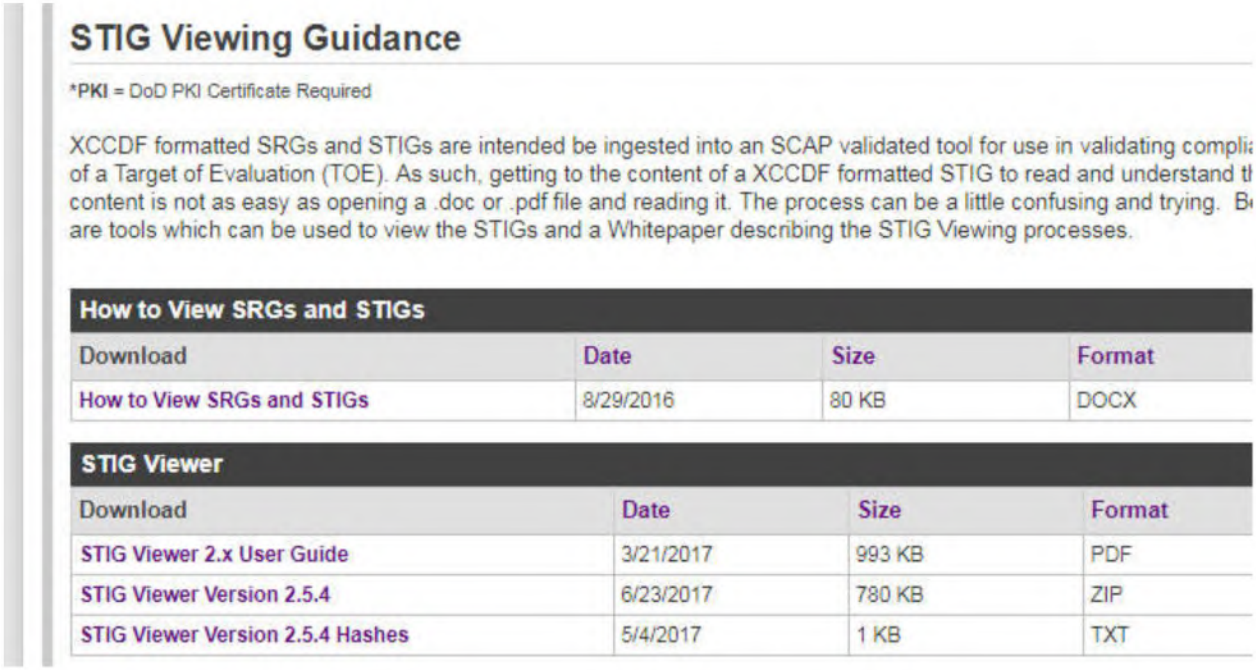
STIGs Master List



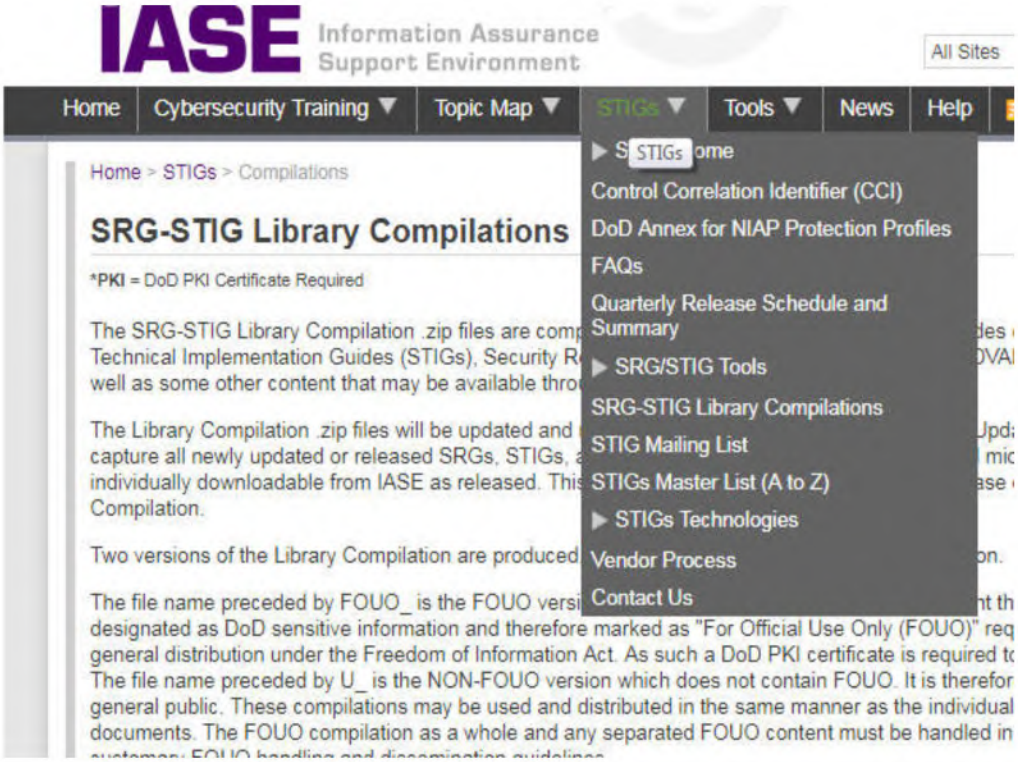
STIGs Viewer



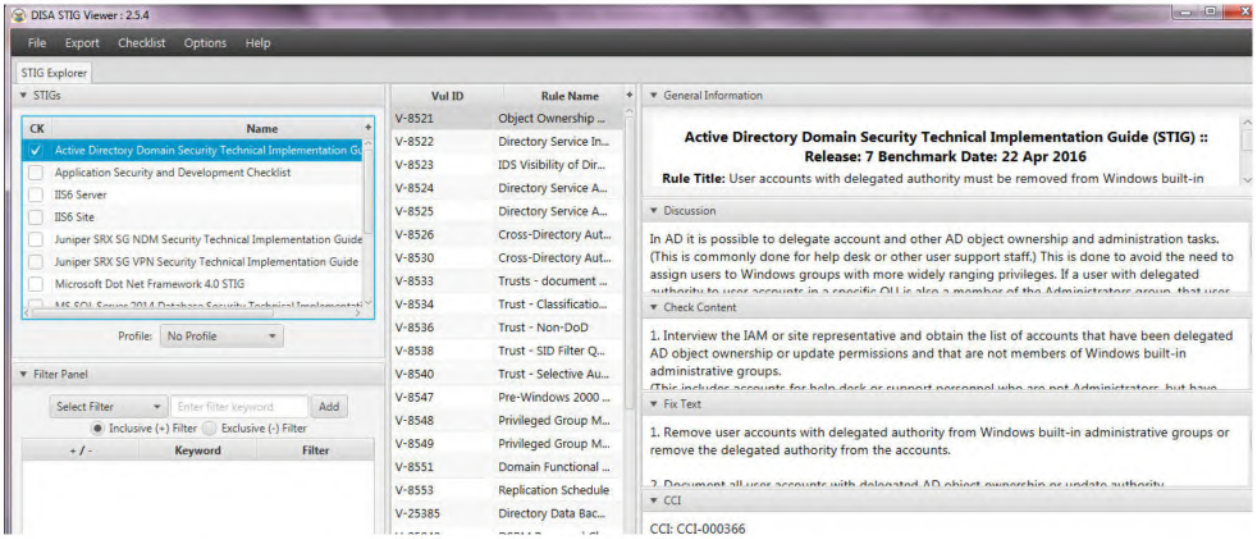
STIG Viewer Download



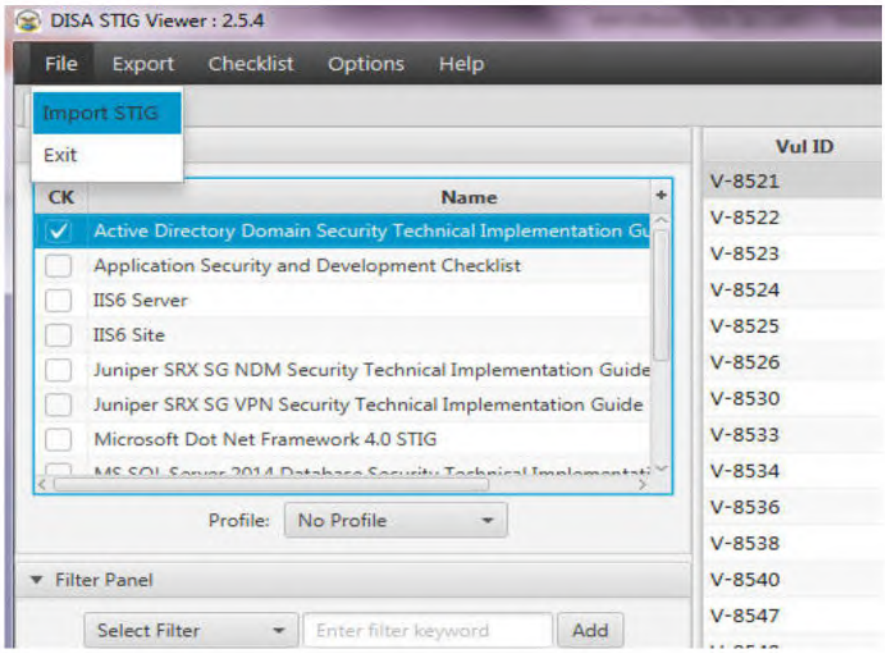
STIG Library Compilation



STIG Viewer Window



Import STIG

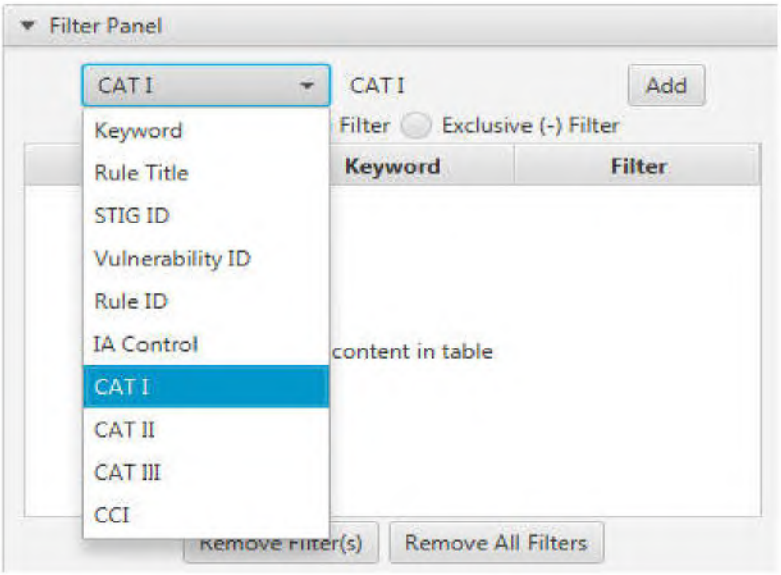


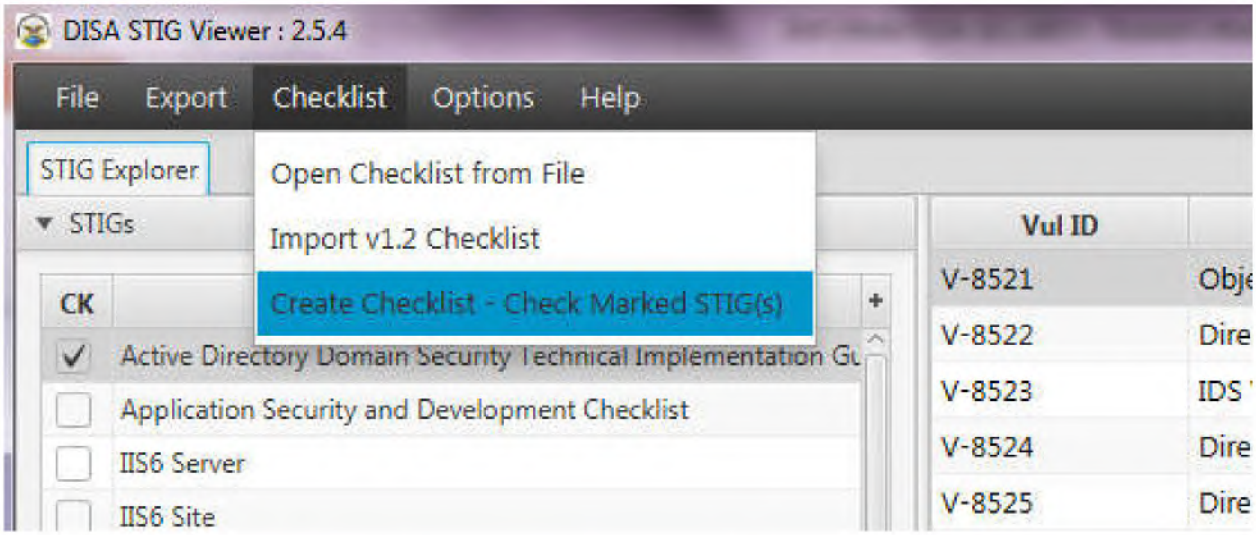
- Completely different mechanism for DISA STIGs

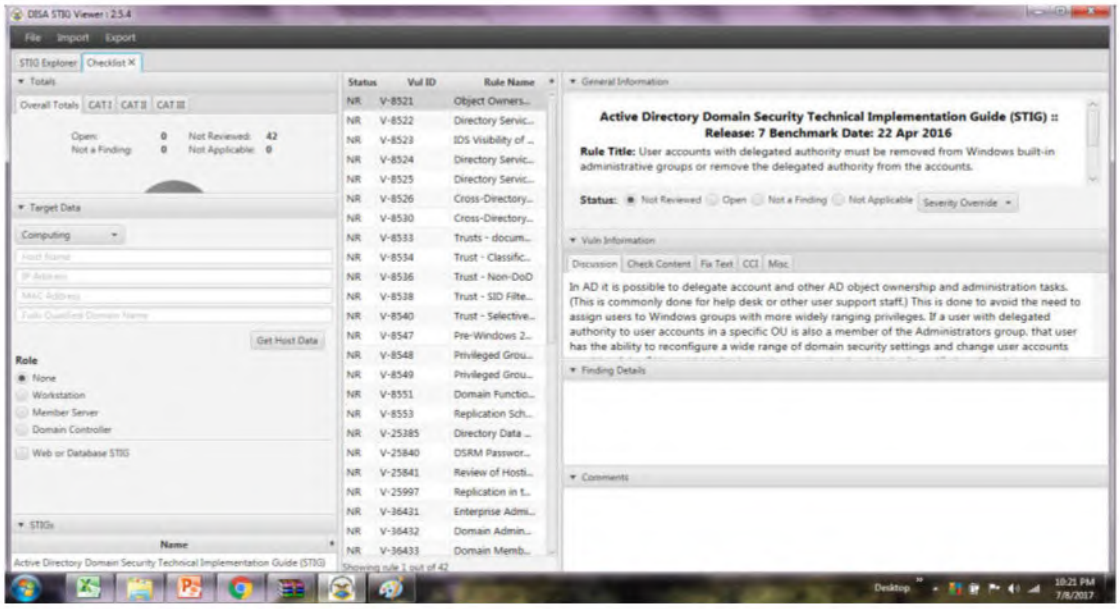
Topic no 67: A Look At DISA STIGs (2)

- **STIG content:**
  - General information (title)
  - Discussion
  - Check content
  - Fix text
  - CCI (References)

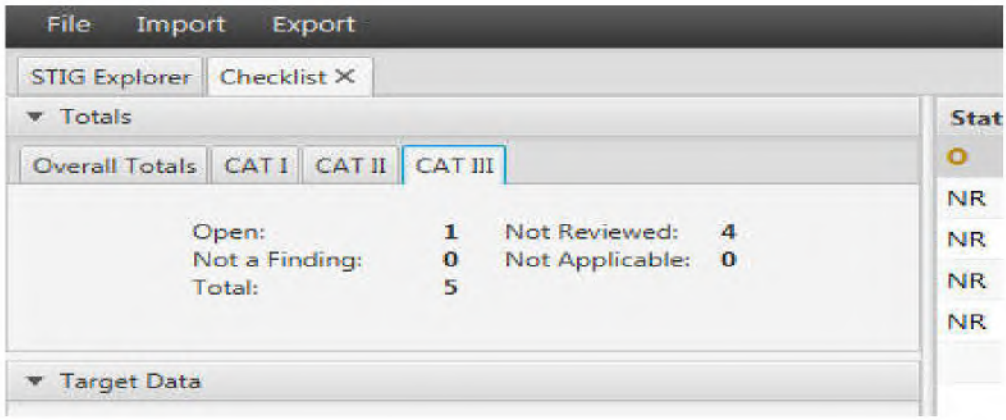
SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

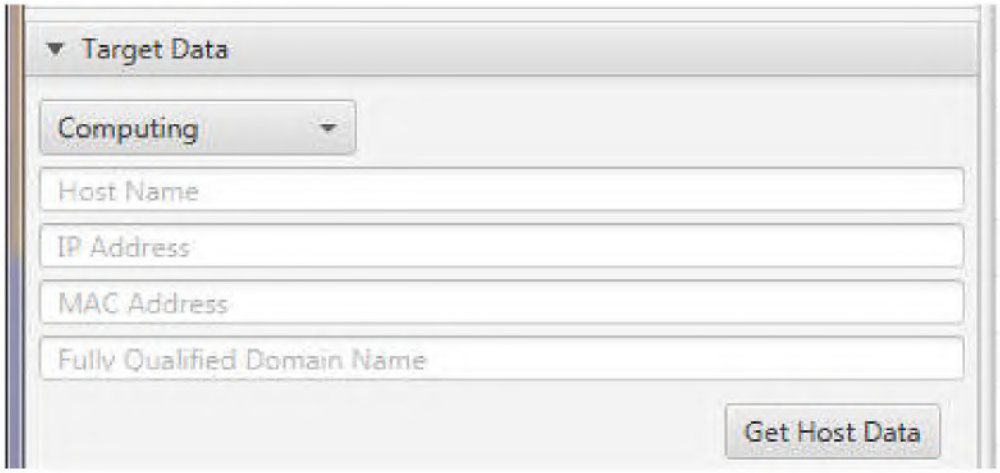

Filter Panel
CAT I
CAT I
Add
Keyword
Rule Title
STIG ID
Vulnerability ID
Rule ID
IA Control
CAT I
CAT II
CAT III
CCI
Filter
Exclusive (-) Filter
Keyword
Filter
content in table
Remove Filter(s)
Remove All Filters

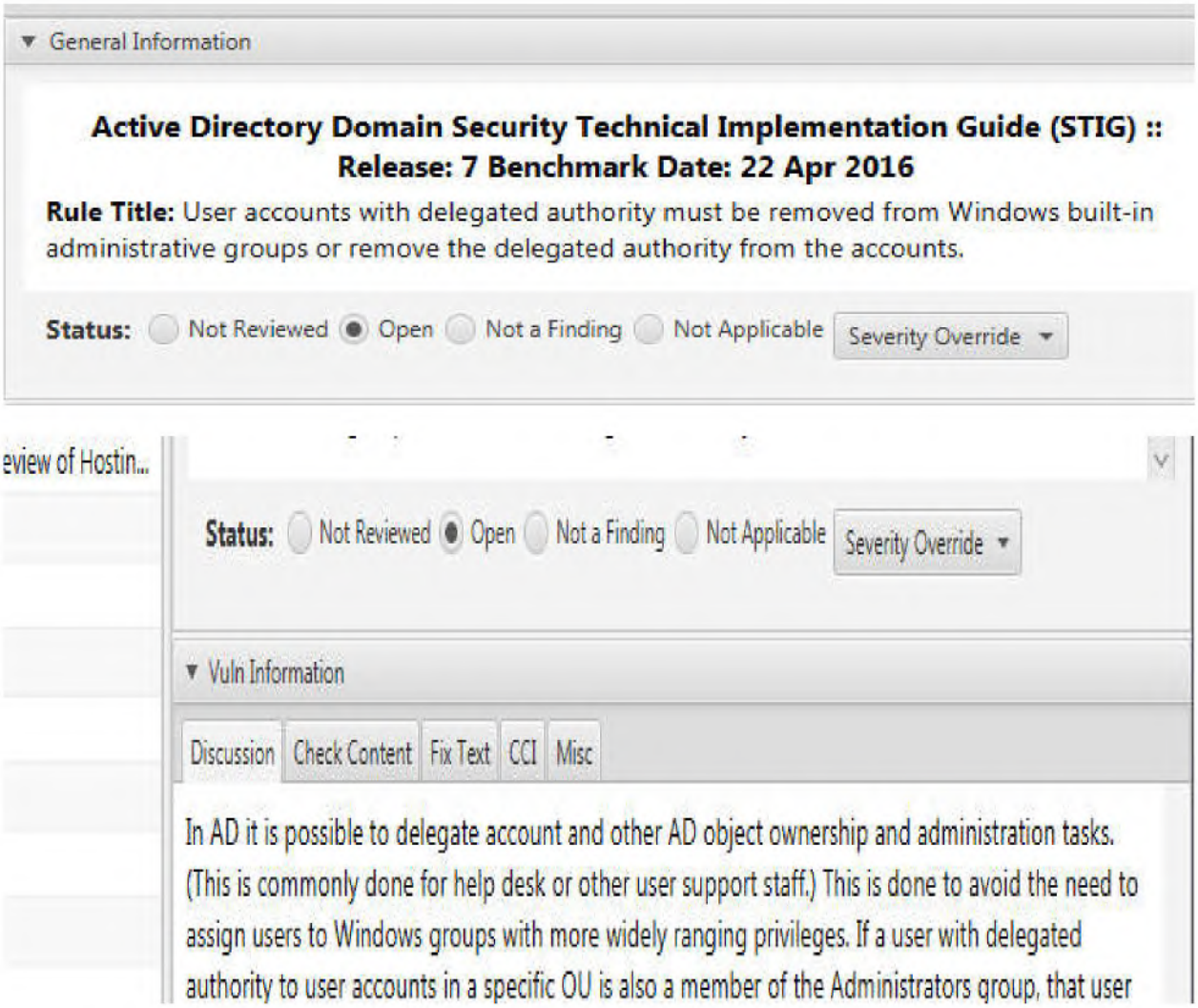

DISA STIG Viewer : 2.5.4
File
Export
Checklist
Options
Help
STIG Explorer
Open Checklist from File
Import v1.2 Checklist
Create Checklist - Check Marked STIG(s)
STIGs
CK
Active Directory Domain Security Technical Implementation Gu
Application Security and Development Checklist
IIS6 Server
IIS6 Site
Vul ID
V-8521
V-8522
V-8523
V-8524
V-8525


Active Directory Domain Security Technical Implementation Guide (STIG) ::
Release: 7 Benchmark Date: 22 Apr 2016

- **Checklist screens:**
  - Overall totals
  - Target data
  - Role
  - Finding details
  - Comments
- **Checklist screens (STATUS):**
  - Not reviewed
  - Open
  - Not a finding
  - Not applicable

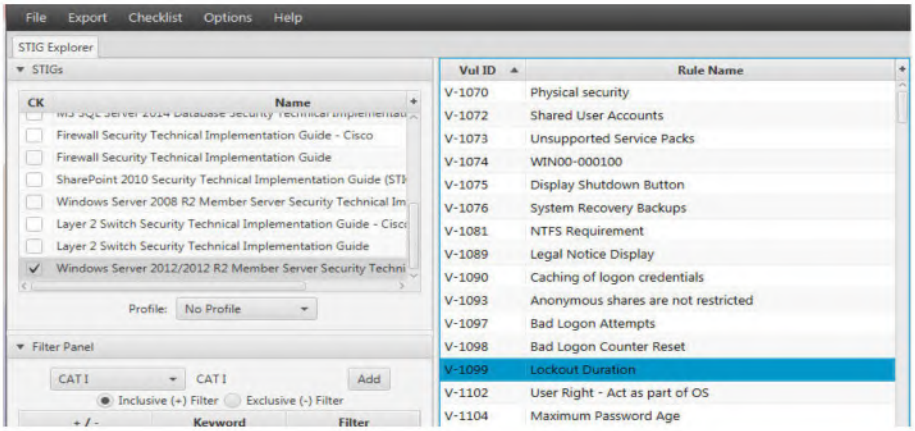


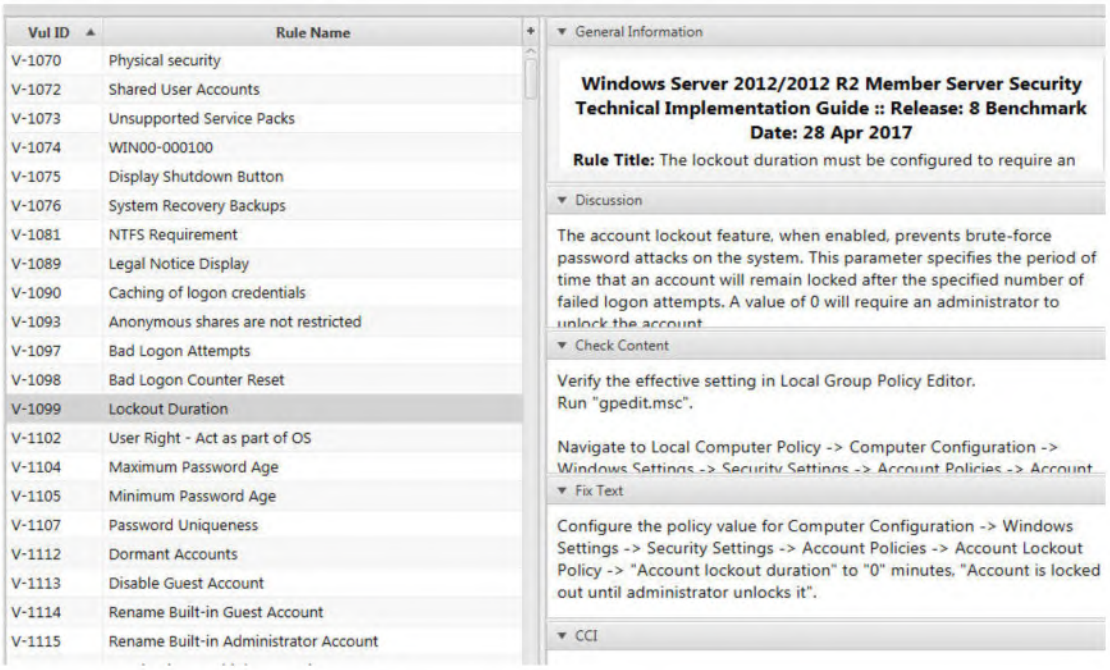




Topic no 68: A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
  - Import STIG
  - V1099 (Lockout duration)

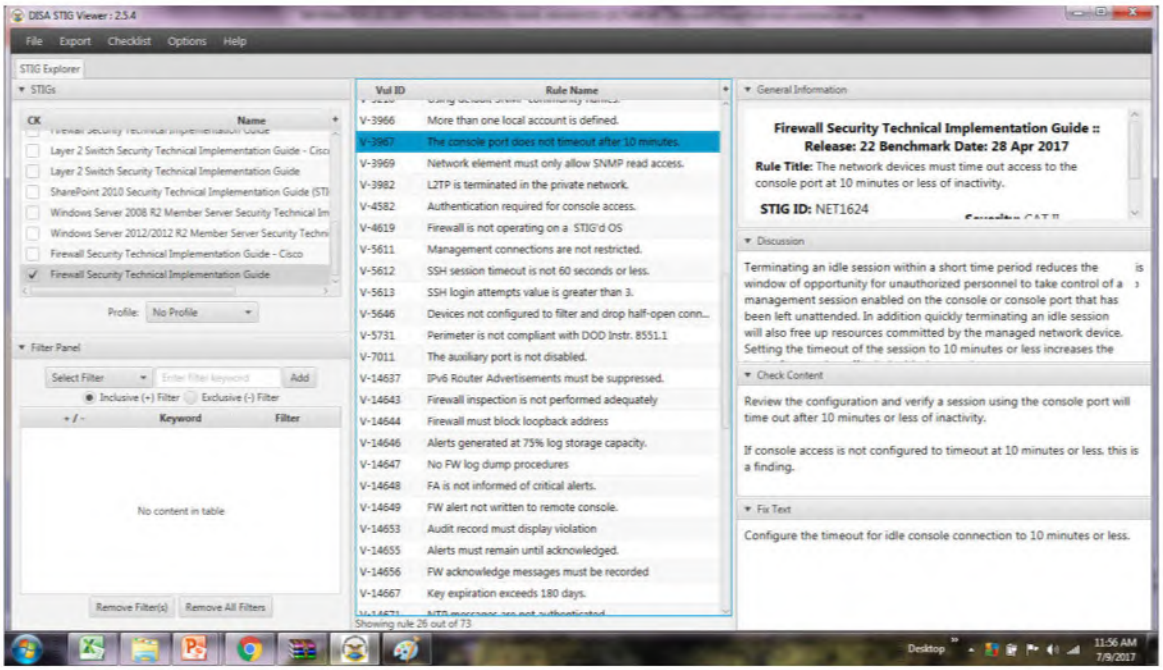




- **Rule Title:**
  - The lockout duration must be configured to require an administrator to unlock an account
  - Severity: CAT II
- **Discussion:**
  - The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.
- **Check Content:**
  - Verify the effective setting in Local Group Policy Editor. Run "gpedit.msc".
  - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy.
  - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock the account, this is a finding.
- **Fix Text:**
  - Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes
  - "Account is locked out until administrator unlocks it".
  - CCI: NIST SP 800-53 Revision 4 :: AC-7 b

Topic no 69: A Look At DISA STIGs (4)

- Firewall Security Technical Implementation Guide
- Vulnerability ID: V-3967
- Rule name: The console port does not timeout after 10 mins



- **General Information:**
  - **Rule Title:** The network devices must time out access to the console port at 10 minutes or less of inactivity
  - **STIG ID**: NET1624
  - **Severity**: CAT II
- **Discussion:**
  - Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes or less increases the level of protection afforded critical network components
- **Check Content:**
  - Review the configuration and verify a session using the console port will time out after 10 mins or less of inactivity.

- If console access is not configured to timeout at 10 minutes or less, this is a finding.

- **Fix Text:**
  - Configure the timeout for idle console connection to 10 minutes or less.

Topic no 70: Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

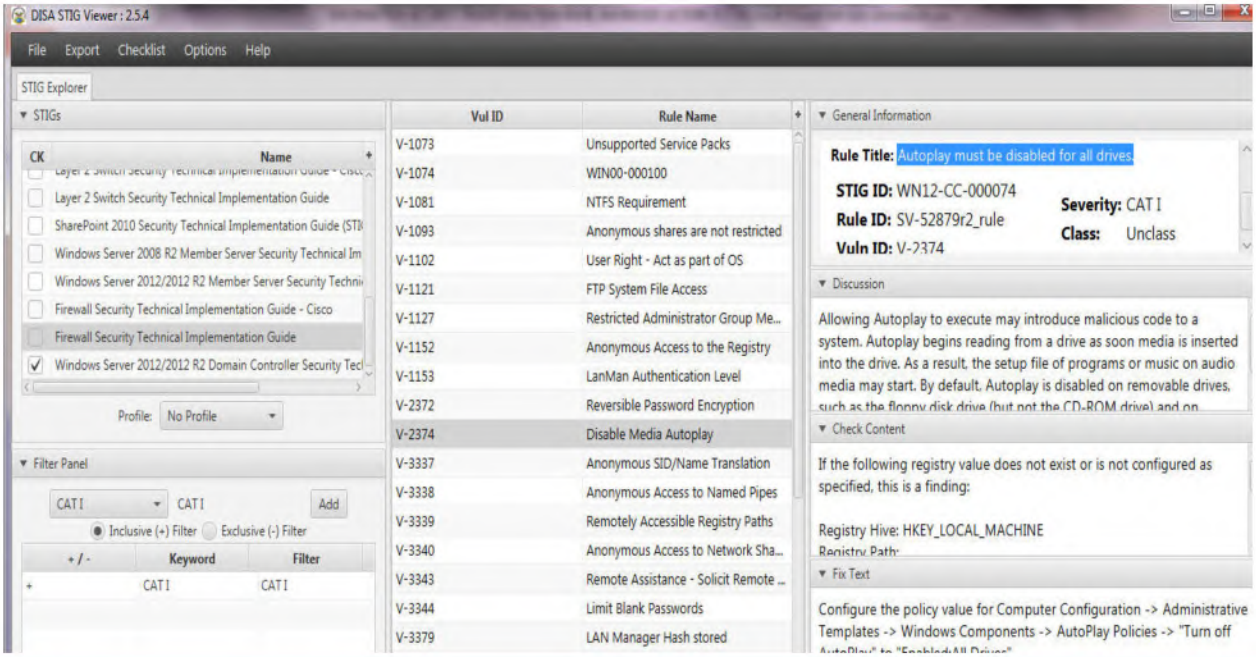
FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

FEATURE	CIS	DISA
CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
FREQUENCY OF UPDATES	FAIR	QUARTERLY
INDUSTRY CREDIBILITY	HIGH	VERY HIGH
INDUSTRY ADOPTION	HIGH	MODERATE

- **How to select CIS/DISA:**
  - Size of organization
  - IT infrastructure extent
  - Nature of business
  - Security program goals
  - Maturity of IT & security staff
- **Rule of thumb:**
  - Smaller orgs use CIS
  - Larger orgs use DISA
  - CIS is part of Homeland Security, DISA is part of US Military
  - DISA more frequently updated and maintained with wider coverage

Topic no 71: Security Hardening – Windows Server 2012R2

- Windows Server 2012 – R2
- DISA, Release 8
  - 28 April 2017
- Domain Controller



- General Information:
  - **Rule Title:** Autoplay must be disabled for all drives
  - **STIG ID**: WN12-CC-000074
  - **Severity**: CAT I
- **Discussion:**

  Allowing Autoplay to execute may introduce malicious code to a system.
  - Autoplay begins reading from a drive as soon media is inserted into the drive. As a result, the setup file of programs or music on audio media may start.
  - By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive) and on network drives.
  - Enabling this policy disables Autoplay on all drives
- **Check Content:**
  - If the following registry value does not exist or is not configured as specified, this is a finding:
  - Registry Hive: HKEY_LOCAL_MACHINE
  - Registry Path: \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\
  - Value Name: NoDriveTypeAutoRun
  - Type: REG_DWORD Value: 0x000000ff (255)
- **Fix Text:**
  - Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies -> "Turn off AutoPlay" to "Enabled: All Drives".
- **CCI (Control Correlation Identifier):**
    - CCI: CCI-001764 The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions and/or rules authorizing the terms and conditions of software program usage. NIST SP 800-53 Revision 4:: CM-7 (2)

Topic no 72: Case Study Security Hardening – Linux

- CIS Benchmarks case study (Red Hat Enterprise Linux 7)

- January 31, 2017
- 347 pages PDF doc
- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
- Profile applicability:
  - Level 1, Server
  - Level 1, Workstation
- 5.2.2 (page 258); *Ensure SSH Protocol is set to 2 (Scored)*
  - Description: SSH supports 2 different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol & was subject to security issues. SSH2 is more advanced and secure.
  - Rationale: SSH v1 suffers from insecurities that do not affect SSH v2.
  - Audit: Run the following command and verify that output matches:

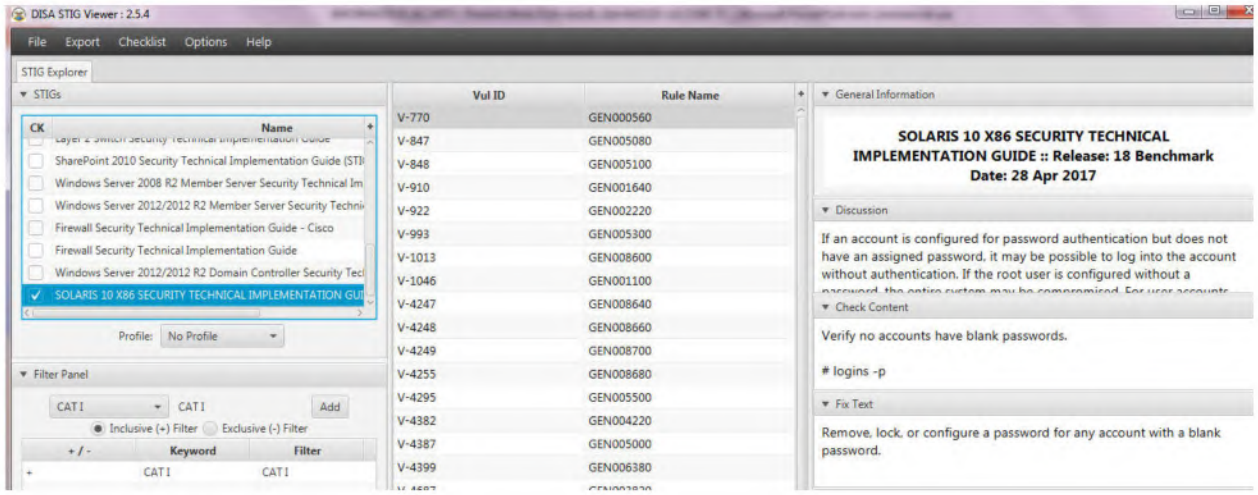
    # grep "^Protocol" /etc/ssh/sshd_config Protocol 2
  - Remediation: Edit the /etc/ssh/sshd_config file to set the parameter as follows:

    Protocol 2
  - **Critical Controls:** 3.4 Use Only Secure Channels For Remote System Administration
  - Critical Controls: 3.4 Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels.

- Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Topic no 73: Security Hardening – Case Study – Solaris

- Solaris 10 X86
- DISA, Release 18
  - 28 April 2017



- **General Information:**
  - **Rule Title:** All shell files must have mode 0755 or less permissive
  - **STIG ID**: GEN002220
  - **Severity**: CAT I
- **Discussion:**
  - Shells with world/group-write permissions give the ability to maliciously modify the shell to obtain unauthorized access.
- **Check Content:**
  - If /etc/shells exists, check the group ownership of each shell referenced. **# cat /etc/shells | xargs -n1 ls -lL**
  - Otherwise, check any shells found on the system.

    # find / -name "*sh" | xargs -n1 ls -lL
  - If a shell has a mode more permissive than 0755, this is a finding
  -

- **Fix Text:**
  - Change the mode of the shell
  - **#chmod 0755 <shell>**
- **CCI (Control Correlation Identifier):**
  - CCI-000225
    The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
  - NIST SP 800-53 :: AC-6
  - NIST SP 800-53A :: AC-6.1
  - NIST SP 800-53 Revision 4 :: AC-6

Topic no 74: Case Study Security Hardening – Apache

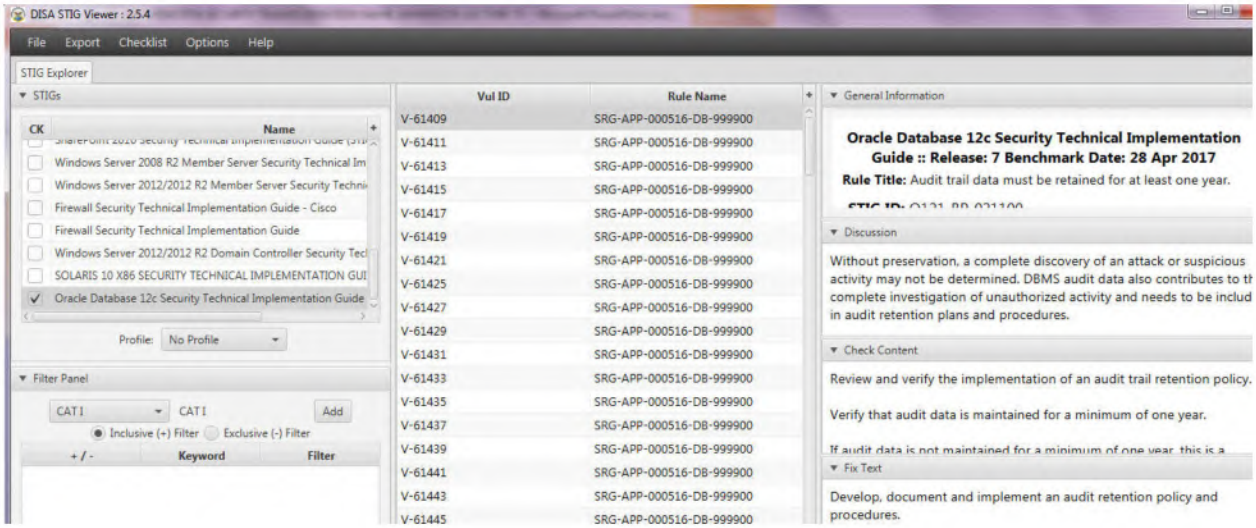
- CIS Benchmarks case study (Apache Tomcat 7)

- April 26, 2016
- 94 pages PDF doc
- **7.7 (page 65);** ***Configure log file size limit (Scored)***
- **Profile applicability:**
  - Level 2
  - **Description:** By default, the logging. Properties file will have no defined limit for the log file size. This is a potential denial of service attack as it would be possible to fill a drive or partition containing the log files.
  - Rationale: Establishing a maximum log size that is smaller than the partition size will help mitigate the risk of an attacker maliciously exhausting disk space
  - **Audit:** Validate the max file limit is not greater than the size of the partition where the log files are stored.

- **Remediation:** Create the following entry in your logging.properties file. This field is specified in bytes:
  java.util.logging.FileHandler.limit=10000
- Default Value: No limit by default

Topic no 75: Security Hardening – Case Study – Oracle

- Oracle Database 12c
- DISA, Release 18
  - 28 April 2017



- **General Information:**
  - **Rule Title:** The Oracle Listener must be configured to require administration authentication
  - **STIG ID**: O121-BP-022700
  - **Severity**: CAT I
- **Discussion:**
  - Oracle listener authentication helps prevent unauthorized administration of the Oracle listener. Unauthorized administration of the listener could lead to DoS exploits; loss of connection audit data, unauthorized reconfiguration or other unauthorized access.
  - This is a Category I finding because privileged access to the listener is not restricted to authorized users.
  - Unauthorized access can result in stopping of the listener (DoS) and overwriting of listener audit logs.

- **Check Content:**
  - If a listener is not running on the local database host server, this check is not a finding
  - For Windows hosts, view all Windows services with TNSListener embedded in the service name
  - The service name format is: **Oracle[ORACLE_HOME_NAME]TNSListener**
  - View the STIGVIEWER for Unix hosts
- **Fix Text:**
  - By default, Oracle Net Listener permits only local administration for security reasons. As a policy, the listener can be administered only by the user who started it. This is enforced through local operating system authentication.
  - **For example**, if user1 starts the listener, then only user1 can administer it. Any other user trying to administer the listener gets an error. The super user is the only exception.
  - Remote administ. of the listener must not be permitted. If listener administ. from a remote system is required, granting secure remote access to the Oracle DBMS server and performing local administration is preferred.

