DSci526:
Secure Systems Administration

Virtualization and Cloud Computing
(Student presentations on Incident Response)
Preparation for Mid-term exam

Prof. Clifford Neuman

Lecture 7
3 March 2021
Online

Announcements

- Mid-term exam is Next Friday
  - Friday March 10th – Noon to 1:40PM Pacific time
  - We will review for the mid-term near end of lecture
  - Exam is open book and open note and online
  - Alternate time available at 6PM

Today's Presentations

Secure Cloud Administration and Incident Response Planning

- Announcements/Logistics (approx. 5 minutes)
- Secure Cloud Administration (approx. 20 min)
  - Sarahzin Chowdhury - Cloud Access Security Brokers
- Lecture component on Cloud Security (55 min)
  - Dr. Neuman
- Break (10 min)
- Incident Response Planning (approx. 40 min)
  - Carol Varkey
  - Amarbir Singh
- Review for Mid-Term Exam (30 min)
- Group Project Discussion (40 min)

March 17th – Secure Networking

- Christopher Samayoa (Network Access Control)
- Shanice Williams – Network Monitoring – WireShark
- Pratyush Prakhar – Web Penetration Tools

Presentations March 24th Configuration Management

- Marco Gomez
- Louis Uuh

March 31st – Security Incident Event Management

- Malavika Prabhakar
- Anthony Cassar
- Dwayne Robinson (Network Perimeter Detection)
- MaryLiza Walker (Attack Forensics)
- Jason Ghetian

Linux Related Topics – April 14th

- Azzam Alsaeed – SELinux
- Alejandro Najera – Linux Administration
- Tejas Pandey – Identity Management in Linux
- Ayush Ambastha – Linux Kernel Security

DSci526:
Secure Systems Administration

Virtualization and Cloud Computing
(Student presentations on Incident Response)
Preparation for Mid-term exam

Prof. Clifford Neuman

Lecture 7
3 March 2021
Online

Cloud access Security Brokers (CASBs)

An overview on the importance of cloud security with examples of CASBs

Sarahzin (Chowdhury) Shane

March 3, 2021

Agenda

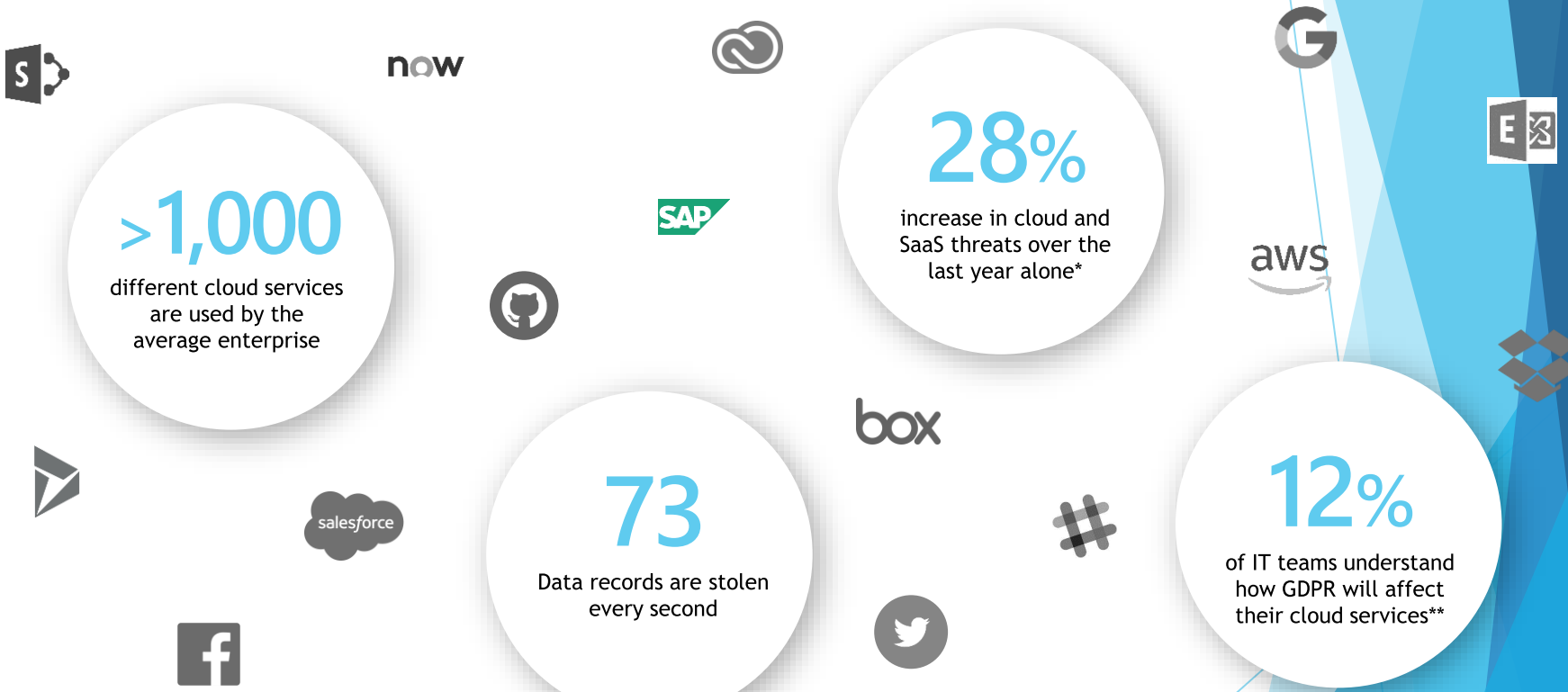
- What is a CASB?
- Capability Categories
- Cloud Discovery
- Threat Detection
- Data Protection
- Challenges CASBs aim to fix
- Questions

What is a CASB?

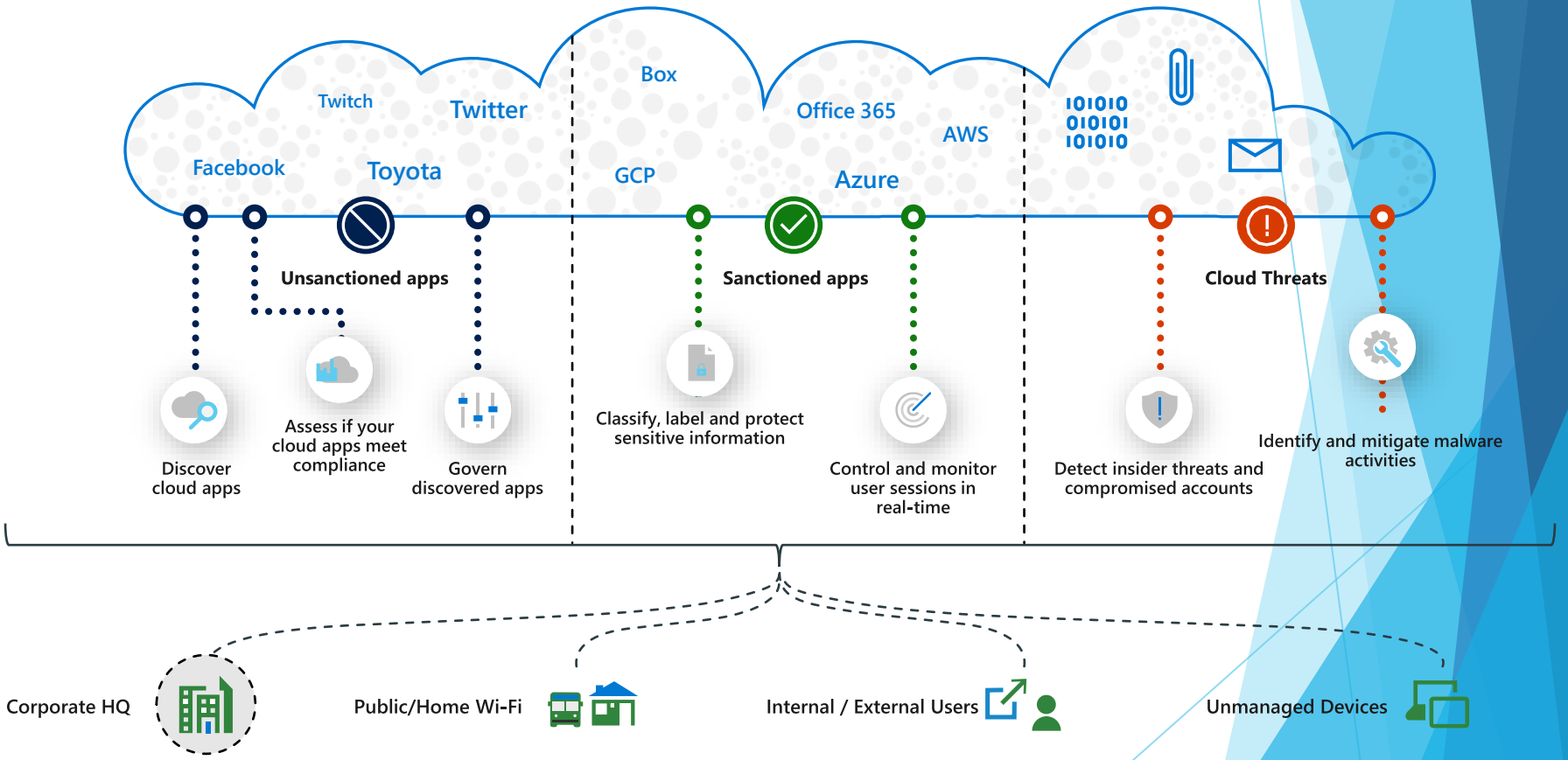
- CASBs are defined by Gartner as:

