(21) CS 301 12/9/22 Objective + Subjective
Data Structures - Final Term Preparation

CS205

Asset Management tools for Security Functions

- Asset management helps with the following Security functions

i) patch management ii) Software whitelisting
iii) Software assets discovery and management
iv) Enterprise tracking and reporting

- Gartner refers this area as Unified endpoint management (UEM)
- (UEM) tools combine the management of multiple endpoint types in a single conside
UEM tools perform following functions

Gartner UEM 2018 Report

i) configure, manage and monitor iOS, Android, windows 10 and macOS, and manage some Internet of Thing (IoT) and wearable end
ii) Unify the application of configurations, manage profiles, device ~~compila~~ compliance and data protection
iii) Provide a Single view of multi device users, enhancing efficiency of end-user Support an gathering detailed workplace analytics
iv) Act as a coordination point to orchest the activities of related endpoint technologi such as identity services and security infra-structure

Date: / /20 Day:

(2) Microsoft Software Restriction Policies 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 microsoft Security and management strategy to assist enterprises in increasing the reliability, integrity and manageability of their computers

UEM (unified endpoint management) tools perform two functions

1. Gartner UEM 2018 Report
2. Microsoft Security Restriction Policie

- SRP are integrated with microsoft Active Directory and Group policy
- You can also create Software restriction policies on Stand-alone computers.

Date: / /20

Security Engineering

- Security engineering is 3rd layer of Security Transformation model
- Consist 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

- Firewall granular access lists
- Building an effective DMZ (Demilitarized zone) architecture (seprate the LAN from untrusted network)
- Segregating (division) of networks with VLANs
- Adding a security tool such as SIEM, FW, DLP, NAC etc → components of IT enterprise
- 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
- These includes web servers, web gateways email gateways

FW Access List case study

- Most of industry has not worked on building granular access lists
- most FWs have "allowall" 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 effort, time and often budget approval

Objectives

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

Example

- First FW 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

(5) → Head of information Security Program manager

Date: / /20

Whose Responsibility

- Security engineering can best be accomplished with effective Team work

Activity	Team
Security Requirement	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 Requirements	Information Sec Team

- NS 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

CIS 20 Critical Security Contro

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorize Software
- Continous Vulnerability Assessment and Remediation
- Data Recovery Capability
- Secure Configurations for Network Devices such as FWS, Routers, and Switche

Inventory of Authorized & Unauthorized Devices

Date: / /20 Day:

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. 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.

CIS CONTROLS

⇒ Basic

1 Inventory and control of hardware assets
2 Inventory and control of Software assets
3 Continuous Vulnerability Management
4 Controlled use of Administrative privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, monitoring and Analysis of Audit Log

⇒ Foundational

7 Email and Web browser protections
8 Malware defenses
9 Limitation and Control of Network ports, Protocols, and Services
10 Data Recovery Capabilities
11 Secure configuration for Network Devices, Such as firewalls, Routers and Switches

12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

198 TO 283
CS205

(8)

How to build effective Infosec Governance?

The key success factors to build effective information Security Governance are

- Leadership
  Executive management role
  Tone at the top
  Supportive budgets and resources
- Strategy
  How the organization will gear up and focus for the Security transformation
- Structure
  How will different teams work together to achieve the common goals
- Reporting
  what will be reported?
  what will be the frequency of reports?
  who will monitor and track progress?
- project management
  How will an exceptional discipline be built?
- Culture

Building effective infosec governance is based on good management, execution and project management skills

Q Infosec Dept Structure for Large sized org

Date: / /20 Day:

A:
- A large organization can have an Infosec Team ranging between 25-50 staff
- 10% of IT (250 to 300 IT Staff)

Q Infosec Dept Structure for mid-sized org
- A mid-sized organization can have an Infosec Team ranging between 10-15 staff
- 10% of IT (100 to 150 IT Staff)