- **CCI (Control Correlation Identifier):**
  - CCI: CCI-000366
    The organization implements the security configuration settings.
  - NIST SP 800-53 :: CM-6 b
  - NIST SP 800-53A :: CM-6.1 (iv)
  - NIST SP 800-53 Revision 4 :: CM-6 b

Topic no 76: Case Study Security Hardening – MS SQL

- CIS Benchmarks case study (MS SQL Server 2012)

- September 30, 2016
- 73 pages PDF doc
- *2.14 Ensure 'sa' Login Account has been renamed (Scored)*

- **Profile applicability:**
  - Level 1 database engine
  - **Description:** The sa account is a widely known and often widely used SQL Server account with sysadmin privileges.
  - **Rationale:** It is more difficult to launch password-guessing and brute-force attacks against the sa account if the username is not known.
  - **Audit:** Use the following syntax to determine if the sa account is renamed:

    SELECT name FROM sys.server_principals WHERE sid = 0x01;

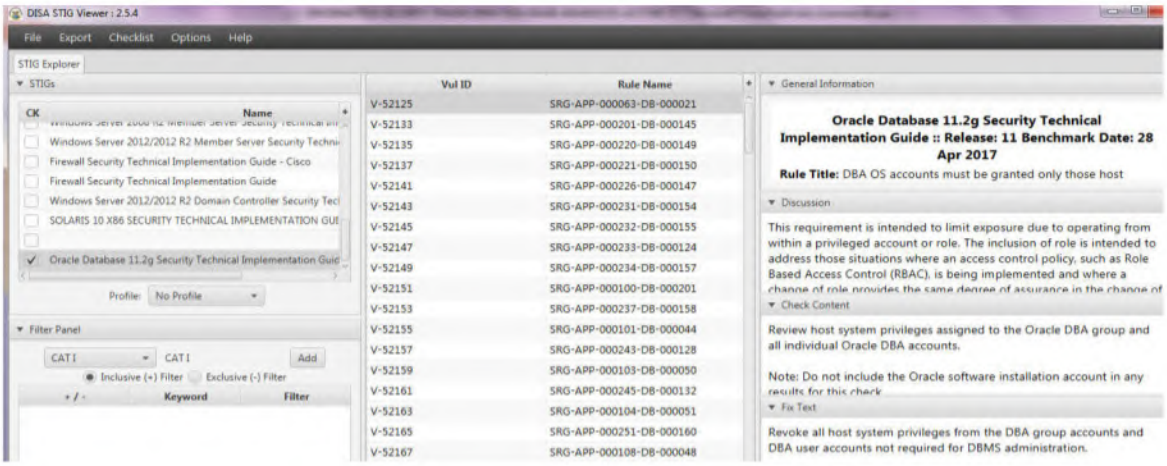
    A name of sa indicates the account has not been renamed
  - **Remediation:** Replace the different_user value within the below syntax and execute rename the sa login:

    ALTER LOGIN sa WITH NAME = <different_user>;

  - **Impact:** It is not a good security practice to code applications or scripts to use the sa account However, if this has been done renaming the sa account will prevent scripts and applications for authenticating to the database server and executing required tasks or functions.
  - **Default Value:** By default, the 'sa‘ account name is 'sa'

Topic no 77: Security Hardening – Case Study – Oracle

- Oracle database 11.2g
- DISA, Release 11
  - 28 April 2017



- **General Information:**
  - **Rule Title:** The Oracle REMOTE_OS_ROLES parameter must be set to FALSE.
  - **STIG ID**: O112-BP-022000
  - **Severity**: CAT I
- **Discussion:**
  - Setting REMOTE_OS_ROLES to TRUE allows operating system groups to control Oracle roles. The default value of FALSE causes roles to be identified and managed by the database.
  - If REMOTE_OS_ROLES is set to TRUE, a remote user could impersonate another operating system user over a network connection.
- **Check Content:**
  - From SQL*Plus: select value from v$parameter where **name = 'remote_os_roles';**
  - If the returned value is not FALSE or not documented in the System Security Plan as required, this is a Finding
- **Fix Text:**
  - Document remote OS roles in the System Security Plan.
  - If not required, disable use of remote OS roles.
  - From SQL*Plus: **alter system set remote_os_roles = FALSE scope = spfile;**
  - The above SQL*Plus command will set the parameter to take effect at next system startup
- **CCI (Control Correlation Identifier):**
  - CCI: CCI-000366 The org implements the security configuration settings.
  - NIST SP 800-53 :: CM-6 b
  - NIST SP 800-53A :: CM-6.1 (iv)
  - NIST SP 800-53 Revision 4 :: CM-6 b

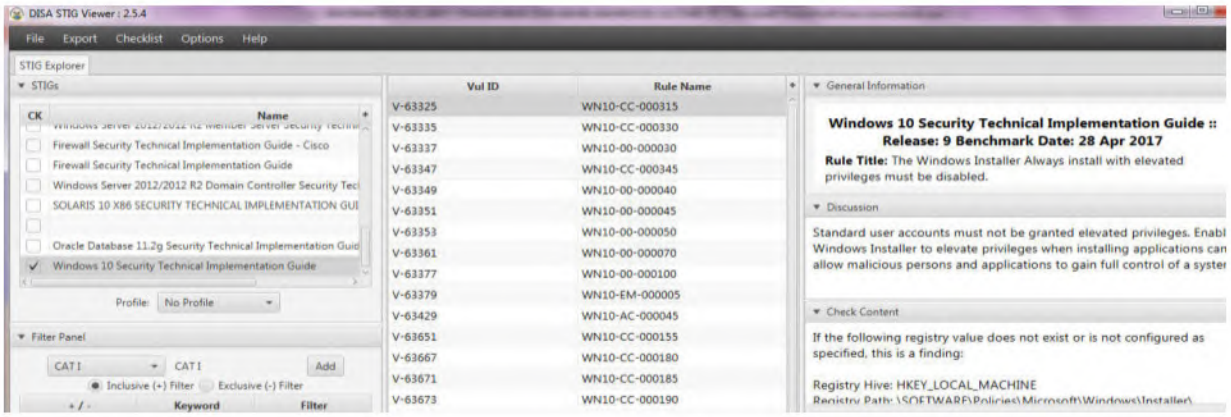
Topic no 78: Case Study Security Hardening – Windows 8

- CIS Benchmarks case study (Windows 8.1)

- January 31, 2017
- 891 pages PDF doc
- *18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)*
- Profile applicability:
  - Level 1
  - Level 1 + BitLocker
- *18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)*
- Description: This policy setting controls whether memory dumps in support of OS-generated error reports can be sent to Microsoft automatically. This policy does not apply to error reports generated by 3rd-party products, or additional data other than memory dumps.
- The recommended state for this setting is: Disabled.
- Rationale: Memory dumps may contain sensitive information and should not be automatically sent to anyone.
- Audit: Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:
  - **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsError Reporting:AutoApproveOSDumps**

Topic no 79: Case Study Security Hardening – Win 10

- Windows 10
- DISA, Release 9
  - 28 April 2017



- **General Information:**
  - **Rule Title:** The antivirus program must be configured to update signature files on a daily basis.
  - **STIG ID**: WN10-00-000046
  - **Severity**: CAT I
- **Discussion:**

  Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Using a virus scan program provides the ability to detect malicious code before extensive damage occurs. Updated virus scan data files help protect a system, as constantly changing malware is identified by the antivirus software vendors
- **Check Content:**
  - This requirement is NA if McAfee VirusScan Enterprise (VSE) is used. It will be addressed with the corresponding McAfee VSE STIG.
  - Configurations will vary depending on the product.
- **Fix Text:**

- Configure the antivirus program to update signature files at least daily. Ensure the updates are occurring on timely basis and are not more than a week old.
- CCI (Control Correlation Identifier):

CCI: 000366 The org implements the security config settings.

NIST SP 800-53 :: CM-6 b

NIST SP 800-53A :: CM-6.1 (iv)

NIST SP 800-53 Revision 4 :: CM-6

Topic no 80: Case Study Security Hardening – MS Exchange

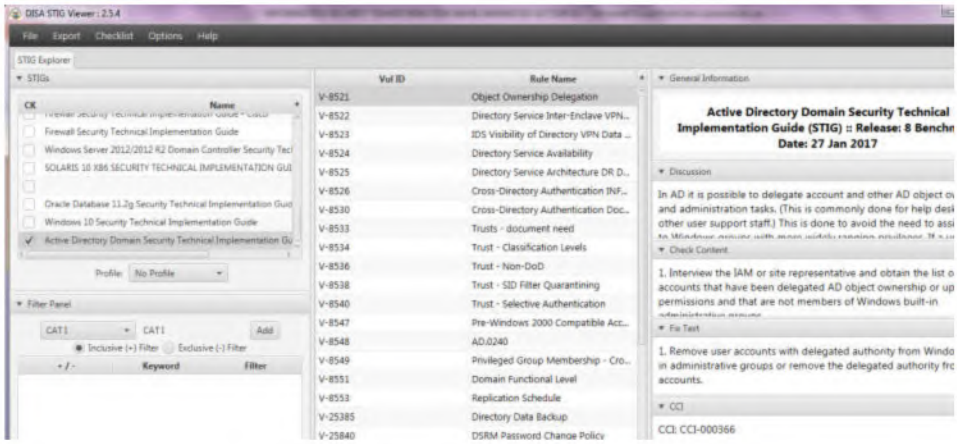
- CIS Benchmarks case study (MS Exchange Server 2016)

- November 16, 2015
- 66 pages PDF doc
- *2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)*
- Profile applicability:
  - **Level 1** - Mailbox Services Security
  - **Description:** This setting allows you to ensure that items are not permanently deleted until the database has been backed up.
  - **Rationale:** To ensure that accidentally deleted items can be recovered, they should not be permanently deleted until the database is backed up.
  - **Audit:** Execute the following cmdlet and ensure **RetainDeletedItemsUntilBackup** is set to 'True': **Get-MailboxDatabase <Mailbox Database Name> | fl -property RetainDeletedItemsUntilBackup**
  - **Remediation:** To implement the recommended state, execute the following PowerShell cmdlet: **Set-MailboxDatabase <Mailbox Database Name> -RetainDeletedItemsUntilBackup $true**
  - **Impact:** The impact of enabling this setting should be minimal. More storage space will be required until any pending items are permanently deleted.
  - **Default Value:** False

Topic No 81: Security Hardening – Case Study – AD

- Active Directory Domain
- DISA, Release 8
  - 27 January, 2017

STIGVIEWER WINDOW



- **General Information:**
  - **Rule Title :** Membership to the Domain Admins group must be restricted to accounts used only to manage the Active Dir domain and domain controllers
  - **STIG ID**: AD.0002
  - **Severity**: CAT I
- **Discussion:**
  - The Domain Admins group is a highly privileged group. Personnel who are system administrators must log on to Active Directory systems only using accounts with the level of authority necessary.
  - Only system administrator accounts used exclusively to manage an Active Directory domain and domain controllers may be members of the Domain Admins group. A separation of administrator responsibilities helps mitigate the risk of privilege escalation resulting from credential theft attacks.
- **Check Content:**
  - Review the Domain Admins group in Active Directory Users and Computers. Each Domain Administrator must have a separate unique account specifically for managing the Active Directory domain and domain controllers.
  - If any account listed in the Domain Admins group is a member of other administrator groups including the Enterprise Admins group, domain member server administrators groups, or domain workstation administrators groups, this is a finding.
- **Fix Text:**

- Create the necessary documentation that identifies the members of the Domain Admins group. Ensure that each member has a separate unique account that can only be used to manage the Active Directory

- **CCI (Control Correlation Identifier):**
  CCI-000366
  The organization implements the security configuration settings.
  NIST SP 800-53 :: CM-6 b
  NIST SP 800-53A :: CM-6.1 (iv)
  NIST SP 800-53 Revision 4 :: CM-6 b

Topic No 82: Case Study Security Hardening – IE Browser

- CIS Benchmarks case study (MS Internet Explorer 11)

- January 12, 2014
- 178 pages PDF doc
- *1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)*
- Profile applicability:
  - Level 1

- **Description:** This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Add-On Manager.
  - If you enable this policy setting, users cannot enable or disable add-ons through Add-On Manager. The only exception occurs if an add-on has been specifically entered into the 'Add-On List' policy setting in such a way as to allow users to continue to manage the add-on.
  - In this case, the user can still manage the add-on through the Add-On Manager. If you disable or do not configure this policy setting, the appropriate controls in the Add-On Manager will be available to the user.

- Configure this setting in a manner that is consistent with security and operational requirements of your organization.

– **Rationale:** Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network.

– **Audit:**
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\InternetExplorer\Restrictions\NoExtensionManagement

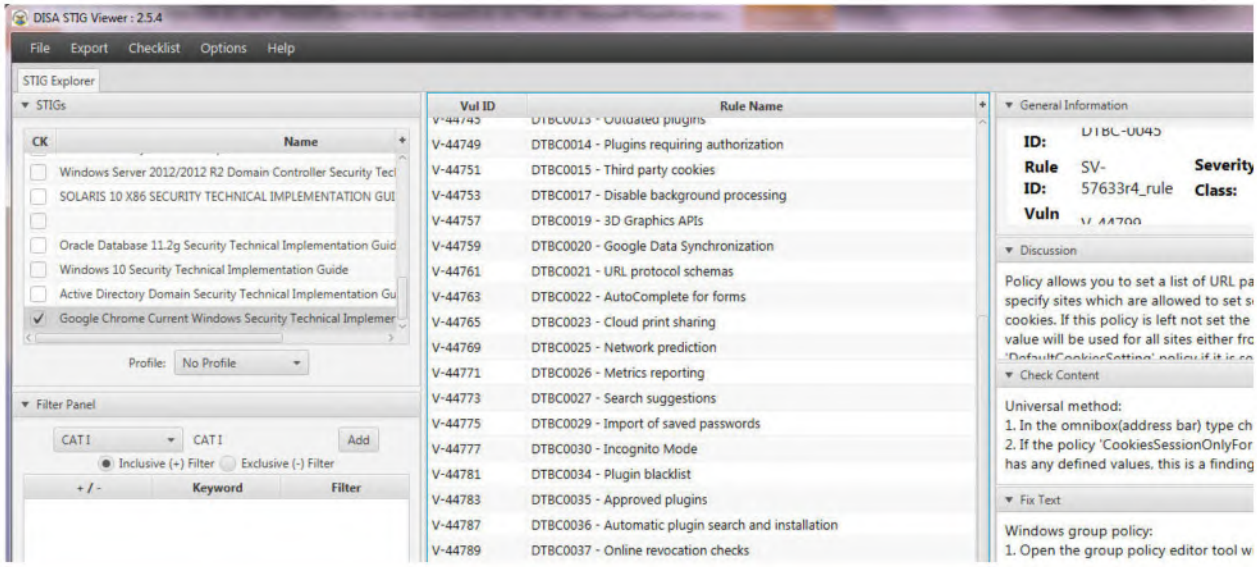
– **Remediation:** To establish the recommended configuration via Group Policy, set the following UI path to Not Configured.
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Do not allow users to enable or disable add-ons

– **Impact:** When the Do not allow users to enable or disable add-ons setting is enabled, users will not be able to enable or disable their own Internet Explorer add-ons. If your organization uses add-ons, this configuration may affect their ability to work.

- ***1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)***
  - Default Value: Disabled

Topic No 83: Security Hardening – Case Study - Chrome

- Google Chrome
- DISA, Release 8
  - 27 April, 2017



- **General Information:**
  - **Rule Title :** Session only based cookies must be disabled.
- General Information:
  - **Vuln ID:** V-44799
  - **STIG ID**: DTBC-0045
  - **Severity**: CAT I

- **Discussion:**

- Policy allows you to set a list of URL patterns that specify sites which are allowed to set session only cookies. If this policy is left not set the global default value will be used for all sites either from the 'DefaultCookiesSetting' policy if it is set, or the user's personal configuration otherwise. If the 'RestoreOnStartup' policy is set to restore URLs from previous sessions this policy will not be respected and cookies will be stored permanently for those sites

- **Check Content:**

- **Universal method:**
  1. In the omnibox (address bar) type chrome://policy
  2. If the policy 'CookiesSessionOnlyForUrls' exists, and has any defined values, this is a finding
- **Windows method:**
  1. Start regedit
  2. Navigate to HKLM\Software\Policies\Google\Google Chrome\Content Settings\CookiesSessionOnlyForUrls
  3. If this key exists and has any defined values, this is a finding

  - **Fix Text:**

  Windows group policy:

  1. Open the group policy editor tool with gpedit.msc
  2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings
     Policy Name: Allow session only cookies on these sites
     Policy State: Disabled Policy Value: N/A

  - **CCI (Control Correlation Identifier):**
    - CCI-000166
      The information system protects against an individual (or process acting on behalf of an

individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

NIST SP 800-53 :: AU-10
NIST SP 800-53A :: AU-10.1
NIST SP 800-53 Revision 4 :: AU-10

Topic No 84: Case Study Security Hardening – Firefox

- CIS Benchmarks case study (Mozilla Firefox)

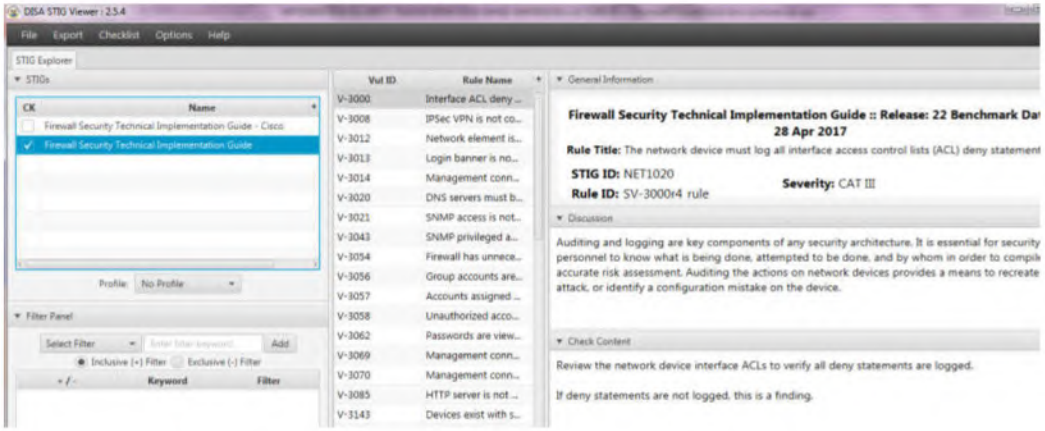
- December 31, 2015
- 72 pages PDF doc
- *3.5 (L2) Enable IDN Show Punycode (Scored)*
- Profile applicability:
  - Level 2
  - **Description:** This feature determines whether all Internationalized Domain Names (IDNs) displayed in the browser are displayed as Punycode or as Unicode.
  - **Rationale:** IDNs displayed in Punycode are easier to identify and therefore help mitigate the risk of accessing spoofed web pages.
  - **Audit:** Perform the following procedure:
    1. Type about:config in the address bar
    2. Type network.IDN_show_punycode in the filter
    3. Ensure the preferences listed are set to the values specified below: **network.IDN_show_punycode=true**
  - **Remediation:** Perform the following procedure:
    1. Open the mozilla.cfg file in the installation directory with a text editor
    2. Add the following lines to mozilla.cfg:
       lockPref("network.IDN_show_punycode", true);
  - **Default Value:** false

Topic No 85: Security Hardening – Case Study – FW

- Firewall STIG
- DISA, Release 22

28 April, 2017

STIGVIEWER WINDOW

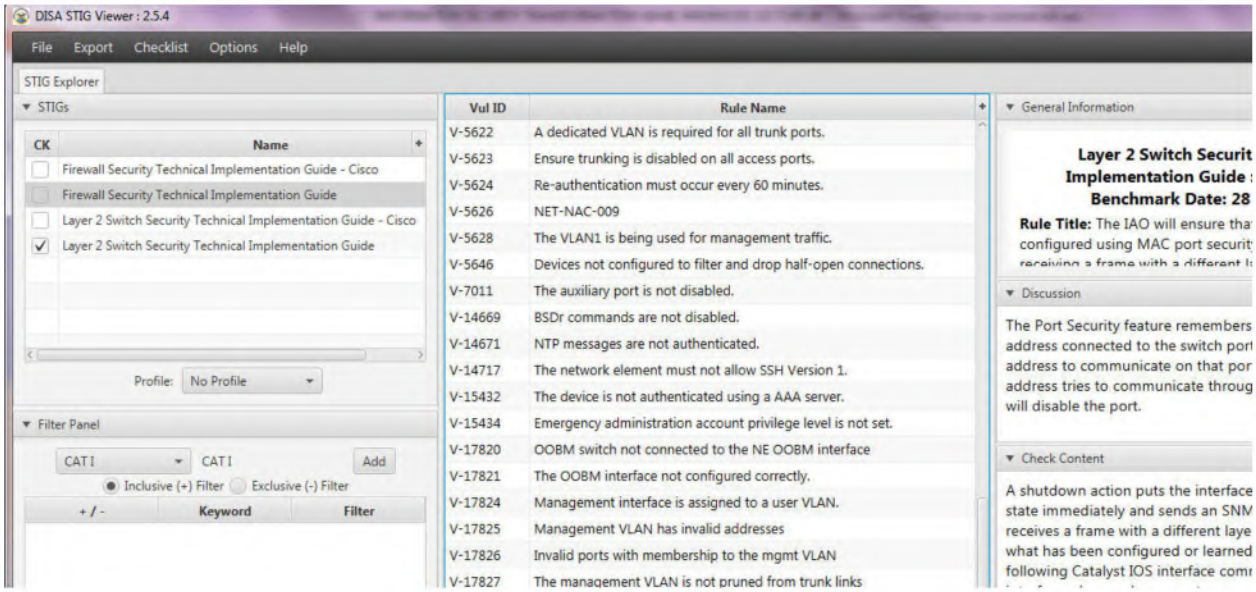


- General Information:
  - **Rule Title :** The device must be configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.
  - **Vuln ID:** V-3156
  - **STIG ID**: NET0375
  - **Severity**: CAT II
- **Discussion:**
  - A SYN-flood attack is a denial-of-service attack where the attacker sends a huge amount of please-start-a-connection packets and then nothing else. This causes the device being attacked to be overloaded with the open sessions and eventually crash.
  - A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers)
- **Check Content:**
  - Review the device configurations to determine if denial of service attacks guarded against.
  - If the device is not configured to mitigate denial of service attacks, this is a finding.
- **Fix Text:**
  - If the firewall support SYN-flood or ping sweep protection then enable these features. If the firewall does not support these features, enable the security features on the router to protect the network from these attacks.
- **CCI (Control Correlation Identifier):**
  - (Misc info)

Topic No 86: Security Hardening – Case Study – Switch

- Layer 2 Switch STIG
- DISA, Release 20
  - 28 Oct, 2016

STIGVIEWER WINDOW



- **General Information:**

  Rule Title : The IAO to that all switchports configured using MAC port security will shutdown upon receiving a frame with a different layer 2 source address than what has been configured or learned for port security

- **General Information:**
  - **Vuln ID:** V-18565
  - **STIG ID**: NET-NAC-032
  - **Severity**: CAT III

- **Discussion:**

– The Port Security feature remembers the Ethernet MAC address connected to the switch port and allows only that MAC address to communicate on that port If any other MAC address tries to communicate through the port, port security will disable the port.

- **Check Content:**

– A shutdown action puts the interface into the error-disabled state immediately and sends an SNMP trap notification if it receives a frame with a different layer 2 source address that what has been configured or learned for port security. The following Catalyst IOS interface command will shutdown the interface when such an event occurs: **switchport port-security violation shutdown**

- **Fix Text:**
  - Configure the port to shutdown when insecure hosts are connected to the wall jack.

Topic No 87: Case Study Security Hardening – Cisco IOS 15

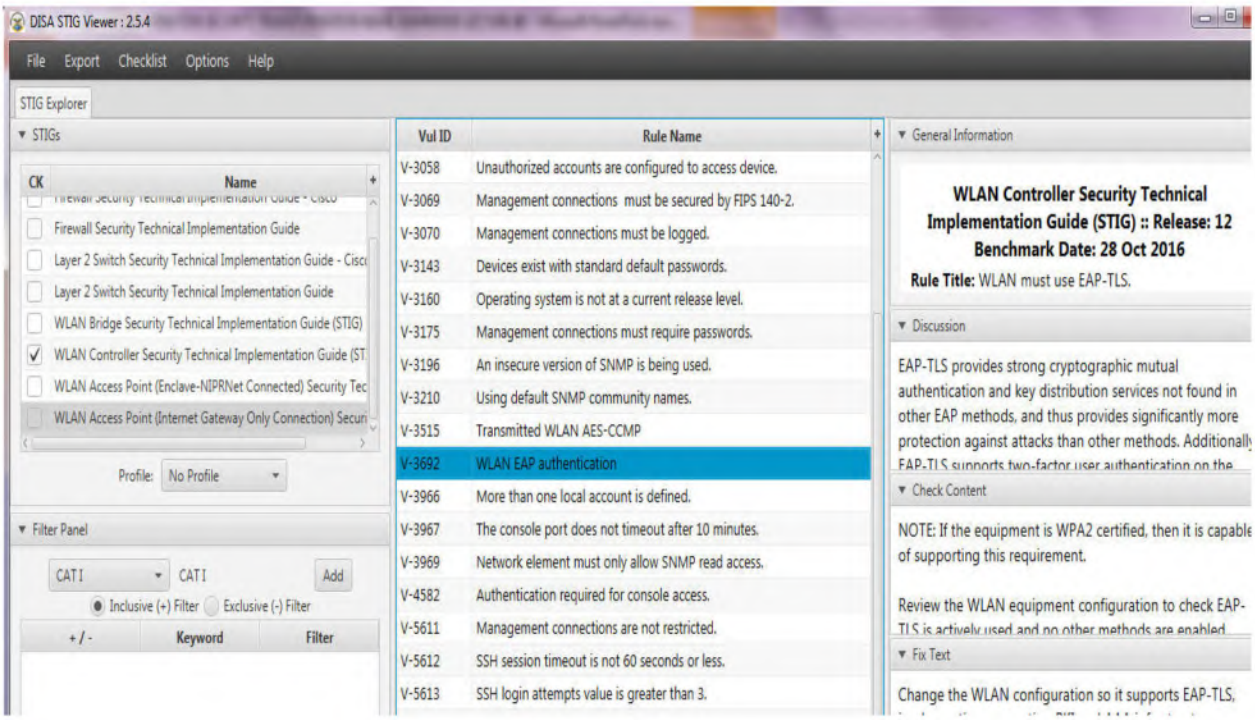
- CIS Benchmarks case study (Cisco IOS 15)
- For Cisco routers running IOS 15M

- June 30, 2015
- 151 pages PDF doc
- *3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)*
- Profile applicability:
  - Level 2
  - **Description:** Enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication.
  - **Rationale:** This is part of the OSPF authentication setup
  - **Audit:** Verify the appropriate md5 key is defined on the appropriate interface(s) **hostname#sh run int {*interface*}**
  - **Remediation:** Configure the appropriate interface(s) for Message Digest authentication **hostname(config)#interface {*interface_name*} hostname(config-if)#ip ospf message-digest-key {*ospf_md5_key-id*} md5 {*ospf_md5_key*}**
  - **Impact:** Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols Configuring the proper interface(s) for 'ip ospf message-digest-key md5' enforces these policies by restricting exchanges between network devices.
  - **Default Value:** Not set

Topic No 88: Security Hardening – Case Study – WLAN

- WLAN Controller STIG
- DISA, Release 12
  - 28 Oct, 2016

STIGVIEWER WINDOW



- General Information:
  - **Rule Title :** WLAN must use EAP-TLS
  - **Vuln ID:** V-3692
  - **STIG ID**: WIR0115-01
  - **Severity**: CAT II
- **Discussion:**
  - EAP-TLS provides strong cryptographic mutual authentication and key distribution services not found in other EAP methods, and thus provides significantly more protection against attacks than other methods.
  - Additionally, EAP-TLS supports two-factor user authentication on the WLAN client, which provides significantly more protection than methods that rely on a password or certificate alone.
  - EAP-TLS also can leverage DoD CAC in its authentication services, providing additional security and convenience.

- **Check Content:**
  - NOTE: If the equipment is WPA2 certified, then it is capable of supporting this requirement.
  - Review the WLAN equipment configuration to check EAP-TLS is actively used and no other methods are enabled.
  - Mark as a finding if either EAP-TLS is not used or if the WLAN system allows users to connect with other methods.

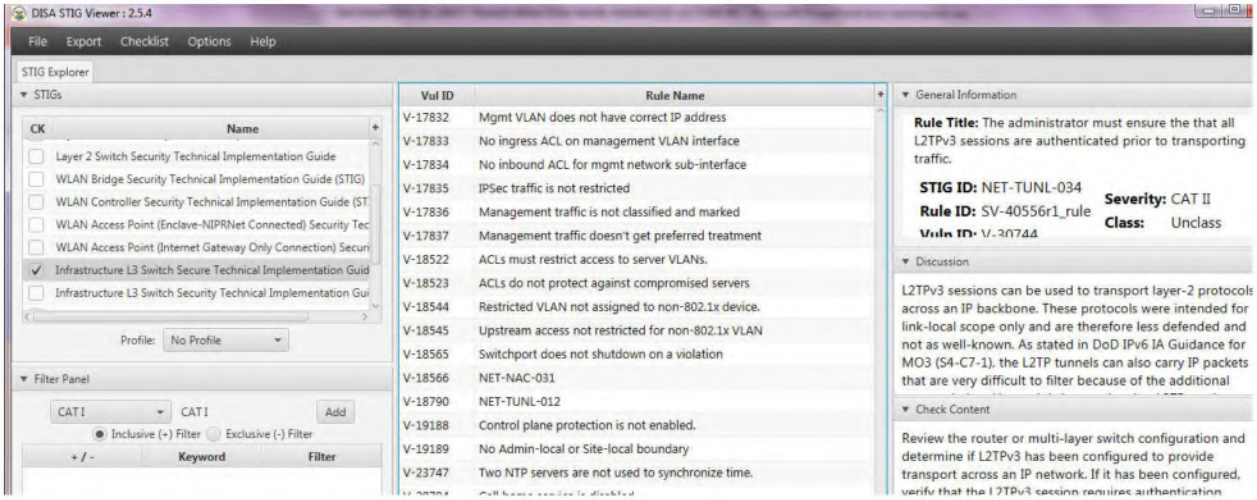
- **Fix Text:**

  - Change the WLAN configuration so it supports EAP-TLS, implementing supporting PKI and AAA infrastructure as necessary.
  - If the WLAN equipment is not capable of supporting EAP-TLS, procure new equipment capable of such support.

Topic No 89: Security Hardening – Case Study – L3 Switch

- Infrastructure Layer 3 Switch STIG
- DISA, Release 22
  - 28 April, 2017

STIGVIEWER WINDOW



- **General Information:**
  - **Rule Title :** The administrator must ensure the that all L2TPv3 sessions are authenticated prior to transporting traffic.
  - **Vuln ID:** V-30744
  - **STIG ID**: NET-TUNL-034
  - **Severity**: CAT II
- **Discussion:**
  - L2TPv3 sessions can be used to transport layer-2 protocols across an IP backbone. These protocols were intended for link-local scope only and are therefore less defended and not as well-known.
  - As stated in DoD IPv6 IA Guidance for MO3 (S4-C7-1), the L2TP tunnels can also carry IP packets that are very difficult to filter because of the additional encapsulation.

- Hence, it is imperative that L2TP sessions are authenticated prior to transporting traffic

- **Check Content:**
  - Review the router or multi-layer switch configuration and determine if L2TPv3 has been configured to provide transport across an IP network. If it has been configured, verify that the L2TPv3 session requires authentication.

- **Fix Text:**
  - Configure L2TPv3 to use authentication for any peering sessions.

Topic No 90: Case Study Security Hardening – VMware

- CIS Benchmarks case study (Vmware ESXi 5.5)

- December 16, 2014
- 132 pages PDF doc
- *5.1 Disable DCUI to prevent local administrative control (Scored)*
- Profile applicability:
  - Level 2
  - **Description:** The Direct Console User Interface (DCUI) can be disabled to prevent any local administration from the Host; Once the DCUI is disabled any administration of the ESXi host will be done through vCenter.

- **Rationale:**
  - The DCUI allows for low-level host configuration such as configuring IP address, hostname and root password as well as diagnostic capabilities such as enabling the ESXi shell, viewing log files, restarting agents, and resetting configurations. Actions performed from the DCUI are not tracked by vCenter Server. Even if Lockdown Mode is enabled, users who are members of the

DCUI.Access list can performed in vCenter Server where they can be centrally audited and monitored.

– **Audit:** Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Settings" -> "System" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "Direct Console UI".
6. Verify the Startup Policy is set to "Start and Stop Manually“

Additionally, the following PowerCLI command may be used:

 # List DCUI settings for all hosts Get-VMHost | Get-VMHostService | Where { $_.key -eq "DCUI" }

- **Remediation:** Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Settings" -> "System" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "Direct Console UI".
6. Click "Stop".
7. Change the Startup Policy "Start and Stop Manually".
8. Click "OK".

- **Impact:**

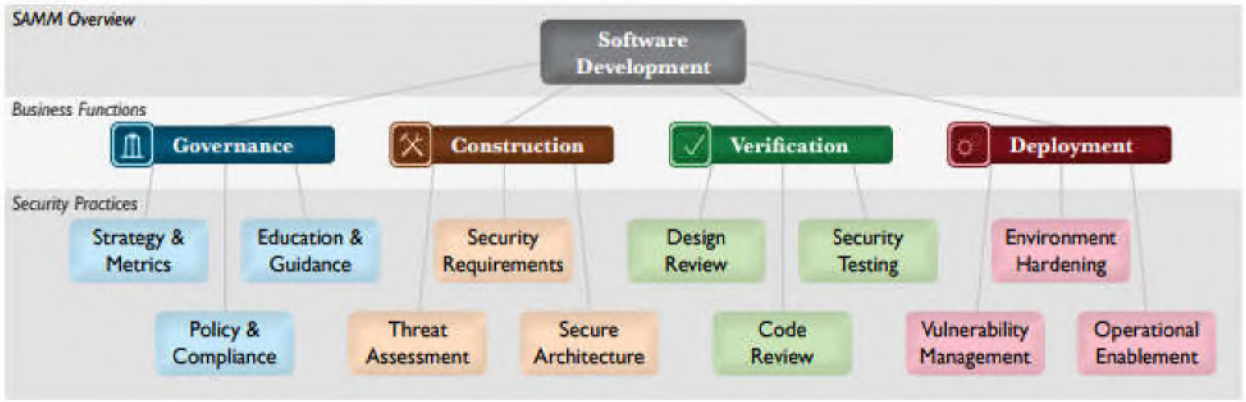
– Disabling the DCUI can create a potential "lock out" situation should the host become isolated from vCenter Server. Recovering from a "lock out" scenario requires re-installing ESXi. Consider leaving DCUI enabled and instead enable lockdown mode and limit the users allowed to access the DCUI using the DCUI.Access list.

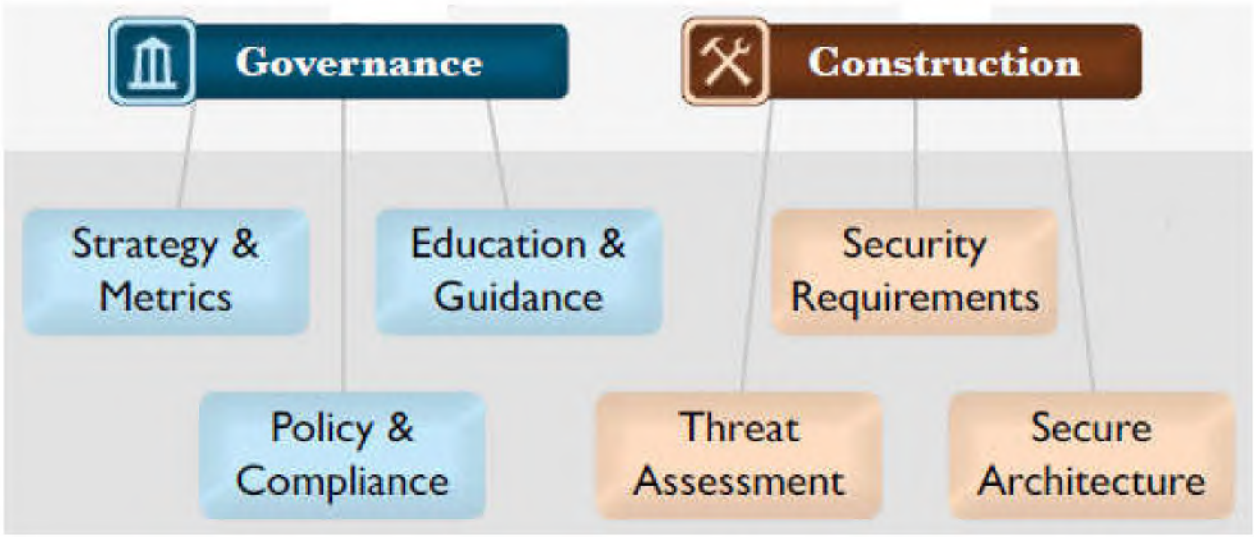
- **Default Value:**

  – The prescribed state is not the default state.

Topic no 91 & 92 : Software Security Fundamentals-SAMM & SAMM-2

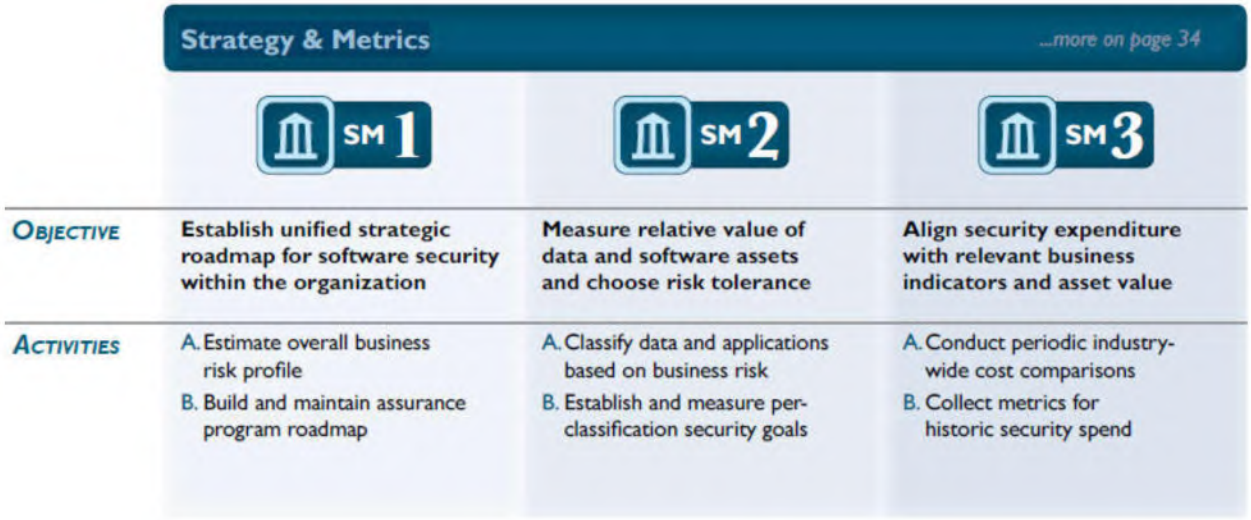
- Software Assurance Maturity Model (SAMM) developed by OWASP
  - A guide to building security into software development
  - 96 page PDF





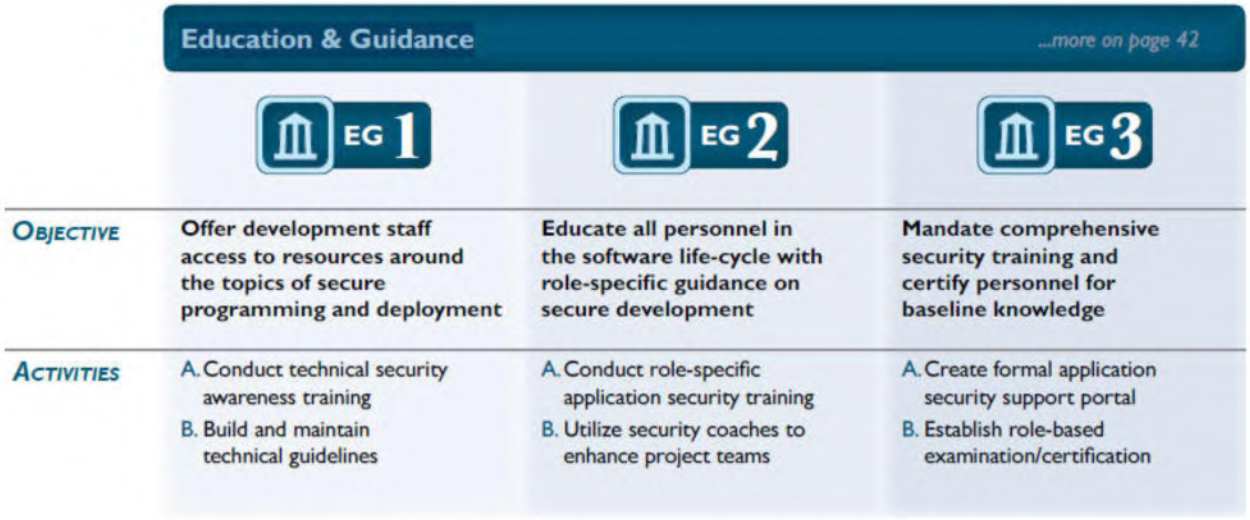
- OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**
  - Strategy & Metrics
  - Education & Guidance
  - Policy & Compliance

- **Strategy & Metrics:**
  - Focused on establishing the framework within an organization for a software security assurance program.
  - This is the most fundamental step in defining security goals in a way that's both measurable and aligned with the organization's real business risk.