On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security polices as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

Security Approach



Top CASB use cases



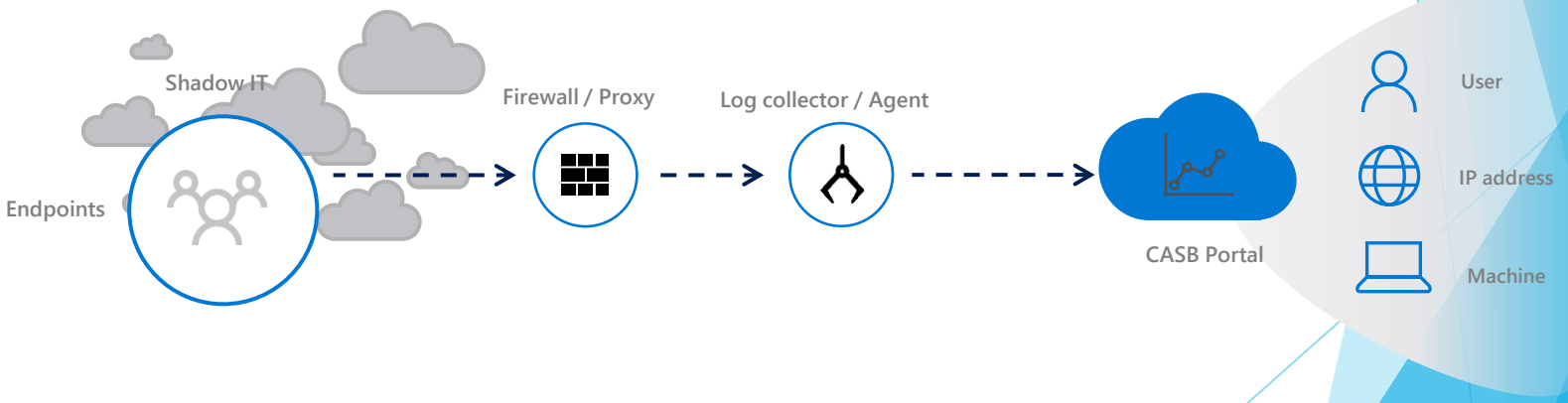
Capability Categories

- Cloud Discovery (Visibility)
- Threat Detection
- Data Protection

- You can also see compliance scattered all around

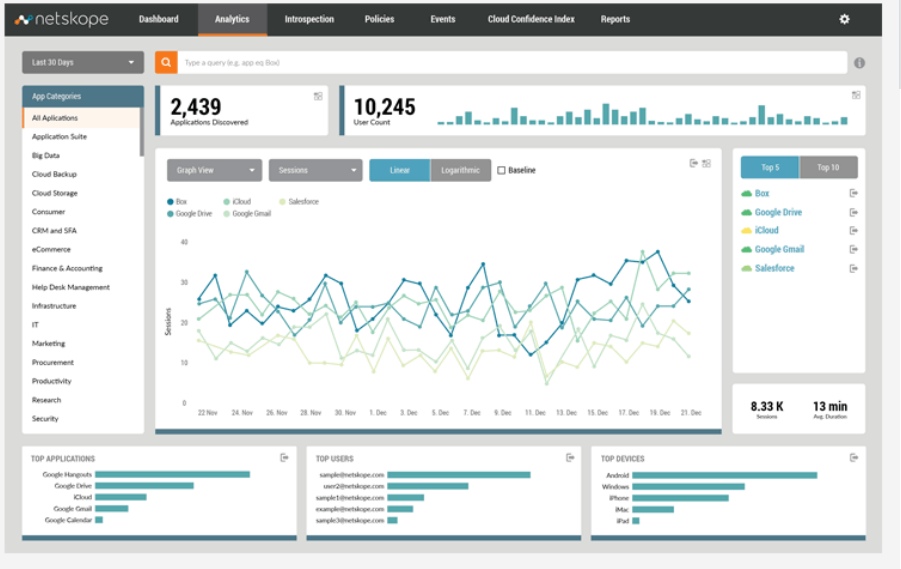
Cloud Discovery

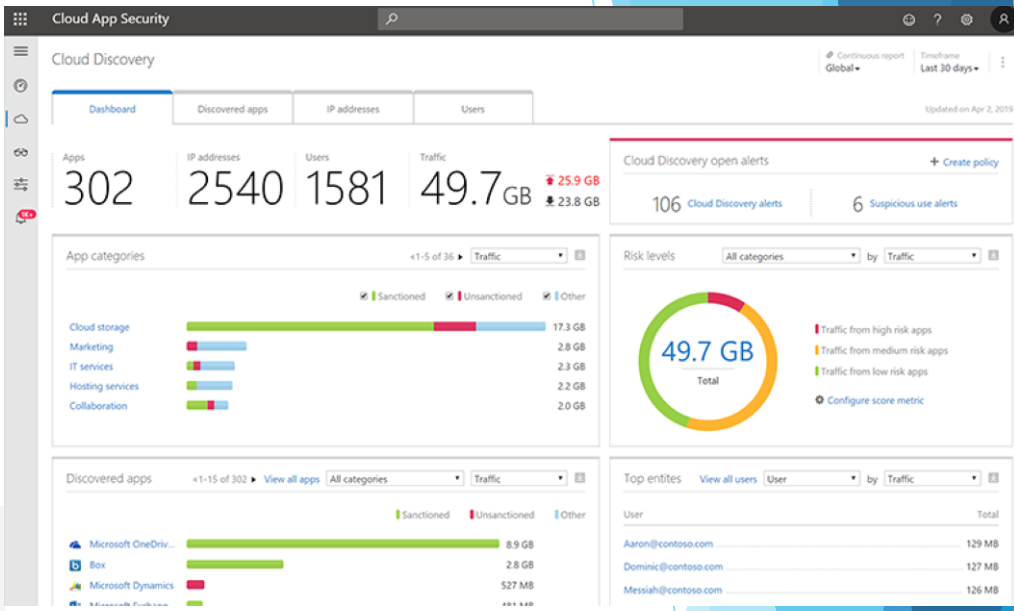
- Identity apps being used in your environment, both approved and unapproved
  - Traffic data
  - Top users and IP addresses
  - Categories and risk scores of Apps
  - Native Integrations