Q Infosec Dept Structure for small org
- A small-sized organization can have Infosec Team ranging between 2-4 staff
- 10% of IT (15 to 50 IT Staff)

Q What is Role of CISO in driving Infosec program

The CISO plays a crucial role in successfully driving the infosec program
- Consists of two factors
  - CISO Skills
  - placement in organizational hierarchy
- CISO Skills

These Skills include
- Technology Domain knowledge (Have Solid technical base)
- Governance Domain knowledge (Policies & SOPs)
- Leadership and Strategy
- People Skills (Good people management skills)

Q what are the key inhibitors for Security program failore

A There may be several inhibitors to achieving a Successful Security transformation project

i) • Executive management
- Allocate budget and approve resources
Set organizational priority & "Tone at the top"

ii) • Strategy & Structure
- Addressing the needs and inter-linkages to make the entire machinary work in a
• Streamlined manner
- Having Sufficient experience to work at various levels of the organization

iii) • Execution
- Allocating tasks to run different phases in parallel and Sequentially
- Team / Steering Committee / Board presentations

* Note: Reasons for Security program failure
i) poor executive management ii) poor Strategy & Structure iii) poor execution

What should be Infosec Strategy for Smaller Organizations
Smaller & newer Organizations face unique challenges which may require a creative approach to implement a Successful Security transformation program

A Smaller and newer organizations face challenges as:
- Limited budget
- Untrained staff
- Adhoc culture
- So, the leaders of small organizations are usually aware of their organizational capacity and limitations with experience
- work with the organizational leadership to deploy competent project lead and team members

Q What are the common challenges to security Documentation?

A As we know policies, SOPs, Checklists, guidlines, and records are all important parts of Information Security management System (ISMS) and are based on documentation.
Challenges are
i) process culture absent: Adhoc culture
- Rapidly changing priorities
ii) Defective and voluminous documentation.
- Effective writing & documentation is a rare skill
iii) Training & Awareness: Incentivize
- Invest in raising competence & skills of staff
iv) Roles & responsibilities: Is right person working at right place?
- Are staff aware of their responsibilities

Q what are policies?

A policies are formal statements produced and suported by senior manageMent.
They can be organization-wide, issue-specific or system-specific
Your policies should be like a building foundation that are built to last and resistant to change or erosion

- Driven by business objectives
- Easily accessible & understandable
- Created with the intent to be in place for several years.

Q what are standards?

Standards are mandatory actions or rules that give formal policies support and direction. one of the more difficult parts of writing standards for an Infosec program is getting a company-wide consensus.

- Used to indicate expected user behavior
- might specify what hardware and software solutions are available and supported
- Compulsory and must be enforced to be effective

Date: / /20 Day:

Q What are the procedures?

A procedures are detailed step by step instructions to achieve a given goal.
They are typically intended for internal departments and should adhere to strict change control processes

- Often act as the "cookbook" for staff
- Detailed enough and yet not too difficult that only a small group will understand
- Installing OS, performing a system back-up are example of procedures

209-285
261

(14)

Date / 19 Day

Q What are guidlines?

A Guidlines are recommendations to users when specific standards do not apply.
Guidlines are designed to streamline certain processes according to what the best practices are

- Guidlines are more general vs. specific rules
- provide flexibility for "unseen" unforseen circumstances.
- Should NOT be confused with formal policy statements

Q How to Develop Effective Security policies
There 6 steps to security policy excelence

- Create & Review
- Distribute
- Achieve consent
- understanding
- Auditability
- Reporting

what are policy pitfalls
i) Poorly worded policy ii) Badly structure policy iii) Out-of date policy iv) Unenforced policies v) Lack of management vi) Inadequately communicated policies

(15)

Q How to best use advantage of ISO27001:2013 (ISMS)

A - Implement Security Transformation model
- Cut off security transformation project with ISO27001:2013 (ISMS) certification
- ISMS as a complementary reference and checklist rather than main framework

Q what are clauses 4-6 of ISO27001:2013 (ISMS)