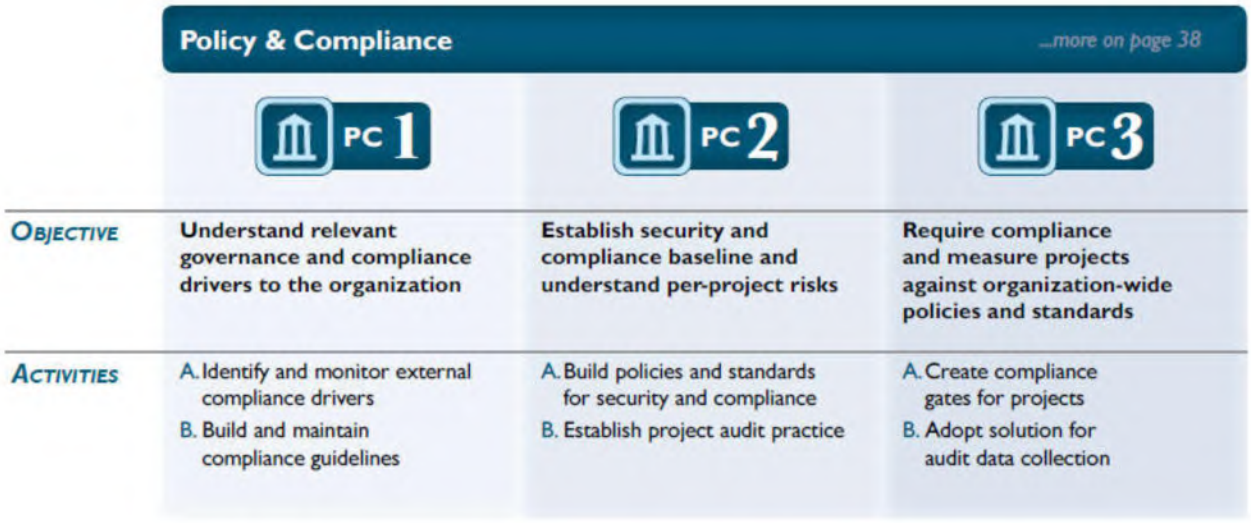
Strategy & Metrics			...more on page 34
	SM 1	SM 2	SM 3
OBJECTIVE	Establish unified strategic roadmap for software security within the organization	Measure relative value of data and software assets and choose risk tolerance	Align security expenditure with relevant business indicators and asset value
ACTIVITIES	A. Estimate overall business risk profile B. Build and maintain assurance program roadmap	A. Classify data and applications based on business risk B. Establish and measure per-classification security goals	A. Conduct periodic industry-wide cost comparisons B. Collect metrics for historic security spend

- **Education & Guidance:**
  - Focused on arming personnel involved in the software lifecycle with knowledge and resources to design, develop, and deploy secure software.
  - With improved access to information, project teams will be better able to proactively identify and mitigate the specific security risks that apply to their organization.



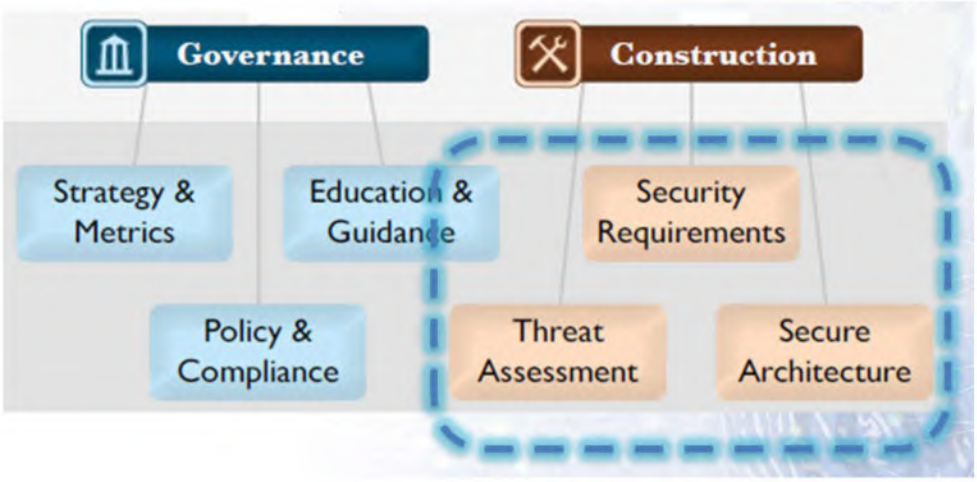
Education & Guidance			...more on page 42
	EG 1	EG 2	EG 3
OBJECTIVE	Offer development staff access to resources around the topics of secure programming and deployment	Educate all personnel in the software life-cycle with role-specific guidance on secure development	Mandate comprehensive security training and certify personnel for baseline knowledge
ACTIVITIES	A. Conduct technical security awareness training B. Build and maintain technical guidelines	A. Conduct role-specific application security training B. Utilize security coaches to enhance project teams	A. Create formal application security support portal B. Establish role-based examination/certification

- **Policy & Compliance:**
  - Focused on understanding and meeting external legal and regulatory requirements while also driving internal security standards to ensure compliance in a way that's aligned with the business purpose of the org.
  - A driving theme for improvement within this Practice is focus on project-level audits that gather information about the organization's behavior in order to check that expectations are being met.



Policy & Compliance	PC 1	PC 2	PC 3
OBJECTIVE	Understand relevant governance and compliance drivers to the organization	Establish security and compliance baseline and understand per-project risks	Require compliance and measure projects against organization-wide policies and standards
ACTIVITIES	A. Identify and monitor external compliance drivers B. Build and maintain compliance guidelines	A. Build policies and standards for security and compliance B. Establish project audit practice	A. Create compliance gates for projects B. Adopt solution for audit data collection

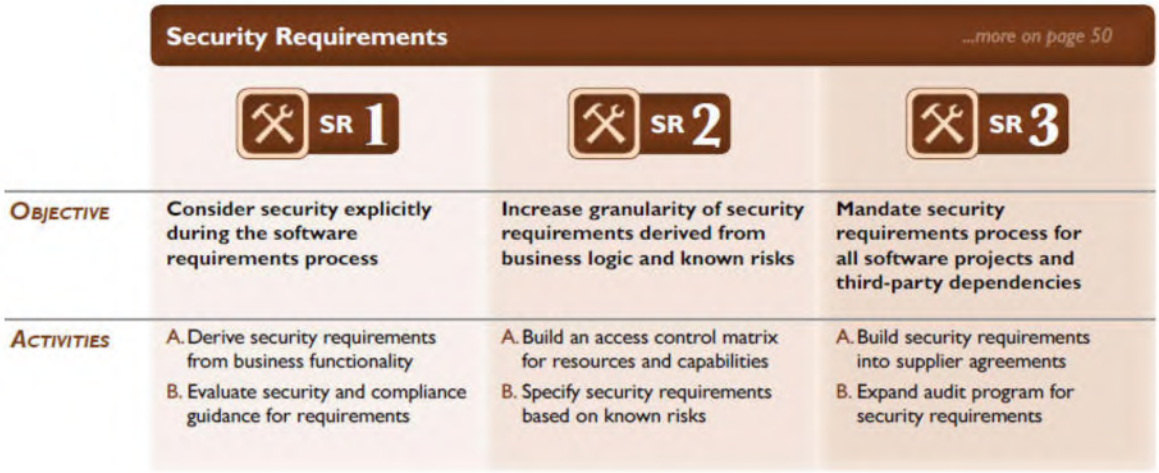
Topic no 93



- OWASP Software Assurance Maturity Model (SAMM) **Construction Phase:**
  - Security Requirements
  - Threat Assessment

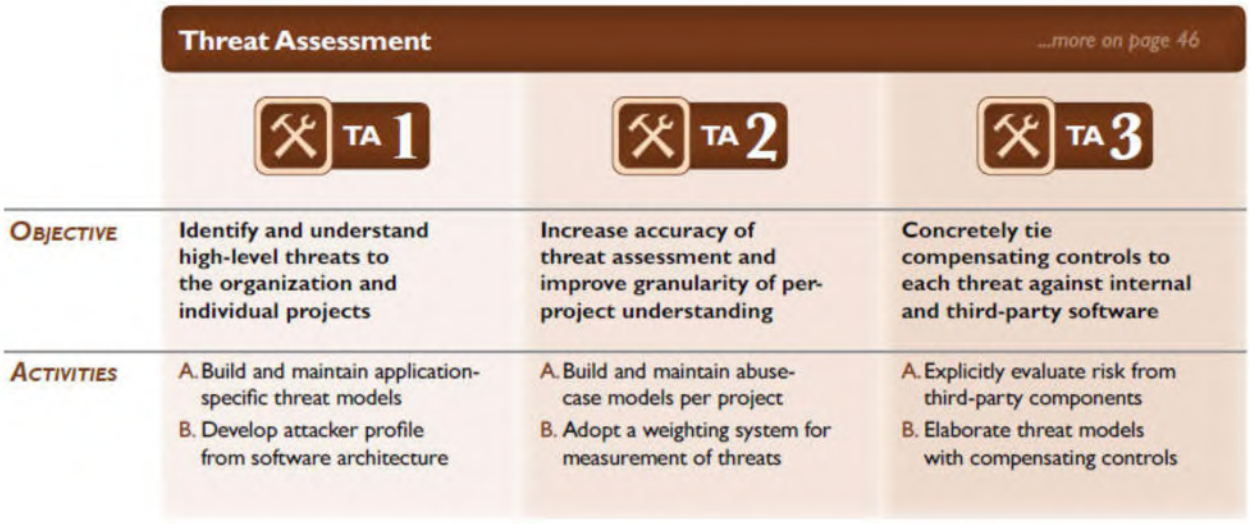
- Secure Architecture

- **Security Requirements:**
  - Focused on proactively specifying the expected behavior of software with respect to security
  - Through addition of analysis activities at the project level, security requirements are initially gathered based on the high-level business purpose of the software



Security Requirements	SR 1	SR 2	SR 3
Objective	Consider security explicitly during the software requirements process	Increase granularity of security requirements derived from business logic and known risks	Mandate security requirements process for all software projects and third-party dependencies
Activities	A. Derive security requirements from business functionality B. Evaluate security and compliance guidance for requirements	A. Build an access control matrix for resources and capabilities B. Specify security requirements based on known risks	A. Build security requirements into supplier agreements B. Expand audit program for security requirements

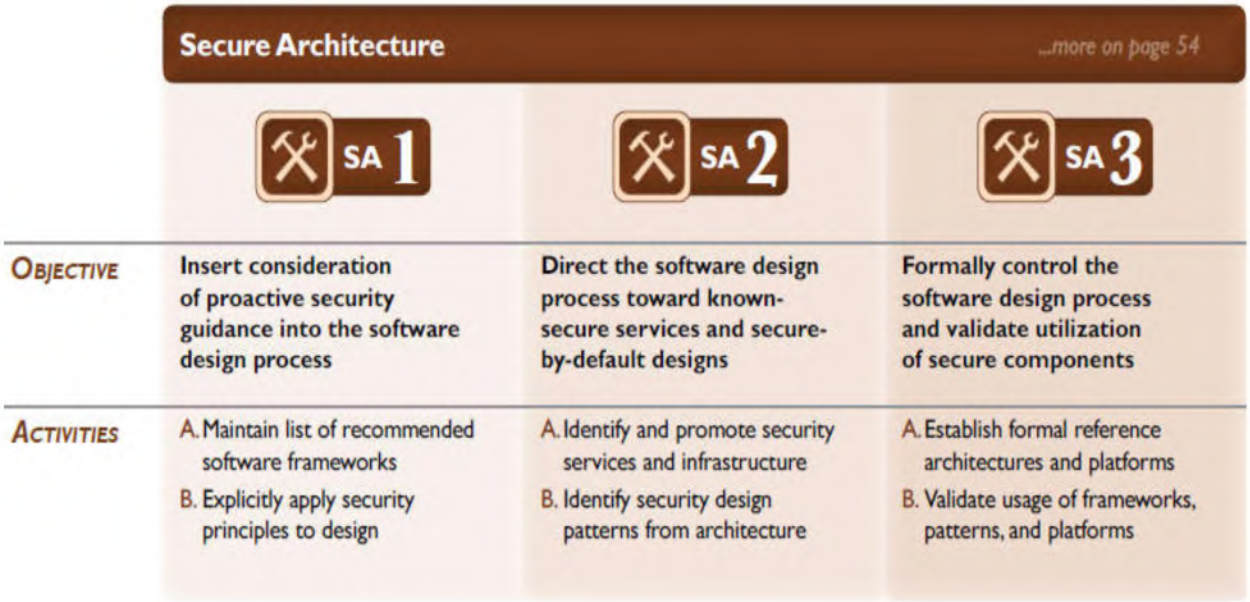
- **Threat Assessment:**
  - Centered on identification and understanding the project-level risks based on the functionality of the software being developed and characteristics of the runtime environment
  - From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security



Threat Assessment	TA 1	TA 2	TA 3
Objective	Identify and understand high-level threats to the organization and individual projects	Increase accuracy of threat assessment and improve granularity of per-project understanding	Concretely tie compensating controls to each threat against internal and third-party software
Activities	A. Build and maintain application-specific threat models B. Develop attacker profile from software architecture	A. Build and maintain abuse-case models per project B. Adopt a weighting system for measurement of threats	A. Explicitly evaluate risk from third-party components B. Elaborate threat models with compensating controls

- **Secure Architecture:**
  - Focused on proactive steps for an organization to design and build secure software by default

– By enhancing the software design process with reusable services and components, the overall security risk from software development can be dramatically reduced.



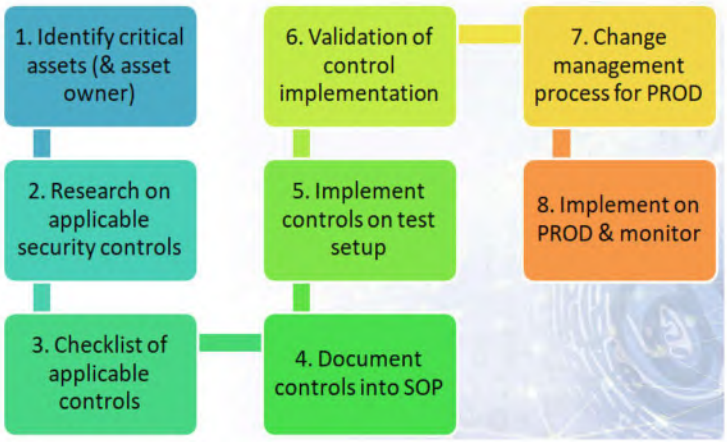
Secure Architecture			...more on page 54
	SA 1	SA 2	SA 3
OBJECTIVE	Insert consideration of proactive security guidance into the software design process	Direct the software design process toward known-secure services and secure-by-default designs	Formally control the software design process and validate utilization of secure components
ACTIVITIES	A. Maintain list of recommended software frameworks B. Explicitly apply security principles to design	A. Identify and promote security services and infrastructure B. Identify security design patterns from architecture	A. Establish formal reference architectures and platforms B. Validate usage of frameworks, patterns, and platforms

SAMM is an excellent model for software security and we look at the verification and deployment phases as part of testing and validation.

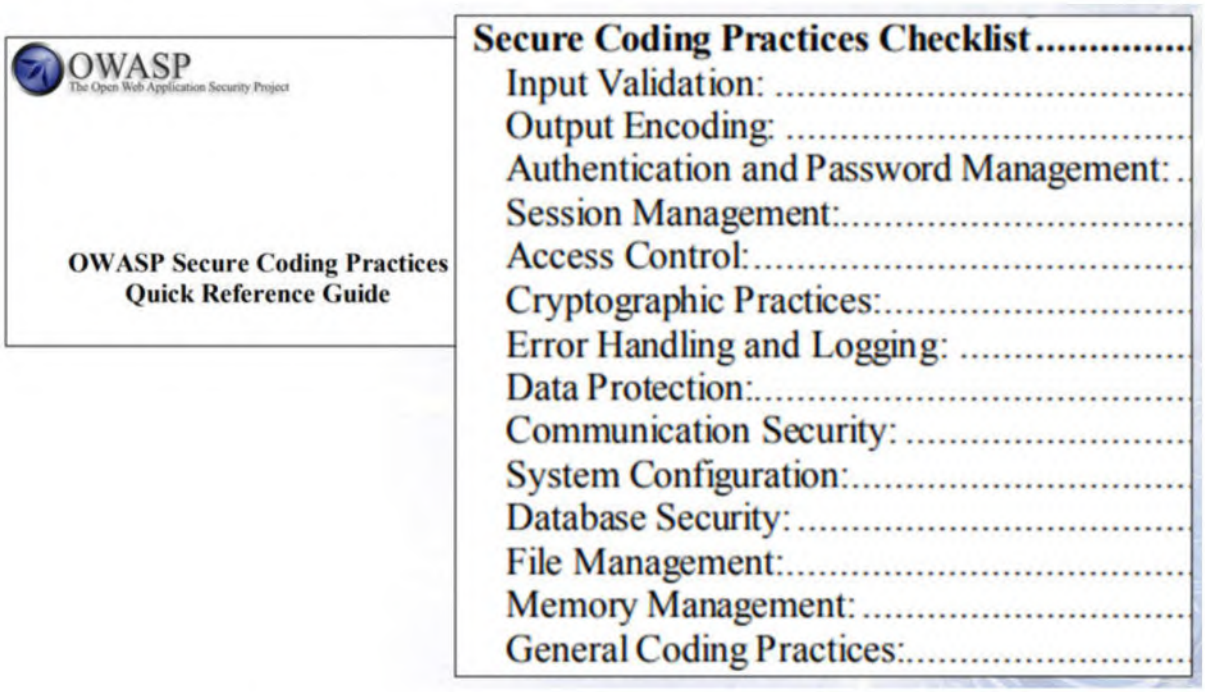
Topic no 94: SECURITY HARDENING – SOFTWARE APPLICATIONS

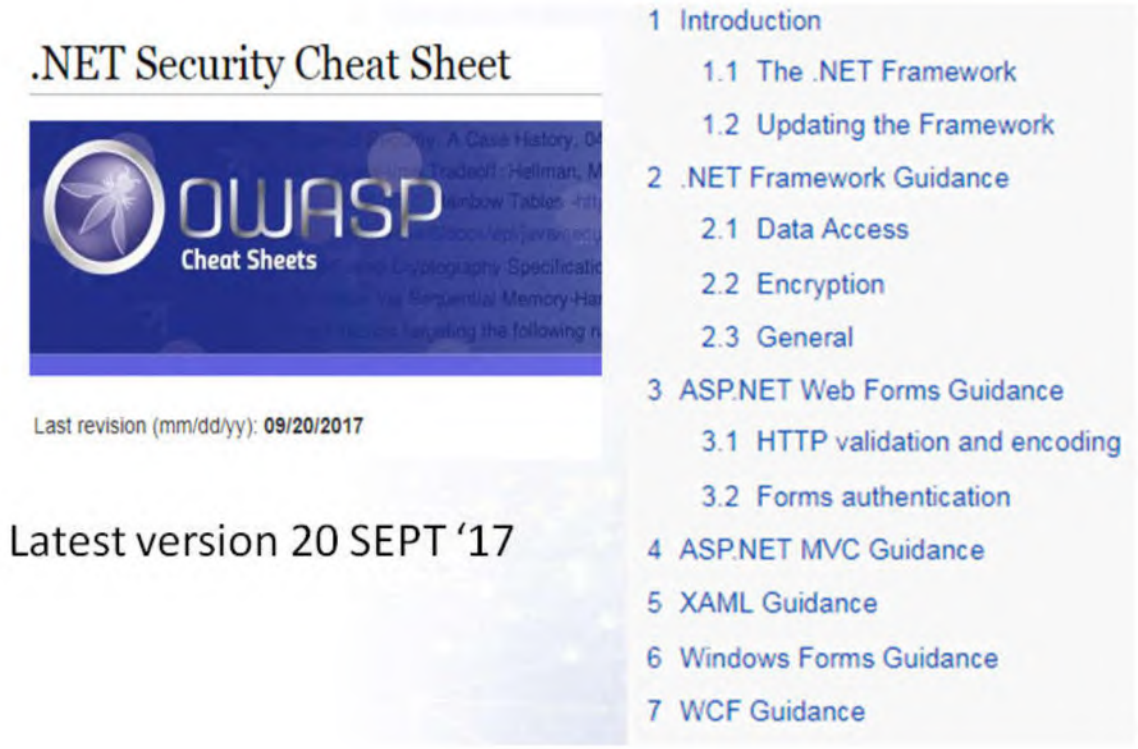
- **Two types of security hardening:**
  - IT assets (systems, network devices, databases, applications)
  - Software developed internally or by third party
- **Typical enterprise software:**
  - ERP (Oracle, SAP, IBM, etc)
  - **Internally or 3rd party developed software in ASP.NET, PHP, Android/IOS, or other platform**

8 STEP SECURITY HARDENING METHODOLOGY



- **Useful resources:**
  - www.OWASP.org
  - www.cloudsecurityalliance.org
  - MS Technet
  - OWASP Top 10
  - OWASP Secure Coding Practices Quick Reference Guide
  - SAMM





- **Conclusion**
  - Software security hardening is a challenging activity
  - Build software security program & integrate with QA
  - Domain specific knowledge required
  - Build capabilities and process following SAMM

Topic no 95: CASE STUDY – ASP.NET SECURITY HARDENING

- OWASP ASP.NET Cheat Sheet
- https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet
- .NET Framework Guidance
- ASP.NET Web Forms Guidance
- ASP.NET MVC Framework Guidance
- **.NET Framework Guidance**
  - Data access
  - Encryption
  - General guidelines
- **NET FRAMEWORK, DATA ACCESS GUIDANCE:**
  - Use Parameterized SQL commands for all data access, without exception.
  - Do not use SqlCommand with a string parameter made up of a concatenated SQL String.
  - Whitelist allowable values coming from the user. Use enums, TryParse or lookup values to assure that the data coming from the user is as expected.
  - Apply the principle of least privilege when setting up the Database User in your database of choice. The database user should only be able to access items that make sense for the use case.
  - Use of the Entity Framework is a very effective SQL injection prevention mechanism. When using SQL Server, prefer integrated authentication over SQL authentication.
  - Use Always Encrypted where possible for sensitive data (SQL Server 2016 and SQL Azure)
- **.NET FRAMEWORK, GENERAL GUIDANCE:**
  - Lock down the config file.
  - Remove all aspects of configuration that are not in use.
  - Encrypt sensitive parts of the web.config using aspnet_regiis -pe
  - For Click Once applications the .Net Framework should be upgraded to use version 4.6.2 to ensure TLS 1.1/1.2 support.
- **ASP.NET Web Forms Guidance**

- HTTPS & some general configuration
- HTTP validation & encoding
- Forms authentication

- **ASP.NET MVC Guidance**
  - ASP.NET MVC (Model-View-Controller) is a contemporary web application framework that uses more standardized HTTP communication
  - Based on OWASP Top 10

Topic no 96: CASE STUDY – PHP SECURITY HARDENING

- PHP Security Guidelines
- https://docs.php.earth/security/intro/

1. Cross site scripting (XSS)
2. Injections
   - SQL injection
   - Directory traversal (path injection)
   - Command injection
   - Code injection
3. Cross site request forgery (XSRF/CSRF)
4. Public files
5. Passwords
6. Uploading files
7. Session hijacking
8. Remote file inclusion
9. PHP configuration
   - Error reporting
   - Exposing PHP version
   - Remote files
   - Open_basedir
   - Session settings
10. Use HTTPS
11. Things not listed

9. PHP Configuration

Always keep the installed PHP version updated. You can use versionscan to check for possible vulnerabilities of your PHP version. Update open source libraries and applications, and keep your web server well maintained. Here are some of the important settings from php.ini that you should check out. You can also use iniscan to scan your php.ini files for best security practices.

- **Error Reporting**

In your production environment, you must always turn off displaying errors to the screen. If errors occur in your application and they are visible to the outside world, an attacker could get valuable data for attacking your application

```
; Disable displaying errors to screen
display_errors = off
; Enable writing errors to server logs
log_errors = on
```

Topic no 97: CASE STUDY – ASP.NET MVC SECURITY HARDENING

- ASP.NET MVC Security Guidelines
- https://www.owasp.org/index.php/.NET_Security_Cheat_Sheet#ASP.NET_MVC_Guidance
- ASP.NET MVC (Model-View-Controller) is a contemporary web application framework that uses more standardized HTTP communication than the Web Forms postback model
- The OWASP Top 10 lists the most prevalent and dangerous threats to web security in the world today and is reviewed every 3 years.
- After covering the top 10 it is generally advisable to assess for other threats or get a professional Penetration Test.
- Your approach to securing your web application should be to start at the top threat A1 below and work down, this will ensure that any time spent on security will be spent most effectively and cover the top threats first and lesser threats afterwards.

A.6 Sensitive data exposure

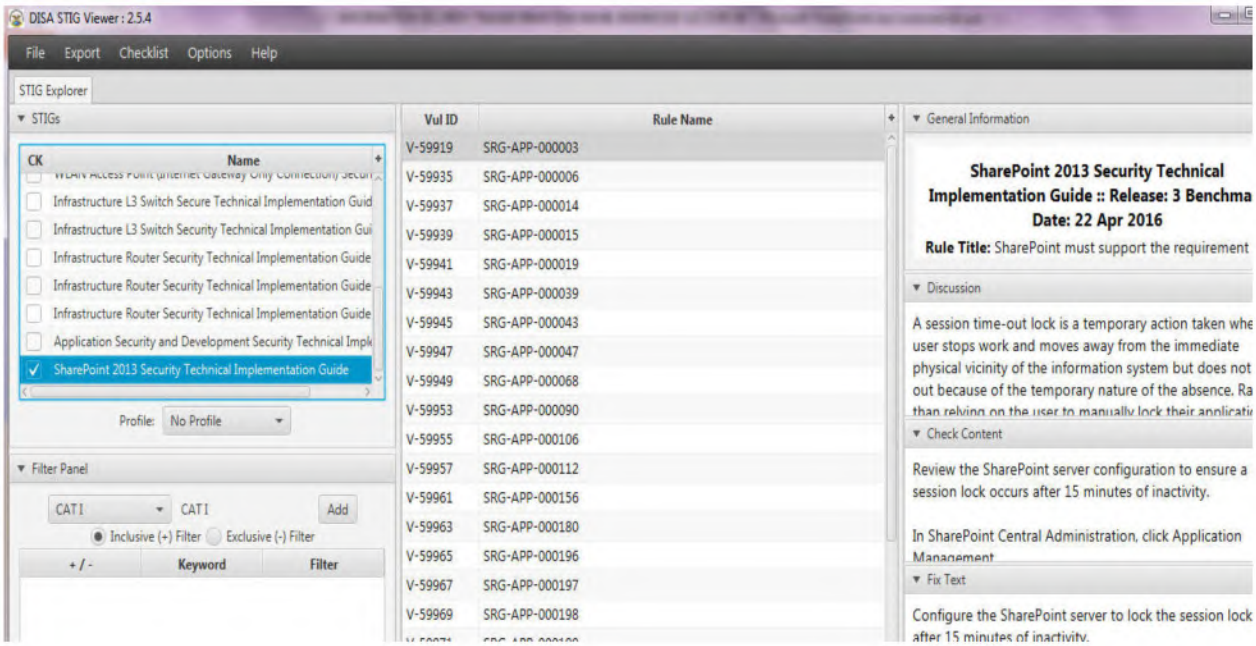
- DO NOT: Store encrypted passwords.
- DO: Use a strong hash to store password credentials. Use PBKDF2, BCrypt or SCrypt with at least 8000 iterations and a strong key.
- DO: Enforce passwords with a minimum complexity that will survive a dictionary attack i.e. longer passwords that use the full character set (numbers, symbols and letters) to increase the entropy.

- DO: Use a strong encryption routine such as AES-512 where personally identifiable data needs to be restored to it's original format. Do not encrypt passwords. Protect encryption keys more than any other asset.
- Apply the following test: Would you be happy leaving the data on a spreadsheet on a bus for everyone to read. Assume the attacker can get direct access to your database and protect it accordingly.
- DO: Use TLS 1.2 for your entire site. Get a free certificate from StartSSL.com or LetsEncrypt.org.
- DO NOT: Allow SSL, this is now obsolete
- DO: Have a strong TLS policy (see SSL Best Practises), use TLS 1.2 wherever possible. Then check the configuration using SSL Test
- DO: Ensure headers are not disclosing information about your application.
- See HttpHeaders.cs , Dionach StripHeaders or disable via web.config:

Topic no 98: Security Hardening – Case Study-SharePoint

- Sharepoint 2013 STIG
- DISA, Release 3
  - 22 April, 2016
- Sharepoint server side configurations

STIGVIEWER WINDOW



- General Information:
  - **Rule Title :** For environments requiring an Internet-facing capability, the SharePoint application server upon which Central Administration is installed, must not be installed in the DMZ.
  - **Vuln ID:** V-59995

- **STIG ID**: SP13-00-000155
- **Severity**: CAT II

- **Discussion:**

- Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to the information.
- SharePoint installed Central Administrator is a powerful management tool used to administer the farm. This server should be installed on a trusted network segment. This server should also be used to run services rather than user-oriented web applications.

- **Check Content:**

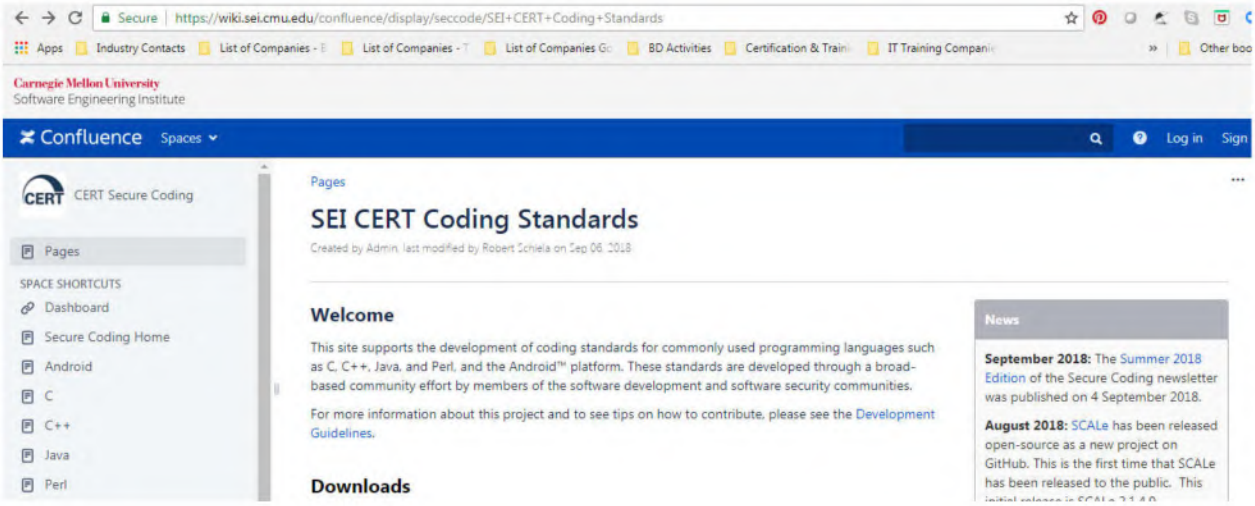
  - For environments requiring an Internet-facing capability, ensure the SharePoint Central Administration application server is not in the DMZ.
  - Inspect the logical location of the server farm web front end servers.
  - Verify the Central Administration site is not installed on a server located in a DMZ or other publicly accessible segment of the network.
  - If Central Administrator is installed on a publicly facing SharePoint server, this is a finding.

- **Fix Text:**

  - For environments requiring an Internet-facing capability, remove the SharePoint Central Administration application server upon which Central Administration is installed from the DMZ.

Topic no 99: CASE STUDY – C APPLICATIONS SECURITY HARDENING

- Carnegie Mellon Software Engineering Institute
- https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards
- https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard



https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

- There are existing compiler implementations that allow const-qualified objects to be modified without generating a warning message.
- Avoid casting away const qualification because doing so makes it possible to modify const-qualified objects without issuing diagnostics.

Noncompliant Code Example

This noncompliant code example allows a constant object to be modified:

```
const int **ipp;
int *ip;
const int i = 42;

void func(void) {
  ipp = &ip; /* Constraint violation */
  *ipp = &i; /* Valid */
  *ip = 0;   /* Modifies constant i (was 42) */
}
```

- The first assignment is unsafe because it allows the code that follows it to attempt to change the value of the const object i.

```
int **ipp;
int *ip;
int i = 42;

void func(void) {
  ipp = &ip; /* Valid */
  *ipp = &i; /* Valid */
  *ip = 0; /* Valid */
}
```

- The compliant solution depends on the intent of the programmer. If the intent is that the value of i is modifiable, then it should not be declared as a constant, as in this compliant solution:

- If the intent is that the value of i is not meant to change, then do not write noncompliant code that attempts to modify it.

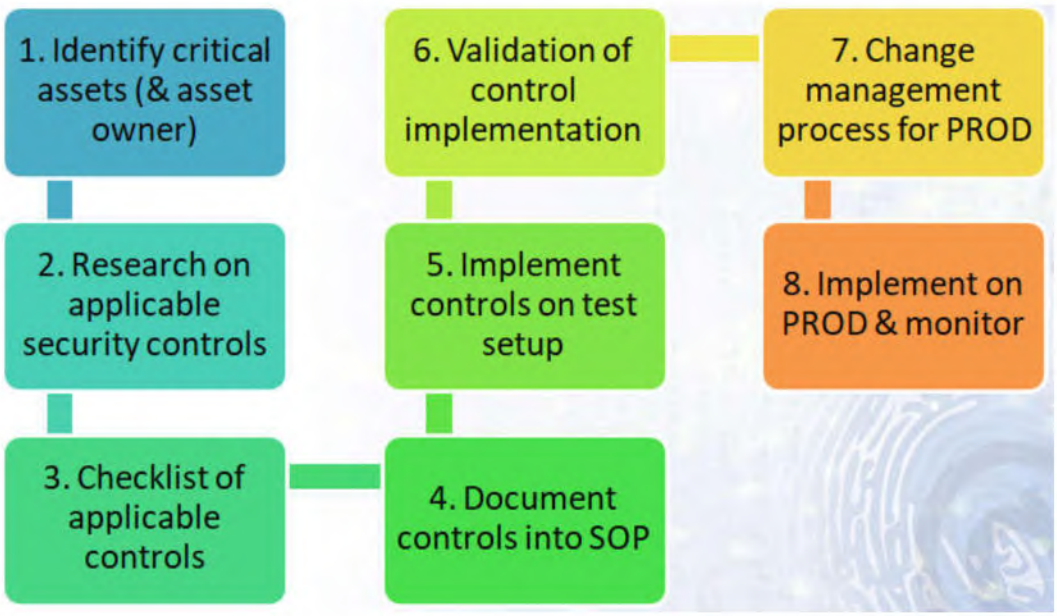
- Risk Assessment

- Automated detection

- Related vulnerabilities

Topic no 100: CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

- Carnegie Mellon Software Engineering Institute
- https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682



- Rule 01. Declarations and Initialization (DCL)
- Rule 02. Expressions (EXP)
- Rule 03. Integers (INT)
- Rule 04. Containers (CTR)
- Rule 05. Characters and Strings (STR)
- Rule 06. Memory Management (MEM)
- Rule 07. Input Output (FIO)
- Rule 08. Exceptions and Error Handling (ERR)Page:
- Rule 09. Object Oriented Programming (OOP)
- Rule 10. Concurrency (CON)
    - Rule 10. Concurrency (CON)
        - CON50-CPP. Do not destroy a mutex while it is locked
        - Mutex objects are used to protect shared data from being concurrently accessed. If a mutex object is destroyed while a thread is blocked waiting for the lock, critical sections and shared data are no longer protected.

- The C++ Standard, [thread.mutex.class], paragraph 5 [ISO/IEC 14882-2014], states the following:
- The behavior of a program is undefined if it destroys a mutex object owned by any thread or a thread terminates while owning a mutex object.

```
#include <mutex>
#include <thread>

const size_t maxThreads = 10;

void do_work(size_t i, std::mutex *pm) {
  std::lock_guard<std::mutex> lk(*pm);

  // Access data protected by the lock.
}

void start_threads() {
  std::thread threads[maxThreads];
  std::mutex m;

  for (size_t i = 0; i < maxThreads; ++i) {
    threads[i] = std::thread(do_work, i, &m);
  }
}
```

- **Non-Compliant Code Example:**

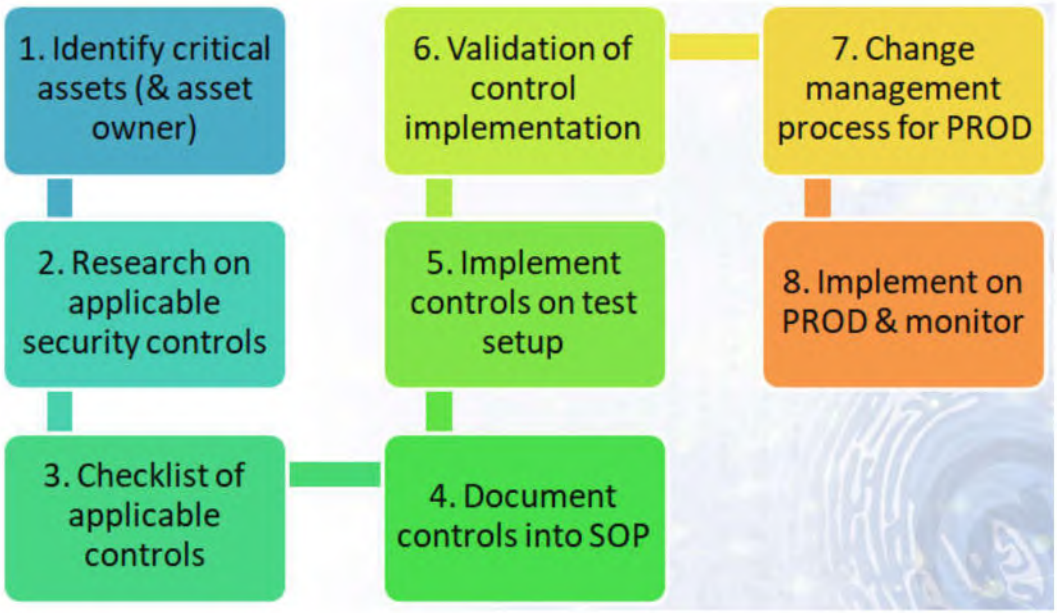
- This noncompliant code example creates several threads that each invoke the do_work() function, passing a unique number as an ID.
- Unfortunately, this code contains a race condition, allowing the mutex to be destroyed while it is still owned, because start_threads() may invoke the mutex's destructor before all of the threads have exited.

```
#include <mutex>
#include <thread>

const size_t maxThreads = 10;

void do_work(size_t i, std::mutex *pm) {
  std::lock_guard<std::mutex> lk(*pm);

  // Access data protected by the lock.
}

std::mutex m;

void start_threads() {
  std::thread threads[maxThreads];

  for (size_t i = 0; i < maxThreads; ++i) {
    threads[i] = std::thread(do_work, i, &m);
  }
}
```

- **Compliant Code Example:**
- This compliant solution eliminates the race condition by extending the lifetime of the mutex.

Topic no 101: CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

- Carnegie Mellon Software Engineering Institute
- https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java



- **Rule 7**

- ERR02-J. Prevent exceptions while logging data

- Exceptions that are thrown while logging is in progress can prevent successful logging unless special care is taken. Failure to account for exceptions during the logging process can cause security vulnerabilities, such as allowing an attacker to conceal critical security exceptions by preventing them from being logged. Hence, programs must ensure that data logging continues to operate correctly even when exceptions are thrown during the logging process.

```
try {
  // ...
} catch (SecurityException se) {
  System.err.println(se);
  // Recover from exception
}
```

- **Non-compliant Code Example:**

- This noncompliant code example writes a critical security exception to the standard error stream:

- Writing such exceptions to the standard error stream is inadequate for logging purposes. First, the standard error stream may be exhausted or closed, preventing recording of subsequent exceptions. Second, the trust level of the standard error stream may be insufficient for recording certain security-critical exceptions or errors without leaking sensitive information. If an I/O error were to occur while writing the security exception, the catch block would throw an IOException and the critical security exception would be lost. Finally, an attacker may disguise the exception so that it occurs with several other innocuous exceptions.

```
try {
  // ...
} catch(SecurityException se) {
  logger.log(Level.SEVERE, se);
  // Recover from exception
}
```

- **Compliant Solution:**

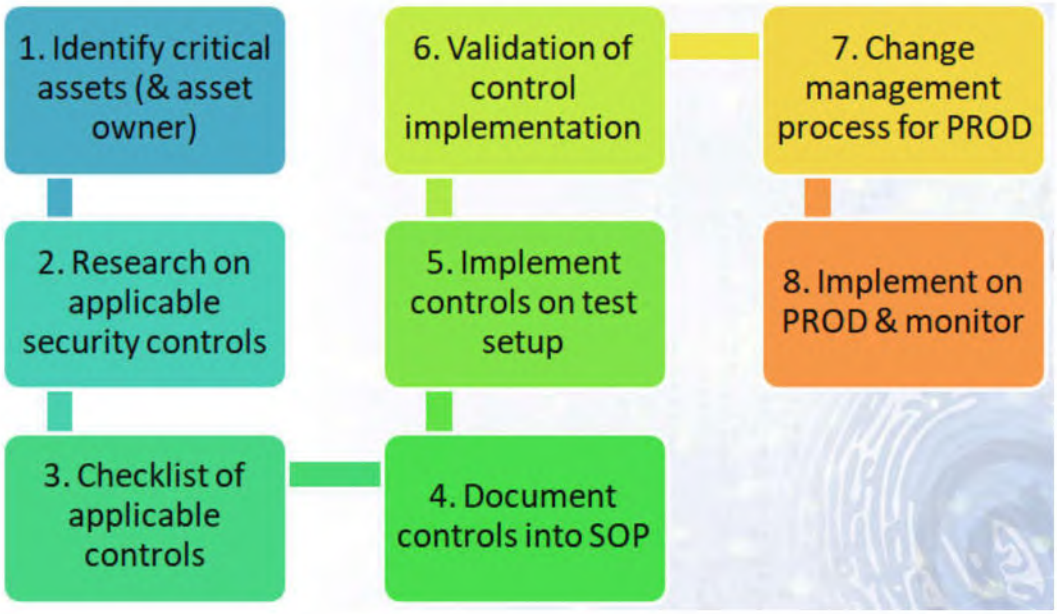
- This compliant solution uses java.util.logging.Logger, the default logging API provided by JDK 1.4 and later. Use of other compliant logging mechanisms, such as log4j, is also permitted.

- Typically, only one logger is required for the entire program.