Examples

netskope





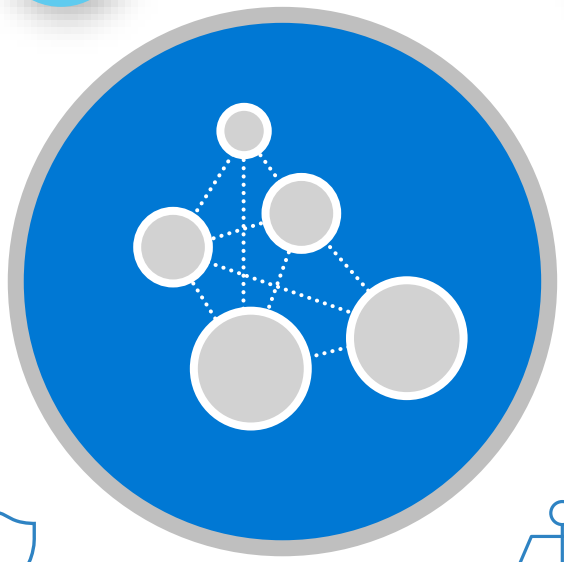
Microsoft

Threat Detection

80 days — Median dwell time of attackers

+250% — inbound phishing attacks

93% — of organizations are dealing with rogue cloud app usage



Malicious Insider

Protect against disgruntled employees before they cause damage

Malware

Detect malware in cloud storage as soon as it's uploaded

Ransomware

Identify ransomware using sophisticated behavioral analytics technology

Rogue Application

Identify rouge applications that access your data

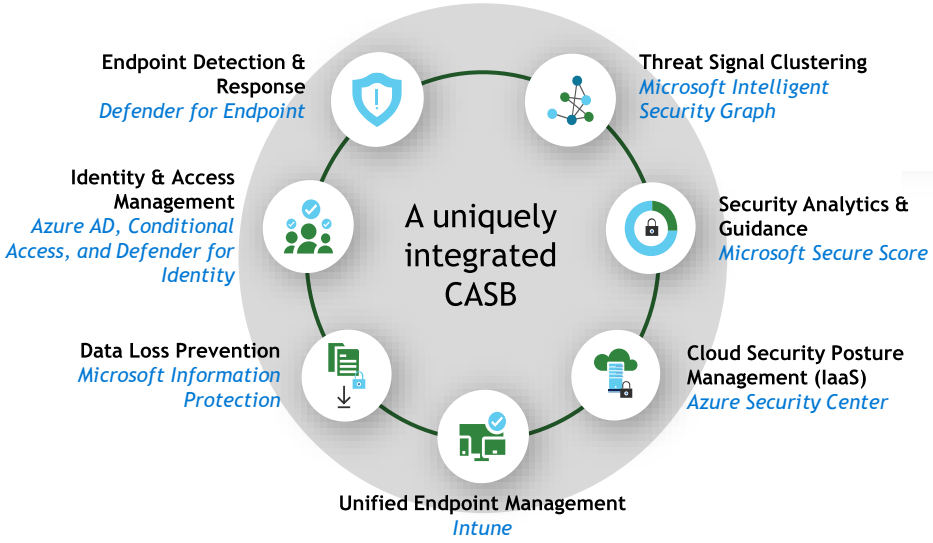
Data exfiltration

Detect unusual flow of data outside of your organization

Compromised Accounts

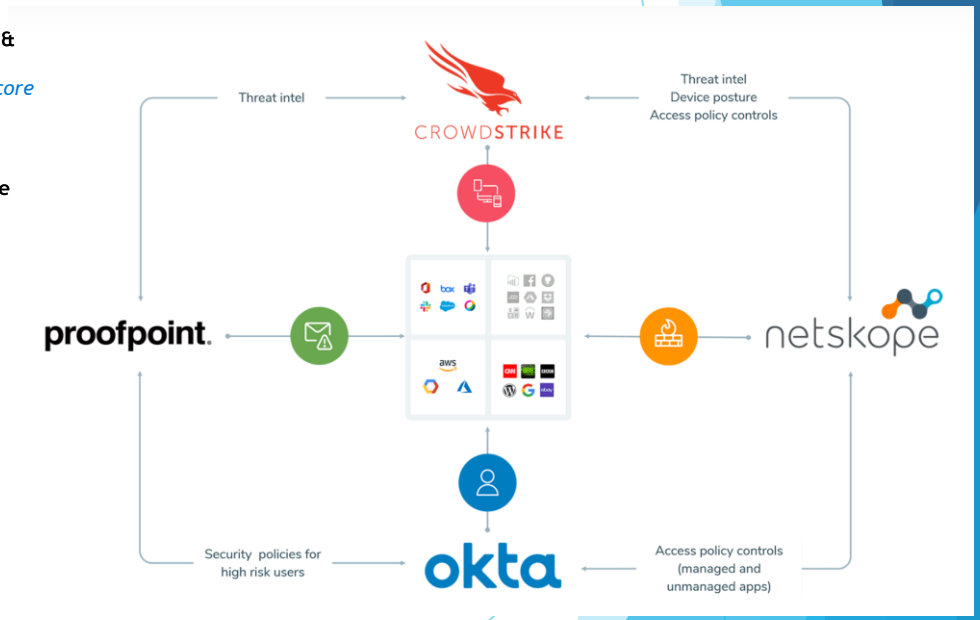
Combat advanced attackers that leverage compromise user credentials

Examples



Microsoft

netskope



Data Protection

Data is abundant; it needs to be accessible, collaborative, and secured

Understand your data and exposure in the cloud

- API-based App Connectors (near real-time)
- Visibility into sharing and data labels
- Quantify over-sharing exposure (external,

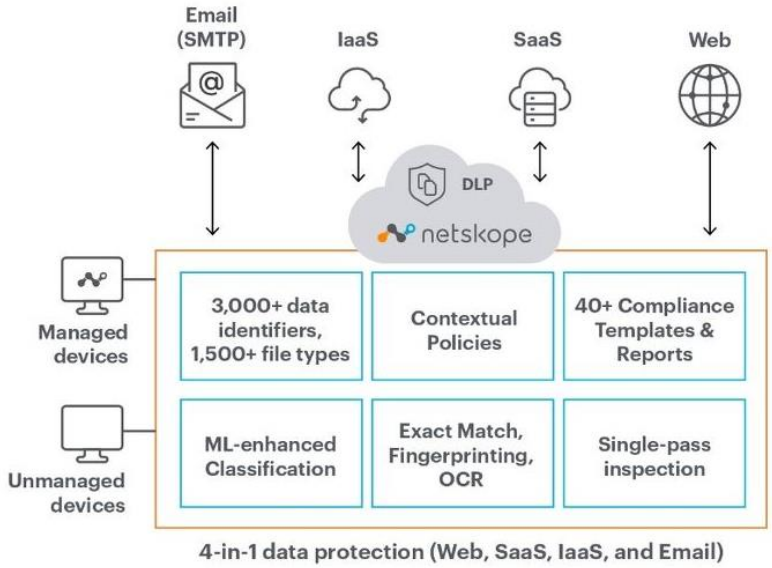
Classify and protect your data no matter where it's stored

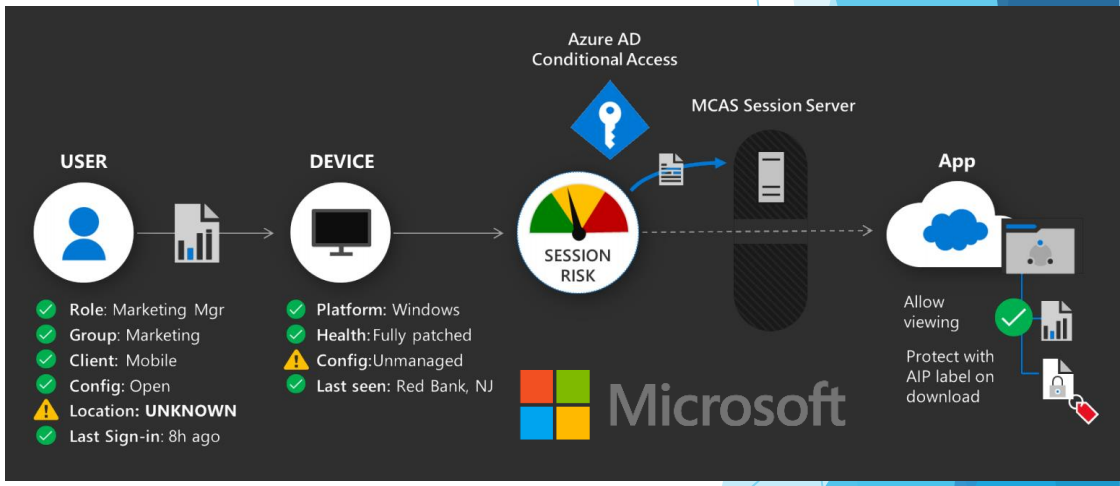
- DLP policies
- Third party or first party DLP solutions
- Automatically protect and encrypt your data
- Real-time Proxy

Monitor, investigate and remediate violations

- Create policies to generate alerts and trigger automatic governance actions
- Identify policy violations
- Investigate incidents and related activities

Examples


Email (SMTP)
IaaS
SaaS
Web
DLP
netskope
Managed devices
Unmanaged devices
3,000+ data identifiers, 1,500+ file types
Contextual Policies
40+ Compliance Templates & Reports
ML-enhanced Classification
Exact Match, Fingerprinting, OCR
Single-pass inspection
4-in-1 data protection (Web, SaaS, IaaS, and Email)


Azure AD Conditional Access
MCAS Session Server
USER
DEVICE
SESSION RISK
App
Role: Marketing Mgr
Group: Marketing
Client: Mobile
Config: Open
Location: UNKNOWN
Last Sign-in: 8h ago
Platform: Windows
Health: Fully patched
Config: Unmanaged
Last seen: Red Bank, NJ
Allow viewing
Protect with AIP label on download
Microsoft

Challenges CASBs aim to fix

- What risky apps are being used in your environment?
- Blocking unapproved apps
- Enforce MFA and SSO to download information or access certain apps
- Provision access to enterprise level apps
- Block uploads/downloads of sensitive data
- Control data sharing
- Continuously monitor all apps in one location

Questions?

Today's Presentations

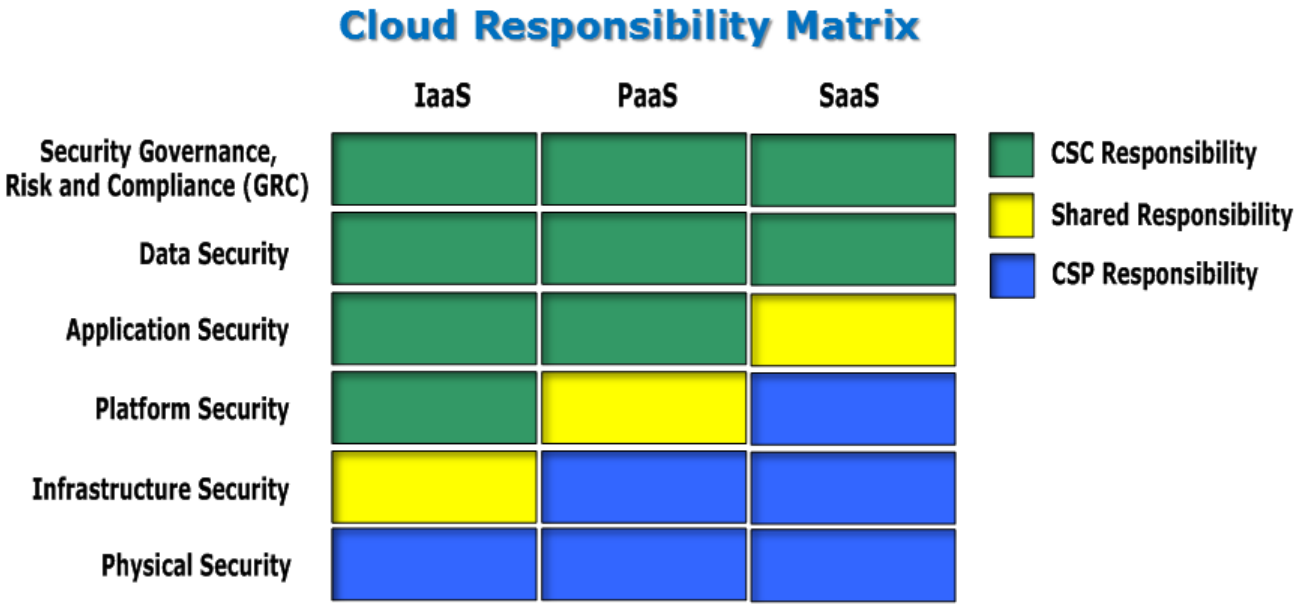
Secure Cloud Administration and Incident Response Planning