- context
  - understanding organization & its context; internal & external issues relevant to its purpose
- Leadership & commitment
  - policy & objectives are established
  - Integrating ISMS into org processes
  - Communicating importance
- planning
  - Address org risks & opportunities & preventions
  - Identify, analyze, evaluate risks

Q what are clauses 7-10 of ISO27001:2013 (ISMS)

A Let's have a look at clauses 7-10

- Support
- operations
- Performance Evaluation
- Improvement

what is (payment card industry) PCI Data Security Standard (DSS)

- Designed to ensure that all companies that accept, process, store or transmit credit card info maintain a secure environment
- managed by Security Standards Council
- SSC is an independent body that was created by major payment cards brands (Visa, mastercard, American Express, Discover and JCB)
- 6 broad goals and 12 requirements
- PCI is specific to card environment to protect cardholder data

Q How can we improve the security posture?
A very useful collection of controls for improving security posture are SANS/CIS 20 Controls

Q. First 5 CIS controls?

- Inventory of Auth & unAuth Devices
  - 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.
  - Both active tools that scan through IPV4 or IPV6 network adress ranges and passive tools that identify hosts based

devices should be employed

- Inventory of Auth & unAuth Software
  - Devise a list of authorized software and version that is required in the enterprise for each types of system, including servers workstations, and laptops of various kinds and use
  - The list should be monitored by file integrity checking tools to validate that the authorized software has not been modified
- Secure config. for SW & HW
  - Establish standard secure configurations of your operating systems and software applications
  - Standardized images should represent hardened versions of underlying operating system and applications installed on syster
  - These images should be validated and refreshed on a regular basis
- Continous Vulnerability assesment & Remediation
  - Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis
  - Deliver prioritized lists of most critical vulnerabilites to each responsible system

administrators and departments in reducing risk
- use a SCAP (Security Content Automation protocol)
- Code-based vulnerabilities & Configuration-based vulnerabilities
- Controlled use of Admin privileges
- minimize administrative privilege and only use administrative accounts when they are required
- Implement focused auditing on the use of administrative privileged functions & monitor for anomalous behavior
- This is an ideal framework for more detailed and specific guidance on deeper security controls

Q what is NIST framework? → National Institute of Standards & Technology
- The Computer Security Resource Center (CSRC) website guides to NIST resources on Computer, cyber, & information security and privacy
- Its main contents are publications, project research, news & events
- Information Technology Laboratory (ITL) two division
- SP800 → 1990-present. Include guidlines, recommendations
- SP1800 → 2015-present (guidlines)

Q What is COBIT?

- Control Objectives for Information Technology (COBIT)
- ISACA framework for IT Governance
- COBIT 5 brings five principle and seven enables ; ~~first five are~~

Q What are risk management components & principles?

Risk management includes five components:

- Integration - Improvement - Evaluation
- Design - Implementation

and 8 principle

- Integrated - Structured & Comprehensive - Customized
- Inclusive - Dynamic - Best Available Information
- Human & Cultural factors - Continual improvement

Q How to implement Risk management?

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

i) Plan
ii) Implement
iii) Measure
iv) Learn

Q Challenges to Cybersecurity
- Reactive
- Superficial
- Compliance
- Box-Approach
- Governance Overkill

Q Frequency of ISMC, Steering Committee and Board meeting
There frequency as weekly, monthly, Quarterly

Q How does CSMM help?
- Cyber Security Maturity Matrix (CSMM) offers a proactive, structured, sequential model to implement security
- Model is certifiable
- Cyber Security Certification Board (CSCB) will certify status of organization

Q Layers of CSMM
Foundation
Fundamental
Hardened
protected
monitored
Secured

Q 8 step Methadology for Security hardening

- Identify critical assets
- Research on applicable security controls
- Checklist of applicable controls
- Document controls into SOP
- Implement controls on test setup
- Validation of control implementation
- Change management process for PROD
- Implement on PROD & monitor