Topic no 102: CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

- Carnegie Mellon Software Engineering Institute

- https://wiki.sei.cmu.edu/confluence/display/perl/SEI+CERT+Perl+Coding+Standard



Rules

- Rule 01. Input Validation and Data Sanitization (IDS)
- Rule 02. Declarations and Initialization (DCL)
- Rule 03. Expressions (EXP)
- Rule 04. Integers (INT)
- Rule 05. Strings (STR)
- Rule 06. Object-Oriented Programming (OOP)
- Rule 07. File Input and Output (FIO)
- Rule 50. Miscellaneous (MSC)

Recommendations

- Rec. 01. Input Validation and Data Sanitization (IDS)
- Rec. 02. Declarations and Initialization (DCL)
- Rec. 03. Expressions (EXP)
- Rec. 04. Integers (INT)
- Rec. 05. Strings (STR)
- Rec. 06. Object-Oriented Programming (OOP)
- Rec. 07. File Input and Output (FIO)
- Rec. 50. Miscellaneous (MSC)

- **Rule 1**
- IDS30-PL. Exclude user input from format strings
- Never call any formatted I/O function with a format string containing user input.
- An attacker who can fully or partially control the contents of a format string can crash the Perl interpreter or cause a denial of service. She can also modify values, perhaps by using the %n|| conversion specifier, and use these values to divert control flow. Their capabilities are not as strong as in C [Seacord 2005]; nonetheless the danger is sufficiently great that the formatted output functions {{sprintf() and printf() should never be passed unsanitized format strings.

```
my $host = `hostname`;
chop($host);
my $prompt = "$ENV{USER}\@$host";

sub validate_password {
  my ($password) = @_;
  my $is_ok = ($password eq "goodpass");
  printf "$prompt: Password ok? %d\n", $is_ok;
  return $is_ok;
};


if (validate_password( $ARGV[0])) {
  print "$prompt: access granted\n";
} else {
  print "$prompt: access denied\n";
};
```

- This **noncompliant code example** tries to authenticate a user by having the user supply a password and granting access only if the password is correct.

```
sub validate_password {
  my ($password) = @_;
  my $is_ok = ($password eq "goodpass");
  print "$prompt: Password ok? $is_ok\n";
  return $is_ok;
};

# ...
```

- This **compliant code example** avoids the use of printf(), since print() provides sufficient functionality.

Topic no 103: Case Study Security Hardening – Android

- CIS Benchmarks case study (Google Android 7)

- January 24, 2017
- 87 pages PDF doc
- *1.15 Ensure Android Device Manager is set to Enabled (Not Scored)*
- Profile applicability:
  - Level 2
  - **Description:** Setup **Android Device Manager** as a Device Administrator.
- **Rationale:**
  - If you lose your Android device, you could use Android Device Manager to find your device and also ring, lock, or erase your device data remotely.
- **Audit:** Follow the below steps to verify that Android Device Manager is enabled:

1. Tap the System Settings Gear Icon.
2. Scroll to Personal.
3. Tap Security.
4. Scroll to Device administration;
5. Tap Device administrators.
6. Verify that Android Device Manager is enabled.

- **Remediation:** Follow the below steps to enable Android Device Manager:

7. Tap the System Settings Gear Icon.
8. Scroll to Personal.
9. Tap Security.
10. Scroll to Device administration;
11. Tap Device administrators.

12. Tap Android Device Manager.
13. Tap Activate this device administrator.

- **Impact:**
  - Google may track your device location anytime.
- **Default Value:**
  - By default, Android Device Manager is not enabled.

Topic no 104: Case Study Security Hardening – Apple IOS 10

- CIS Benchmarks case study (Apple IOS 10)

- May 15, 2017
- 138 pages PDF doc
- *3.2.1.12 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Not Scored)*
- **Profile applicability:**
  - Level 2 - Institutionally Owned Devices
  - **Description:** This recommendation pertains to modifying the use of cellular data by apps.
- **Rationale:**
  - It is appropriate for an institution to have remote locating and erasure capability with their devices. Forcing cellular data to remain active is a means of supporting this goal.
- **Audit:**
  - From the Configuration Profile:

1. Open Apple Configurator
2. Open the Configuration Profile
3. In the left windowpane, click on the Restrictions tab.

4. In the right windowpane, verify that under the tab

Functionality, that the checkbox for Allow modifying cellular data app settings is unchecked. Or, from the device:

- Tap Settings.
- Tap General.
- Tap Profile.
- Tap <_Profile Name_>.
- Tap Restrictions.
- Confirm Changing app cellular data usage not allowed is displayed.

- **Remediation:**

  - Open Apple Configurator.
  - Open the Configuration Profile.
  - In the left windowpane, click on the Restrictions tab;
  - In the right windowpane, under the tab Functionality, uncheck the checkbox for **Allow modifying cellular data app settings.**
  - Deploy the Configuration Profile.

- **CIS Controls:**

- 5.1 Minimize And Sparingly Use Administrative Privileges Minimize administrative privileges and only use administrative accounts when they are required;
- Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior

Topic no 105: CASE STUDY – ASTERISK VOIP SECURITY HARDENING

1. Physically secure your IP PBX and network hardware

- The first step to security of your system

2. Never, Never, Never use the default passwords on any system. (Use Strong Passwords)

- This will stop most of the attacks as hackers use weak passwords to break in

3. Never use the same Username and password on your extensions

- "This is another VERY common issue, especially within the Asterisk community. Using password 101 for extension 101 is asking for big trouble. DON'T DO IT!"

4. Place your PBX behind a Firewall

- Use VPNs for remote access and limit to specific IP addresses
- Allow access on ports which are absolutely necessary
- Disable anonymous WAN requests (ICMP or PING) access to your IP PBX

5. Use the "permit=" and "deny=" lines in sip.conf

- "Use the "permit=" and "deny=" lines in sip.conf to only allow a small range of IP addresses access to extension/user in your sip.conf file. This is true even if you decide to allow inbound calls from "anywhere" (default), it won't let those users reach any authenticated elements!"

6. Keep inbound and outbound routing separate (asterisk)

- This is probably the biggest cause and source of toll fraud. By keeping your inbound call routing in a different context than your outbound routing, if an intruder does happen to make it into your system, he can't get back out again.

Topic no 106: CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

7. Limit registration by extensions to your local subnet.

- Restrict the IP addresses your extensions can register onto the local subnet. Asterisk PBXs can use the ACL (permit/deny) in SIP.conf to block IP addresses. This can fend off brute force registration attempts.

8. Disable channels and services that are not in use

- Disable channels that you aren't using like skinny and MGCP. For Asterisk PBXs, you can "unload" these modules in the /etc/modules.conf file

9. Make it harder for sip scanners (Set "alwaysauthreject=yes")

- Set "alwaysauthreject=yes" in your sip configuration file. What this does is prevent Asterisk from telling a sip scanner which extensions are valid by rejecting authentication requests on existing usernames with the same rejection details as with nonexistent usernames. If they can't find you they can't hack you!
- Another way to make it hard for SIP scanners is to install a SIP port firewall. This will block "scanning" of port 5060 and 5061 and can disable the attempting endpoint for a specific time when it detects a violation.

10. Limit and restrict routing and phone number dial plans

- Restrict calling to high-cost calling destination and don't allow calling to 0900 + Premium numbers)

11. Audit your system security regularly

Topic no 107: Version Control For IT Assets

- Benefits of version control
- Security implications
- **Benefits of version control**
    - http://its.unl.edu/bestpractices/version-management

    1. Organized, coordinated management of changes to software assets by one or many individuals, some of whom may be geographically dispersed
    2. Organized, coordinated management of changes to software assets for emergency hot-fixes, routine maintenance, upgrades …& new features with potentially overlapping dev timeframes (e.g., work on new features occurs simultaneously with work on routine maintenance and/or hot-fixes)
    3. An auditable change history (e.g., what changed, when, and by whom)
    4. A reliable master copy of what assets are currently in production
    5. A reliable master copy of assets from which to build and/or configure the production environment
    6. Reliable copies of previous production versions of assets
    7. Ability to see the specific differences between distinct versions of a given asset
- Security controls:
    - Access control measures
    - Privileged management
    - Backups

Topic no 108: Version Control Best Practices

- **Version control best practices**
  - https://intland.com/blog/sdlc/source-control-management-best-practices/

1. Starting with the basics, choose a source control system.
2. Keep your source code in source control (but not files generated / compiled from it).
3. Ensure the working file is from the latest version of the source file.
4. Only Check-out the file being worked upon.
5. Check in immediately after alterations are completed.
6. Review every change before committing, utilize the diff function!
7. Commit often, – every commit provides a rollback position.
8. Make extensive, – detailed notes in the check-in comments about why the changes were made.
9. Developers must commit their own changes (only).
10. Use the ignore button for files that should not be committed, consider adding pre-commit filters to prevent the wrong kinds of file (such as accidental check-in of personal user settings docs) from entering the source control
11. Ensure external dependencies are added to the source control, a common problem where everything works great on the contributing developers system but not elsewhere because they forgot to add dependent files to the system.

Topic no 109: SECURITY HARDENING - SECURE SOFTWARE IMAGES

- CIS 20 CRITICAL SECURITY CONTROLS
- CONTROL 5, VERSION 7
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

5.1 Establish Secure Configurations

- Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.2 Maintain Secure Images

- Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.

5.3 Securely Store Master Images

- Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.

5.4 Deploy System Configuration Management Tools

- Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

5.5 Implement Automated Configuration Monitoring Systems

- Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Topic no 110: SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Manual & Automated mechanisms for security hardening & validation
- **Step 1:** Scan an IT asset using Qualys compliance scan, NESSUS compliance scan, or CIS CAT PRO Tool
    - Acquire report of failed controls
- **Step 2:** Apply the failed controls using AD (for Windows) or manually for other systems & devices
- **Step 3:** Use the automated feature of Qualys compliance scan, Nessus compliance scan or CIS CAT Pro Tool to verify that the applied controls are in place

- Compare the ‘before’ and ‘after’ report

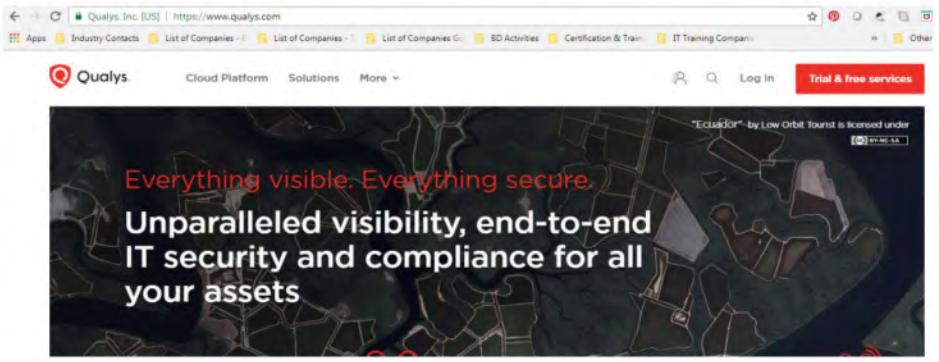
- **Step 4:** Manually verify if any discrepancy is found (control should be in place but not being validated by the tool)

- **Step 5:** For any system or device for which the Qualys compliance scan, Nessus compliance scan, or CIS CAT Pro Tool scan cannot be performed, conduct the validation of control implementation manually

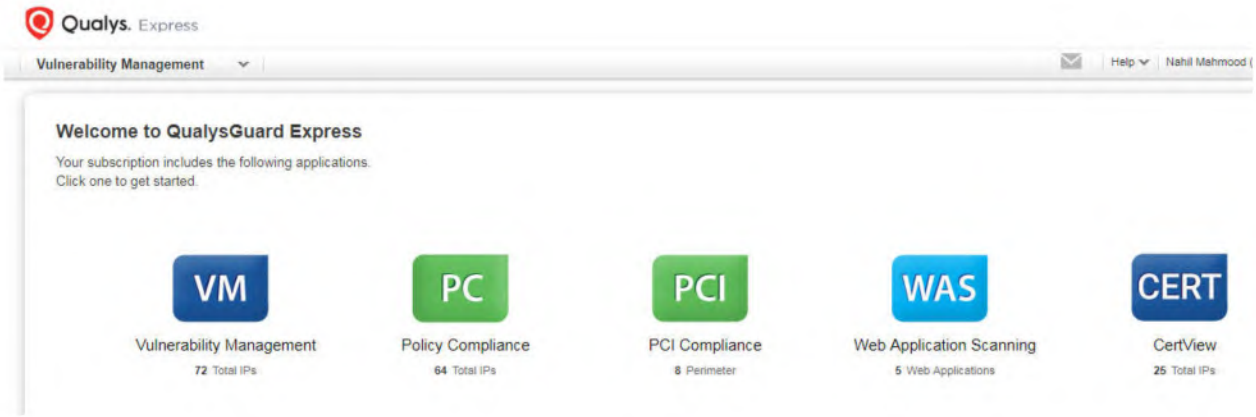
  - Use sampling where necessary during manual validation work to reduce workload
  - For example, 15-20 % of assets may be checked at random
  - Or 15-20% of controls may be checked on an asset

Topic no 111 & 112 : QUALYS DEMO – SECURITY HARDENING

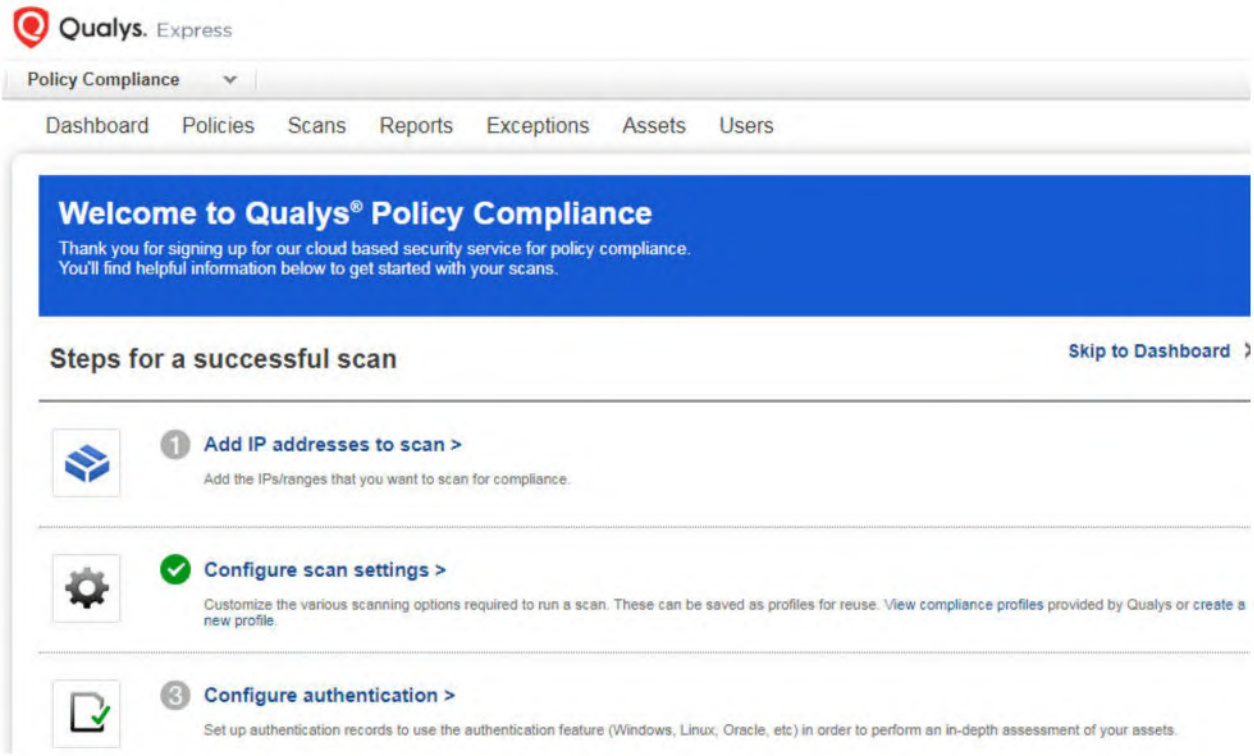
- Lets have a look at how Qualys can aid in the security hardening process



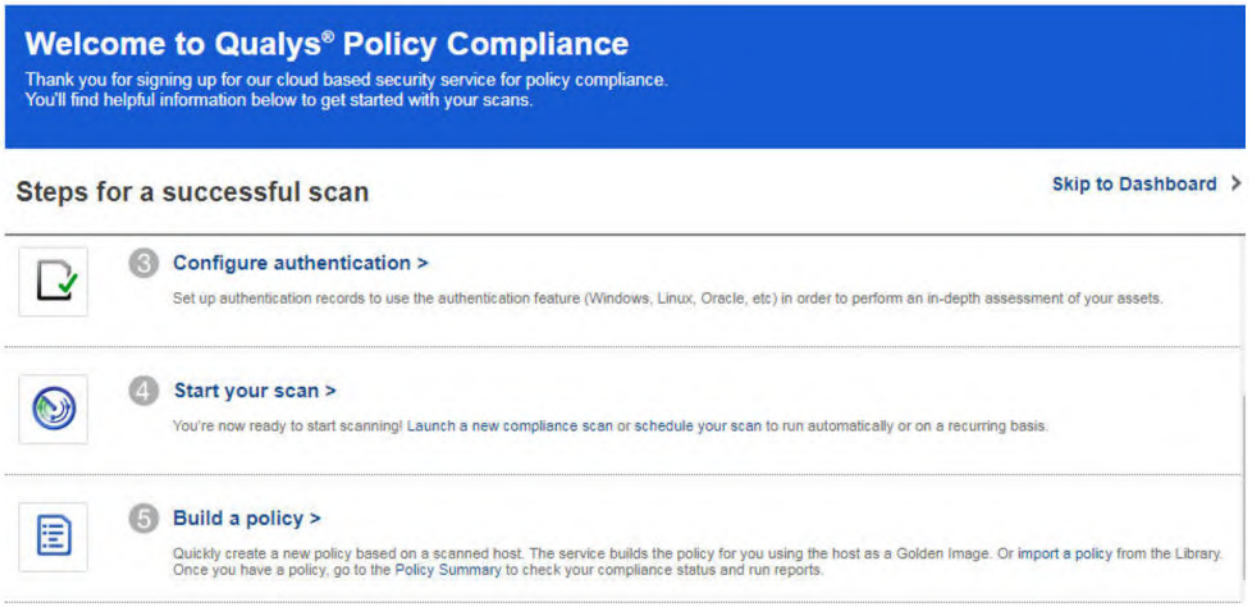
QUALYS WEBSITE – FREE TRIAL



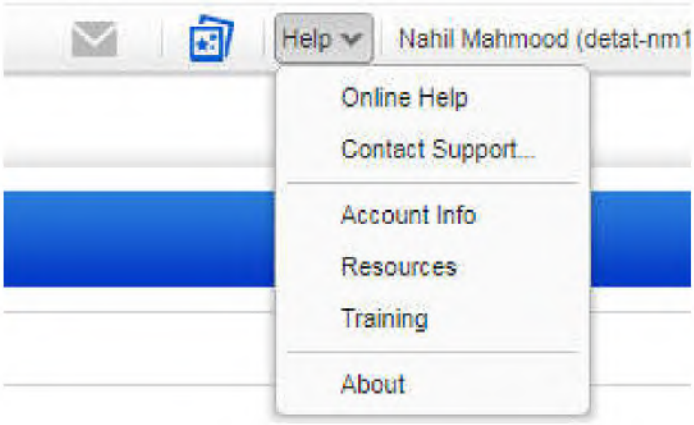
QUALYS GUARD – HOME SCREEN



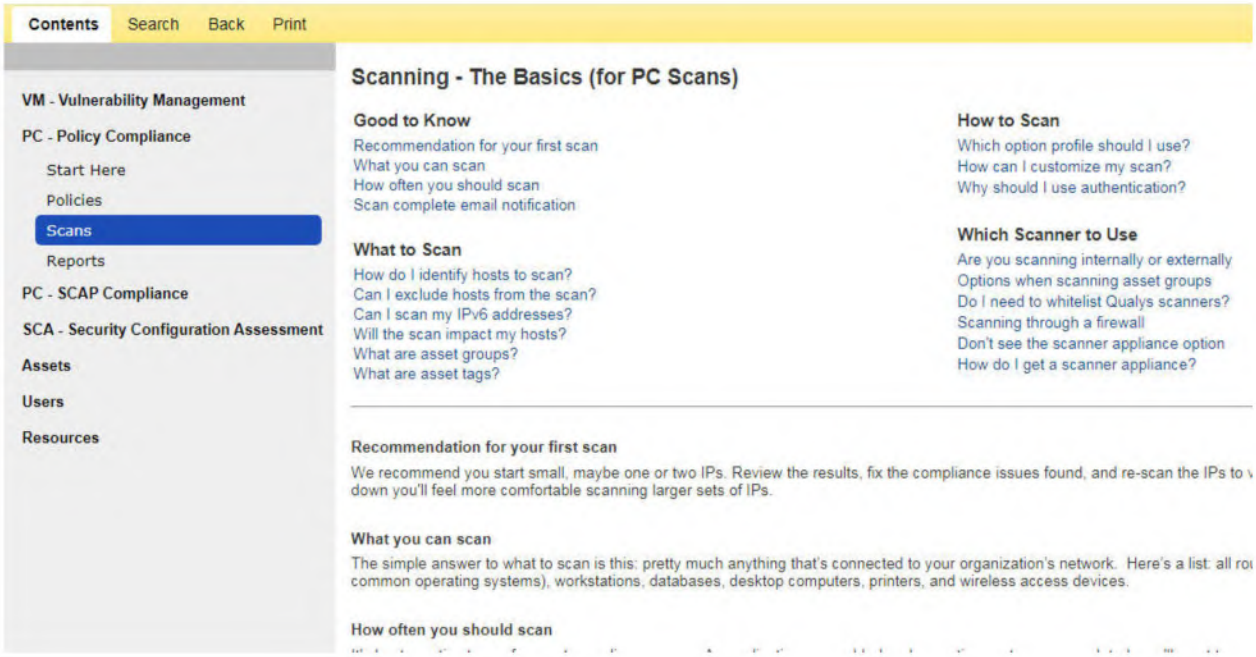
POLICY COMPLIANCE – HOME SCREEN



POLICY COMPLIANCE – 5 STEPS



HELP OPTIONS



ONLINE HELP – POLICY COMPLIANCE

Resources

Look to these resources to help you with our cloud security and compliance solutions.

Get Started
Quick Tour
Evaluator's Guide
Community Edition
Securing Amazon Web Services with Qualys

Watch Videos
VM | PC | WAS | WAF | AWS EC2 | Express Lite | More Videos

Get started with your applications
CloudView
Container Security
Indication of Compromise
Web Application Scanning
- Crawling REST services using WAS
- Jenkins Plugin for WAS: user guide | download
- Qualys Browser Recorder: user guide | download
Web Application Firewall
Policy Compliance
SCAP Compliance
Security Configuration Assessment
PCI Compliance
File Integrity Monitoring

Scan Authentication
Get system and account requirements for supported technologies below.

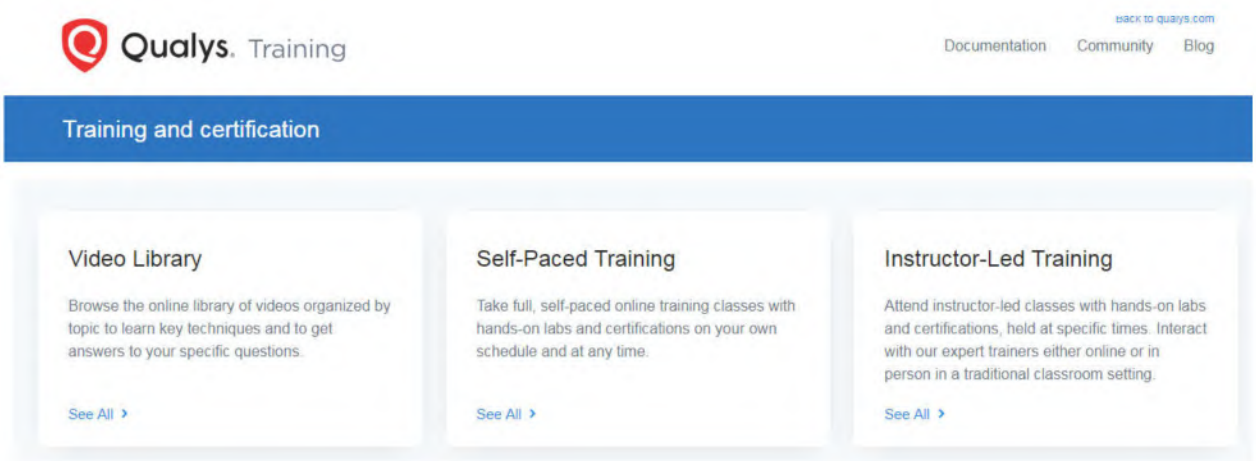
Cloud Agents
Cloud Agent Getting Started Guide
Windows Installation Guide
Linux Installation Guide
Unix Installation Guide
Mac Installation Guide

Using a scanner appliance?
Scanner Appliance User Guide
Scanner Appliance Quick Start (prior version)
Virtual Scanner Appliance User Guide
Offline Scanner Appliance User Guide
Consultant Scanner Personal Edition User Guide
Cloud Platforms: AWS | Azure | GCE | OpenStack
Qualys Scanner - Static Route Configuration
Qualys Scanner - VLAN Scanning Guide
Scanner Appliance FAQs

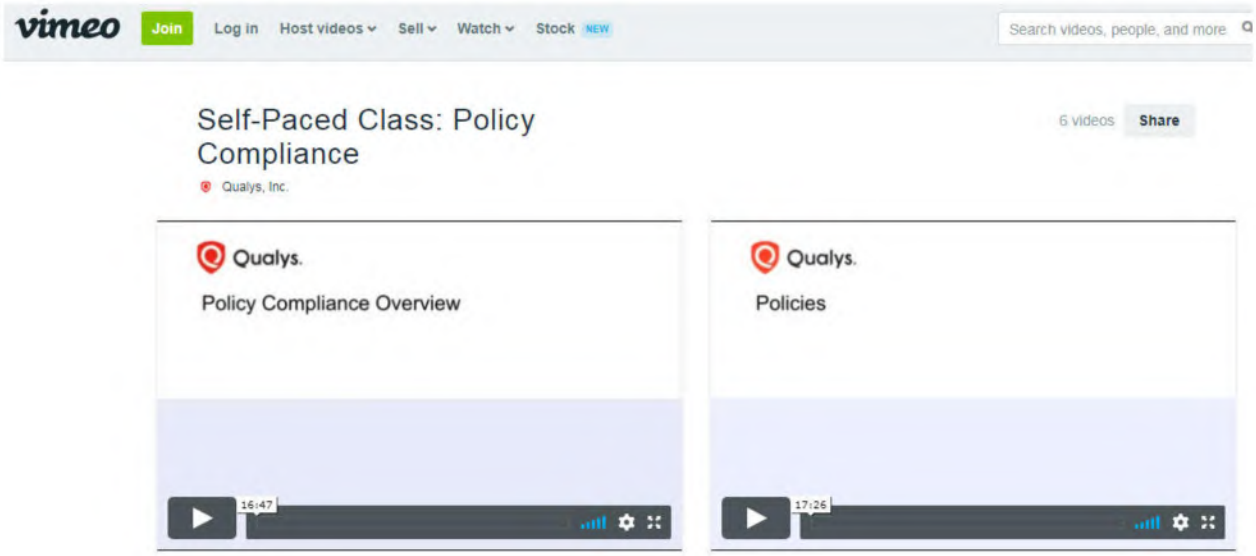
API Documentation
Qualys API Quick Reference for all APIs
Qualys API (VM, SCA, PC)

Cloud Agent (CA) API
Web Application Scanning (WAS) API
Web Application Firewall (WAF) API
Malware Detection (MD) API

RESOURCES

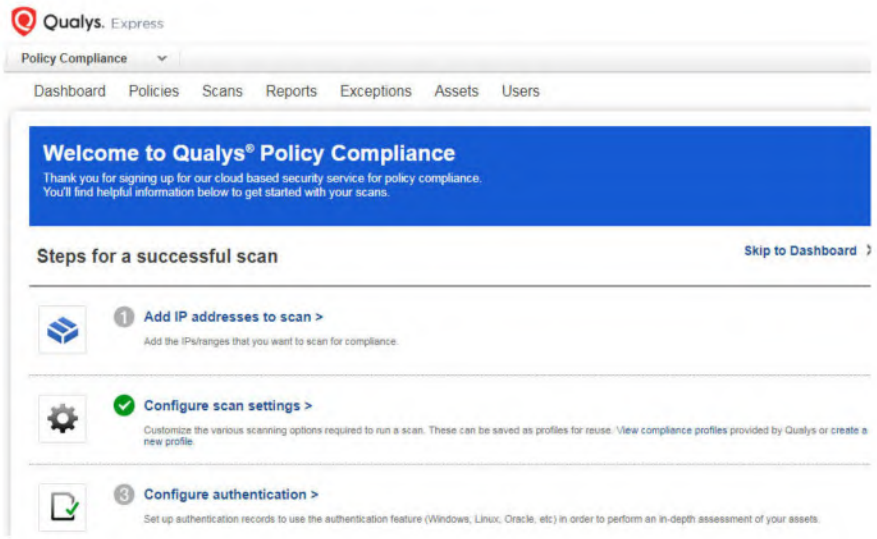


QUALYS WEBSITE - TRAINING

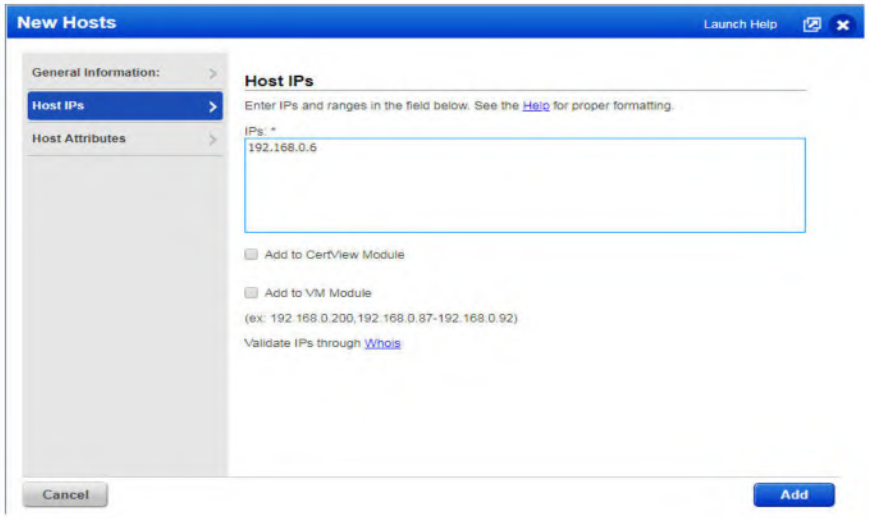


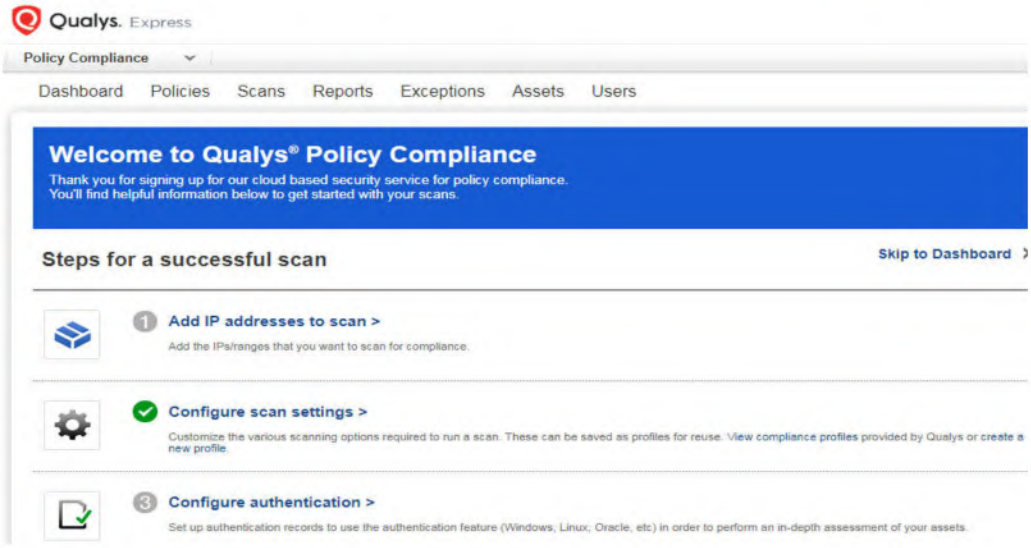
TRAINING VIDEOS - VIMEO

- Qualys is an excellent tool with detailed online help, training, and resources to aid the new user