- Announcements/Logistics (approx. 5 minutes)
- Secure Cloud Administration (approx. 20 min)
  - Sarahzin Chowdhury - Cloud Access Security Brokers
- Lecture component on Cloud Security (55 min)
  - Dr. Neuman
- Break (10 min)
- Incident Response Planning (approx. 40 min)
  - Carol Varkey
  - Amarbir Singh
- Review for Mid-Term Exam (30 min)
- Group Project Discussion (40 min)

Secure Administration of Services Running in the Cloud

- Distinct from Secure Administration of Cloud Services
  - This is about how to ensure that your applications are administered securely.
  - Your applications would otherwise run on your own systems.
- Similarities
  - All the tools that we have discussed (or will discuss) must still be implemented for cloud deployments.
  - Encryption, Firewalls, VPNs, Identity Management, Configuration Management, Software Security
  - Running in the cloud does not make your buggy code correct.
- Differences
  - You do not have physical control of parts of your system.
  + Parts of your system may be more professionally managed.

Shared Responsibility Matrix for Cloud Services



General Discussion of Services and who is responsible

- Containment Architecture
  - Networking
  - Firewalls
  - Access controls to and on servers
  - Access control to storage
  - Choice of data relegated to the cloud
- Physical Security
  - Distributed Application/Services
  - Placement / Geolocation / Employees
- Software Security
  - See previous slide
- Platform management – administering administration
- Identity Management
- DoS Defenses
- Intrusion Detection

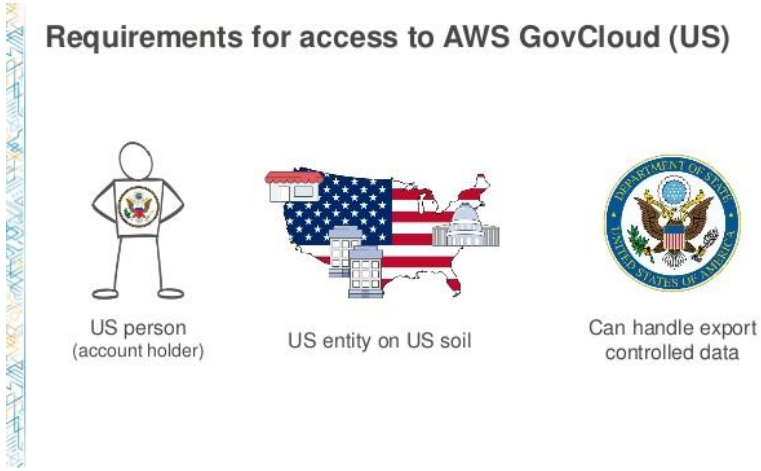
One example

AWS GovCloud (US) Region

Designed to address the specific regulatory needs of United States federal, state and local agencies, education institutions and the supporting ecosystem.

AWS GovCloud (US) Region:

- Subject to FedRAMP High and Moderate baselines
- Allow customers to host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads
- Operated by employees who are U.S. citizens on U.S. soil
- Only accessible to vetted U.S. entities and root account holders, who must confirm they are U.S. Persons to gain access



One example

Gives vetted government customers and their partners the **flexibility to architect** secure cloud solutions that comply with:

Federal Risk and Authorization Management Program (FedRAMP) Moderate and **High. Learn	Federal Information Security Management Act (FISMA) Low, Moderate and **High	Department of Defense Security Requirements Guide (SRG) Impact Levels 2, **4 and **5. Learn more.	U.S. International Traffic in Arms Regulations (ITAR)	**Department of Commerce Export Administration Regulations (EAR)	**IRS-1075 Encryption Standards for Federal Tax Information (FTI) Section 6103 (p)

**Department of Justice Criminal Justice Information Service Security Policy	**National Institute of Standards and Technology (NIST) SP 800--53 (rev4) and SP 800-171	**Federal Information Processing Standard Publication	**Defense Federal Acquisition Regulation Supplement (DFARS)	Healthcare Insurance Portability & Accountability Act Privacy Standards	Payment Card Industry Security Standards

Other Vendors may provide similar services and it is up to you to validate the accreditation of such services (including this example).

Incident Response Planning

Carol Varkey, Amarbir Singh

What is Incident Response Planning

An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

-Cisco

A sufficient incident response plan offers a course of action for all significant incidents.

If an incident is nefarious, steps are taken to quickly contain, minimize, and learn from the damage.

Incident Examples

SolarWinds-

Sunburst Incident Response Playbook

"may need to rebuild all network assets"

RTH building flood

Events vs Incidents

An *event* is any observable occurrence in a system

Server receiving a request, user sending an email, login failure

A *computer security incident (adverse events)* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

High volume connection requests from a botnet, sensitive information disclosure thru peer-to-peer file sharing, email malware infection

Need for Incident Response Plan

- No System is 100% secure
- Risk analysis
- Critical to respond quickly and effectively
- Incident response capability supports responding to incidents systematically and with consistent methodology
- Minimize loss or theft of information and disruption of services
- Information gained during incident handling can be used to better prepare for handling future incidents
- Helps dealing properly with legal issues

Laws and Regulations

- Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information System*
- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
- OMB's Circular No. A-130, Appendix III, "ensure that there is a capability to provide help to users when a security incident occurs……"
- FISMA Requires agencies to have "procedures for detecting, resporting, and responding to security incidents"

Data breach notifications

California Civil Code 1798:29 and 1798:80

- Entities that own or license computerized personal information to give notice to residents of California of any data breach that results or could result in the unauthorized acquisition of unencrypted personal information.
- Notification must be made in the most expedient time possible and without unreasonable delay….
- Any customer injured by a violation of this title may institute a civil action to recover damages

https://www.itgovernanceusa.com/data-breach-notification-laws

Incident Response Policy Elements

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies)
- Definition of computer security incidents and related terms
- Organizational structure, roles, responsibilities and authority
- Prioritization or severity ratings
- Performance measures
- Reporting and contact forms

Incident Response Plan Elements

- Organizations develop this plan based on their unique requirements
- Includes:
  - Mission
  - Organizational approach to incident response
  - Team Coordination
  - Metrics on effectiveness of incident response
  - Guidance on maturing the incident response

Incident Response Team Structure

Functions:

- Analyze incident data
- Determine impact of incident
- Act

Team Models

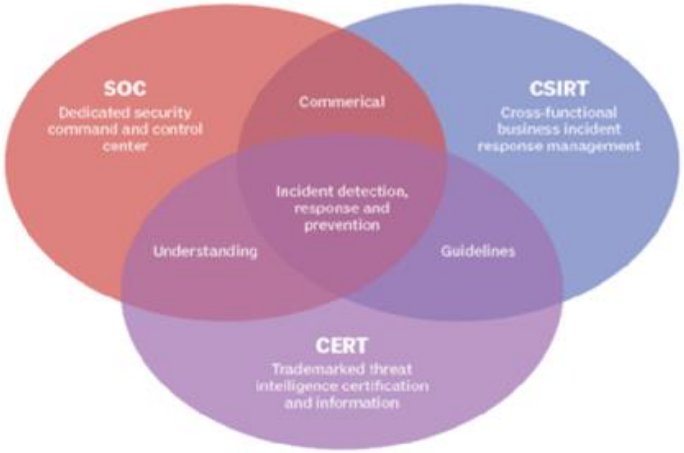
- Central Incident Response Team
- Distributed Incident Response Teams

Incident Response Team Roles

Cyber Security Incident Response Team (CSIRT)

- IR Commander
- Incident Response Team Members
- Recorder

Computer Emergency Response Team (CERT)

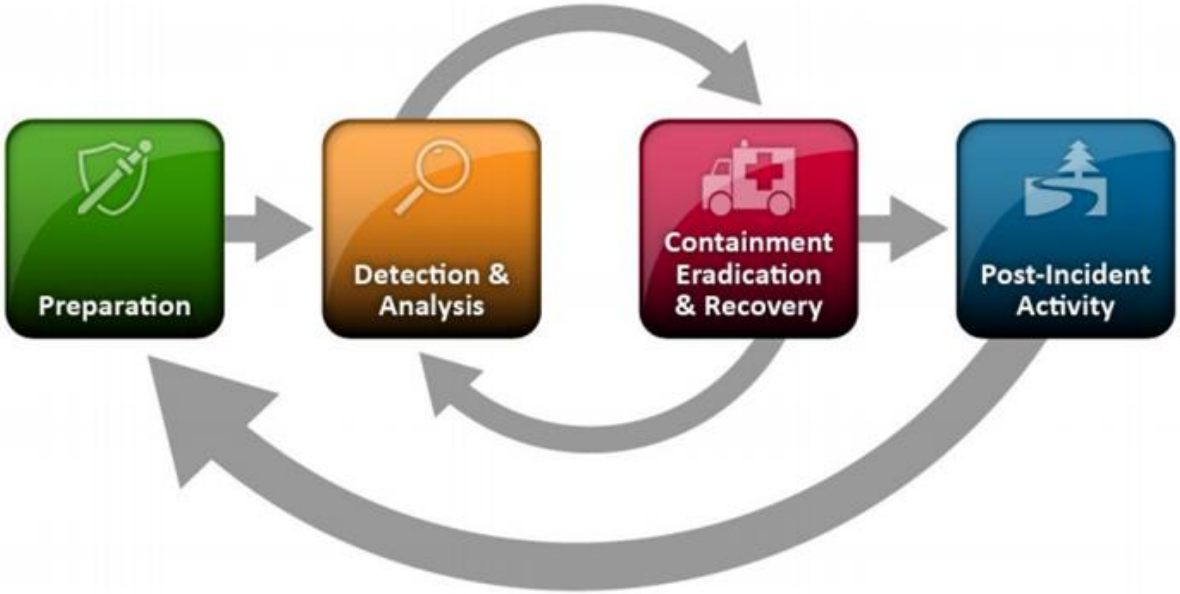


NIST vs SANS Steps

Incident Response Steps

NIST	SANS
1) Preparation	1) Preparation
2) Detection and Analysis	2) Identification
3) Containment, Eradication, & Recovery	3) Containment
	4) Eradication
	5) Recovery
4) Post-Incident Activity	6) Lessons Learned

Incident Response Steps



Preparation

Preparing to Handle Incidents

- Incident Handler Communications and Facilities
  - Contact information, incident reporting mechanism, issue tracking system, encryption software, war rooms, secure storage facility

- Incident Analysis Hardware and Software
  - Forensics workstation and backup devices, spare workstations/virtualized equivalent, blank removable media, printers, forensics software, packet sniffers, evidence gathering tools

Preparation

Preparing to Handle Incidents

- Incident Analysis Resources
  - Port lists, documentation, network diagrams or list of critical assets, current baselines, cryptographic hashes

- Incident Mitigation Software
  - Access to images of clean OS and application installations for restoration and recovery purposes, *jump kit*

Preparation

Preventing Incidents

- Risk Assessments
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training

Detection and Analysis

Attack Vectors- External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Loss or Theft

Signs of an Incident- Network based/host-based IDPS, antivirus software, log analyzers, specialized technical knowledge and extensive experience

Precursors- Vulnerability scanner usage log entries, announcement of a new exploit, threat from a group

Indicators- IDS attempt, antivirus alert, unusual filenames, auditing configuration change, failed logins, bounced emails

Detection and Analysis

Sources of Precursors and Indicators- Alerts, Logs, Publicly available information, People

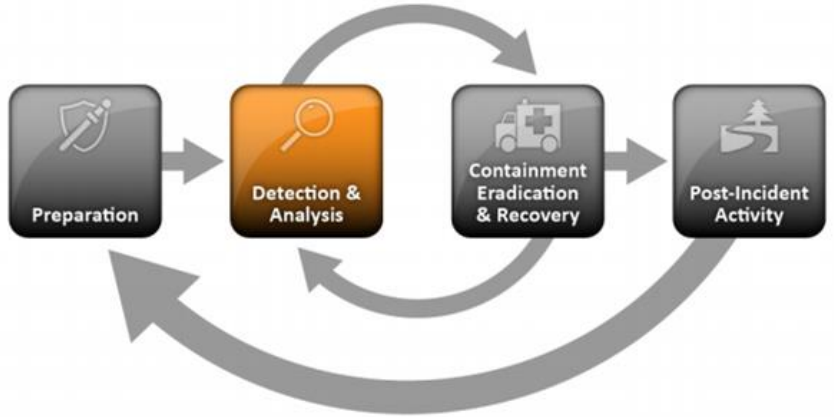
Incident Analysis- Profile network and systems, understand normal behaviors, create log retention policy, perform event correlation, keep clocks synchronized, packet sniffers, filter data, seek assistance from others

Incident Documentation- Status of the incident, summary, indicators, actions taken, impact assessments, contact information, evidence gathered, next steps to be taken

Detection and Analysis

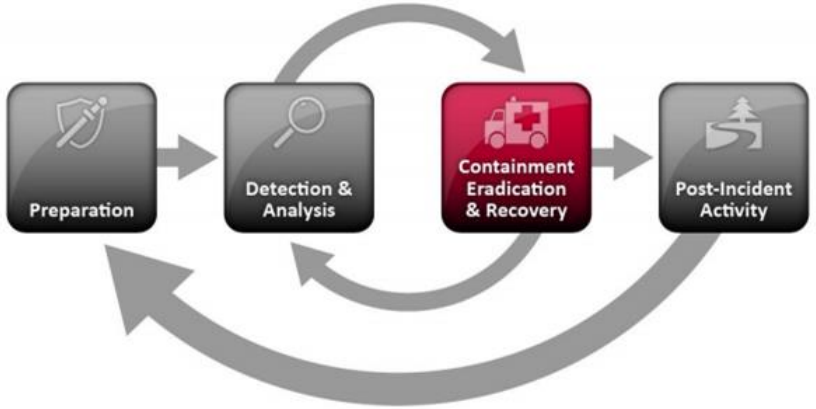
Incident Prioritization- Functional impact of the incident, Informational Impact, Recoverability from the incident

Incident Notification- CIO, head of information security, other ir teams, system owner, human resources, public affairs, legal departments, US-CERT, law enforc
Email, website, in person, paper



Containment

Choosing a Containment Strategy- Potential damage, evidence preservation, service availability, time and resources needed, effectiveness, duration of the solution



Evidence Gathering and Handling- Identifying information, Name, title, Phone number, Time and date, location

Identifying the Attacking Hosts- Validating IP address, researching attacking host, Incident database, monitoring communication channel

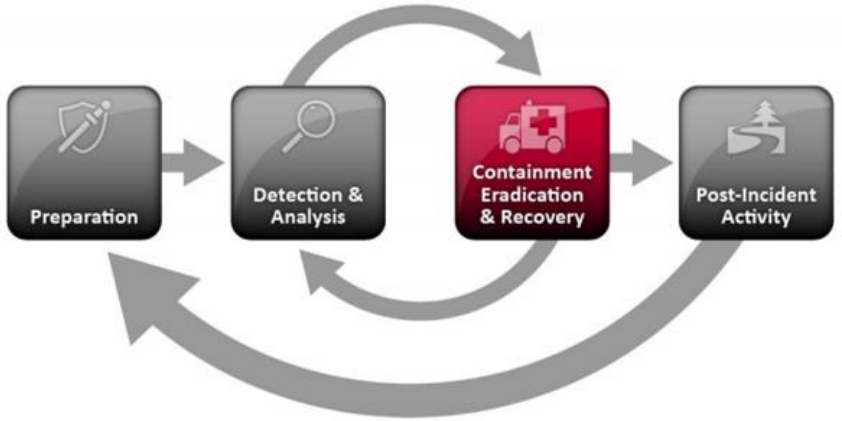
Eradication

Cleanup

- Disabling breaches accounts and reset sessions
- Identify and mitigate vulnerabilities

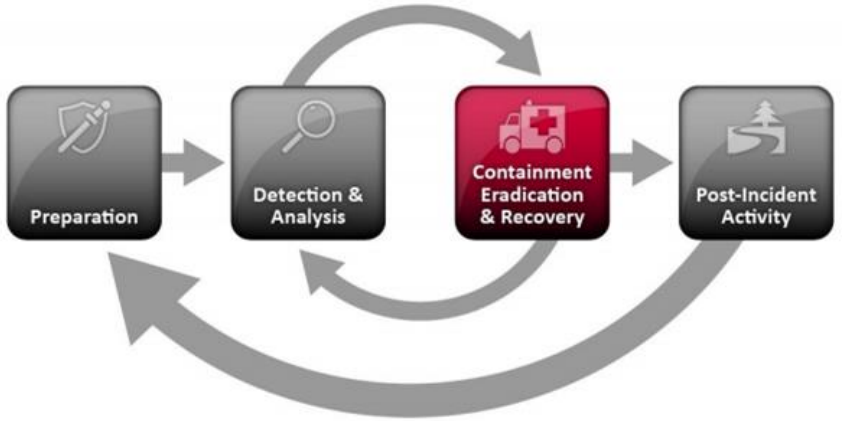
Re-Install:

- Clean install of affected OS/application



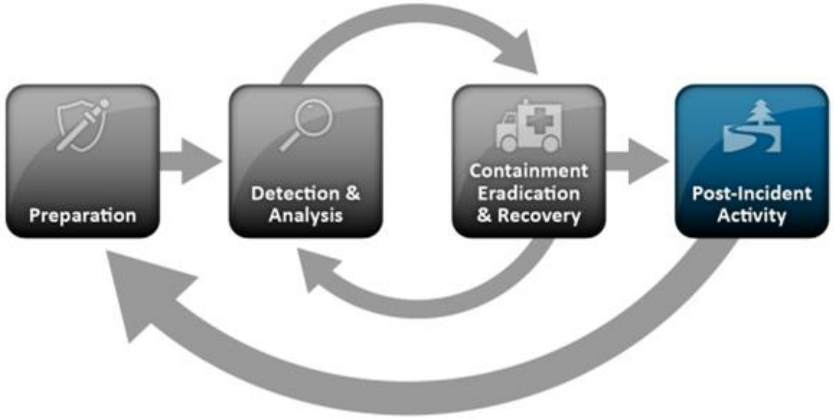
Recovery

- Restore Operations
  - Validate eradication
  - Restore to normal operations
  - Remediate similar incident vulnerabilities
- Performed in a phased approach
- Tools:
  - System Backups,
  - Patch Management
  - Log Analysis