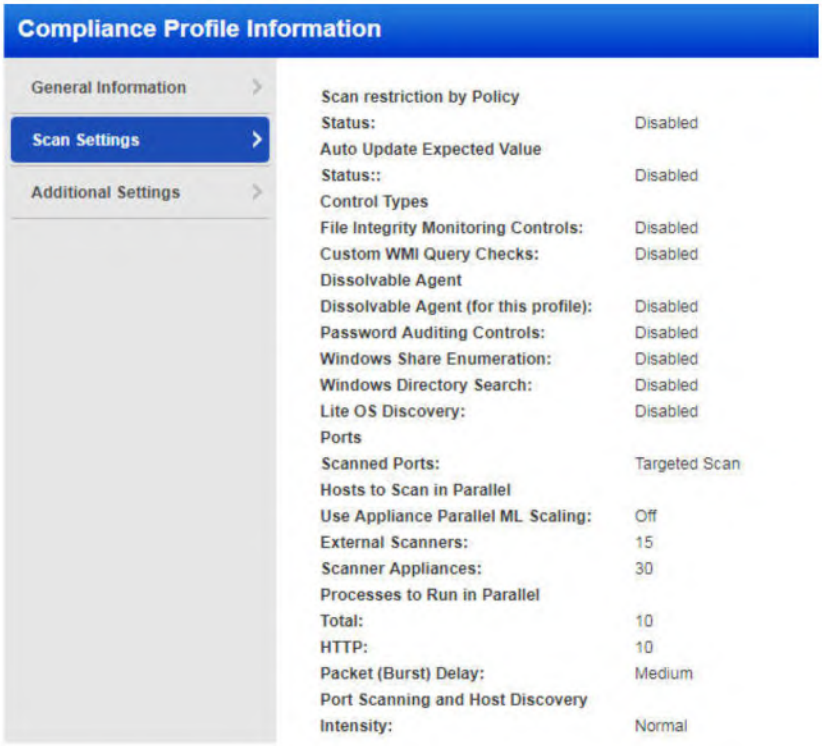


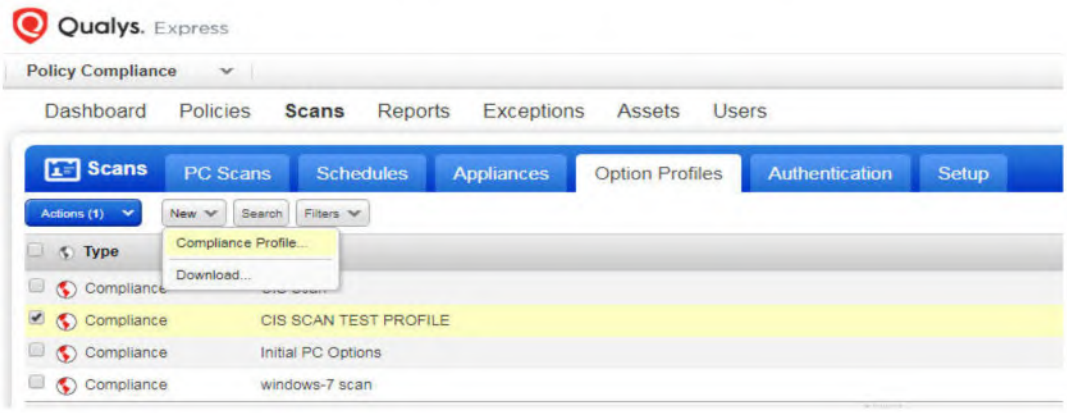
1. ADD IP ADDRESSES TO SCAN



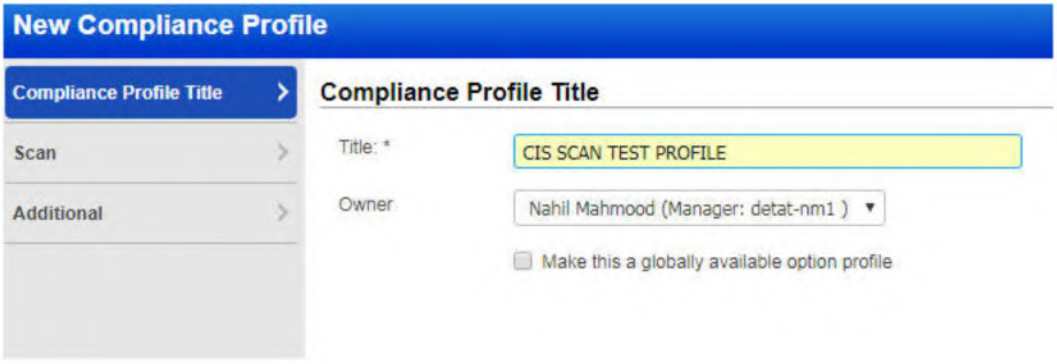


2. CONFIGURE SCAN SETTINGS

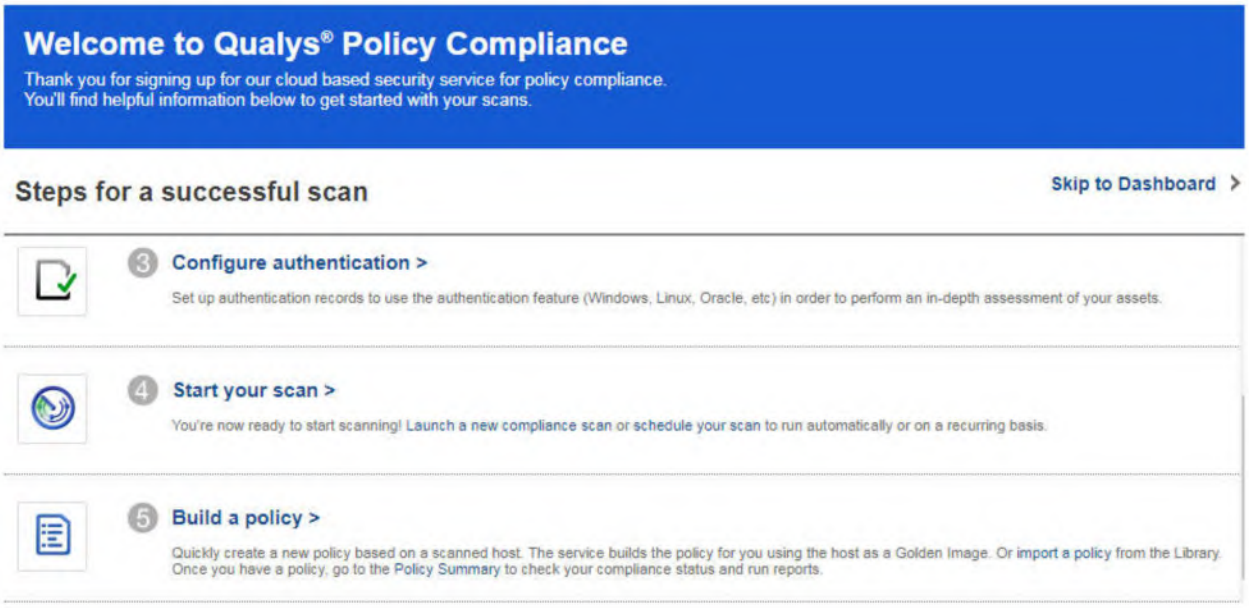




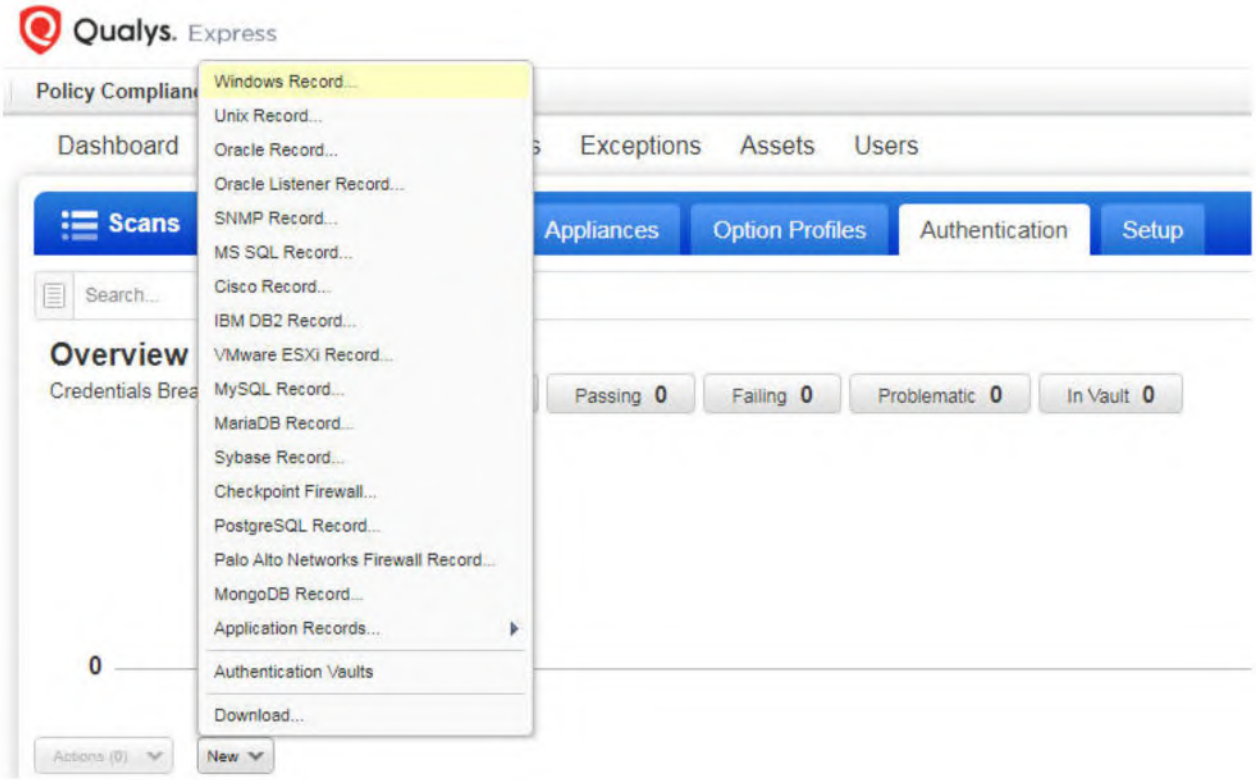
NEW COMPLIANCE PROFILE

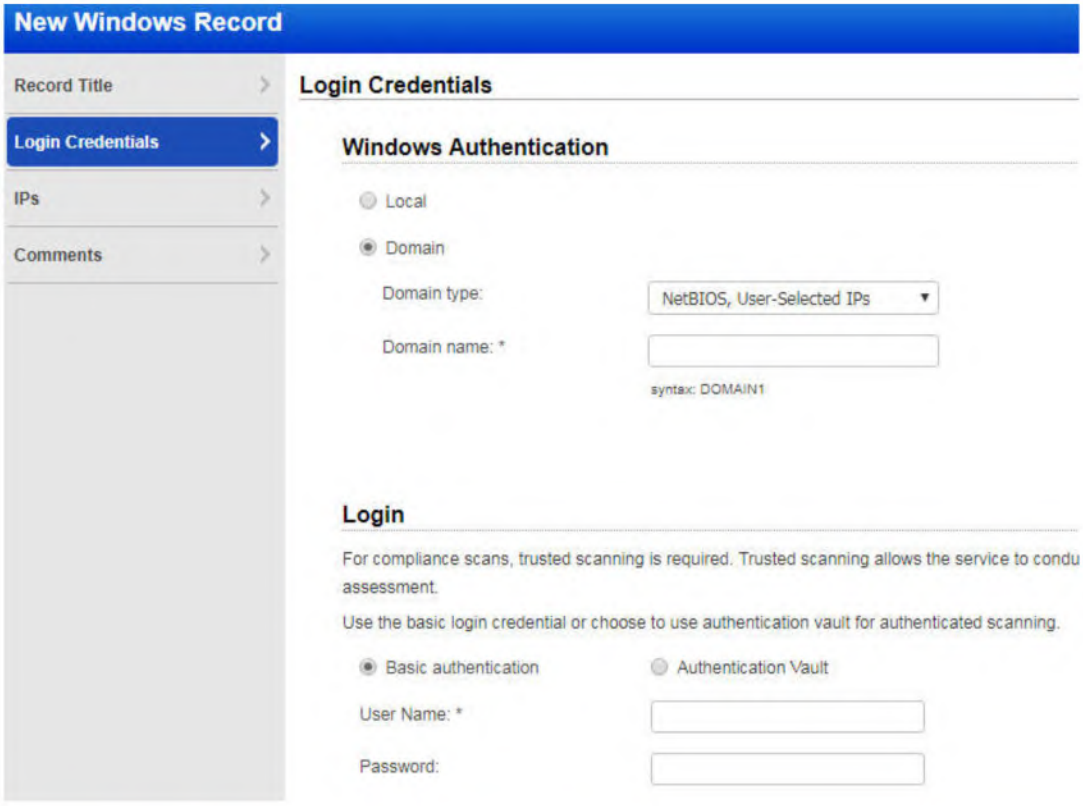


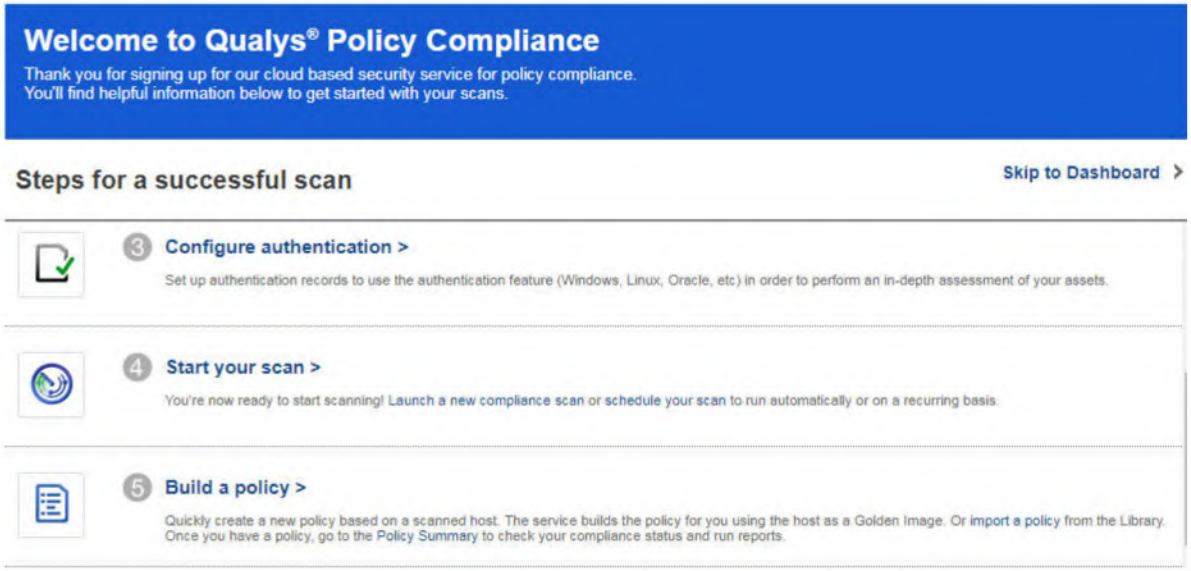
'CIS SCAN TEST PROFILE' CREATED

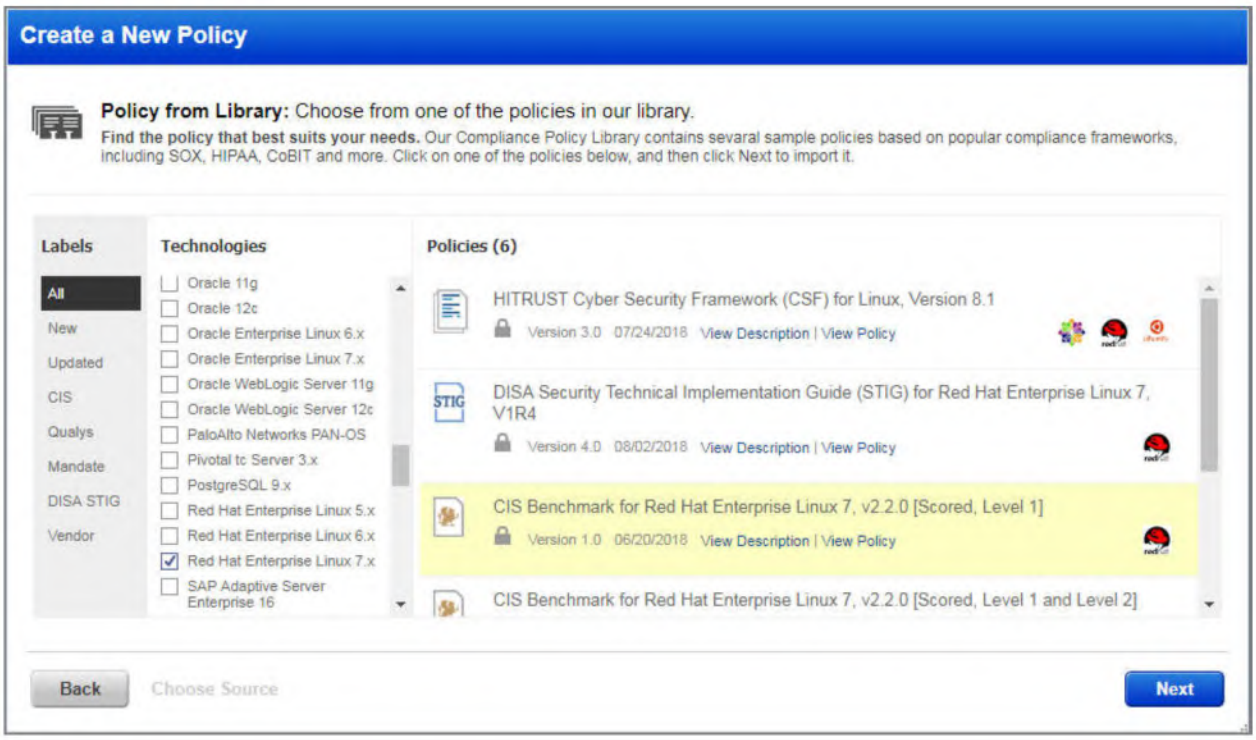


3. CONFIGURE AUTHENTICATION

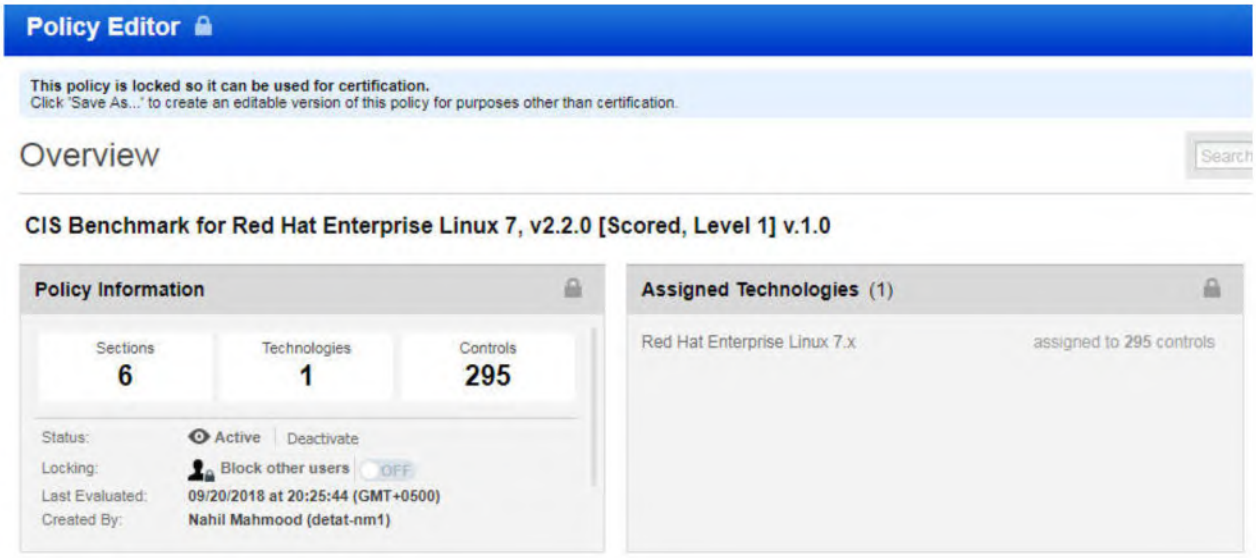



New Windows Record
Record Title
Login Credentials
IPs
Comments
Login Credentials
Windows Authentication
Local
Domain
Domain type:
NetBIOS, User-Selected IPs
Domain name: *
syntax: DOMAIN1
Login
For compliance scans, trusted scanning is required. Trusted scanning allows the service to condu
assessment.
Use the basic login credential or choose to use authentication vault for authenticated scanning.
Basic authentication
Authentication Vault
User Name: *
Password:

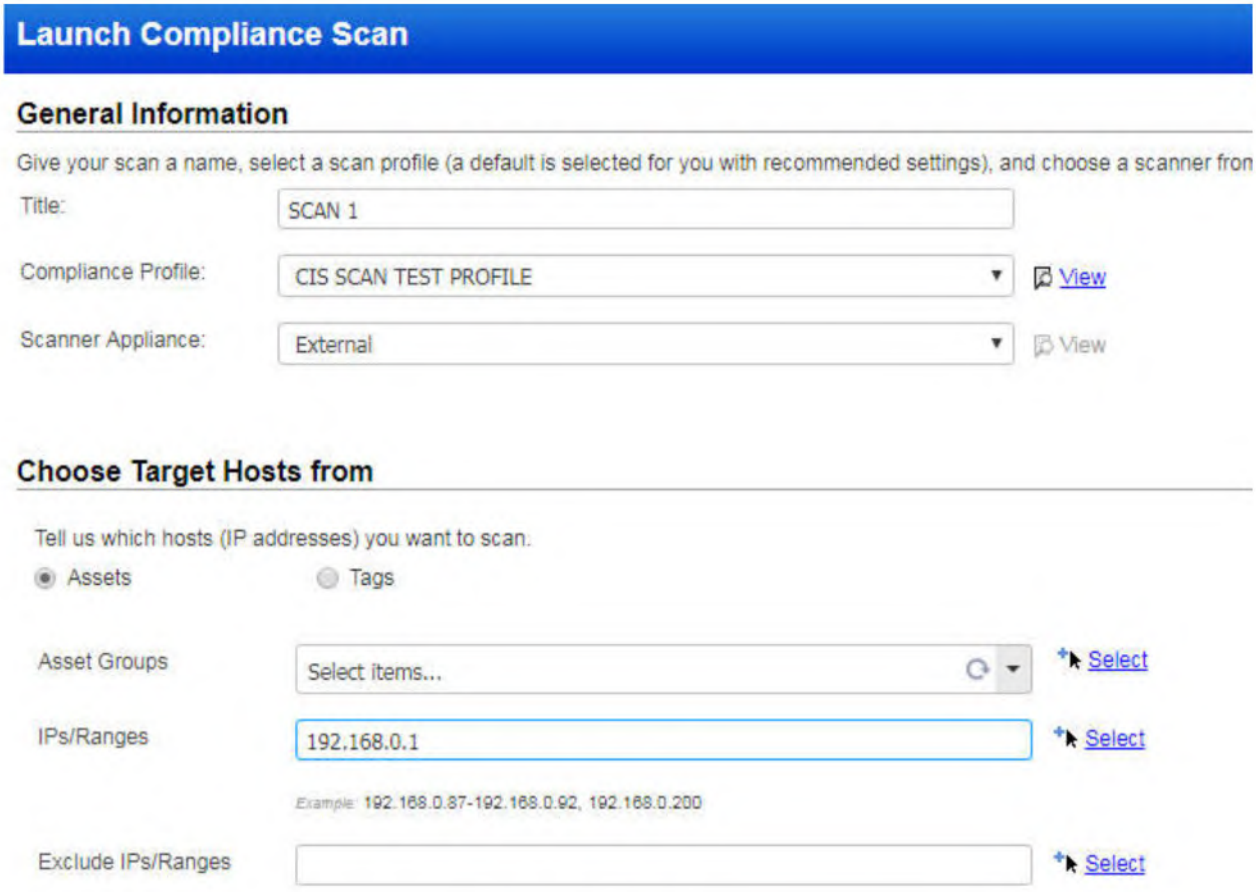

Welcome to Qualys® Policy Compliance
Thank you for signing up for our cloud based security service for policy compliance.
You'll find helpful information below to get started with your scans.
Steps for a successful scan
Skip to Dashboard
3 Configure authentication >
Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.
4 Start your scan >
You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.
5 Build a policy >
Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library.
Once you have a policy, go to the Policy Summary to check your compliance status and run reports.



COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7



POLICY EDITOR



LAUNCH COMPLIANCE SCAN

- The scan features may also be adjusted from the main Qualys dashboard

Topic no 113: SECURITY HARDENING – LIFECYCLE

- Security Hardening Lifecycle: Maintaining An Integrated & Current Program

1: Harden IT Asset

Pursue the 8 step hardening methodology

2: Periodic Validation

Check periodically (every quarter) for changes to the established standard or baseline

3: Seek Updated On Hardening Benchmarks

- Benchmarks are periodically updated
- Subscribe to feeds from CIS, DISA, NIST NCP (National Checklist Program) Repository

4: Implement Additional Controls

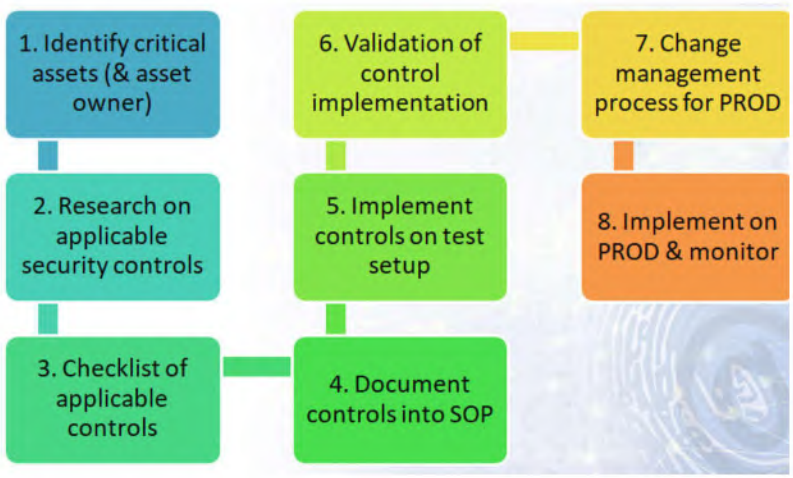
- Update the security controls by studying the changes

5: Pursue & Implement Controls That May Require Additional Working

- Some controls may have caused a crash or malfunction
- Some controls may have not been possible due to dependencies or missing utilities
- Enhance the % of implemented controls

Topic no 114: Hardening When CIS/DISA STIG Not Available

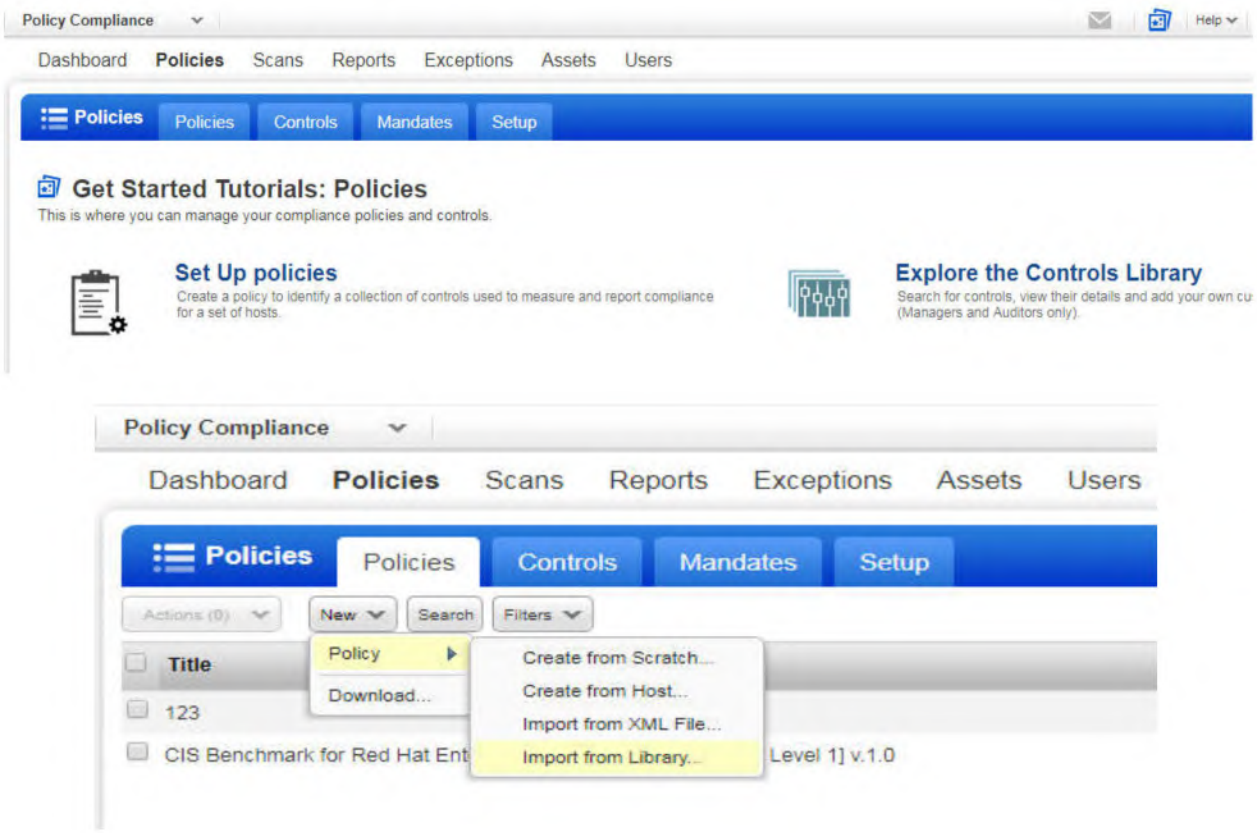
- What type of IT assets do not have a CIS/DISA STIG ?
  - Software applications (ASP.NET, PHP, Other)
  - Other applications such as asterisk deployments



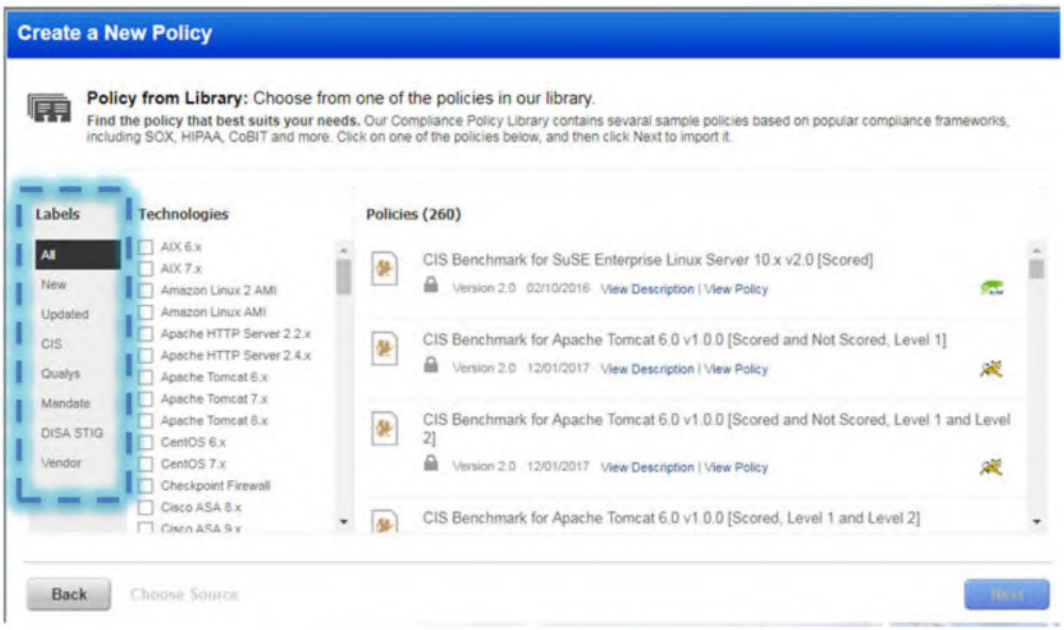
- **Step 2: Research:**
  - Look up google
  - Look for case studies and whitepapers
- **Other considerations:**
  - Implement on test setup
  - Test the controls
  - Security testing tools
  - Perform third-party security testing (penetration testing)
  - Vendor best-practices for application security hardening
- With efforts and by following the 8-step methodology, all types of assets can be hardened

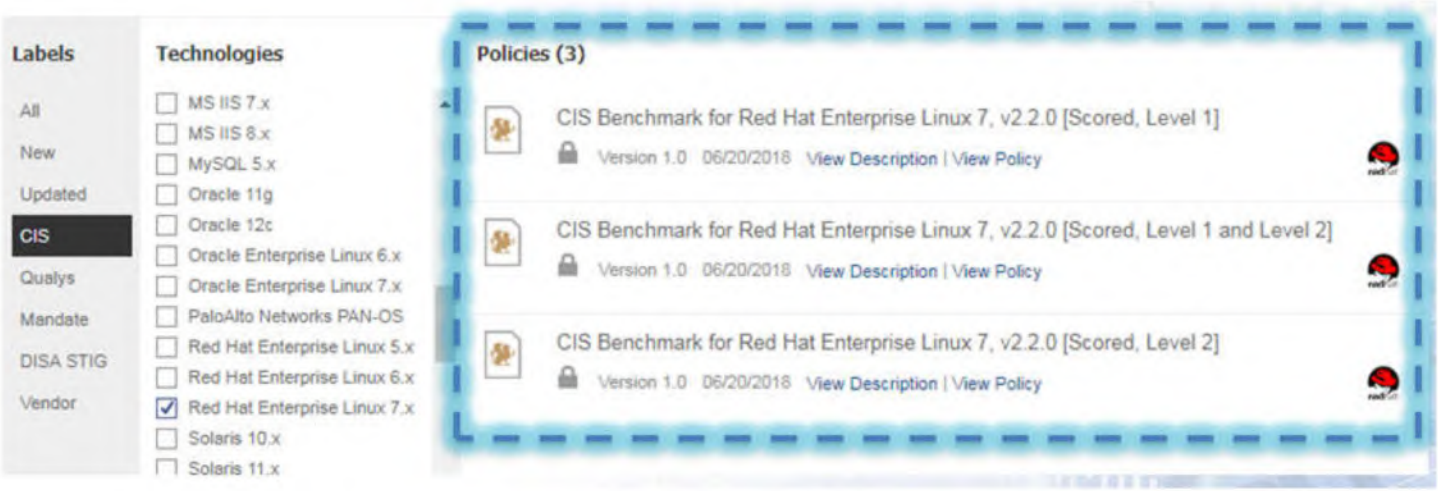
Topic no 115: QUALYS POLICY LIBRARIES

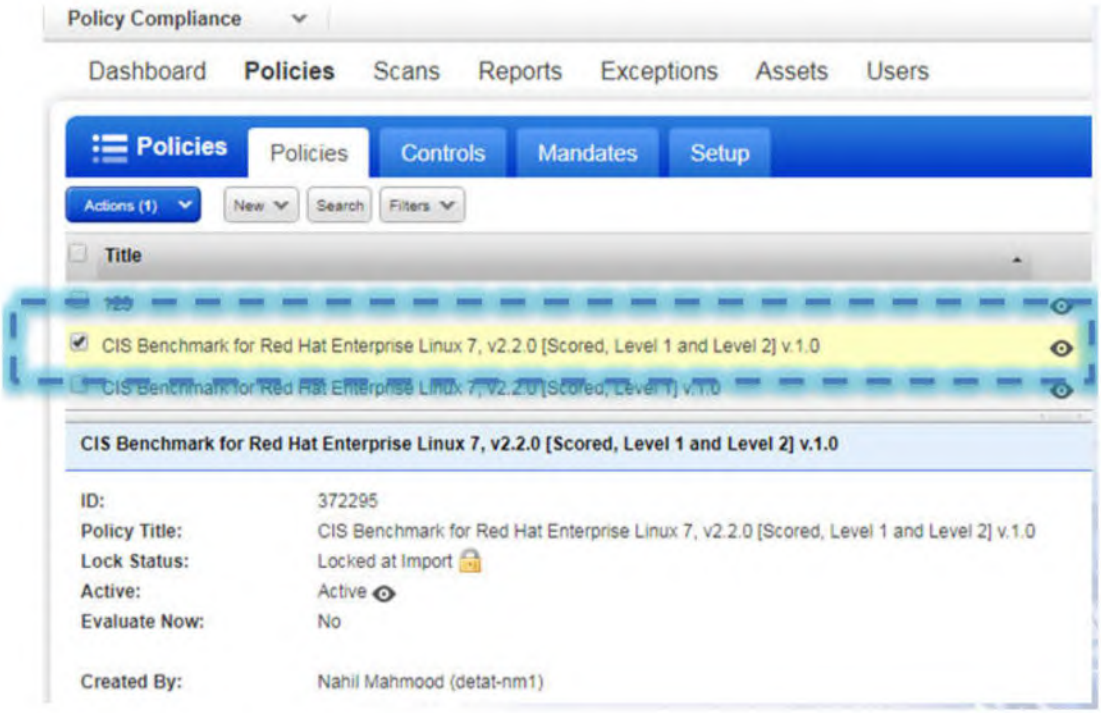
- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR



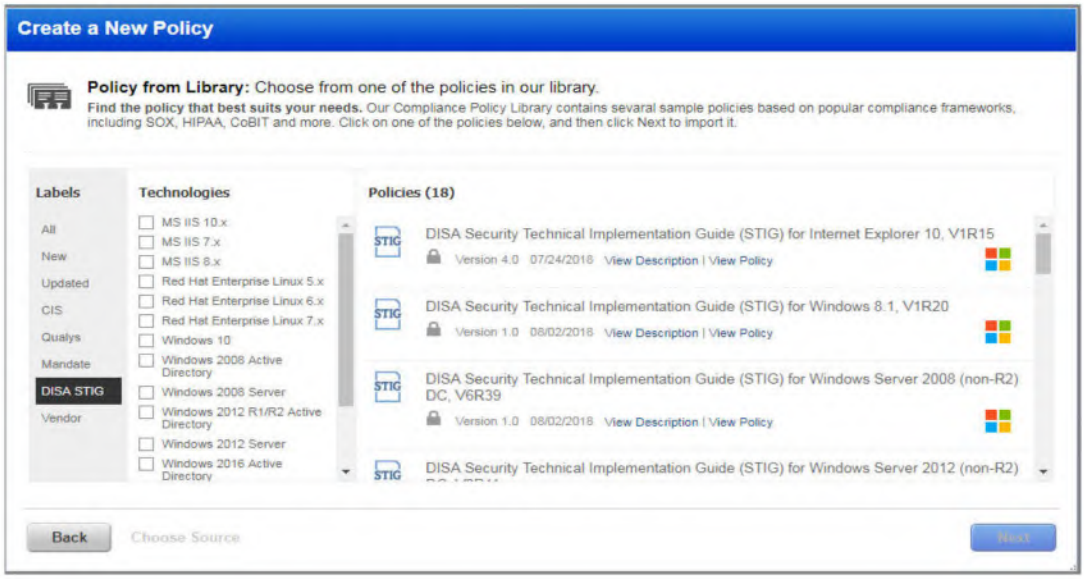
CREATE NEW POLICY > IMPORT FROM LIBRARY


Create a New Policy
Policy from Library: Choose from one of the policies in our library.
Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.
Labels
All
New
Updated
CIS
Qualys
Mandate
DISA STIG
Vendor
Technologies
AIX 6.x
AIX 7.x
Amazon Linux 2 AMI
Amazon Linux AMI
Apache HTTP Server 2.2.x
Apache HTTP Server 2.4.x
Apache Tomcat 6.x
Apache Tomcat 7.x
Apache Tomcat 8.x
CentOS 6.x
CentOS 7.x
Checkpoint Firewall
Cisco ASA 8.x
Policies (260)
CIS Benchmark for SuSE Enterprise Linux Server 10.x v2.0 [Scored]
Version 2.0 02/10/2016 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]
Version 2.0 12/01/2017 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 and Level 2]
Version 2.0 12/01/2017 View Description | View Policy
CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]
Back
Choose Source

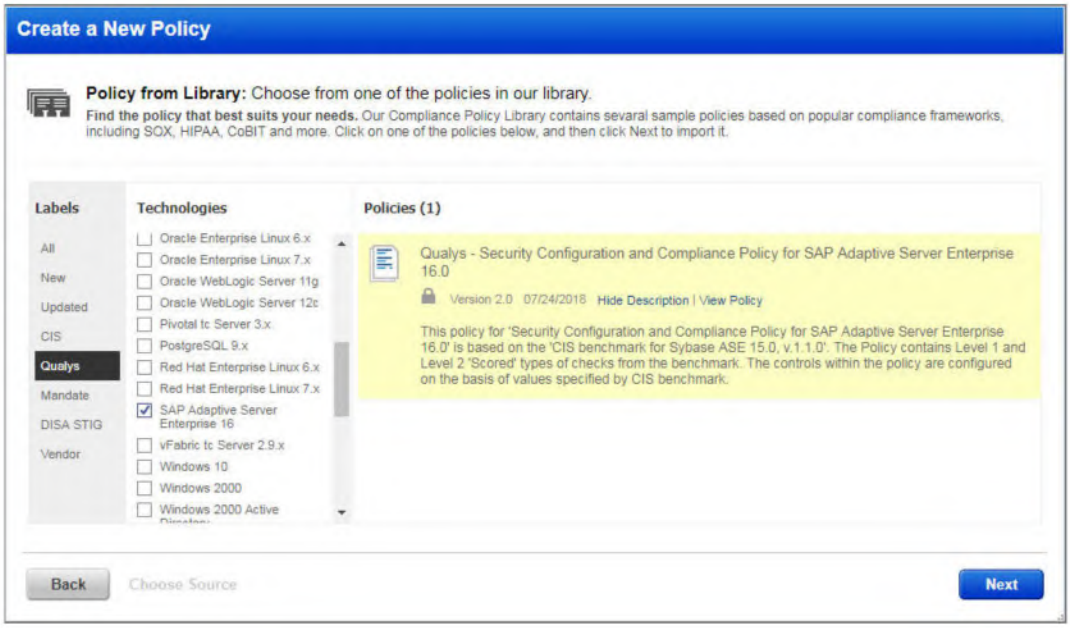

Labels
All
New
Updated
CIS
Qualys
Mandate
DISA STIG
Vendor
Technologies
MS IIS 7.x
MS IIS 8.x
MySQL 5.x
Oracle 11g
Oracle 12c
Oracle Enterprise Linux 6.x
Oracle Enterprise Linux 7.x
PaloAlto Networks PAN-OS
Red Hat Enterprise Linux 5.x
Red Hat Enterprise Linux 6.x
Red Hat Enterprise Linux 7.x
Solaris 10.x
Solaris 11.x
Policies (3)
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1]
Version 1.0 06/20/2018 View Description | View Policy
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]
Version 1.0 06/20/2018 View Description | View Policy
CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 2]
Version 1.0 06/20/2018 View Description | View Policy



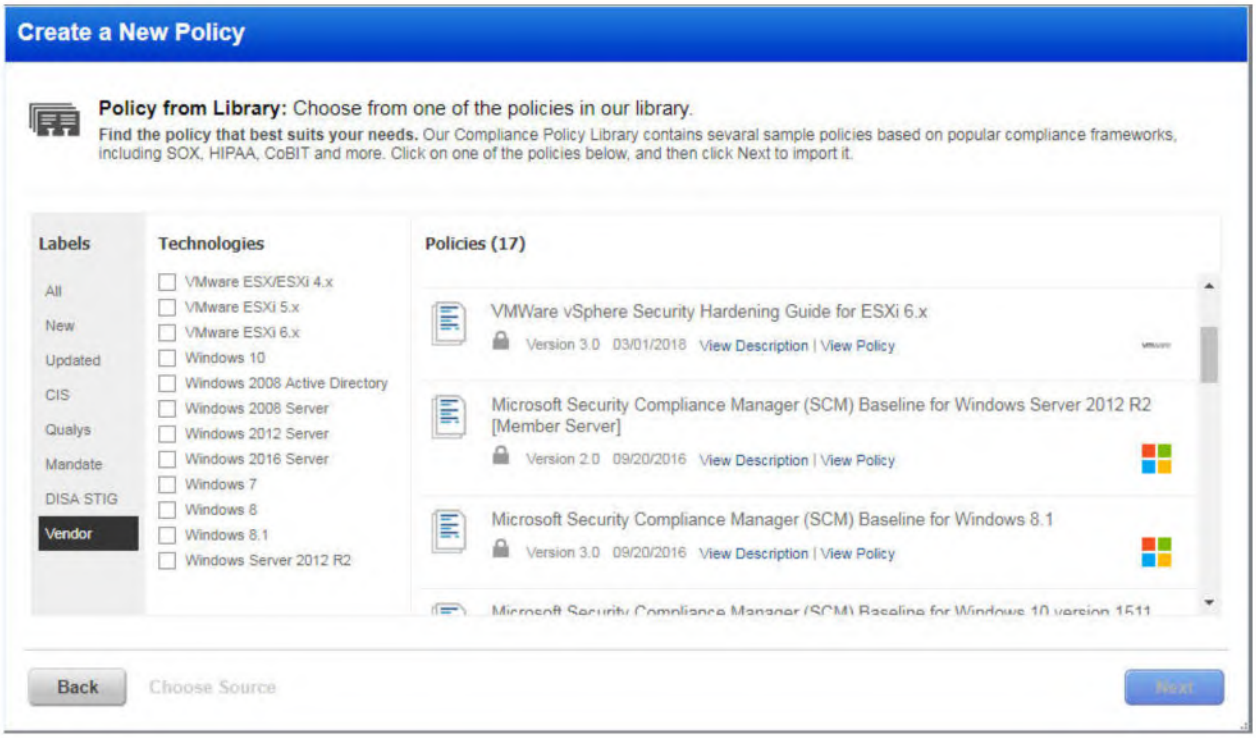
POLICIES DASHBOARD



DISA STIG



QUALYS SAP ADAPTIVE SERVER ENT 16



VENDOR POLICIES

- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

Topic no 116: Security Hardening For Outsourced IT Assets

- IT Outsourcing
- Mechanism to harden outsourced IT assets
- Important considerations
- **IT Outsourcing examples:**
  - Call centers
  - Hosted servers
  - Software development
  - Workstation helpdesk functions
  - Network services
  - Any other arrangement
- **Mechanism:**
  - Information Security Policy
  - Vendor contract (right-to-audit clause)
  - Set up security project with security project manager
  - Periodic reviews
  - Penalties for non-compliance
- **Important considerations:**
  - Enter security requirements into RFP
  - Part of vendor evaluation
  - Proceed with contract including InfoSec clauses
  - Awareness training
- **Security evaluations:**
  - Include outsourced scope in periodic internal audit
  - Ask for third-party security review
  - Vulnerability assessment and penetration test (if applicable)
  - Spot security checks

Topic no 117: What is Vulnerability Management?

- **What is vulnerability?**
  - Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures or in anything that leaves information security exposed to a threat.

- **How do you fix vulnerabilities?**
  - Computer users and network personnel can protect computer systems from vulnerabilities by keeping software security patches up to date. These patches can remedy flaws or security holes that were found in the initial release. Computer and network personnel should also stay informed about current vulnerabilities in the software they use and seek out ways to protect against them.

- **What is vulnerability management?**
  - Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities"

- **What is vulnerability assessment (VA)?**
  - A process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

- **What are some of the common vulnerability scanners?**
  - OpenVAS
  - Nessus
  - Qualys
  - Rapid7

Topic no 118: What Are The Steps In VM Lifecycle?

VM Steps:

1. Analyze assets
2. Prepare scanner
3. Run vulnerability scan
4. Assess results
5. Patch systems
6. Verify (re-scan)

1. **Analyze Assets:**
   - Examine assets to scan
   - Gather details on IP subnet
   - Look at potential issues with network traffic
   - Inform asset owners and relevant department heads

2. **Prepare Scanner:**
   - Set scanner parameters
   - Select type of scan
   - Look at credentials-based scan
   - Explore and research plug-ins
   - Do a test run
   - Coordinate with asset owner

3. **Run Vulnerability Scanner:**
   - Run the automated scan
   - Monitor network performance degradation issues
   - Generate report

4. **Assess Results:**
   - Evaluate results
   - Prioritize according to the risk level
   - Collate results for asset owners
   - Communicate the results and remediation timelines

5. **Patch Systems:**
   - Research vulnerabilities
   - Evaluate fixes and remediation method
   - Test the patches and fixes
   - Apply patches/fixes
   - Monitor results

6. **Verify (Re-scan)**
   - Re-scan to confirm that the vulnerability scanner gives a positive report
   - Collate results of vulnerability scan
   - Report findings

Topic no 119: Why Is Software Insecure?

- Software is everywhere in IT
- Software is being developed in a manner which leaves many defects which may be exploited by attackers
- Race to meet software deadlines with little emphasis on security
- **Result:** insecure software
- Gary McGraw, "trinity of trouble" for software security:
  - **Connectivity;** ever-increasing computer connectivity & to the internet enhances exposure to attacks

- **Extensibility: "**Second, an extensible system is one that supports updates and extensions and thereby allows functionality to evolve incrementally. Web browsers, for example, support plug-ins that enable users to install extensions for new document types. Extensibility is attractive for purposes of increasing functionality, but also makes it difficult to keep the constantly-adapting system free of software vulnerabilities."

- **Complexity:** Software systems are growing exponentially in size and complexity, which makes vulnerabilities unavoidable.

- Carnegie Mellon University's CyLab Sustainable Computing Consortium estimates that commercial software contains 20 to 30 bugs for every 1,000 lines of code and Windows XP contains at least 40 million lines of code That's 1 million bugs in Windows XP

- **Monoculture: Dan Greer:** "The security situation is deteriorating, and that deterioration compounds when nearly all computers in the hands of end users rely on a single operating system subject to the same vulnerabilities the world over."

Topic no 120: Why Is A VM Program Required?

- **What is a patch?**
  - "A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing **security** vulnerabilities and other bugs"

- **What is patch management?**

  - Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

- **Patch management tasks :**

  - Maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.
- **Risk of not patching:**

  - By not applying a patch you might be leaving the door open for a malware attack

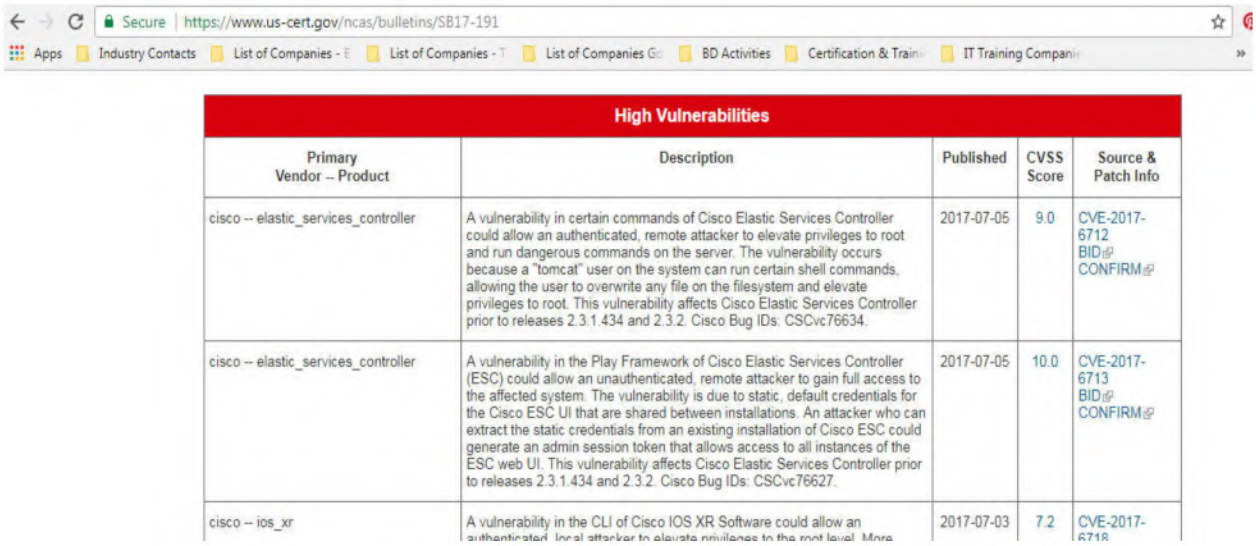
- Malware exploits flaws in a system in order to do its work. In addition, the timeframe between an exploit and when a patch is released is getting shorter
- Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer with no action on your part other than viewing or listening to the website, message, or media

A VM program addresses timely management of patching to ensure that vulnerabilities are not present for hackers to exploit

Topic no 121: What Is CVE & Vulnerability Database?