Post-Incident Activity

- Hold Lessons Learned Meeting
- Develop Follow-Up Report
  - Formal chronology of events
- Use of Incident-Related Data
- Audit of IR Programs
- Evidence Retention
- Tools:
  - Forensics Evidence Gathering And Preservation



Coordination and Information Sharing

- Cross-Organization Coordination in IRP Process
- Communication with Outside Parties
  - Law Enforcement
  - Incident Reporters
  - ISACs
- Restrictions
  - Business Info
  - Technical Info

SolarWinds Information Sharing Concerns

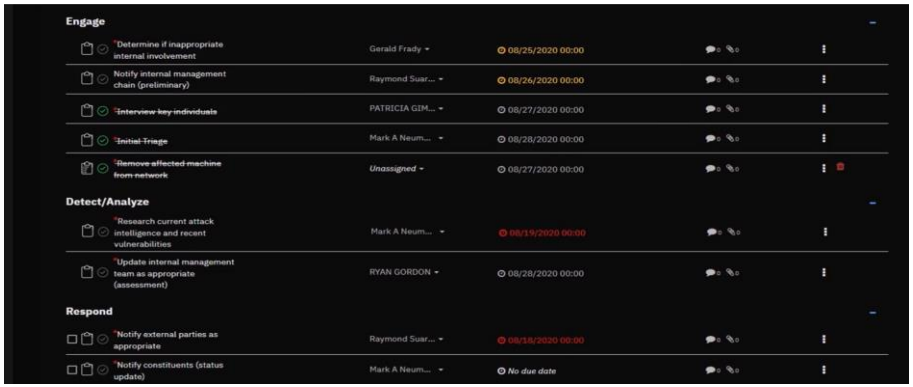
Experts Call for Increased Cyber Info Sharing in Wake of SolarWinds Breach

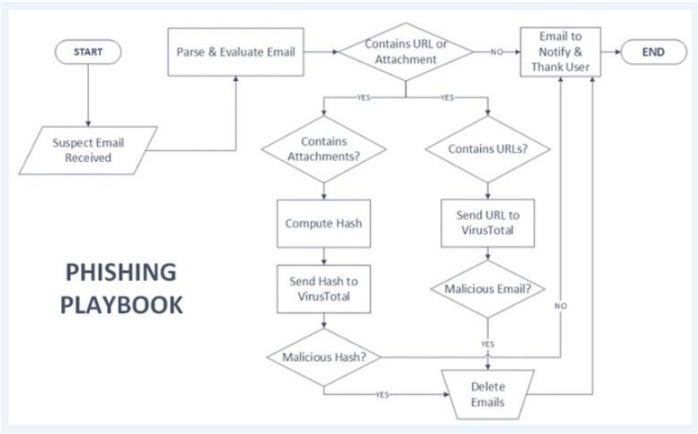
solarwinds

Security Orchestration, Automation and Response (SOAR)

IBM Security SOAR Platform

- Case Management
- IBM's Resilient Dynamic Playbook

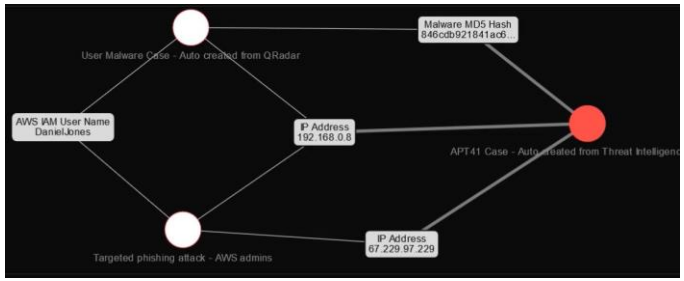


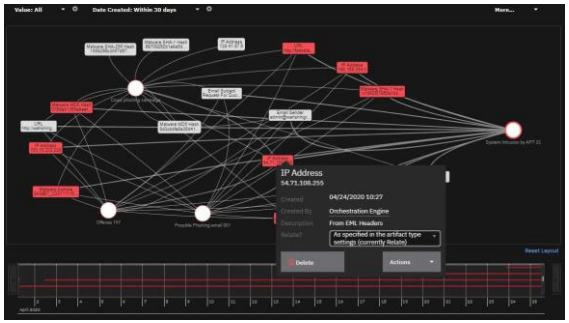


SOAR

IBM Security SOAR Platform

- Incident Enrichment
  - Threat Intelligence Insights
  - Data Explorer
- Artifact Visualization





Cisco Umbrella Investigate

"Uncover attacker infrastructure and stop attacks before they launch"

"Identify what alerts need additional investigation"

"Gain greater context for faster decision making and remediation"

IRP Template

https://frsecure.com/resource/incident-management-plan-template.pdf

Contact Information

Roles and Responsibilities

Incident Response Framework

Notification and Communication

Plan testing and Review

Sources

[1] NIST Computer Security Incident Handling Guide - Computer Security Incident Handling Guide (nist.gov)

[2] Cisco IRP - What Is an Incident Response Plan for IT? - Cisco

[3] Incident Response Steps and Frameworks for SANS and NIST - 2021 Incident Response Steps for NIST and SANS Framework | AT&T Cybersecurity

[4] SANS Incident Handler's Handbook - Incident Handler's Handbook (sans.org)

[5] FRSecure Security Incident Management Plan Template - Template

[6] IBM Security SOAR Platform - IBM Security SOAR Platform - Overview | IBM

[7] Data Breach Notification by State - Data Breach Notification Laws by State | IT Governance USA

[8] SolarWinds Information Sharing Concerns - Experts Call for Increased Cyber Info Sharing in Wake of SolarWinds Breach – MeriTalk

[9] Building Playbooks - How to Build an Incident Response Playbook | Swimlane

[10] SolarWinds Incident Response- https://www.datacenterknowledge.com/security/solarwinds-breach-shaking-incident-response

DSci526:
Secure Systems Administration

Preparation for Mid-term exam

Prof. Clifford Neuman

Lecture 7
3 March 2021
Online

Mid-Term Exam is Wednesday March 10th

Exam will be 100 minutes, from 2PM-3:40PM PST.

- For students in distant time zones, an alternative time will be 6PM-7:40PM PST. You MUST contact me in advance to arrange for this alternate time.
- A lecture will follow from 4PM to 5:20PM

- Format of the exam
  - The exam is open book, open note and online
  - Previous exams will posted on the class website http://ccss.usc.edu/526
  - Material to be covered will be the start of the semester through Today's lecture.

Mid-Term Exam Logistics

Full Instructions will be sent by Monday through email.

By 10 minutes before the time of the exam on Wednesday, three versions of exam (PDF,TXT,and Word) will be sent to students.

Students will complete exam by editing the exam files (the word file is preferred; the other formats are provided in case students do not have ability to use the word version).

At conclusion, exam will be uploaded through the D2L dropbox.

Students will self certify that you completed the exam in the allotted time and neither received or provided assistance.

Review of Material for Mid-term

Introduction to Secure System Administration

- Secure
  - Ability to correctly implement relevant policy
- System
  - A computer?
  - A network?
  - The combination of all system components implementing a particular function
- Administration
  - Selection of components (purchases of products)
  - Architecture – how the pieces fit together
  - Installation and configuration
  - Security Testing
  - Operation
  - Monitoring
  - Repair and Maintenance
  - Threat response

Application Architecture

- What are the functional requirements of the system?
  - This guides equipment needs
    - Processing, Storage, and Network.
  - What are the functional goals of the system.
- This defines the meaning of availability
  - What constitutes a breach of availability – the system no longer meets its functional goals.
  - Critical Infrastructure
  - Critical for you
- Consequences of failure

Positive and Negative Requirements

- Functional requirements are positive.
  - This is what most developers focus on
  - And why our systems are not secure.
  - Functionality over security
- Security requirements tend to be negative
  - What should not be possible (conf and integ)
  - But availability is a positive requirement
- How do we test for negative requirements
  - *absence of evidence is not evidence of absence*

Information Flow and Containment

- Understand your applications Information Flow:
  - What is to be protected
  - Against which threats
  - Who needs to access which apps
  - From where must they access it
- Do all this before you invest in the latest products that salespeople will say will solve your problems.

Configuration Management

- Catalog of systems
  - What is approved for connection
- Catalog of software
  - What is approved for use
  - Patch management
- Configuration checkers
- Change detectors
  - E.g. tripwire, AFIK

A Reasonable Outline(1)

- Motivation and Principles
  - Written altruistically, but in reality, the goals are to protect your organization.
  - Mentions Classes of Data and Consequences
    - E.g. Some Material from NIST Risk Management Framework
  - Acknowledgement of the threat environment
    - E.g. The Global System Environment (from GIACS)

A Reasonable Outline(1)

- Description of System (applicability)
  - Inventory: Systems, Devices, Data
- Motivation and Principles
  - Written altruistically, but in reality, the goals are to protect your organization.
  - Mentions Classes of Data and Consequences
    - E.g. Some Material from NIST Risk Management Framework
  - Acknowledgement of the threat environment
    - E.g. The Global System Environment (from GIACS)
- High level assignment of responsibilities

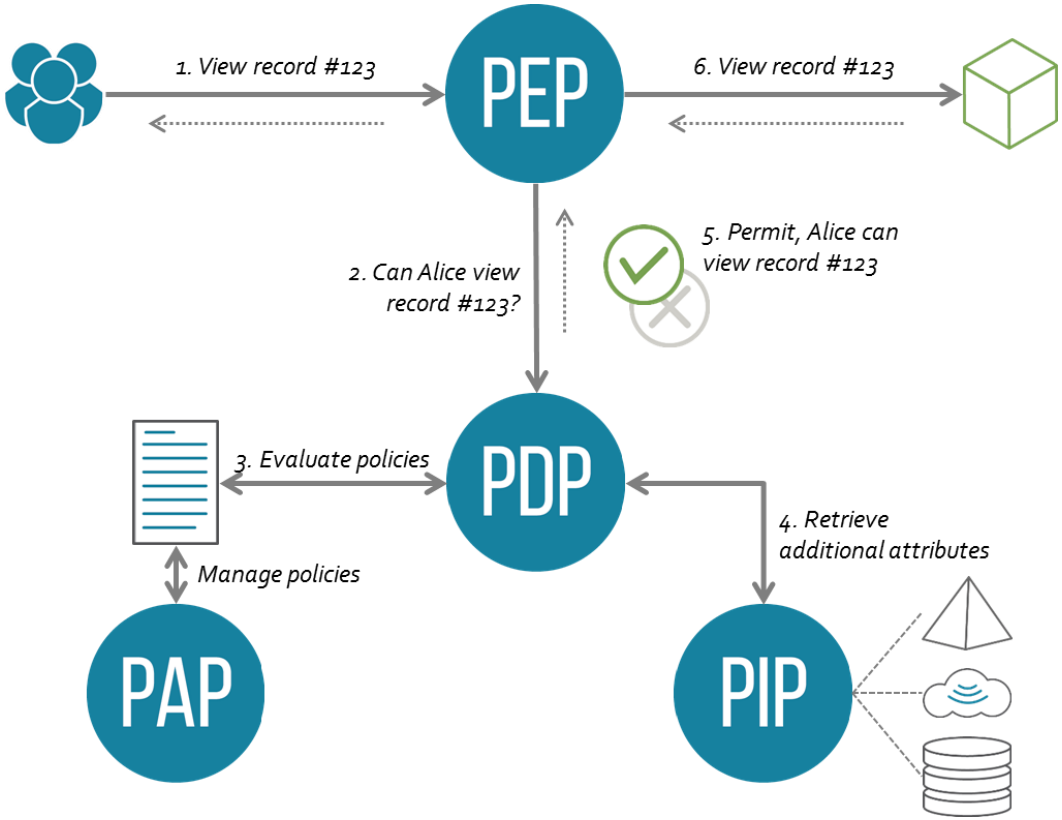
A Reasonable Outline(2)

- Security Requirements and Metrics
  - What is to be protected against what threats
    - Consequences to organization of breaches
  - Required level of protection to each class of asset
    - Required approaches to providing that protection
    - Metric regarding strength of mechanisms to be applied.
- Physical and Personnel Security Constraints
  - Who will have access
  - Access controls on physical systems

A Reasonable Outline(3)

- Requirements on Specific Categories of Controls
  - Access Control
  - Training
  - Audit
  - Configuration Management
  - Identity Management
  - Incident Response
  - Maintenance
  - Vendor Requirements
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk Assessment
  - Security Assessment
  - Sys and Comm Protection
  - Integrity
  - Software Requirements

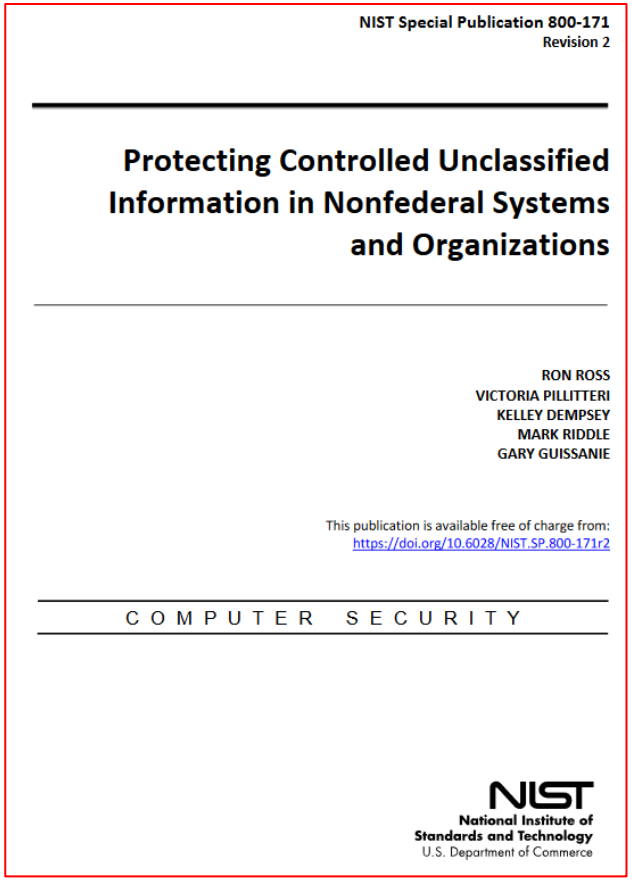
Points of Policy



- By Axiomatics - Axiomatics, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=48397652

This Weeks Reading

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Containment Architecture

- The requirements apply to components of … systems that process, store, or transmit CUI,or that provide security protection for such components. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain.
  - Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

-- Section 1.1 (page 2[14])

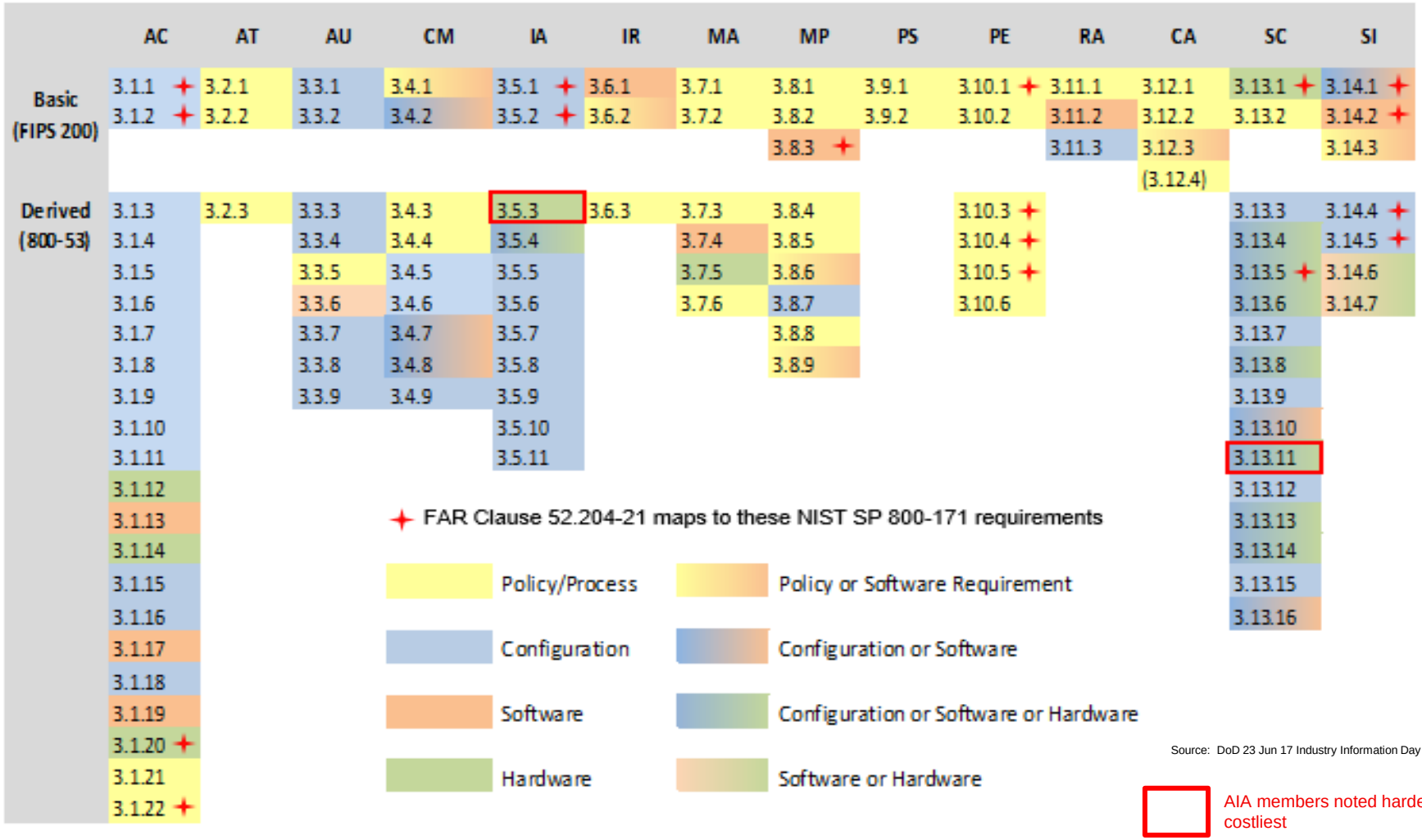
Families of Controls

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

NIST SP 800-171 Controls
What to Expect

- What does fully implemented mean?
  - You have processes in place to ensure that the control is met
    - And that you honestly consider the process that is in place to be sufficient (adequate)
  - It does not mean that the process is fool-proof
- Different ways to meet the control:
  - Configuration, Hardware, Software, or Policy
  - Policy may simply involve not using systems for certain purposes



Source: DoD 23 Jun 17 Industry Information Day slide deck

AIA members noted hardest and costliest

Host Administration

Many security issues today are the result of poor system administration.