- **What is CVE?**
  - CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

SNAPSHOT OF US-CERT VULNERABILITY BULLETINS

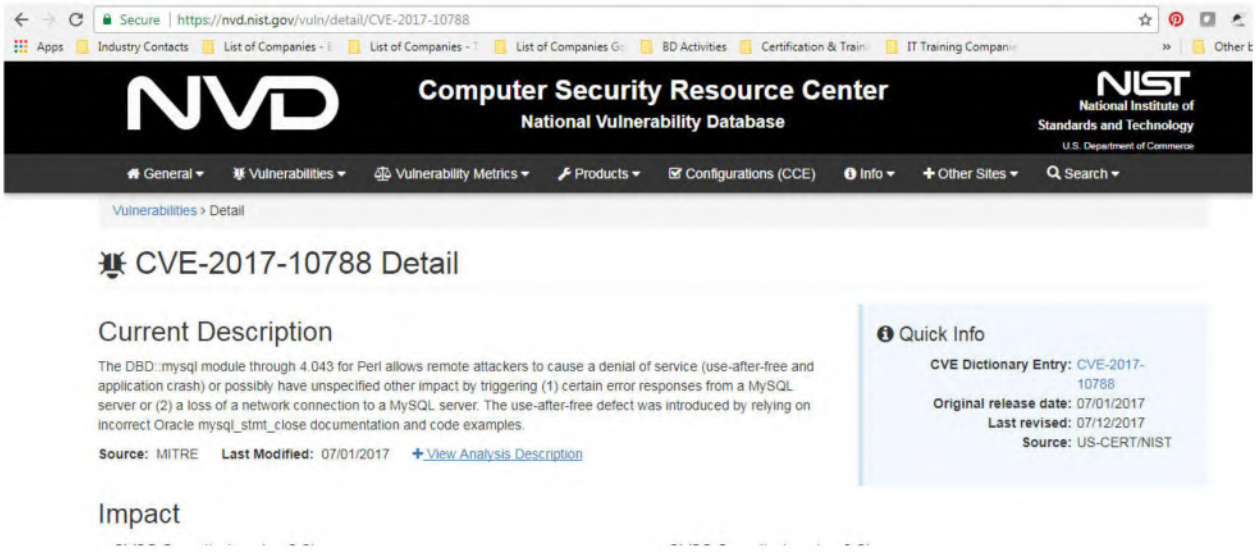


High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- elastic_services_controller	A vulnerability in certain commands of Cisco Elastic Services Controller could allow an authenticated, remote attacker to elevate privileges to root and run dangerous commands on the server. The vulnerability occurs because a "tomcat" user on the system can run certain shell commands, allowing the user to overwrite any file on the filesystem and elevate privileges to root. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76634.	2017-07-05	9.0	CVE-2017-6712 BID CONFIRM
cisco -- elastic_services_controller	A vulnerability in the Play Framework of Cisco Elastic Services Controller (ESC) could allow an unauthenticated, remote attacker to gain full access to the affected system. The vulnerability is due to static, default credentials for the Cisco ESC UI that are shared between installations. An attacker who can extract the static credentials from an existing installation of Cisco ESC could generate an admin session token that allows access to all instances of the ESC web UI. This vulnerability affects Cisco Elastic Services Controller prior to releases 2.3.1.434 and 2.3.2. Cisco Bug IDs: CSCvc76627.	2017-07-05	10.0	CVE-2017-6713 BID CONFIRM
cisco -- ios_xr	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to elevate privileges to the root level. More	2017-07-03	7.2	CVE-2017-6718

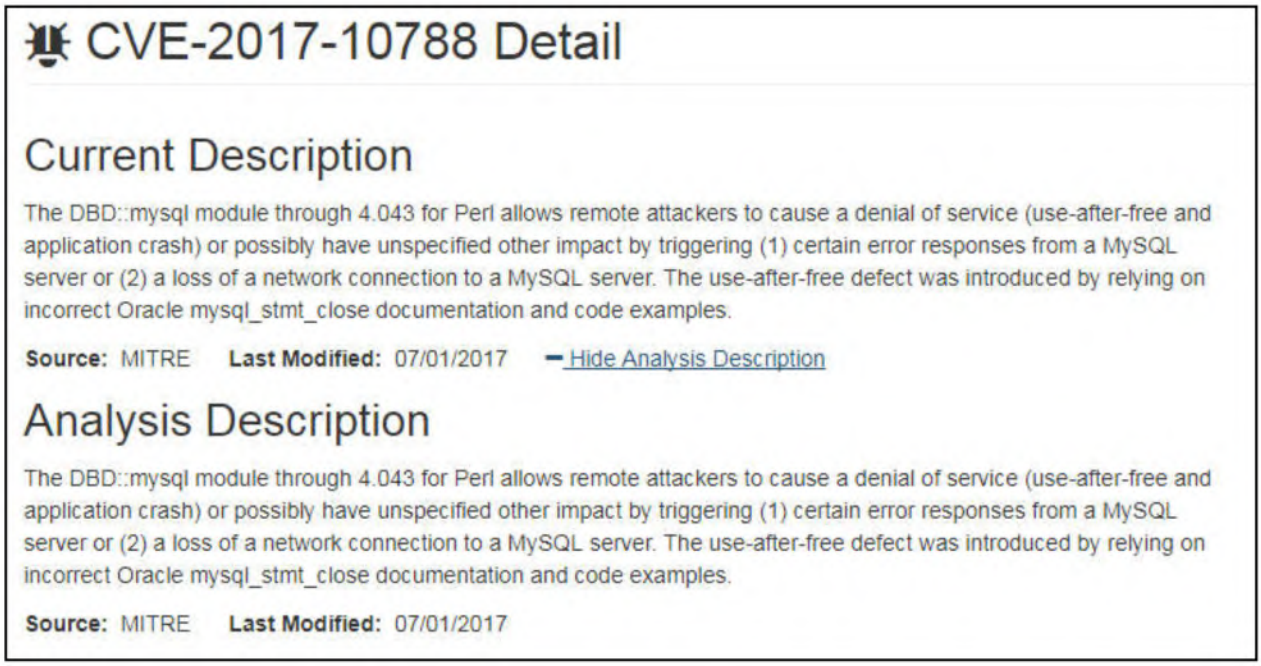
- **What is NVD?**
  - The NVD is the CVE dictionary augmented with additional analysis, a database, and a fine-grained search engine. The NVD is a superset of CVE. The NVD is synchronized with CVE such that any updates to CVE appear immediately on the NVD.

SNAPSHOT OF NATIONAL VULNERABILITY DATABASE - NVD



- **What is the NVD severity score?**
  - The NVD uses the Common Vulnerability Scoring System (CVSS) Version 2, which is is an open standard for assigning vulnerability impacts that is used by a variety of organizations
  - NISTIR 7946 - CVSS Implementation Guidance describes methodologies developed by the NVD for using CVSS, and along with Appendix B describes the NVD's entire vulnerability assessment process.

SNAPSHOT OF CVE-2017-10788



Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 9.8 Critical
Vector: CVSS:3.0/AV:N/AC:L/I
(legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

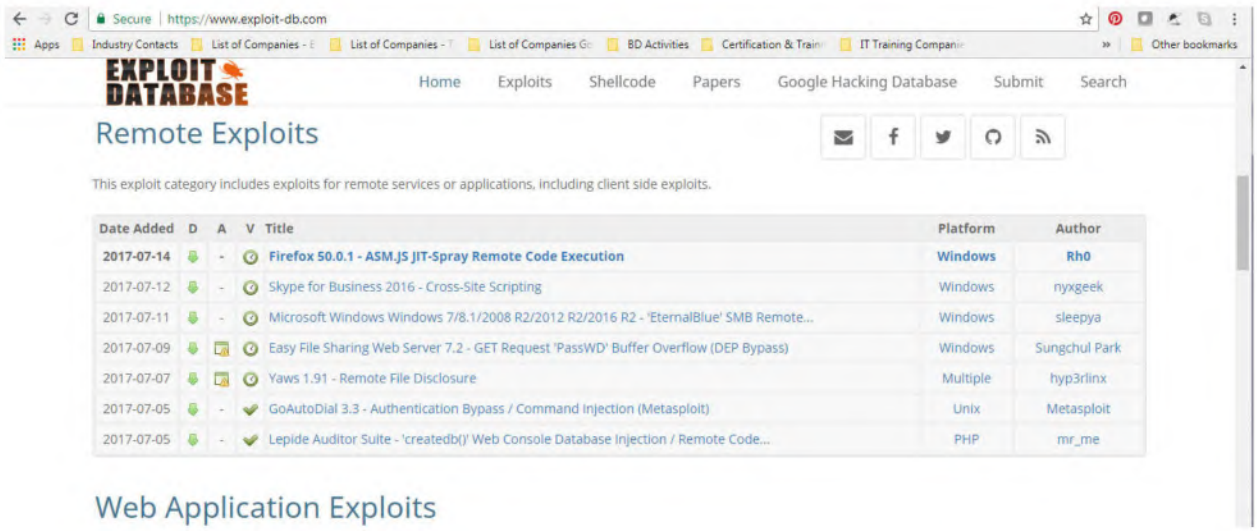
CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

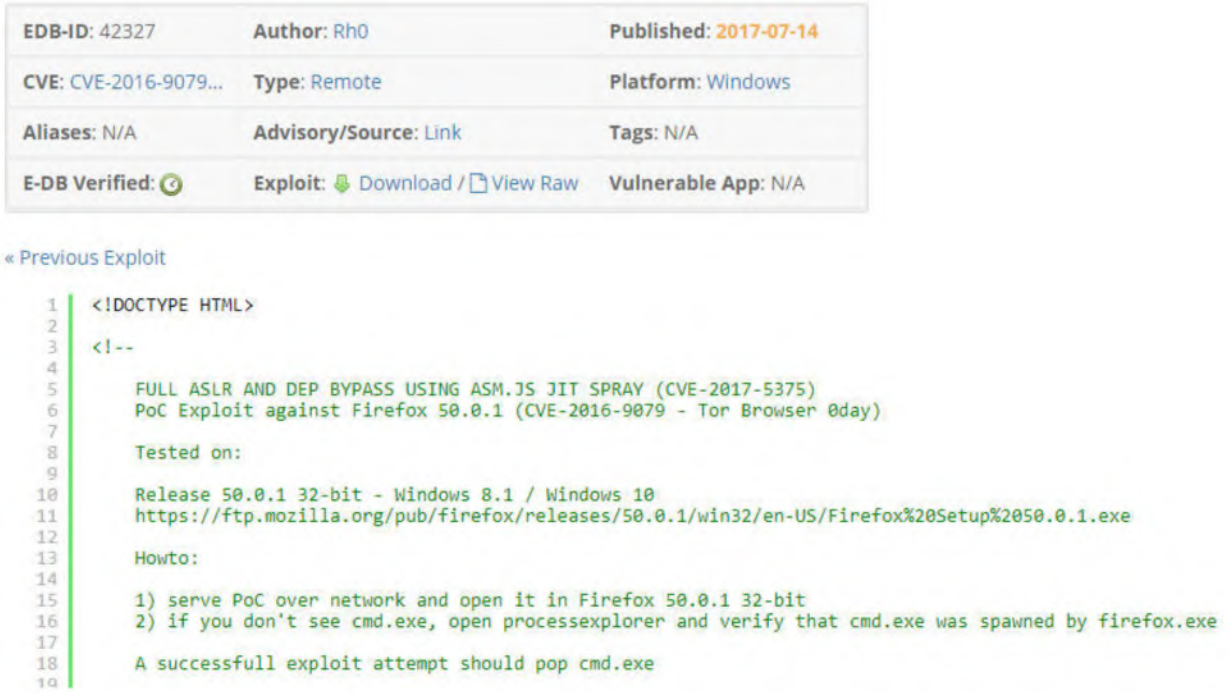
- Note that all the major vendors publish their security vulnerabilities online
  - Microsoft
  - Oracle
  - Cisco
  - Etc

Topic no 122: What Is An Exploit?

- **What is an exploit?**
  - Program or some code that takes advantage of a security hole (i.e. a vulnerability) in an application or system, so that an attacker can use it for their benefit.
- **Remote exploit:**
  - A *remote exploit* works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
- **Local exploit:**
  - A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.
- **Exploit database:**
  - The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database.
  - The Exploit Database is a repository for *exploits and proof-of-concepts rather than advisories*, making it a valuable resource for those who need actionable data right away.



SNAPSHOT OF EXPLOIT CODE



EDB-ID: 42327	**Author**: Rh0	**Published**: 2017-07-14
CVE: CVE-2016-9079...	**Type**: Remote	**Platform**: Windows
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

```
<!DOCTYPE HTML>

<!--

    FULL ASLR AND DEP BYPASS USING ASM.JS JIT SPRAY (CVE-2017-5375)
    PoC Exploit against Firefox 50.0.1 (CVE-2016-9079 - Tor Browser 0day)

    Tested on:

    Release 50.0.1 32-bit - Windows 8.1 / Windows 10
    https://ftp.mozilla.org/pub/firefox/releases/50.0.1/win32/en-US/Firefox%20Setup%2050.0.1.exe

    Howto:

    1) serve PoC over network and open it in Firefox 50.0.1 32-bit
    2) if you don't see cmd.exe, open processexplorer and verify that cmd.exe was spawned by firefox.exe

    A successfull exploit attempt should pop cmd.exe
```

- **Zero-day exploit:**
  - A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it this **exploit** is called a zero day attack.

Topic no 123: Effective Vulnerability Management: Stage 2

Another look at the security transformation model

- Stage 1: Security hardening
  - Taking stock of your assets
  - Prioritizing the assets
  - Establishing an MSB
  - Implement security controls with CIS/DISA/Other benchmarks
  - Basic/broader security hardening
- Note that Stage 1 (Hardening) and Stage 2 (Patching) are shown sequentially to show priority
- In practical terms, the two efforts may be done slightly staggered depending upon resources available
- Establish one program and then the other
- Stage 1 (Hardening) is equivalent to tightening all the screws on machinery and will reduce impact of an attack (like a shield)

- Stage 2 (Patching) will seal all the entry points for an attacker to gain access or to penetrate a system
- Note that both Stage 1 and Stage 2 are equally important and necessary and assist in enhancing the security posture in their unique manner

Topic no 124: Security Breach Case Study 1: Home Dept 2014

- 56 million payment cards compromised
- Early September 2014
- Sequence of events:
  - The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials
  - Then they exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment.
  - Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).
  - This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014).
  - The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.
- Home Depot didn't have secure configuration of the software or hardware on the POS terminals.
- There was no proof of regularly scheduled vulnerability scanning of the POS environment.
- They didn't have proper network segregation between the Home Depot corporate network and the POS network.
- Overall: several controls missing, vendor management of IDs and access management missing, and monitoring of the network was missing

Topic no 125: Security Breach Case Study 2: Anthem

- Health Insurer Anthem
- Affected 78.8 million individuals
- **Sequence of events:**
  - Data breach began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content

- Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse
- Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in the environment
- The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse a system that stores a large amount of consumer personally identifiable information
- Queries to that data warehouse resulted in access to an ex filtration of approximately 78.8 m unique user records

- **Vulnerabilities:**
    - Exploitable vulnerabilities were found in anthem network
    - User security awareness training conducted to prevent phishing and social engineering
- **Remediation measures:**
    - Implemented two-factor authentication on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions
    - Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs

Topic no 126: Best Practices For Applying Security Patches

- "The risk of implementing the service pack, hotfix and security patch should ALWAYS be LESS than the risk of not implementing it."
- “You should never be worse off by implementing a service pack, hotfix and security patch. If you are unsure, then take steps to ensure that there is no doubt when moving them to production systems.”

1. **Use a change control process**
    - A good change control procedure has an identified owner, a path for customer input, an audit trail for any changes, a clear announcement and review period, testing procedures, and a well-understood back-out plan.
    - Change control will manage the process from start to finish

2. **Read all related documentation:**
   - Before applying any service pack, hotfix or security patch, all relevant documentation should be read and peer reviewed. The peer review process is critical as it mitigates the risk of a single person missing critical and relevant points when evaluating the update
   - Ensure the update is relevant, and will resolve an existing issue
   - Ensure adoption won't cause other issues resulting in a compromise of the production system
   - There are dependencies relating to the update, (i.e. certain features being enabled or disabled for the update to be effective.)
   - Potential issues will arise from the sequencing of the update, as specific instructions may state or recommend a sequence of events or updates to occur before the service pack, hotfix or security patch is applied

3. Apply updates on a need-only basis
4. Testing
5. Plan to uninstall
6. Working backup and production downtime
7. Always have roll-back plan
8. Don't get more than 2 service packs behind

Topic no 127: Who Conducts Vulnerability Management

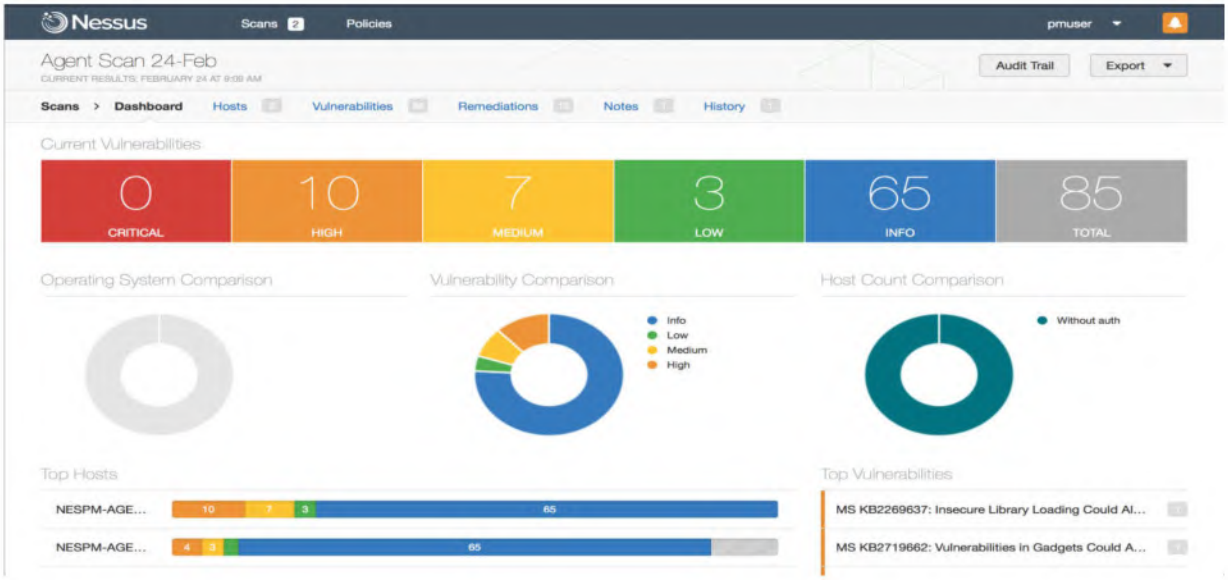
- A number of teams and resources may be involved in the VM lifecycle

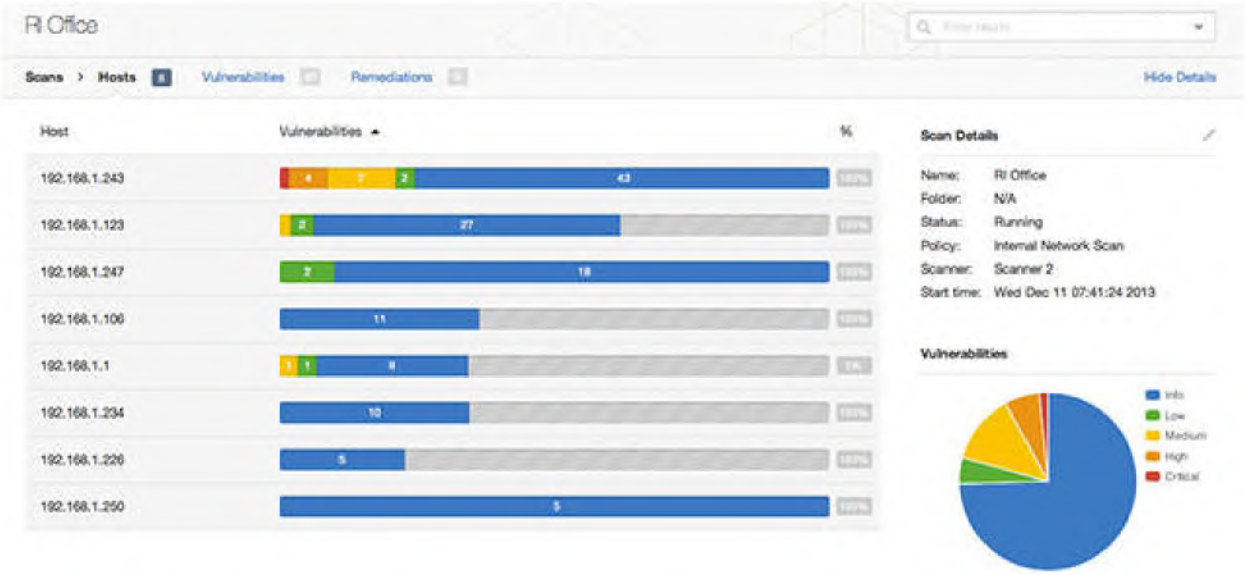
SN	ACTIVITY	TEAM	SUPPORTED BY
1	ANALYZE ASSETS	INFOSEC	IT OPS TEAM
2	PREPARE SCANNER	INFOSEC	-
3	RUN VULNERABILITY SCAN	INFOSEC	-
4	ASSESS RESULTS	INFOSEC	IT OPS TEAM
5	TEST & PATCH SYSTEMS	IT OPS TEAM	INFOSEC
6	VERIFY (RE-SCAN)	INFOSEC	IT OPS TEAM
7	REPORT FINDINGS	INFOSEC	IT STEERING COMMITTEE

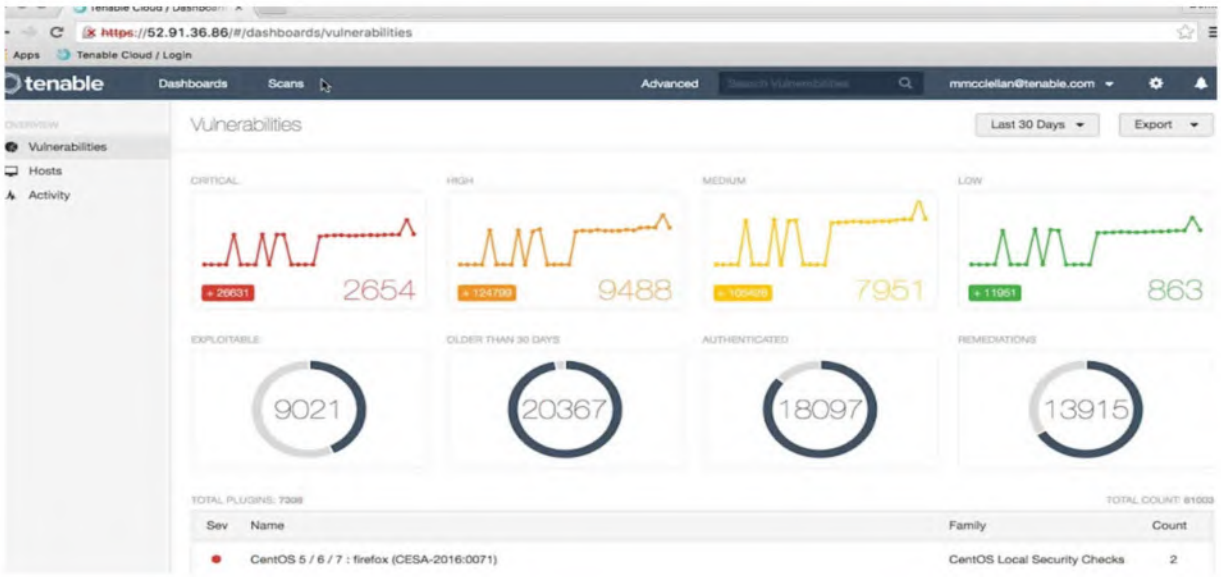
- **Role of Infosec team:**
  - Takes the primary ownership of the vulnerability management process
  - Runs scanning after coordinating with the relevant IT Ops team
  - Shares scanning reports with IT teams and management
  - Tracks remediation timelines
  - Understands criticality issues and helps to prioritize
  - Studies the security patch details as a backup resource
  - Assists with change management process
- **Role of IT Ops team:**
  - Owner of the IT asset
  - Receives the vulnerability scan report from Infosec team
  - Studies the vulnerability
  - Understands criticality, impact, & dependencies
  - Helps Infosec team develop a project plan (if required) and timelines for the patching
  - Tests the patches in test environment
  - Takes backups, develops roll-back plan
  - Takes downtime and takes ownership of the change management process
  - Implements the patches
  - Monitors the systems after patch implementation
  - Rolls-back if necessary
  - Creates the necessary documentation

Topic no 128: Nessus Features

- Lets take a look at Nessus features
- Nessus (Reports):
  - Customize reports to sort by vulnerability or host
  - Create an executive summary or compare scan results
  - Targeted email notifications of scan results
- Nessus (Scan Types):
  - Asset discovery
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening & missing patches
- Nessus (Compliance & Config Scans):
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA
- Nessus (Risk scores):
  - Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk
- Nessus is a cost-effective scanner that gets most of the job done for vulnerability scanning
- It has CIS and DISA compliance templates
- Has some flaws and bugs but overall useful tool

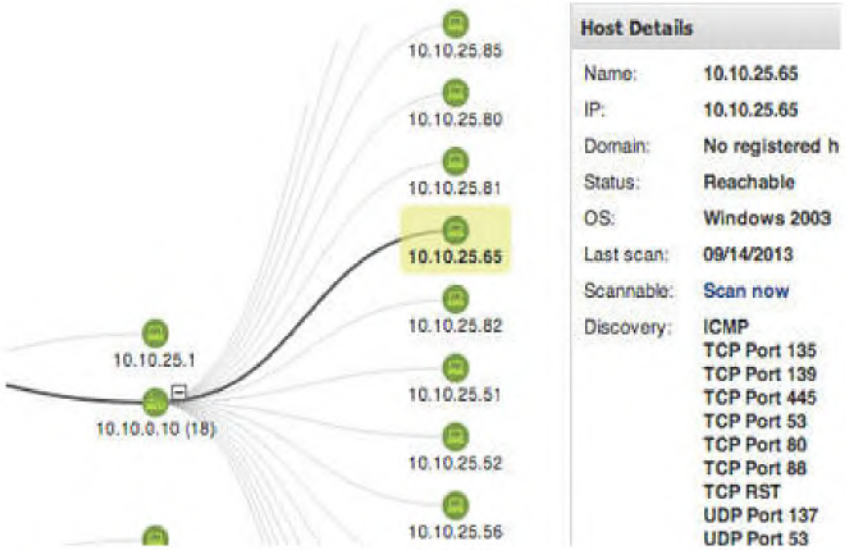

Nessus
Scans 2
Policies
pmuser
Agent Scan 24-Feb
Audit Trail
Export
Scans > Dashboard
Hosts
Vulnerabilities
Remediations
Notes
History
Current Vulnerabilities
0 CRITICAL
10 HIGH
7 MEDIUM
3 LOW
65 INFO
85 TOTAL
Operating System Comparison
Vulnerability Comparison
Info
Low
Medium
High
Host Count Comparison
Without auth
Top Hosts
NESPM-AGE...
NESPM-AGE...
Top Vulnerabilities
MS KB2269637: Insecure Library Loading Could Al...
MS KB2719662: Vulnerabilities in Gadgets Could A...

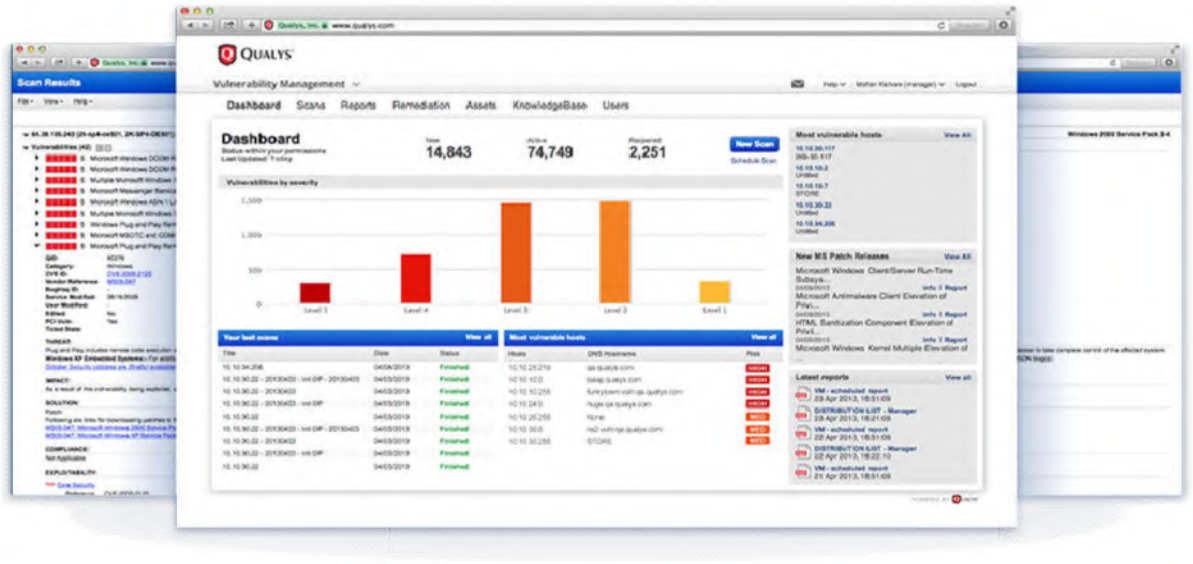

RI Office
Scans > Hosts
Vulnerabilities
Remediations
Hide Details
Host
Vulnerabilities
%
192.168.1.243
192.168.1.123
192.168.1.247
192.168.1.100
192.168.1.1
192.168.1.234
192.168.1.226
192.168.1.250
Scan Details
Name: RI Office
Folder: N/A
Status: Running
Policy: Internal Network Scan
Scanner: Scanner 2
Start time: Wed Dec 11 07:41:24 2013
Vulnerabilities
Info
Low
Medium
High
Critical

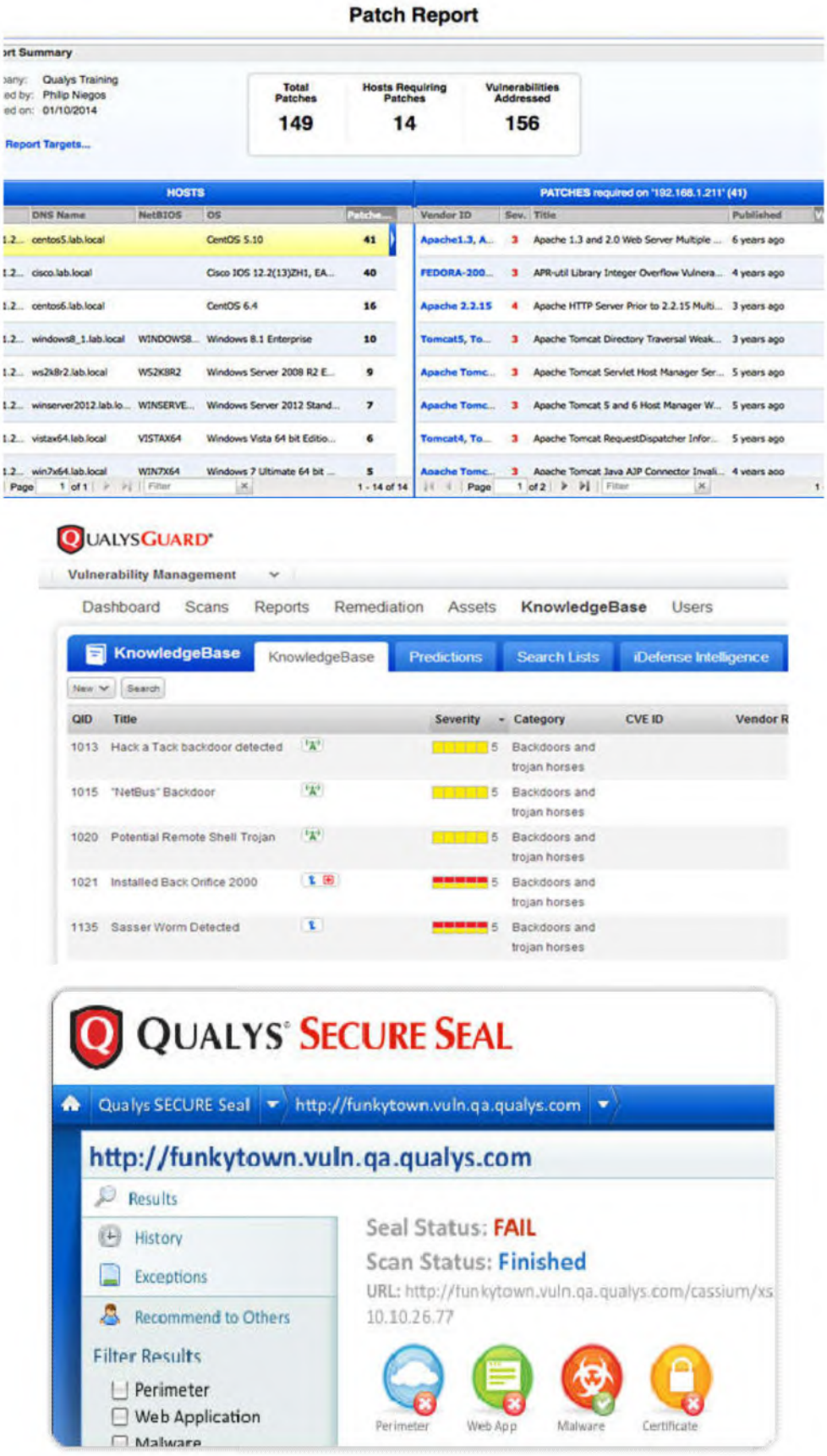

https://52.91.36.86/#/dashboards/vulnerabilities
Apps
Tenable Cloud / Login
tenable
Dashboards
Scans
Advanced
mmcclellan@tenable.com
Vulnerabilities
Hosts
Activity
Vulnerabilities
Last 30 Days
Export
CRITICAL
HIGH
MEDIUM
LOW
2654
9488
7951
863
EXPLOITABLE
OLDER THAN 30 DAYS
AUTHENTICATED
REMEDIATIONS
9021
20367
18097
13915
Sev
Name
Family
Count
CentOS 5 / 6 / 7 : firefox (CESA-2016:0071)
CentOS Local Security Checks
2

Topic no 129: Qualys Features

- Qualys:
  - Cloud-based service
  - On-premise device
  - Complete suite
  - Scalable and immediate deployment
  - Asset discovery; find and organize hosts
  - Prioritize & manage remediation tickets
  - Continuous monitoring service
  - Policy compliance scanning
  - Qualys Secure Seal for websites






Patch Report
ort Summary
Qualys Training
Philip Niegos
01/10/2014
Report Targets...
Total Patches
149
Hosts Requiring Patches
14
Vulnerabilities Addressed
156
HOSTS
DNS Name
NetBIOS
OS
PATCHES required on '192.168.1.211' (41)
Vendor ID
Sev.
Title
Published
centos5.lab.local
CentOS 5.10
41
cisco.lab.local
Cisco IOS 12.2(13)ZH1, EA...
40
centos6.lab.local
CentOS 6.4
16
windows8_1.lab.local
WINDOWS8...
Windows 8.1 Enterprise
10
ws2k8r2.lab.local
WS2K8R2
Windows Server 2008 R2 E...
9
winserver2012.lab.lo...
WINSERVE...
Windows Server 2012 Stand...
7
vistax64.lab.local
VISTAX64
Windows Vista 64 bit Editio...
6
win7x64.lab.local
WIN7X64
Windows 7 Ultimate 64 bit ...
5
Apache1.3, A...
Apache 1.3 and 2.0 Web Server Multiple ...
6 years ago
FEDORA-200...
APR-util Library Integer Overflow Vulnera...
4 years ago
Apache 2.2.15
Apache HTTP Server Prior to 2.2.15 Multi...
3 years ago
Tomcat5, To...
Apache Tomcat Directory Traversal Weak...
3 years ago
Apache Tomc...
Apache Tomcat Servlet Host Manager Ser...
5 years ago
Apache Tomc...
Apache Tomcat 5 and 6 Host Manager W...
5 years ago
Tomcat4, To...
Apache Tomcat RequestDispatcher Infor...
5 years ago
Apache Tomc...
Apache Tomcat Java AJP Connector Invali...
4 years ago
QUALYSGUARD
Vulnerability Management
Dashboard
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
KnowledgeBase
KnowledgeBase
Predictions
Search Lists
iDefense Intelligence
New
Search
QID
Title
Severity
Category
CVE ID
Vendor R
1013
Hack a Tack backdoor detected
5
Backdoors and trojan horses
1015
"NetBus" Backdoor
5
Backdoors and trojan horses
1020
Potential Remote Shell Trojan
5
Backdoors and trojan horses
1021
Installed Back Orifice 2000
5
Backdoors and trojan horses
1135
Sasser Worm Detected
5
Backdoors and trojan horses
QUALYS SECURE SEAL
Qualys SECURE Seal
http://funkytown.vuln.qa.qualys.com
http://funkytown.vuln.qa.qualys.com
Results
History
Exceptions
Recommend to Others
Filter Results
Perimeter
Web Application
Malware
Seal Status: FAIL
Scan Status: Finished
URL: http://funkytown.vuln.qa.qualys.com/cassium/xs
10.10.26.77
Perimeter
Web App
Malware
Certificate

- Qualys:
  - Website scanning
  - compliance
  - Annual subscription service model

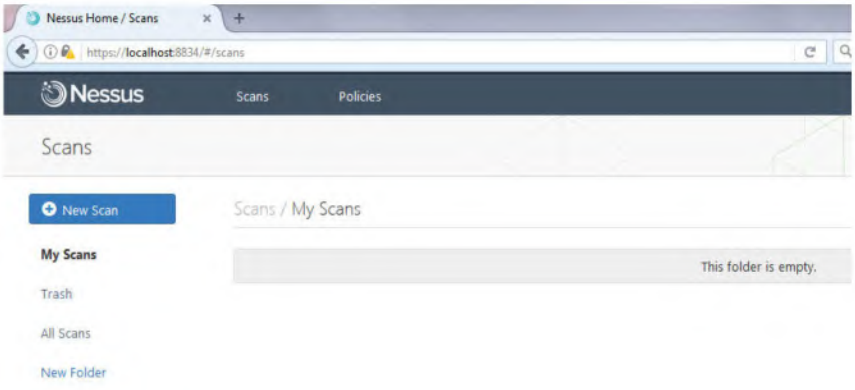
- Qualys is a convenient and scalable VM tool that comes with several modules
- Subscription-based pricing model which can be expensive
- Several advantages due to cloud-based service

Topic no 130: Nessus Demo – 1

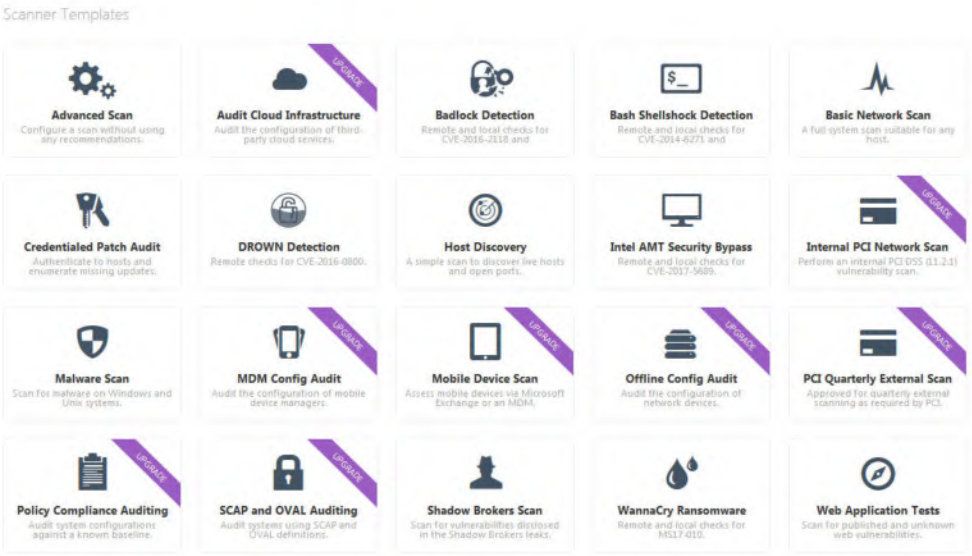
- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