- Failure to implement least privilege
- Poor management of user accounts
- Mismanagement of remote access
- Managing permissions incorrectly
- Allowing vulnerable programs to run
- Not keeping required programs up to date
- Misconfiguration of applications

- Not just Linux, but many server machines are implemented on Linux, so that is our focus

Least Privilege - Users

Users

- Restrict host access to users with need to access
- Don’t share root password
  - Separate account and limited use of sudo
- Account Management
  - /etc/passwd and shadow password file
    - Strong passwords
  - Network based password mechanisms
    - YP/NIS (bad)
    - Encryption Based (good)
    - SSH pk based login
  - Group management

Least Privilege - Processes

- Programs / Processes
  - UserID
    - Create unique for process or application
    - Have system startup run as user
      /etc/init.d and update-rc.d
  - Data Access
    - Set groups on files / devices
    - Chmod, chown, and chgrp
  - Linux Containers
    - Better than the old standby “chroot”, it provides a lightweight virtual environment, not quite as isolated as a separate VM.

Host Administration Guidance

- Create multiple protection domains
  - Don’t run anything as root (or as little as possible)
- Configure access to resources carefully
- Use Host Based Firewalls as added barrier to communications
  - Reduce the attack surface
  - Consider iptables (packet filters)

Host Administration Guidance

- Create multiple protection domains
  - Don’t run anything as root (or as little as possible)
- Configure access to resources carefully
- Use Host Based Firewalls as added barrier to communications
  - Reduce the attack surface
  - Consider iptables (packet filters)

Host Administration Guidance

- Create multiple protection domains
  - Don’t run anything as root (or as little as possible)
- Configure access to resources carefully
- Use Host Based Firewalls as added barrier to communications
  - Reduce the attack surface
  - Consider iptables (packet filters)

Summer 16 Midterm Q1

- Minimization - Provide examples of three distinct uses of minimization in system and network administration. (30 points)

Summer 16 Midterm Q2

A Biotech company has faced many security breaches since the start of this year. The enterprise risk services team wants to evaluate the cyber risk capability of the network infrastructure. You have been hired as a "Penetration tester" to complete this job. As part of your responsibilities, you will advise the biotech company on the techniques criminals might use to attack their platform, both from the perspective of an outsider, and when the attack originates from adversaries with inside information. As a penetration tester you will, with their authorization, use some of these techniques to see how far you can get.

Describe some of the steps that an adversary (and you in your role as a pen tester) would take to gather information about the system that is the subject of your engagement. List the kinds of information that is being gathered, and how it might be used by an attacker.

Justify your answer by giving relevant details about the process and related examples from the class or real world. Please be to the point. (30 points)

Summer 16 Midterm Q3

Policy Administration

Explain the function that exists at and give two examples of each of the following policy points within a system. (40 points)

- Policy Enforcement Point (10 points)
- Policy Decision point. (10 points)
- Policy Administration Point (10 points)
- Policy Information Point. (10 points).

Review of Quiz 1Spring 2017

Policy Administration - A system is secure if it correctly applies policies for access to system resources. The application of policy has several distinct components that may occur in different places, or different modules within a system.

- Policy Enforcement Point
- Policy Decision Point
- Policy Administration Point
- Policy Information Point

Web Server – Spring 2017 Midterm

For each of the systems described below, use your best explanation to describe what constitutes each function and where that function occurs in the system or supporting infrastructure.

- Access control for files exported through a web server such as apache when page permissions are managed using the .htaccess file.
- PEP:
- PDP:
- PAP:
- PIP:

Appliance Firewall – Spring 2017 Midterm

For each of the systems described below, use your best explanation to describe what constitutes each function and where that function occurs in the system or supporting infrastructure.

- Filtering of packets passing through an appliance firewall.
- PEP:
- PDP:
- PAP:
- PIP:

Unix/Linux Filesystem- Spring 2017 Mid-term

For each of the systems described below, use your best explanation to describe what constitutes each function and where that function occurs in the system or supporting infrastructure.

- Access to local files with standard unix permissions on a system running Linux or Unix.
- PEP:
- PDP:
- PAP:
- PIP:

Banking Application – Spring 2017 Mid-term

For each of the systems described below, use your best explanation to describe what constitutes each function and where that function occurs in the system or supporting infrastructure.

- Access to your customers account balance through a web server in the banking example that we have been discussing in class.
- PEP:
- PDP:
- PAP:
- PIP:

Minimization – Spring 2017 Mid-term

Minimization, Provide examples of minimization, and steps that you can take to achieve such minimization, in each of the situations discussed below.

- Reduction of the attack surface for servers running within your corporate network.

Minimization – Spring 2017 Mid-term

Minimization, Provide examples of minimization, and steps that you can take to achieve such minimization, in each of the situations discussed below.

- Reduction of impact for insider threats, or for compromise resulting from subversion of server processes.

Minimization – Spring 2017 Midterm

Minimization, Provide examples of minimization, and steps that you can take to achieve such minimization, in each of the situations discussed below.

- Reduction of the impact to other systems on your network when one system is compromised or subverted.

Security Requirements Documents Spring 2017 Mid-term

List the kinds of requirements that should be specified in a security requirements document.

- Include a 1 or 2 sentence description of what is described by the requirement.

(A security requirements document might sometimes be referred to as a security policy, or an organizational security policy, but I am avoiding the term “security policy” because that term is sometimes used to refer to other policies within a system. Here I am concerned with the broader use of the term.)

Spring 2017 Midterm Discussion

1. STRIDE and Adversarial Security Planning - For each of the classes of threats identified using the Stride model as applied to a system or network, provide an example of an exploit that fits the class, explain what part of the system is directly affected, what the impact might be for the security of the system as a whole, and also suggest a countermeasure or approach that can be used to mitigate the threat. (30 points)

- a) Spoofing
- b) Tampering
- c) Repudiation
- d) Information Disclosure
- e) Denial of Service
- f) Elevation of Privilege

Spring 2017 Midterm Discussion

2. Ethical Hacking and Pen Testing

Why are network scanning tools such as Nessus, or NMAP useful to an attacker, and why might they be useful to a pen tester or system/network administrator. (20 points)

Spring 2017 Midterm Discussion

3. Response and recovery planning - This question describes the phases of a recovery and/or response plan in phases that are not precisely in line with those covered in class. The basic flow is the same however, and you are asked to explain what activities should best be performed in each of these sections or phases of such a plan, and to also describe the importance of each the activities you describe. (30 points).

a) Risk identification, vulnerability assessment, analysis of impact
b) The preparation phase
c) Detection and/or activation plans
d) The runbook, the recovery section, or the response plans. In answering this part, be sure to explain what this section might look like. Will a response follow all the steps in this section?
e) The recovery phase (as applied to a cyber response plan) or other post incident activities.
f) Testing and ongoing maintenance

Spring 2017 Midterm Discussion

4.System and Host Administration (20 points)

- List some of the techniques available within Linux to minimize the privileges (implement least privilege) for server processes running on the system, and how does this improve the security of the system as a whole. Provide sufficient detail to show how one would implement each technique as a system administrator.

DSci526:
Secure Systems Administration

First Group Project
(second week reports)

Prof. Clifford Neuman

Lecture 7
3 March 2021
Online

Teams for First Group Project

- Team One
  - Shagun Bhatia
  - Anthony Cassar
  - Sarahzin Chowdhury
  - Aditya Goindi
  - Tejas Kumar Pandey
  - Malavika Prabhakar
  - Pratyush Prakhar
  - Dwayne Robinson
  - Christopher Samayoa
  - Amarbir Singh
  - Louis Uuh
  - Shanice Williams
- Team Two
  - Azzam Alsaeed
  - Ayush Ambastha
  - Jason Ghetian
  - Marco Gomez
  - Alejandro Najera
  - Doug Platt
  - Abhishek Tatti
  - Carol Varkey
  - MaryLiza Walker
  - Yang Xue
  - Hanzhou Zhang

Banking Scenario

- Your organization must:
  - Maintain a database of account holders
  - A database of account balances
  - Enable web access by customers who:
    - Can update their personal information
    - Check their account balance
    - Transfer funds to another account (by number)
    - View transactions on their account
    - Submit an image of a check for deposit
      - (check should be viewable, but you do not need to scan it or process it)
- Access is needed
  - Via web from the open internet
  - Outbound email confirming transactions
  - All other interactions may be limited by information flow policies to internal machines.

Reports from Both Teams

- 1640-1650 Group One Reporting
- 1650-1700 Group Two Reporting
- 1700-1720 Open Discussion among class
- then Breakout Rooms for Groups