LOGIN SCREEN

DASHBOARD

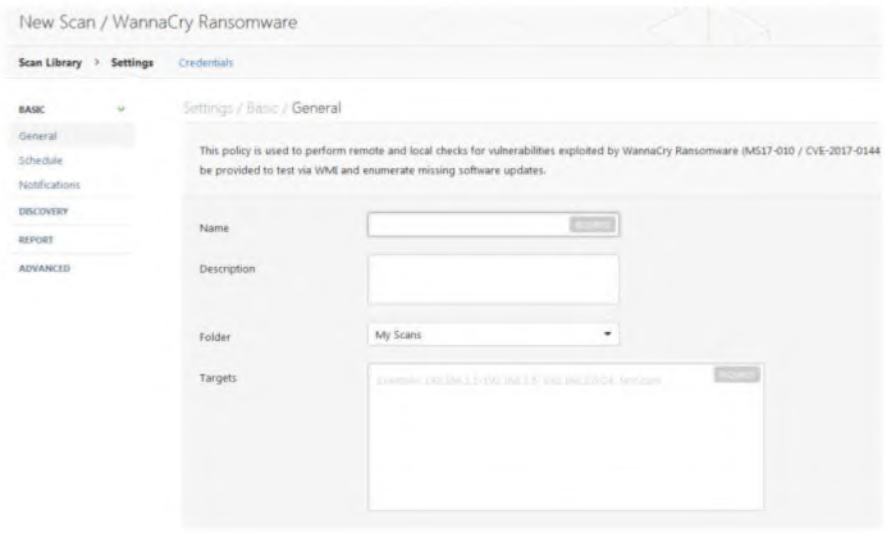


NEW SCAN



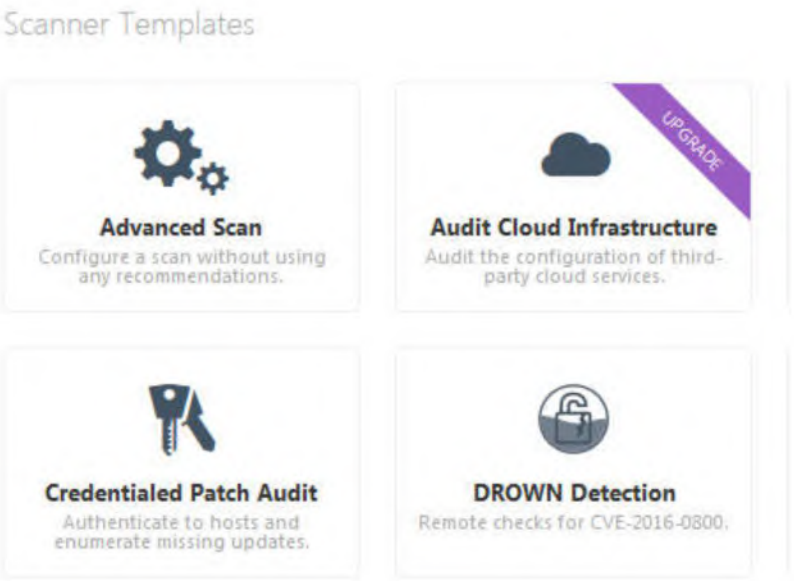
WANNACRY RANSOMWARE SCAN

NEW SCAN WINDOW

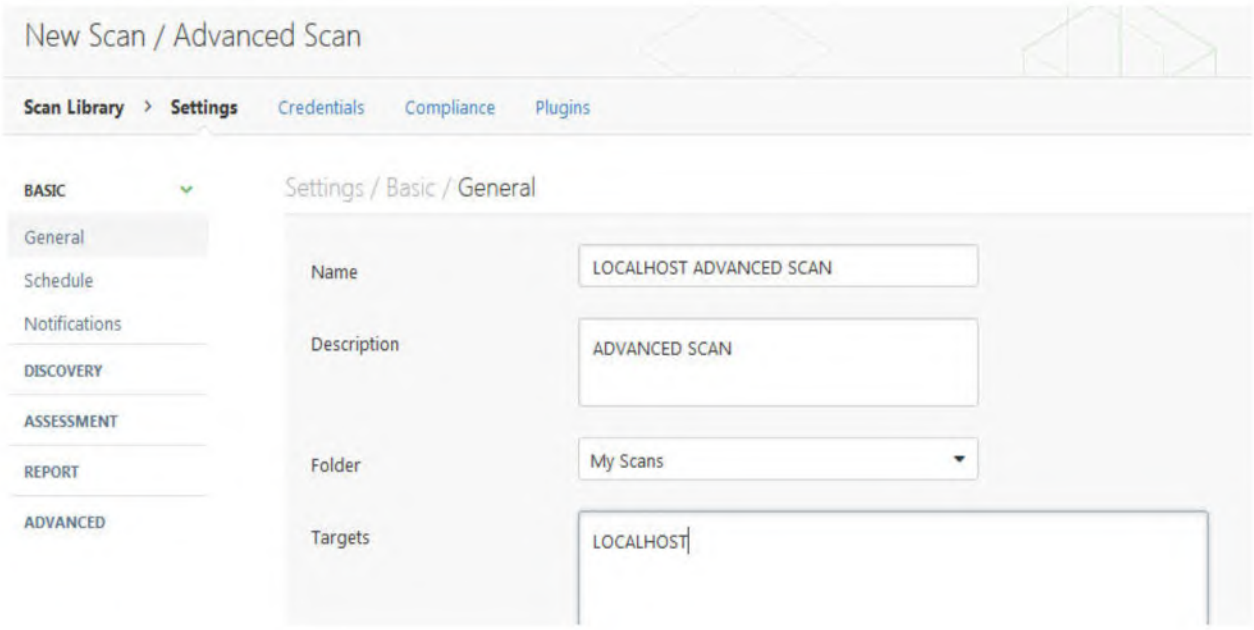


DASHBOARD VIEW WITH SCANS

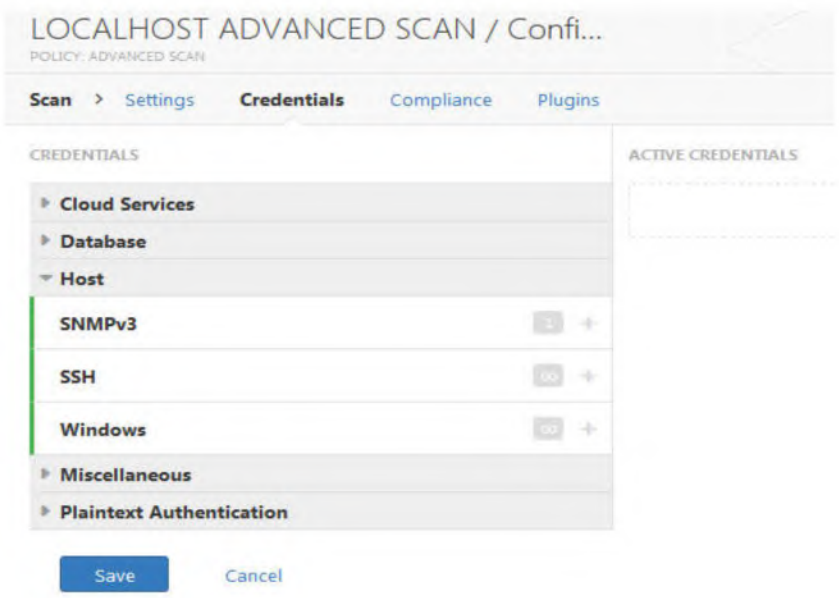
NEW SCAN…



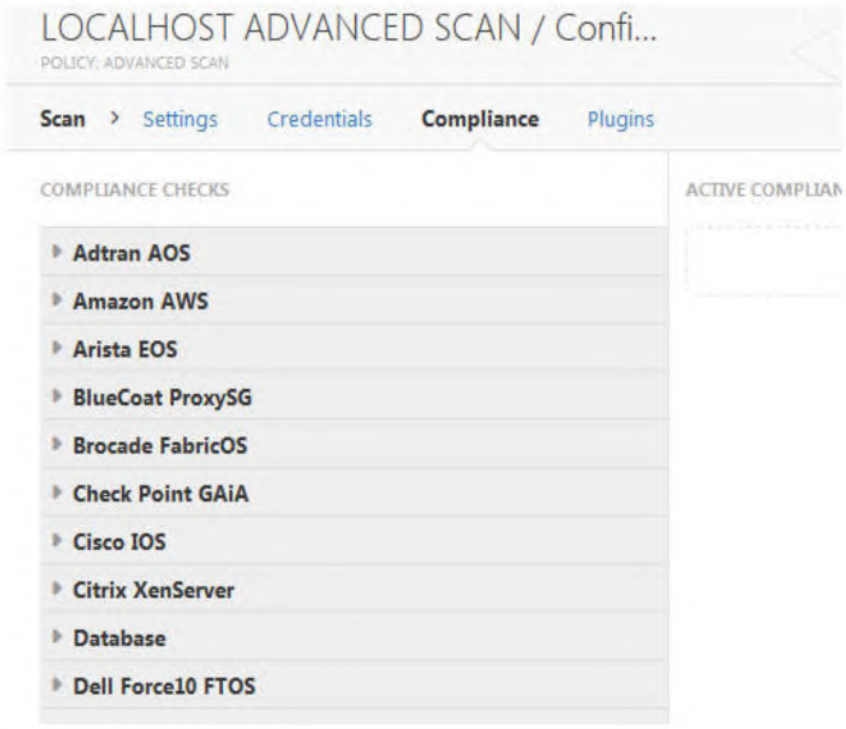
ENTER SCAN DETAILS



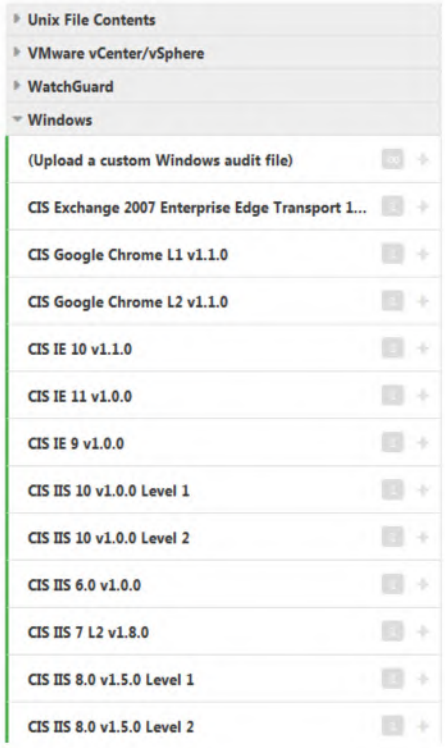
CREDENTIAL SCAN



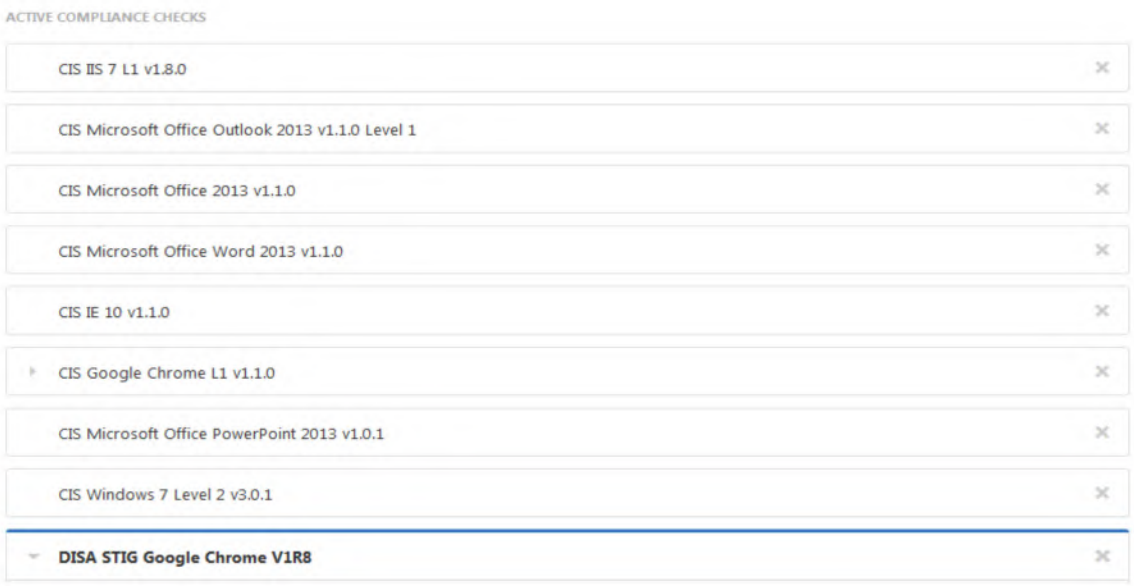
COMPLIANCE SCAN



WINDOWS COMPLIANCE MENU (CIS)



WINDOWS COMPLIANCE MENU (CIS)…

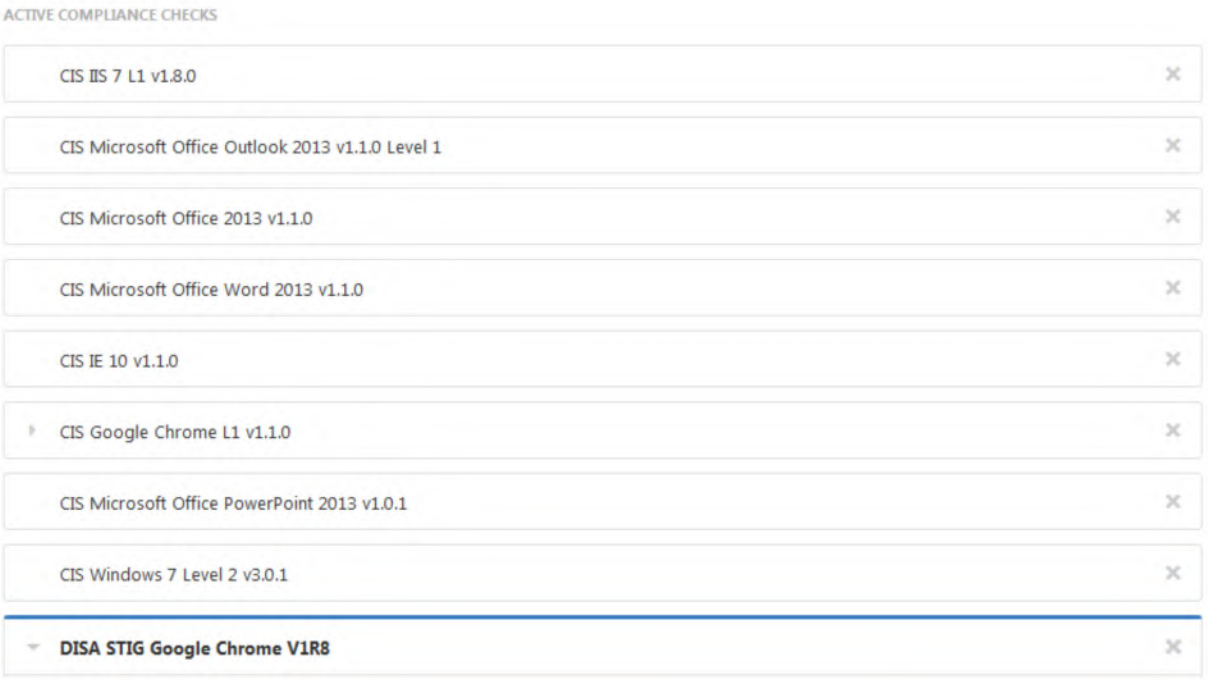


- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

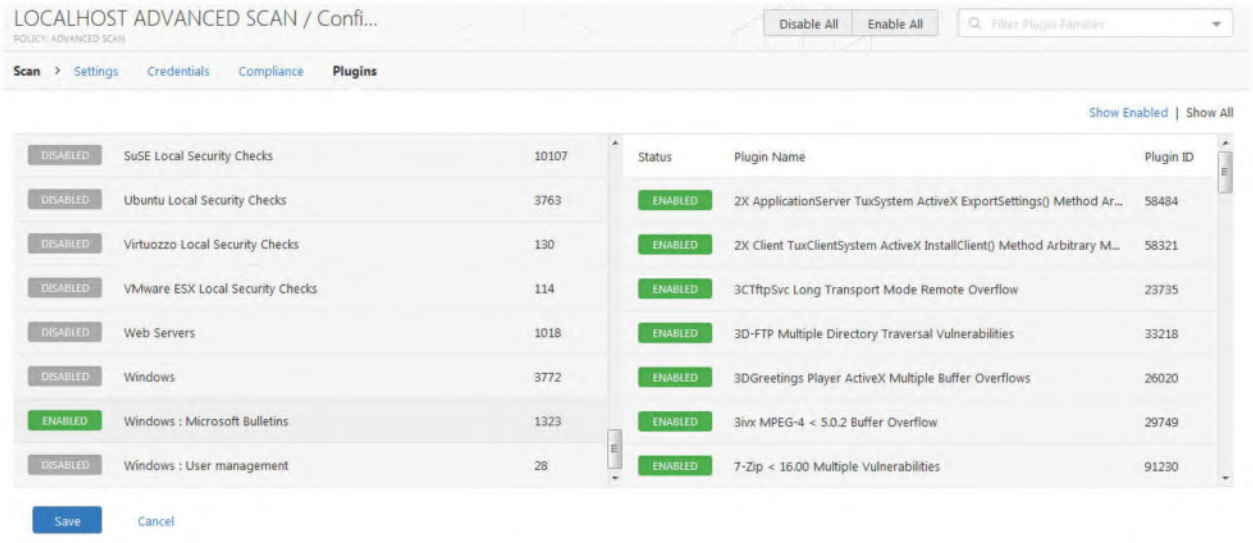
Topic no 131: Nessus Demo – 2

- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

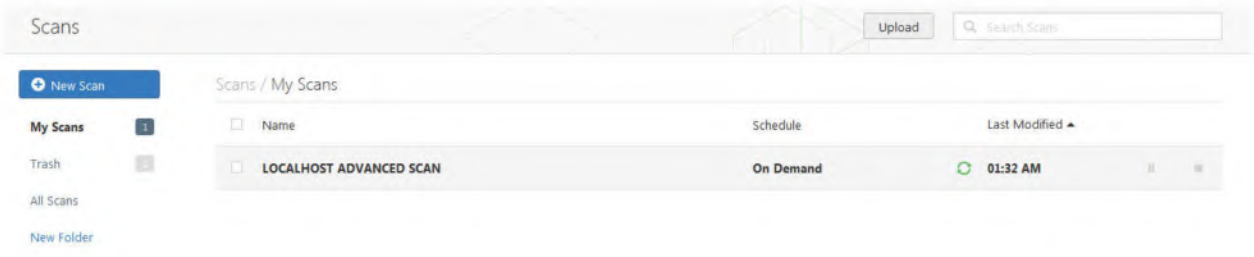
- **ADVANCED SCAN / COMPLIANCE**



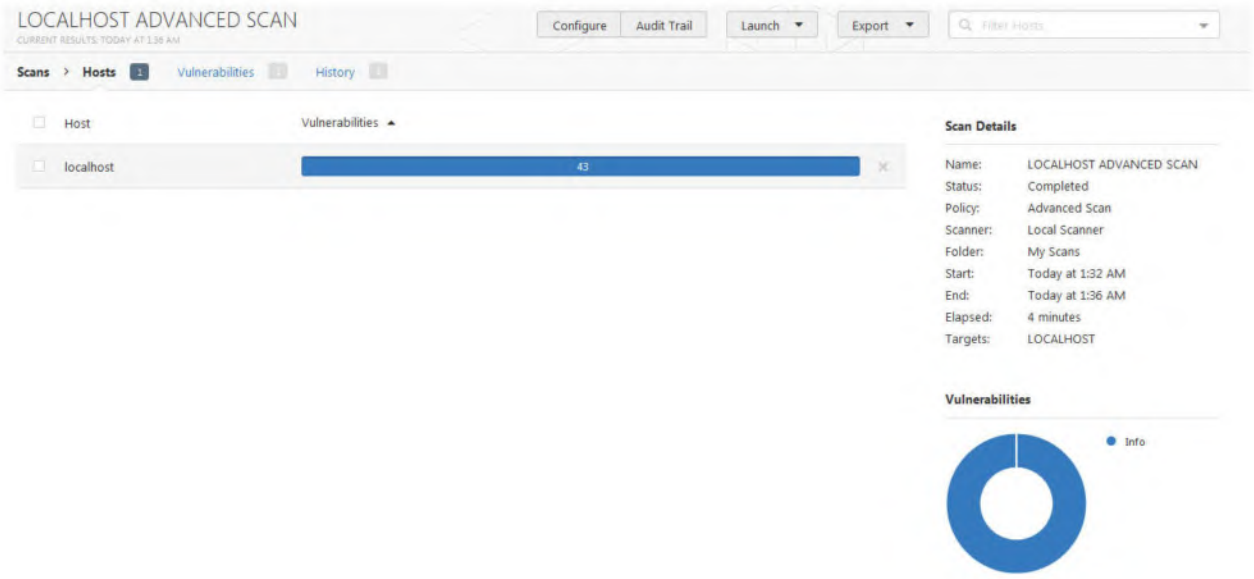
ADVANCED SCAN / PLUG-INS



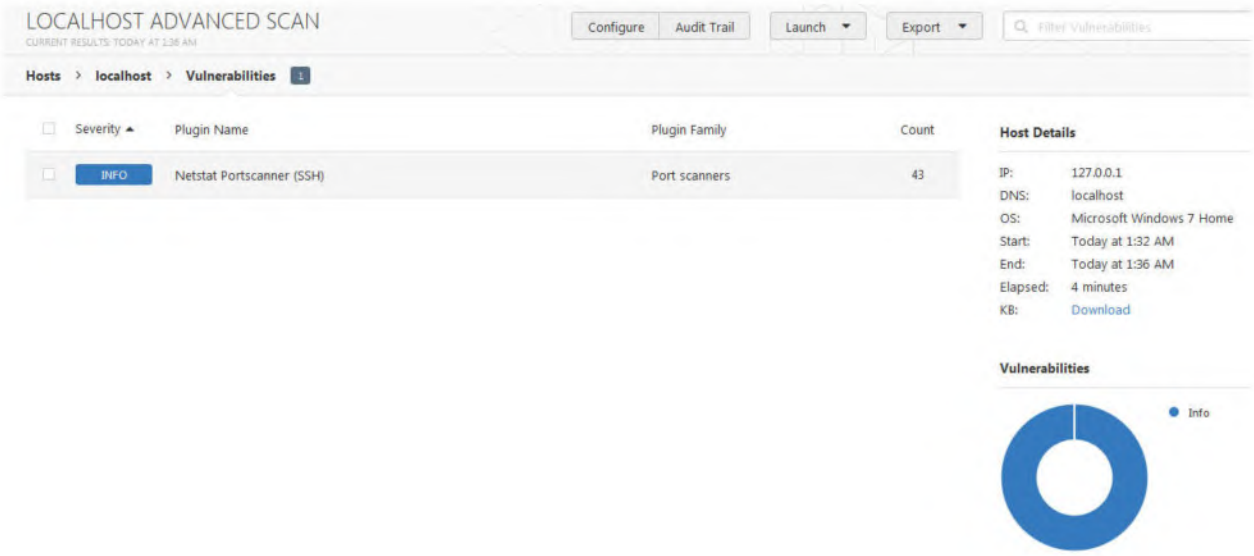
SCAN…IN PROGRESS



SCAN REPORT [43 INFO]



SCAN REPORT [DETAILS]



SCAN REPORT [DETAILS…]

https://en.wikipedia.org/wiki/Netstat

Output

Port 68/udp was found to be open

Port	Hosts
68 / udp	localhost

Port 123/udp was found to be open

Port	Hosts
123 / udp	localhost

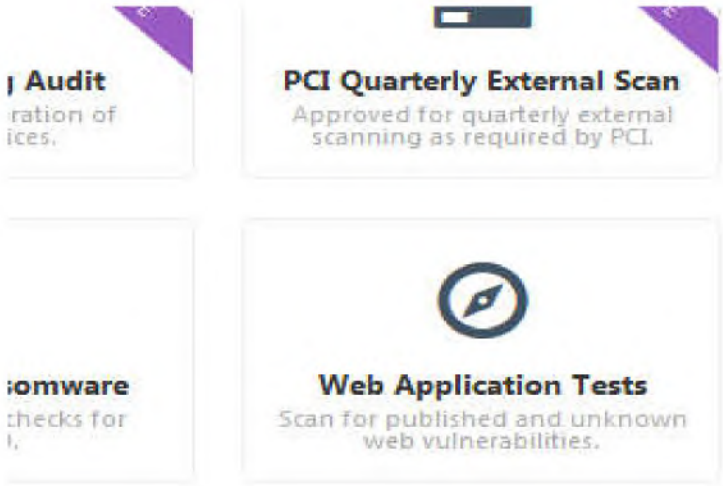
Port 135/tcp was found to be open

Port	Hosts
135 / tcp / epmap	localhost

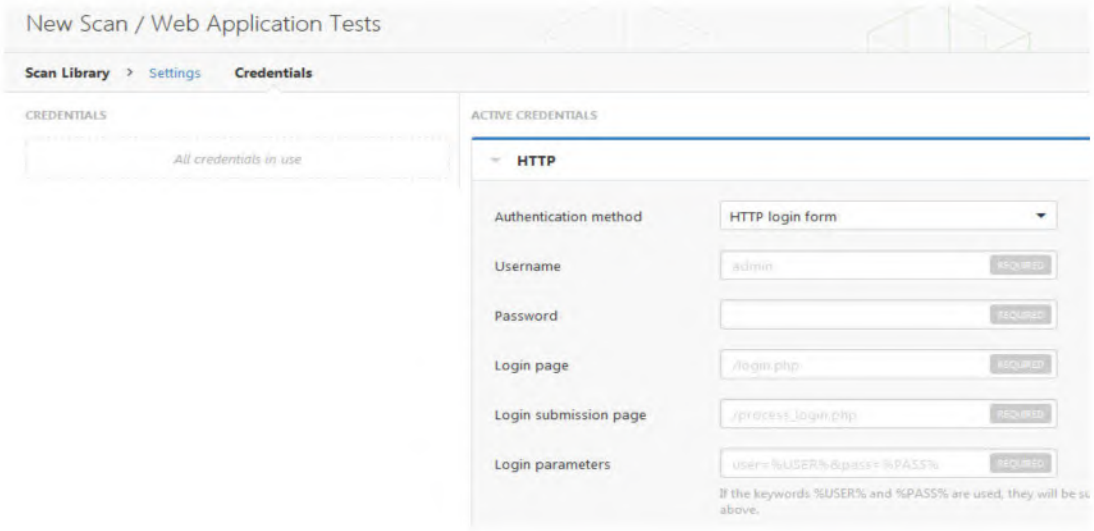
Port 137/udp was found to be open

Port	Hosts
137 / udp	localhost

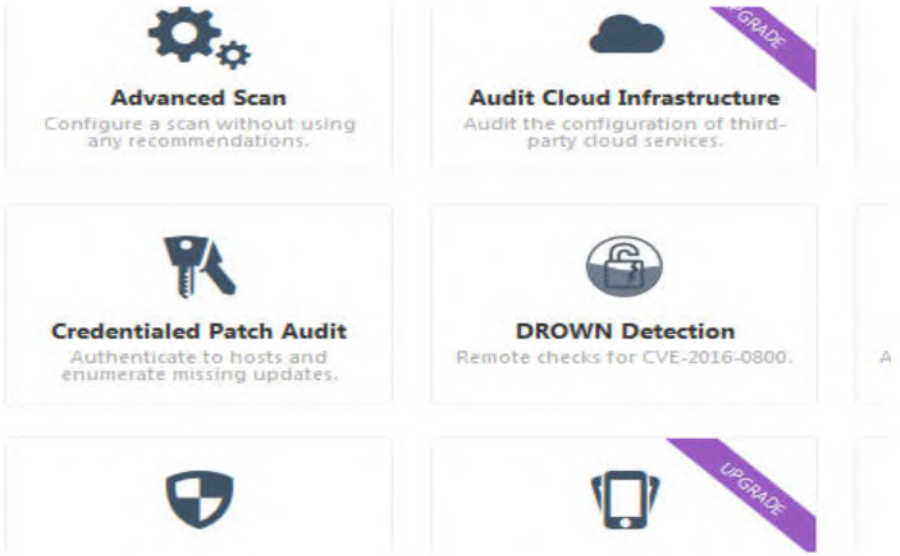
WEB APPLICATION TEST



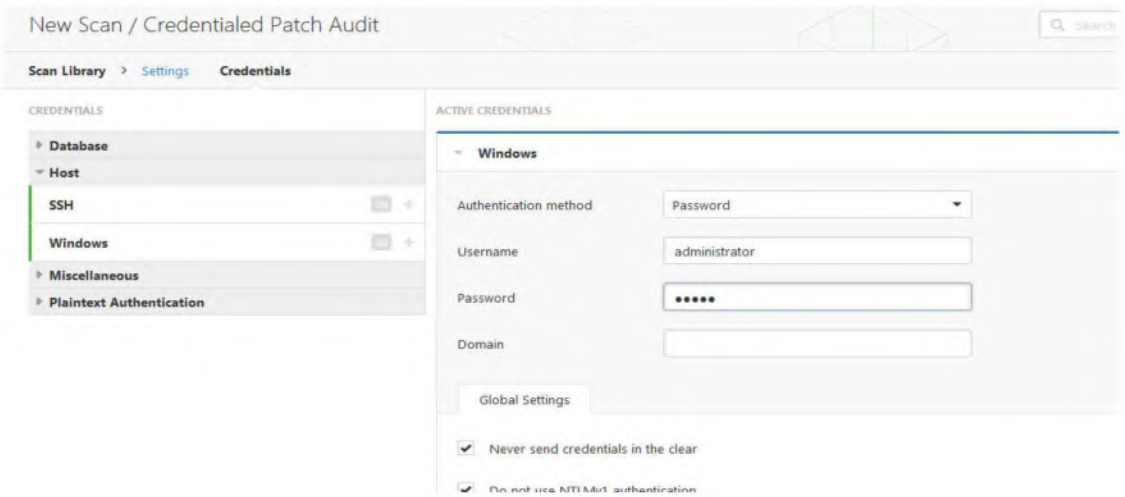
WEB APPLICATION TEST - CREDENTIALS



CREDENTIALED PATCH AUDIT

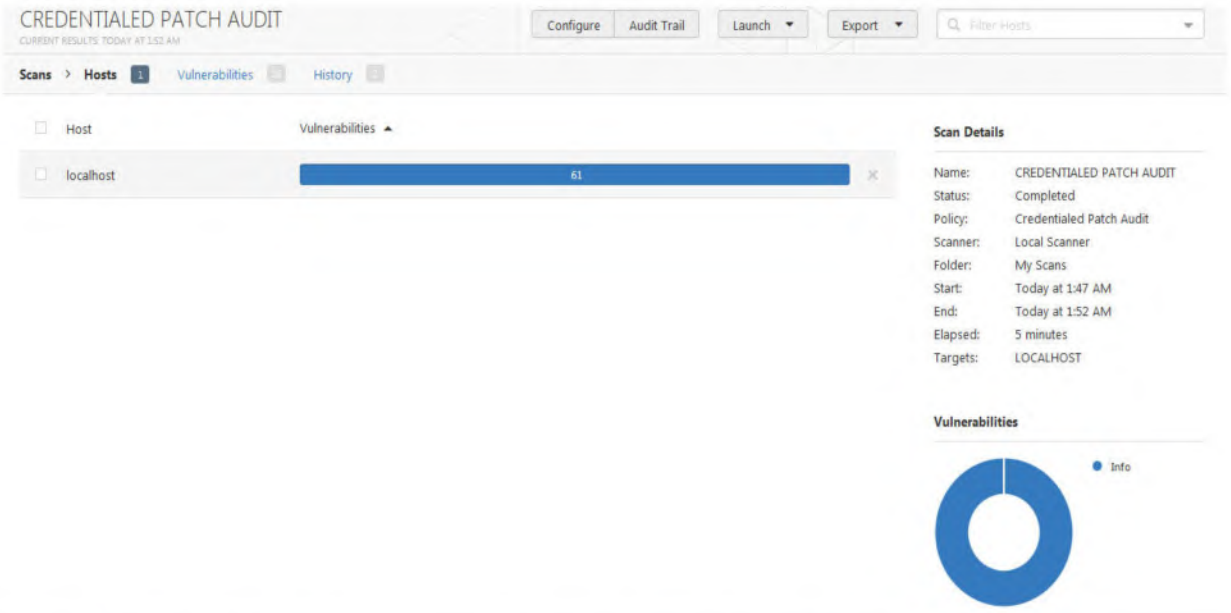


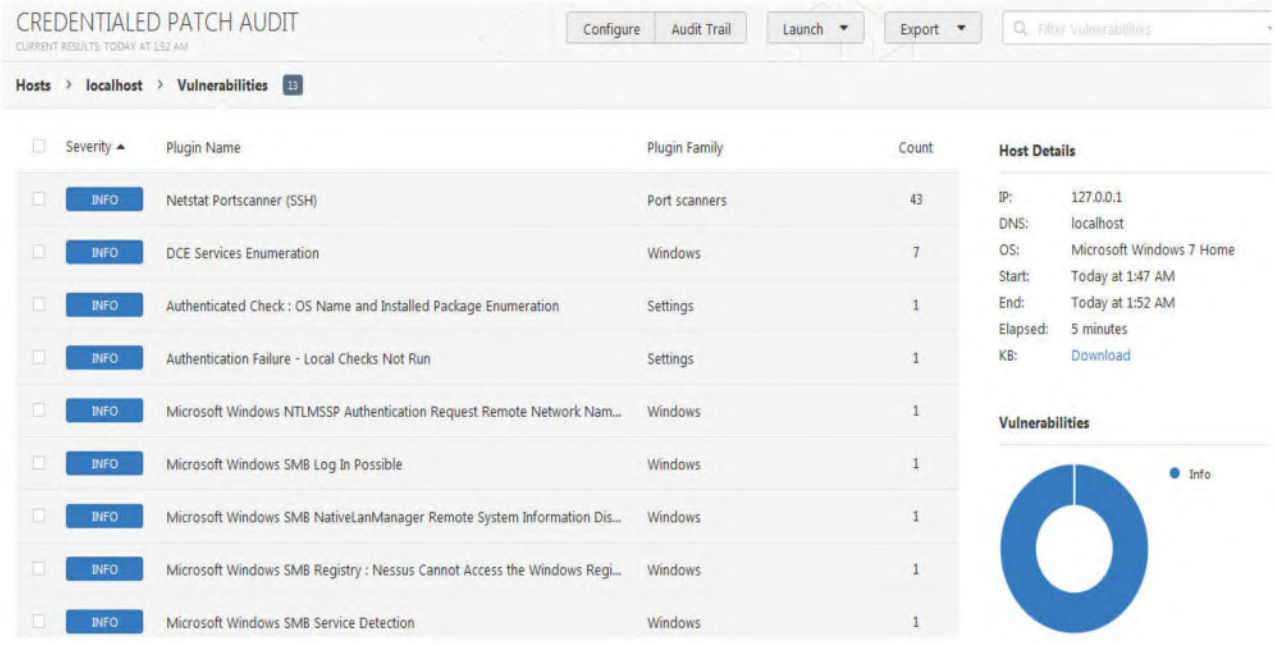
CREDENTIALED PATCH AUDIT



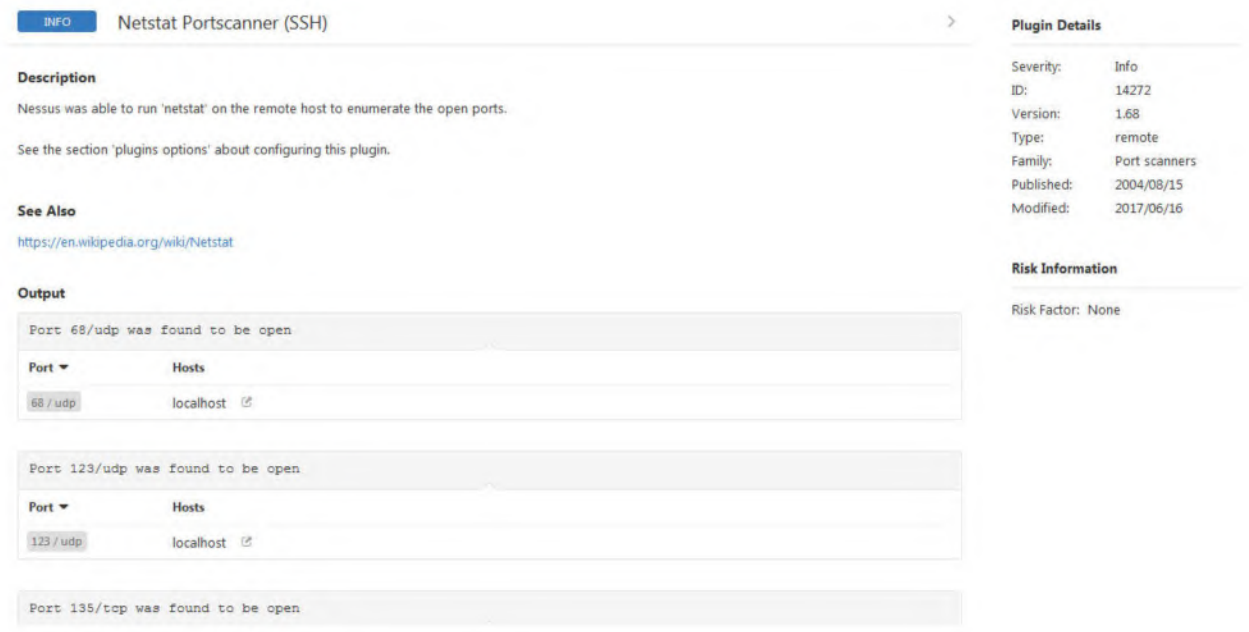
SCANS DASHBOARD

- **CREDENTIALED AUDIT SCAN RESULTS [61 INFO]**





CREDENTIALED AUDIT SCAN RESULTS [DETAILS]



Topic no 136: How Do VM Scanners Work?

- Lets take a look at Qualys scanning technique:
- QualysGuard scanning methodology mainly focuses on the different steps that an attacker might follow in order to perform an attack.
- It tries to use exactly the same discovery and information gathering techniques that will be used by an attacker.
  - **Checking if the remote host is alive**
  - The first step is to check if the host to be scanned is up and running in order to avoid wasting time on scanning a dead or unreachable host
  - This detection is done by probing some well-known TCP and UDP ports. If the scanner receives at least one reply from the remote host, it continues the scan
  - **Firewall detection**
  - The second test is to check if the host is behind any firewalling/filtering device. This test enables the scanner to gather more information about the network infrastructure and will help during the scan of TCP and UDP ports.
  - **TCP / UDP Port scanning**
  - The third step is to detect all open TCP and UDP ports to determine which services are running on this host. The number of ports is configurable, but the default scan is approximately 1900 TCP ports and 180 UDP ports.

- **OS Detection**
- Once the TCP port scanning has been performed, the scanner tries to identify the operating system running on the host.
- This detection is based on sending specific TCP packets to open and closed ports.

- **TCP / UDP Service Discovery**
- Once TCP/UDP ports have been found open, the scanner tries to identify which service runs on each open port by using active discovery tests

- **Vulnerability assessment based on the services detected**
- Once the scanner has identified the specific services running on each open TCP and UDP port, it performs the actual vulnerability assessment.
- The scanner first tries to check the version of the service in order to detect only vulnerabilities applicable to this specific service version. Every vulnerability detection is non-intrusive, meaning that the scanner never exploits vulnerability if it could negatively affect the host in any way.

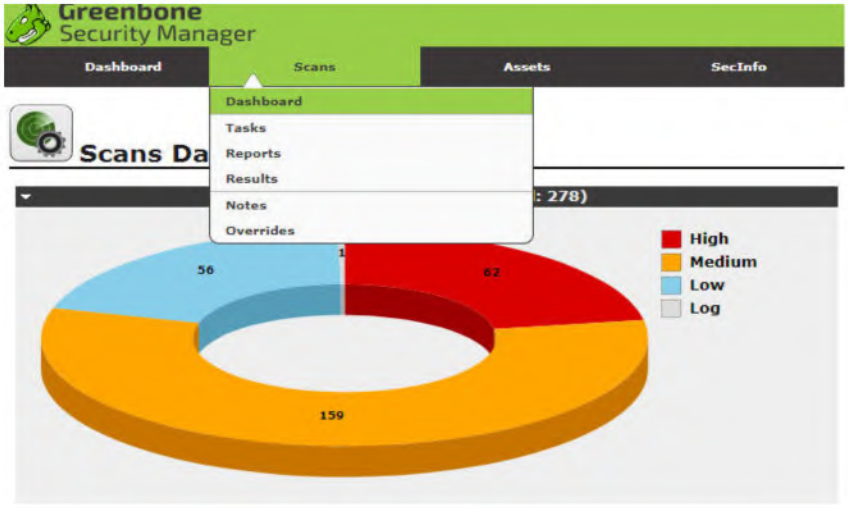
- **Limitations:**

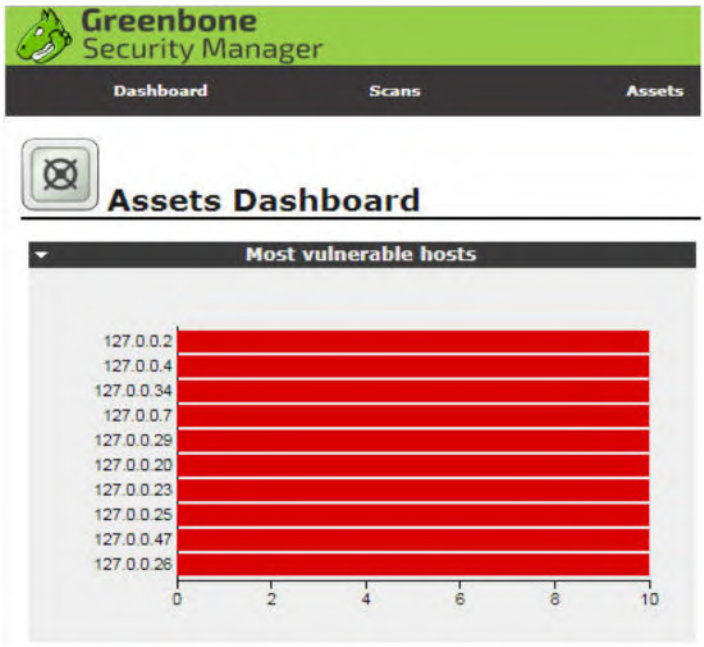
a. Vulnerability scanners work in the same manner as antivirus programs do by using databases that store descriptions of different types of vulnerabilities

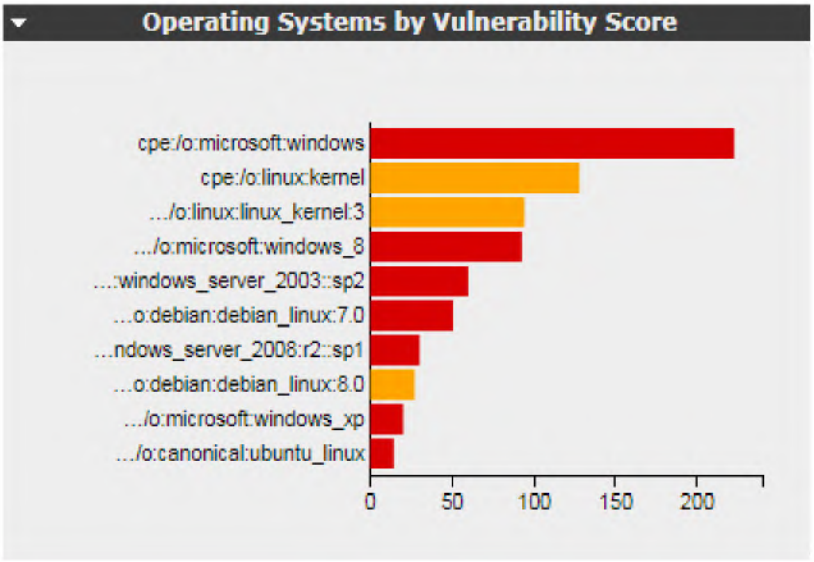
b. False positive or false negative rate

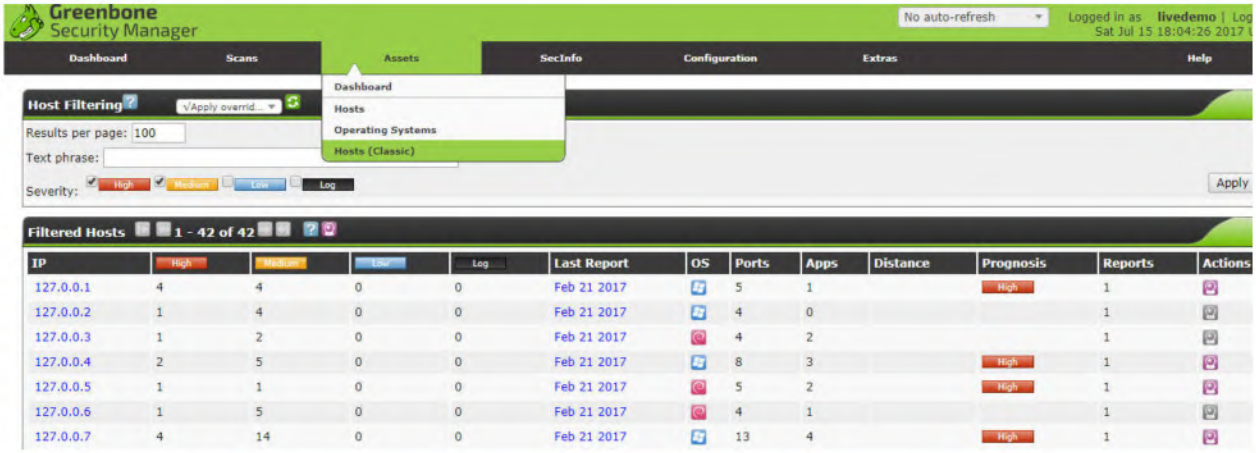
Topic no 139: Open Source Vulnerability Scanners

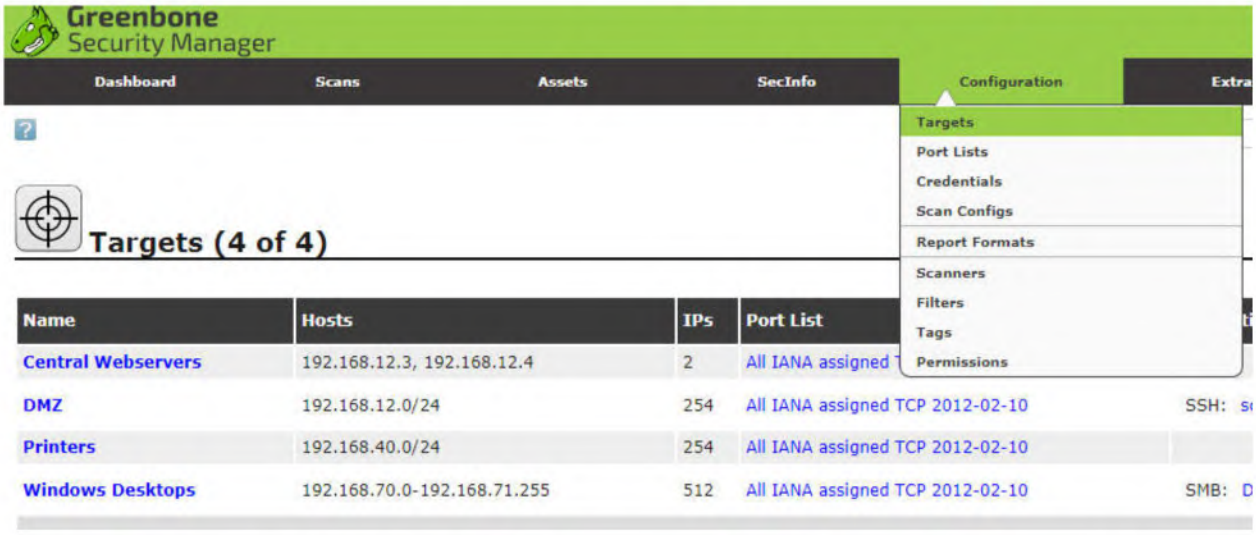
- Lets take a look at OpenVAS
- http://www.openvas.org/livedemo.html
- Login and password: livedemo

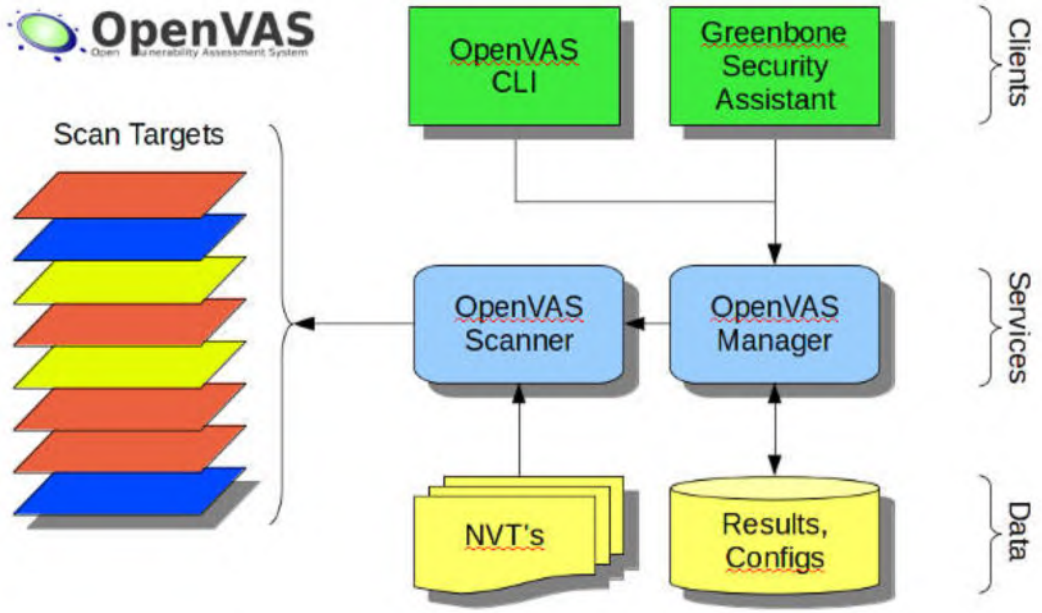

Greenbone
Security Manager
Dashboard
Scans
Assets
SecInfo
Dashboard
Tasks
Reports
Results
Notes
Overrides
Scans Da
: 278)
High
Medium
Low
Log
56
1
62
159


Greenbone
Security Manager
Dashboard
Scans
Assets
Assets Dashboard
Most vulnerable hosts
127.0.0.2
127.0.0.4
127.0.0.34
127.0.0.7
127.0.0.29
127.0.0.20
127.0.0.23
127.0.0.25
127.0.0.47
127.0.0.26
0
2
4
6
8
10


Operating Systems by Vulnerability Score
cpe:/o:microsoft:windows
cpe:/o:linux:kernel
.../o:linux:linux_kernel:3
.../o:microsoft:windows_8
...:windows_server_2003::sp2
...o:debian:debian_linux:7.0
...ndows_server_2008:r2::sp1
...o:debian:debian_linux:8.0
.../o:microsoft:windows_xp
.../o:canonical:ubuntu_linux
0
50
100
150
200







APPROXIMATELY 50k NETWORK VULNERABILITY TESTS

- OpenVAS is a simple, free (opensource) VA scanner
- It has source code documentation, virtual images for download, and mailing lists on its website

Topic no 140: Suggested Frequency For VM Scanning

- **Pre-requisites**
  - Information security team
  - Vulnerability management policy
  - Inhouse scanner or openvas tool
  - Trained staff
- **At the start:**
  - Organizations scanning once a year or not at all
  - Vulnerabilities identified by internal scanning or external VA report
  - Not remediated
  - Lack of discipline and management support
- **As organizations get more mature in scanning discipline:**
  - Quarterly scan
  - Quarterly remediation by IT teams
  - Quarterly report to IT Steering Committee
- **Mature organizations:**
  - Monthly scan
  - Monthly remediation
  - Quarterly or bi-annual external VA/PT
  - Monthly reports to IT Steering Committee
- **Most mature organizations:**
  - Fortnightly scan
  - Fortnightly remediation
  - Monthly reporting

Topic no 141: VM Challenges & Pitfalls

- **Challenges:**
  - Internal expertise on VM tool
  - Not enough support from IT teams
  - Vulnerability patching causing application failure
  - Management support

- **Internal expertise on VM tool**
  - Not too much expertise required
  - Create testbed
  - Monitor traffic pattern
  - Train staff if possible
  - Patch small portions of the network first
- **Not enough support from IT teams:**
  - Create reports and share among IT management
  - Highlight and educate risks to IT management and board
  - Create departmental competition and relationship-building
- **Patching causing application failure:**
  - In test environment create work around or compensating controls
  - Test the compensating controls
  - Document the compensating controls
- **Not enough management support:**
  - Share reports with management highlighting recent incidents
  - Share industry-specific or geographically relevant breach reports
  - Create awareness

Topic no 142: IT Asset Management Challenges

- The typical enterprise has hundreds or thousands of IT assets with a fast-paced business environment
- Tough challenge to keep all IT assets tracked and updated with all the right software patches and updates
- **Challenges:**
  - Asset discovery & tracking
  - Antivirus status
  - Windows & OS updates
  - Patch management
  - Change management

- **Asset discovery & tracking**
  - New assets added & old assets removed
  - Temporary or replacement machines
  - Travelling staff
  - Test beds
  - Vendor environments
- **Antivirus status:**
  - Working and updated antivirus critical to a security managed network
  - Geographically dispersed network
  - Some stations not responding or updating
- **Windows & OS updates:**
  - Windows, Linux, Unix, AIX and database systems
  - Vendor patches from multiple sources
  - Testing the patches
  - Acquiring downtime windows
  - Monitoring the performance
- **Patch management:**
  - Scanning for vulnerabilities
  - Passing on reports to IT teams
  - Tracking the remediation
  - Re-scanning for verification
  - Reporting to management
- **Change management:**
  - Change management inherent to all change processes
  - Change management requires reviews and approvals
  - Configuration management database or repository

Topic No 144: ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

- Asset management helps with the following security functions:
    1. Patch management
    2. Software whitelisting
    3. Software assets discovery and management
    4. Enterprise tracking and reporting
- Gartner refers to this area as Unified endpoint management (UEM):

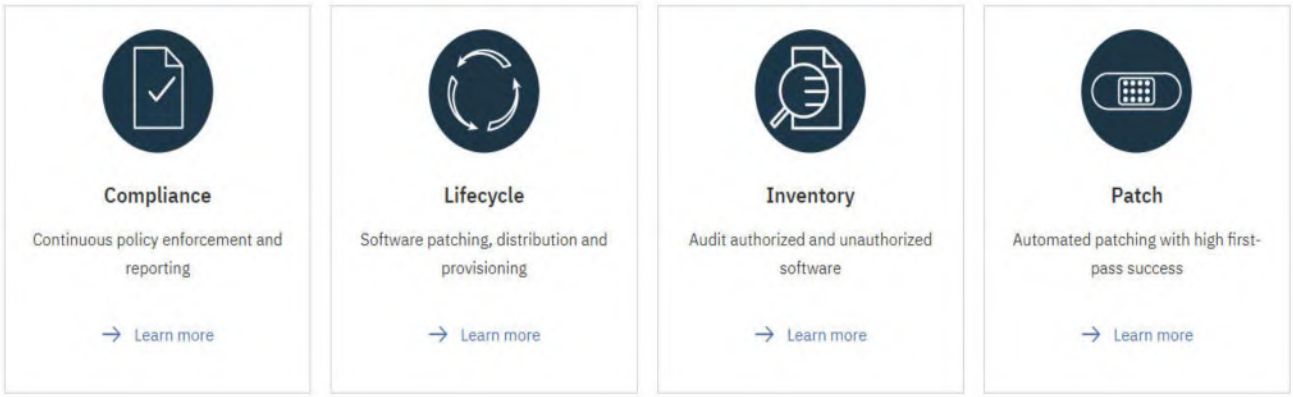
GARTNER MAGIC QUADRANT FOR

UNIFIED ENDPOINT MANAGEMENT 2018

- Unified endpoint management (UEM) tools combine the management of multiple endpoint types in a single console. UEM tools perform the following functions:

GARTNER UEM 2018 REPORT

1. Configure, manage and monitor iOS, Android, Windows 10 and macOS, and manage some Internet of Things (IoT) and wearable endpoints.
2. Unify the application of configurations, management profiles, device compliance and data protection.
3. Provide a single view of multi device users, enhancing efficacy of end-user support and gathering detailed workplace analytics.
4. Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure.

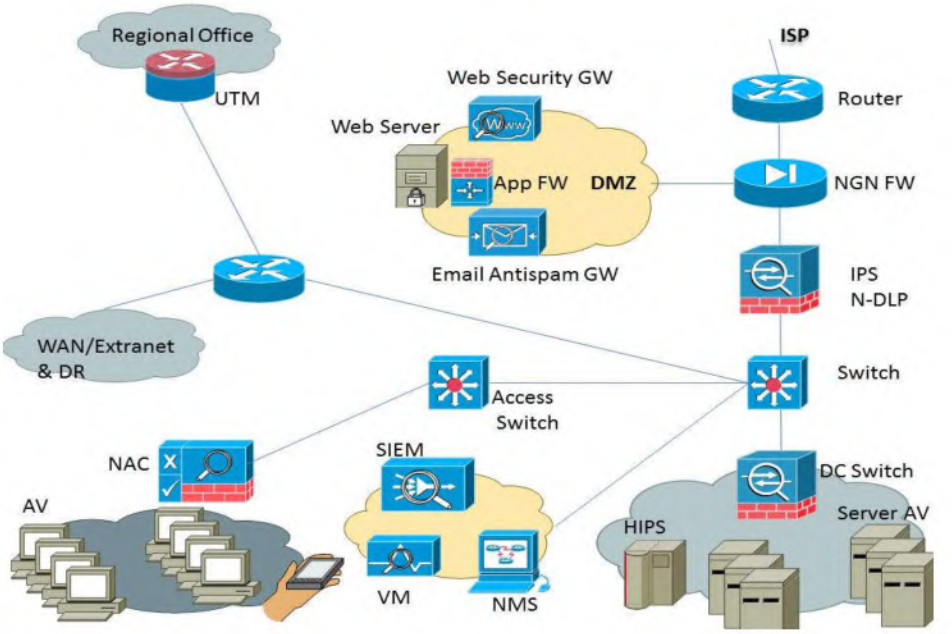


MICROSOFT SOFTWARE RESTRICTION POLICIES (SRP) FOR WHITELISTING

- Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run.
- Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.
- You can also use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. Software restriction policies are integrated with Microsoft Active Directory and Group Policy.
- You can also create software restriction policies on stand-alone computers. Software restriction policies are trust policies, which are regulations set by an administrator to restrict scripts and other code that is not fully trusted from running.

Topic No 145: WHAT IS SECURITY ENGINEERING?

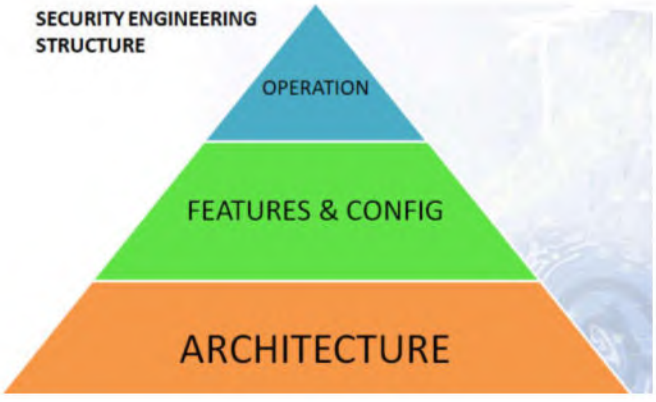
- Security Engineering is the third layer of the Security Transformation Model
- Consists of more in-depth and complicated security activities which take more time and effort
- Many times related to security architecture
- **Types of activities for security engineering:**
    - FW granular access lists
    - Building an effective DMZ architecture
    - Segregating the network with VLANs
    - Adding a security tool such as SIEM, FW, DLP, NAC, etc
    - App-DB encryption
- **DMZ Architecture Case Study:**
    - DMZ is an important zone in the overall security architecture
    - Devices which need to communicate to outside world placed in DMZ
    - Web servers, email gateways, web gateways



- **FW Access List Case Study:**
  - Most of the industry has not worked on building granular access lists
  - Most FWs have "allow all" for traffic
  - Granular access lists need to be built based on servers, or traffic flows
- **Why at Layer 3 of Security Transformation Model?**
  - Low hanging fruit first
  - Teams tend to get bogged down with advanced security tasks
  - These take time, effort, and often budget approval

Topic No 146: WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING?

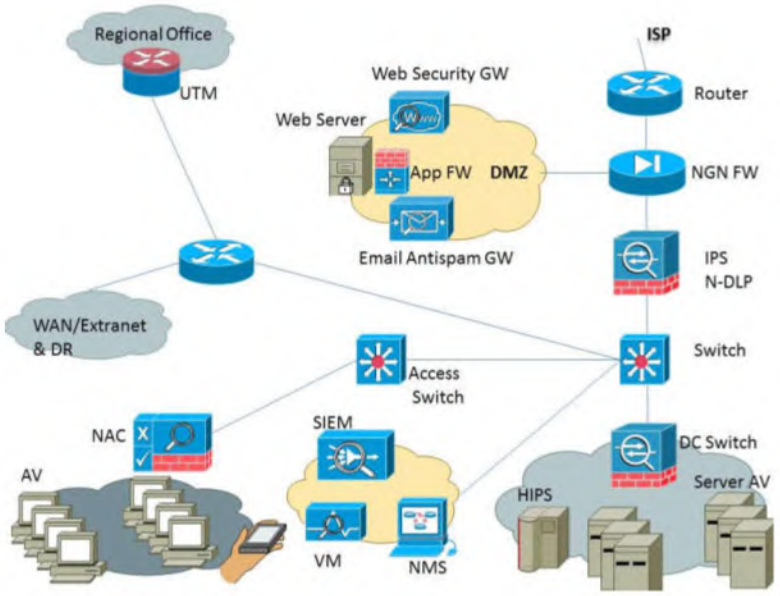
- Security architecture as per best-practices
- The right security devices in the right places
- Effective security configuration of security devices (features)
- Optimum operation of security devices
- Aggregate controls



Examples:

- FW first and then IPS
- Edge FW, data center FW
- Malware protection at the network edge

- VPN termination on remote access VPN device
- VPN tunnels for extranet connectivity

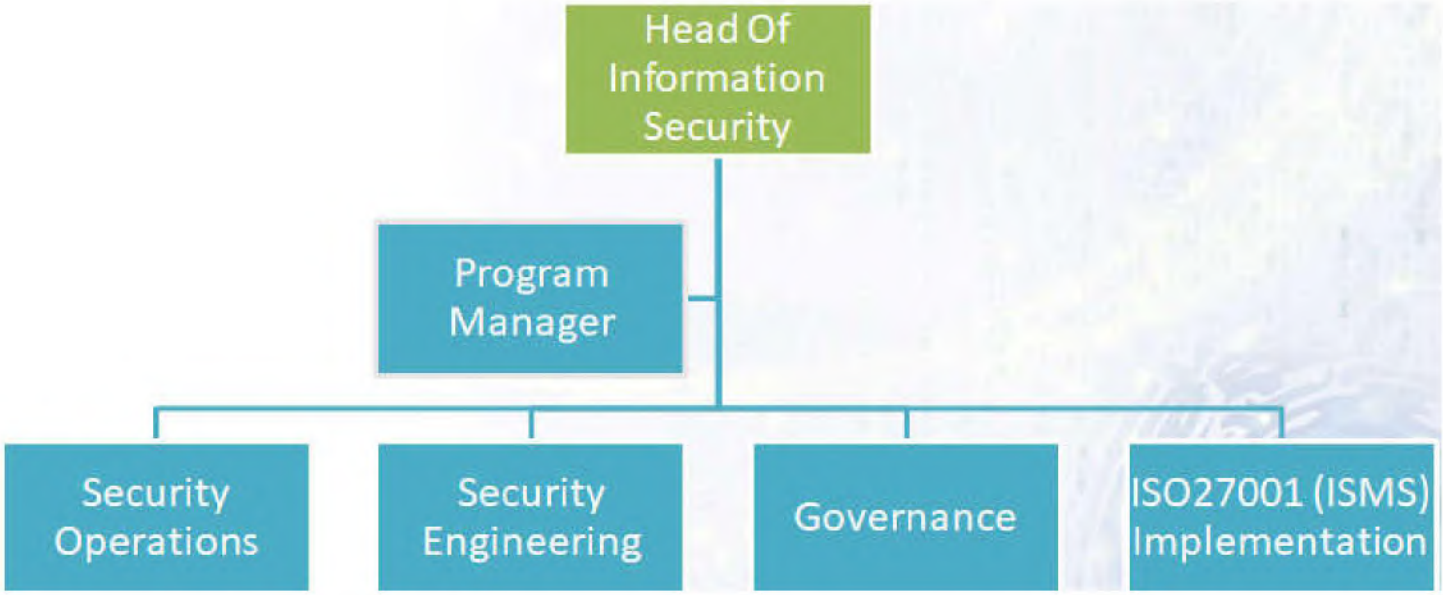


- The right time for setting up security engineering is when a new network is being designed & implemented
- Fixing a poorly architected operational network is an arduous task

Topic No 147: WHOSE RESPONSIBILITY IS SECURITY ENGINEERING?

- Security Engineering can best be accomplished with effective team work

TYPICAL STRUCTURE OF AN INFORMATION SECURITY TEAM

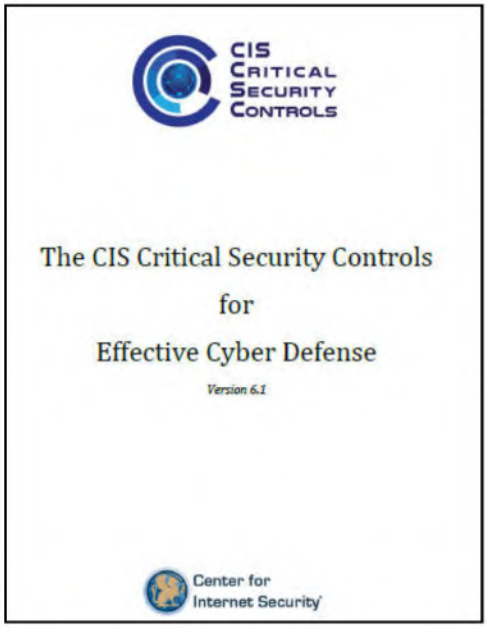


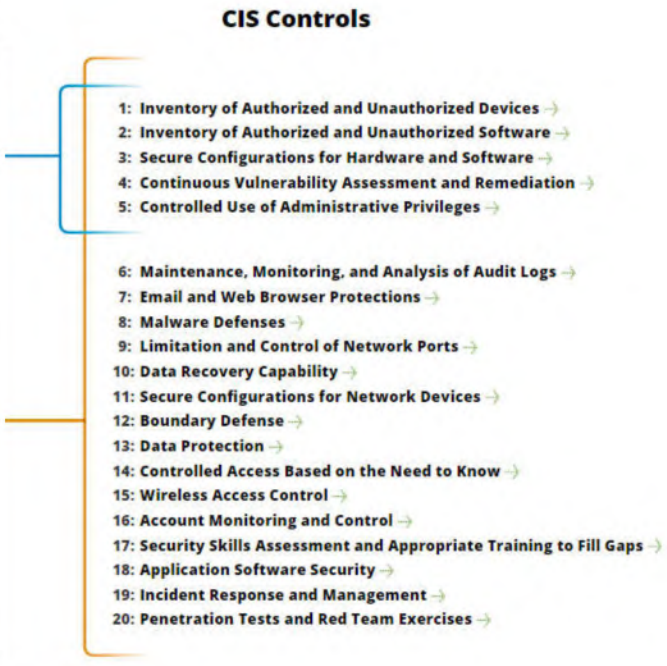
ACTIVITY	TEAM
SECURITY REQUIREMENTS	INFORMATION SECURITY WITH IT CONSULTATION
SECURITY DESIGN	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY DESIGN	INFORMATION SECURITY
SECURITY IMPLEMENTATION	NETWORK/IT SECURITY ASSISTED BY VENDOR
VALIDATING SECURITY REQMTS MET	INFORMATION SECURITY TEAM

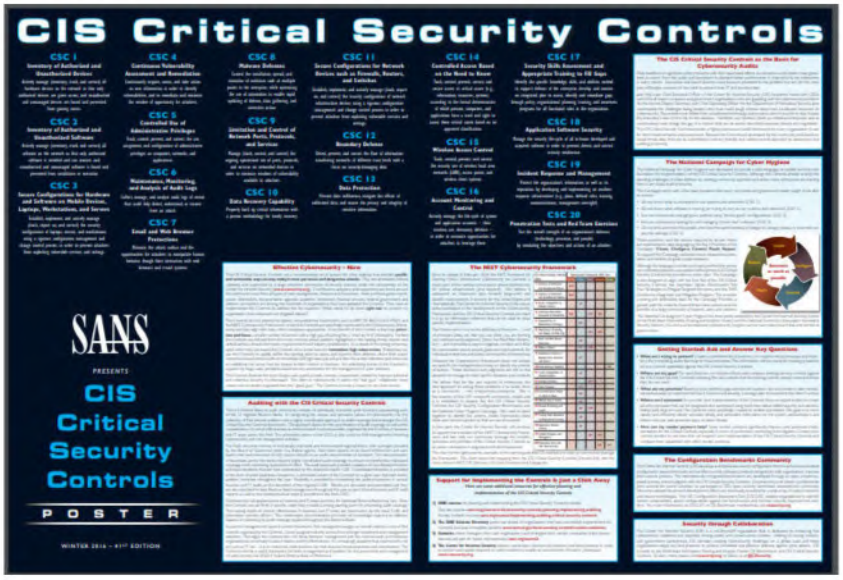
- As Security Engineering involves in-depth knowledge of IT & Security, the necessary resources, knowledge, skills, and people need to be pooled to achieve the objectives effectively

Topic No 148: CIS 20 CRITICAL SECURITY CONTROLS

- What are the CIS 20 Critical Security Controls?







- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

Topic No 149: CSC1: Inventory Of Authorized & Unauthorized Devices

1.1: Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

1.2: If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.

1.3: Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.

1.4: Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device and the department associated with each device.

- The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.
- The asset inventory created must also include data on whether the device is a portable and/or personal device.
- Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

1.5: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.

1.6: Use client certificates to validate and authenticate systems prior to connecting to the private network.

Topic No 150: CSC2: Inventory Of Authorized & Unauthorized Software

2.1: Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

2.2: Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

- The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software.
- Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

2.3: Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops.

- The software inventory system should track the version of the underlying operating system as well as the applications installed on it.
- The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

2.4: Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

Topic No 151: CSC3-I: Secure Configurations For HW & SW

3.1 Establish standard secure configurations of your operating systems and software applications.

- Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.
- These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

3.2: Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise.

- Any existing system that becomes compromised should be re-imaged with the secure build.
- Regular updates or exceptions to this image should be integrated into the organization's change management processes.
- Images should be created for workstations, servers, and other system types used by the organization.

3.3: Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

- Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

3.4: Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels.

- Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Topic No 152: CSC3-II: Secure Configurations For HW & SW

3.5: Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.

- The reporting system should have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command).

- These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

3.6: Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur.

- This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system.
- Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

3.7: Deploy system configuration management tools, such as **Active Directory Group Policy Objects** for Microsoft Windows systems or **Puppet for UNIX systems** that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

- They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

Topic No 153 & 154: CSC4-I: Continuous Vuln. Assessment & Remediation

4.1: Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

- Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common
- Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

4.2: Correlate event logs with information from vulnerability scans to fulfill two goals.

- First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged.
- Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

4.3: Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

- Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
- Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user

4.4: Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis.

- Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.

4.5: Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

- Patches should be applied to all systems, even systems that are properly air gapped.

4.6: Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans

4.7: Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.

- Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.

4.8: Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops).

- Apply patches for the riskiest vulnerabilities first.
- A phased rollout can be used to minimize the impact to the organization.
- Establish expected patching timelines based on the risk rating level.

Topic No 155: CSC5-I: Controlled Use Of Administrative Privileges

5.1: Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.2: Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

5.3: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

5.4: Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system

5.5: Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account

5.6: Use multifactor authentication for all administrative access, including domain administrative access Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

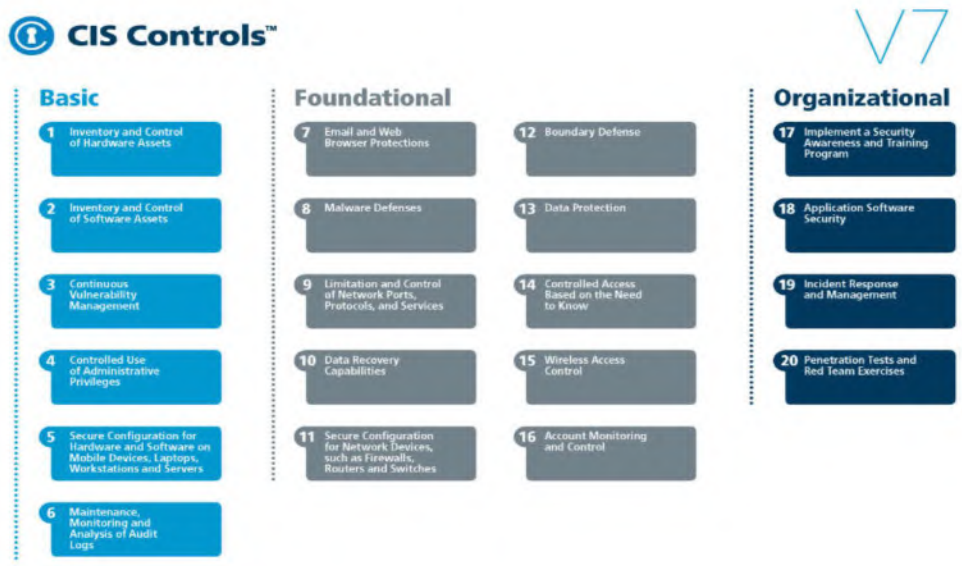
5.7: Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

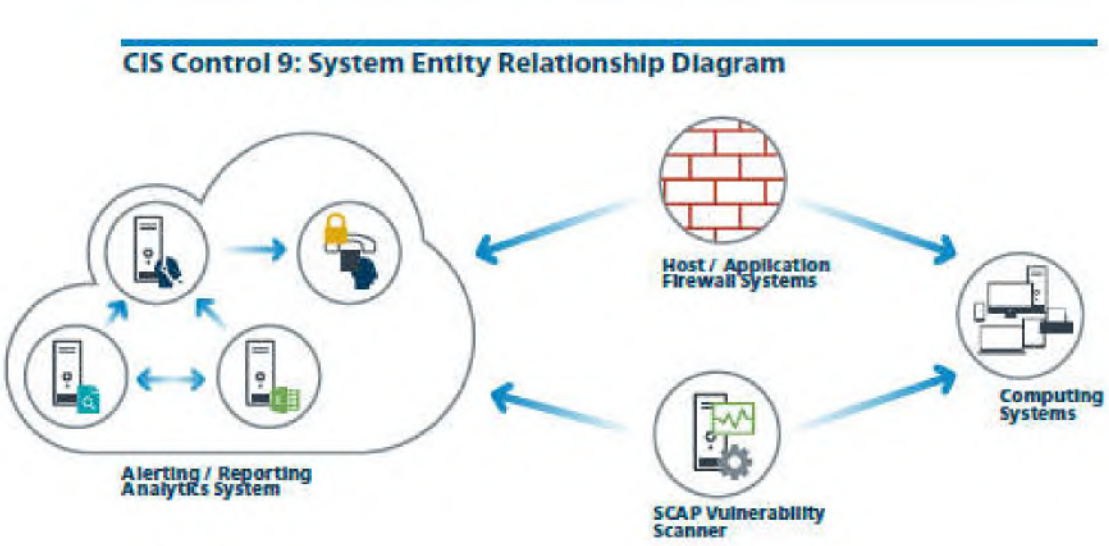
5.8: Administrators should be required to access a system using a fully logged and non-administrative account Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

5.9: Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Topic No 163: CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

CIS 20 Critical Security Controls





9.1: Associate Active Ports, Services and Protocols to Asset Inventory

- Associate active ports, services and protocols to the hardware assets in the asset inventory.

9.2: Ensure Only Approved Ports, Protocols and Services Are Running

- Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

9.3: Perform Regular Automated Port Scans

- Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

9.4: Apply Host-based Firewalls or Port Filtering

- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

9.5: Implement Application Firewalls

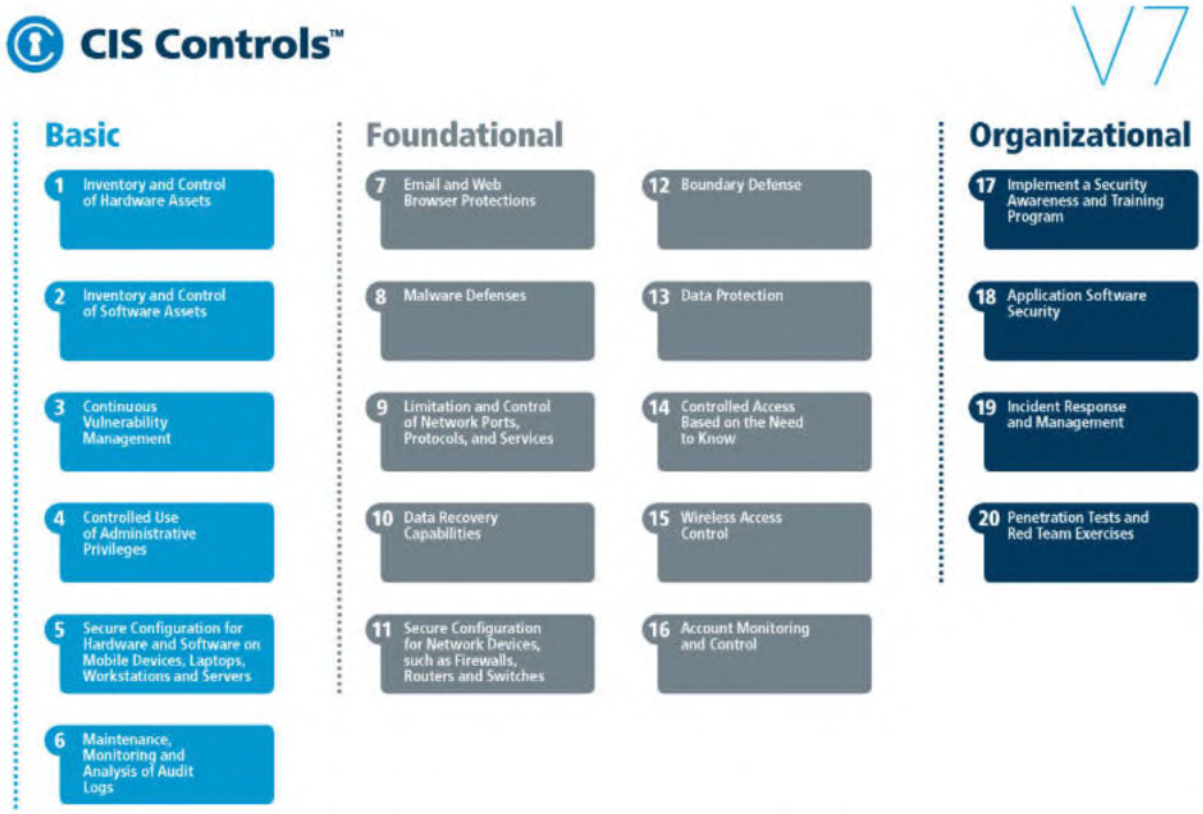
- Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

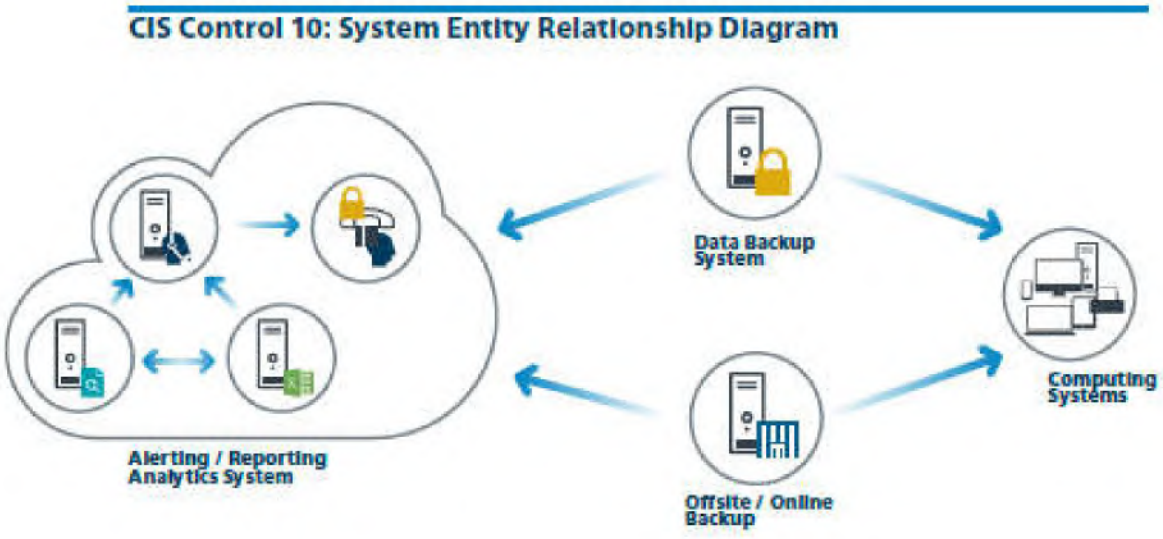
PROCEDURES & TOOLS:

- Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system.
- Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

Topic No 163: CIS CONTROL 10: DATA RECOVERY CAPABILITIES

CIS 20 Critical Security Controls





10.1: Ensure Regular Automated Back Ups

- Ensure that all system data is automatically backed up on regular basis.

10.2: Perform Complete System Backups

- Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

10.3: Test Data on Backup Media

- Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

10.4: Ensure Protection of Backups

- Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

10.5: Ensure Backups Have At least One Non-Continuously Addressable Destination

- Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

Procedures & Tools:

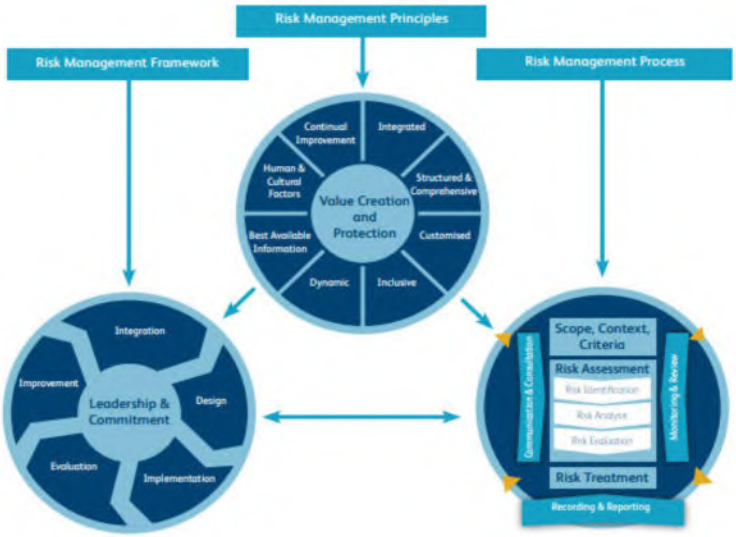
- Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.
- In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

Topic No 236: ISO31000:2018 – RISK MANAGEMENT – PROCESS

A Risk Practitioners Guide To ISO31000:2018

https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

Figure 3: Principles, framework and risk management process from ISO 31000



Topic No 237: ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

A Risk Practitioners Guide To ISO31000:2018

https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf

Successful implementation of a risk management initiative is an ongoing process that involves working through 10 activities below on a continuous basis. These activities relate to:

(1) Plan;

(2) Implement;

(3) Measure; and

(4) Learn.

Plan:

1. Identify intended benefits of the RM initiative and gain board support

2. Plan the scope of the RM initiative and develop common language of risk

3. Establish the RM strategy, framework and the roles and responsibilities

Implement:

4. Adopt suitable risk assessment tools and an agreed risk classification system

5. Establish risk benchmarks (risk criteria) & undertake risk assessments

6. Determine risk appetite and risk tolerance levels and evaluate the existing controls

Measure:

7. Evaluate effectiveness of existing controls and introduce improvements

8. Embed risk-aware culture and align RM with other activities in the organization

Learn

9. Monitor and review risk performance indicators to measure RM contribution

10. Report risk performance in line with obligations and monitor improvement

Although ISO 31000 covers the full scope of requirements for a management system, it is for the organization to convert those requirements into a checklist and action plan.

Topic No 238 & 239: INCIDENT MANAGEMENT- I & II

Information Security Incident Management

- Have a look at ISO27002: 2013 (Page 67+) for best practices guidance

Objective:

- "To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses."

Top 10 Considerations For Incident Response

https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf

1. Audit & Due Diligence

Performing an audit will let you know how well prepared the organization is for Incident Responsein terms of:

- People
- Process
- Equipment

2. Create Response Team

- An Incident Response team should consist of people with sufficient technical skills. It is important that the team members consist of SME's (Subject Matter Experts) or Knowledge Engineers from different domains across the organization.
- Team lead
- Triage officer
- Incident handler

3. Create Documented IR Plan

- An organization should have a well-documented IR plan that would guide the IR Team during an incident.
- A comprehensive plan at minimum , should cover Roles & Responsibilities, Investigation, Triage and Mitigation, Recovery, and Documentation process.

4. Identify Indicators & Triggers

- What would be categorized as an incident at your organization?
- How important or weighty are the factors that would trigger an incident?
- Clearly define what can trigger an incident

5. Investigate the Problem

- Establishing , clearly what has occurred
- Identify what systems, people or processes have been compromised or affected based on incident
- Determine what happened & what was compromised
- Determine the point of origin of the incident where possible. This infers that you establish the source of the threat or attack vector
- Specify your investigation objectives, triage and resolution methodology

6. Triage & Mitigation

Investigation leads to the triage and resolution process. As the team identifies potential exposure, they should plan and execute effective mitigation accordingly:

- Classification of Incident
- Incident Prioritization
- Assigning specific tasks to specific people

7. Recovery

- Once a thorough investigation has been carried out, recovery is a significant step for restoring services or materials that might have been affected during an incident. This could be the task of the technical team (transition from active incident to standard monitoring)

8. Documentation & Reporting

- A comprehensive incident report is required in keeping with best practices and with the Incident Response plan. The type of reports that might be required might vary but should help in managing and reviewing incidents satisfactorily.

9. Process Review

Make intelligent decisions about important factors:

- Should I increase or decrease the number of Incident Handlers?
- What risks did we identify during the incident that needs to be followed up for action and monitored closely?

10. Practice, Practice, Practice

- Do not wait until an incident occurs before you put your team to work. Once the organization has a workable plan in place, it is advisable to run through part or all of it as a tabletop exercise, and run through various scenarios and drills.

Topic No 240: CHANGE MANAGEMENT-I

Itil Change Management Best Practices

http://www.bmc.com/guides/itil-change-management.html

ITIL change management is a process designed to understand and minimize risks while making IT changes. Businesses have two main expectations of the services provided by IT:

1. The services should be stable, reliable, and predictable.
2. The services should be able to change rapidly to meet evolving business requirements.

3. These expectations are in conflict. The objective of change management is to enable IT service management to meet both expectations—to enable rapid change while minimizing the possibility of disruption to services.

Types Of Changes

Standard changes are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront.

- These changes are managed according to policies that are the IT organization already has in place.
- Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require approval from a risk management perspective.

Normal Changes

- **T**hose that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.

Emergency Changes

- Arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately.