1.0 Threat and Vulnerability Management

1.1. Explain the importance of threat data and intelligence

- *Intelligence sources*

- Open-source intelligence

- Open-source feeds, available without subscription.
- Publicly accessible reputation lists and malware signature databases.
- Government agencies - sources of public threat information (US-CERT)
- Blogs and contributions to discussion forums from experienced practitioners.

digitalguardian.com/blog/top-50-infosec-blogs-you-should-be-reading

OSINT refers to methods of obtaining information about a person or organization through public records, websites, and social media.

- Proprietary / closed-source intelligence

- Commercial service offering, subject to a subscription fee.
- Often repackaged information coming from free public registries
- Also derived from the provider's own research and analysis efforts, such as data from honeynets that they operate, plus information mined from its customers' systems, suitably anonymized.
- Examples: IBM X-Force Exchange, FireEye

- Timeliness

Intelligence sources must be up to date. Threats diminish, change, evolve. Adversary groups adopt different tactics. You must assess whether an intelligence source can research and disseminate updates in a timely manner.

- Relevancy

Intelligence sources must match their use case. Example: a threat intelligence source that focuses on Windows security is of limited use if your systems are primarily cloud applications accessed via Chrome OS workstations.

- Accuracy

Intelligence sources must produce effective results. Accuracy can also refer to whether the intelligence is of a general or specific nature.

• *Confidence levels*

The admiralty scale rates sources with letters from a (reliable) to g (purposefully deceptive) and information credibility from 1 (confirmed by multiple sources) to 6 (cannot be validated).

TABLE I

EXAMPLE SUBJECTIVE OPINION MAPPINGS FOR A 6 × 6 'ADMIRALTY SCALE'.

Credibility of Source *Collector's assessment of Source's reliability*			Reliability of Information *Source's assessment of the likelihood of information*		
Score	**Interpretation**	**Belief**[a]	**Score**	**Interpretation**	**Belief**[a]
A	Almost Always Reliable	$(0.95, 0.05, 0.0, a)$	**1**	Almost Certainly True	$(0.95, 0.05, 0.0, a)$
B	Usually Reliable	$(0.8, 0.2, 0.0, a)$	**2**	Very Likely	$(0.8, 0.2, 0.0, a)$
C	Fairly Reliable	$(0.6, 0.4, 0.0, a)$	**3**	Likely	$(0.6, 0.4, 0.0, a)$
D	Fairly Unreliable	$(0.4, 0.6, 0.0, a)$	**4**	Unlikely	$(0.4, 0.6, 0.0, a)$
E	Unreliable	$(0.1, 0.9, 0.0, a)$	**5**	Very Unlikely	$(0.1, 0.9, 0.0, a)$
F	Untested	$(0.0, 0.0, 1.0, a)$	**6**	Unknown	$(0.0, 0.0, 1.0, a)$

[a] The numbers in the parentheses constitute subjective logic beliefs in the form (b, d, u, a) – denoting *belief*, *disbelief*, *uncertainty* and *base rate*, respectively. For more information, please consult Appendix A.

• *Indicator management*

- Structured Threat Information eXpression (STIX)

The Structured Threat Information eXpression (STIX) - describes standard terminology for documenting IoCs & ways of indicating relationships between them.

The STIX architecture is built from high-level STIX domain objects (SDO). The attributes of SDOs and the terminology and format for attribute values are defined in the STIX patterning language. Some of the SDOs are as follows:

Observed Data — Examples of observables include an IP address, a change in an executable file property or signature, an HTTP request, or a firewall blocking a connection attempt.

Indicator — A pattern of observables that are "of interest," or worthy of cybersecurity analysis.

Attack Pattern — Known adversary behaviors, starting with the overall goal and asset target (tactic), and elaborated over specific techniques and procedures. This information is used to identify potential indicators and intrusion sets.

Campaign and Threat Actors — The adversaries launching cyberattacks are referred to in this framework as Threat Actors.

Course of Action (CoA) — Mitigating actions or use of security controls to reduce risk from attacks or to resolve an incident.

- Trusted Automated eXchange of Indicator Information (TAXII)

For sharing STIX data. TAXII protocol provides a means for **transmitting CTI data between servers and clients over HTTPS** and a REST API.

For example, a CTI service provider would maintain a repository of CTI data. Subscribers to the service obtain updates to the data to load into analysis tools over TAXII. This data can be requested by the client (referred to as a collection), or the data can be pushed to subscribers (referred to as a channel).

TAXII services can support various sharing models:

- Hub and spoke - one central clearing house
- Source / subscriber - one org is a single source of info
- P2P - multiple entities exchanging info

- OpenIoC

Source: github.com/mandiant/OpenIOC_1.1

OpenIOC uses XML-formatted documents. Each entry comprises meta-information such as author, category information, confidence level, and usage license, plus a description and a definition. The definition is built from logical statements defining detection rules, such as DNS host name or a string pattern for a filename.

Malware Information Sharing Project (MISP) (misp-project.org) - provides a server platform for CTI sharing as well as a file format. MISP servers can import and export STIX CDOs over TAXII. It also supports OpenIOC definitions.

- *Threat classification*

6 Categories:

1. Human - spies, terrorists, employees, etc.

2. Natural - floods, earthquakes
3. Technical - hardware failure, malicious code
4. Physical - perimeter security breaches, CCTV failure
5. Environmental - traffic congestion, power outage, biohazards
6. Operational - processes and procedures that can affect the CIA triad

- Known threat vs. unknown threat

Cybersecurity techniques depend on the identification of "static" **known threats**, such as viruses, rootkits, Trojans, and botnets. It is straightforward to identify and scan for this type of threat with automated software by matching the malicious code to a signature in a database of known malware.

An example of a known unknown is that malware authors can use various obfuscation techniques to circumvent signature-matching. The exact form that such malware will take is unknown, but it's likely use and operation within an attack is predictable.

Recycled threats - combining and modifying parts of existing exploit code to create new threats that are not as easily identified by automated scanning.

Unknown unknowns - completely new attack vectors and exploits. One of the purposes of security research is to try to discover these, using techniques such as analysis of data collected in honeypots and monitoring of discussion boards used by threat actors.

- Zero-day

A zero-day is a vulnerability that is discovered or exploited **before the vendor can issue a patch to fix it**.

Security researchers who discover new vulnerabilities should inform the vendor privately and allow time for a fix to be developed before making the vulnerability public. The time allowed is often 90 days by convention, but this may be reduced depending on the status of the vulnerability.

Zero-day vulnerabilities have significant financial value. Consequently, an adversary will only use a zero-day vulnerability for high value attacks. State security and law enforcement agencies are known to stockpile zero-days to facilitate the investigation of crimes.

- Advanced persistent threat

APT - **nation-state and organized crime actors**.

APTs typically target large organizations, such as financial institutions, companies in healthcare, and other organizations that store large PII data sets. APTs also target governments to carry out political objectives, interfere in elections, or to spy.

APTs spend considerable effort in gathering intelligence on their target and are able to craft highly specific custom exploits. Another characteristic of the advanced nature of APTs is that they often combine many different attack elements into an overall threat architecture.

APTs have diverse overall goals, but since a large part of the attack is about stealth, most APTs are interested in maintaining access — or **persistence** — to networks and systems. There are several techniques that can grant attackers access for months or even years on end without being detected. Because of this, APTs are some of the most insidious and harmful threats to an organization.

- *Threat actors*

- Nation-state

The goals of nation-state actors are primarily espionage and strategic advantage.

Each state may sponsor multiple adversary groups, and that these groups may have different objectives, resources, and degrees of collaboration with one another.

Crowdstrike's blog - overview of currently identified APTs.

- Hacktivist

A hacktivist group, such as Anonymous, WikiLeaks, or LulzSec, uses cyber weapons to promote a political agenda. Hacktivists might attempt to obtain and release confidential information to the public domain, perform denial of service (DoS) attacks, or deface websites.

- Organized crime

An organized crime gang can operate across the Internet from different jurisdictions than its victims, increasing the complexity of prosecution. Organized crime will seek any opportunity for criminal profit, but typical activities are financial fraud (both against individuals and companies) and blackmail.
Security Intelligence blog - the strategies and tools used by organized crime.

- Insider threat

An insider threat arises from an actor who has been identified by the organization and granted some sort of access. Within this group of internal threats, you can distinguish insiders with permanent privileges, such as employees, from insiders with temporary privileges, such as contractors and guests.

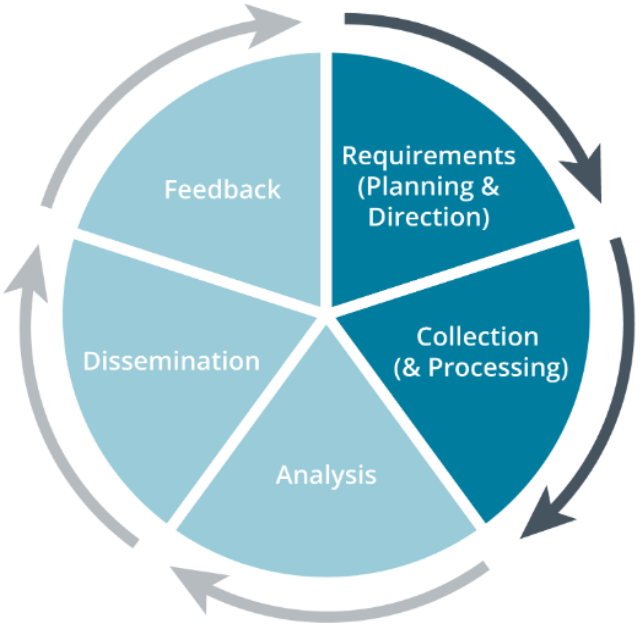
"A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

- Intentional / Unintentional

The examples above = intentional threats. An unintentional threat is created by an insider acting with no malicious intent. Those usually arise from lack of awareness or from carelessness - users accidentally leaking data or using recycled passwords.

Shadow IT - unauthorised devices plugged in by employees, usually not for malicious reasons but for convenience (access points, etc.). But nobody knows those devices are connected to the network.

- *Intelligence cycle*



Security intelligence cycle.

- Requirements

The requirements phase sets out the goals for the intelligence gathering effort. One should define specific requirements for intelligence sources, what customers need and how it should be collected.

- Collection

Collection phase is when one gathers data from a wide array of desired and reliable sources.

SIEM can be configured with connectors or agents that can retrieve data from firewalls, routers, IDS sensors, and servers.

Data enrichment - automatically combines multiple disparate sources of information together to form a complete picture of events or enable proactive threat hunting.

- Analysis

Organizations now collect so much data as to make human analysis impractical. Software solutions = artificial intelligence (AI) and machine learning (ML) techniques.

- Dissemination

Means publishing information produced by the analysis to consumers who need to act on the insights developed. Dissemination can take many forms, from status alerts sent to incident responders to analyst reports circulated to C-suite executives.

- Feedback

Feedback and review utilizes the input of both intelligence producers and intelligence consumers. The goal of this phase is to improve the implementation of the requirements, collection, analysis, and dissemination phases.

- *Commodity malware*

Commodity malware - malicious code packaged for general sale, typically through dark web marketplaces. Examples - remote access Trojans (RATs), such as PoisonIvy, Dark Comet, and XtremeRAT. Generally available through online marketplaces or download sites.

Commodity malware vs targeted or custom malware - developed and deployed with a target in mind, following careful reconnaissance of that target. The difference is similar to that between general phishing campaigns and spear phishing campaigns.

- *Information sharing and analysis communities*

ISAC = Information Sharing and Analysis Center

- Healthcare

Healthcare Ready, H-ISAC -https://h-isac.org/

- Financial

FS-ISAC - https://www.fsisac.com/

- Aviation

A-ISAC - https://www.a-isac.com/

- Government

EI-ISAC (elections), DIB-ISAC (defense), NEI (nuclear)

- Critical infrastructure

E-ISAC (electricity), ONG-ISAC (oil & gas), PT-ISAC (public transit)

1.2. Given a scenario, utilize threat intelligence to support organizational security.

- *Attack framework*

- MITRE ATT&CK

MITRE ATT&CK - a **database of known tactics, techniques, and procedures (TTPs)**. Source: attack.mitre.org.

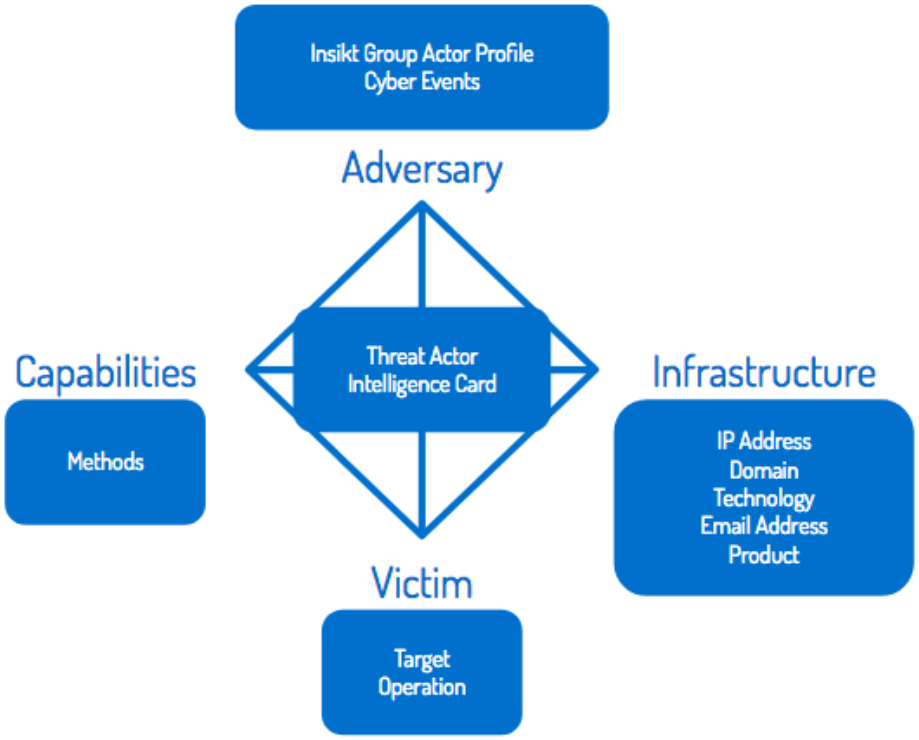
The sequence in which attackers may deploy any given tactic category is not made explicit. This means analysts must interpret each attack life cycle from local evidence.

- The Diamond Model of Intrusion Analysis

Source: activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

The Diamond Model suggests a framework to analyze an intrusion event (E) by exploring the relationships between four core features: **adversary, capability, infrastructure, and victim**. These four features are represented by the four vertices of a diamond shape.

In this model, the adversary develops a capability that exploits the victim, usually through a vulnerability in the system.



- Kill chain

Source:
https://www.osintme.com/index.php/2020/05/31/the-cyber-kill-chain-explained-along-with-some-2020-examples/

- *Threat research*

- Reputational

One can identify a threat by associating indicators with reputation data. A reputation threat research source identifies IP address ranges and DNS domains that are

associated with malicious activity, such as sending spam or participating in DDoS attacks. See Talos Reputation Center.

- Behavioral

Most threat sources cannot be identified from a single indicator. Behavioral threat research correlates IoCs into attack patterns. The analysis of previous hacks and intrusions produces definitions of the tactics, techniques, and procedures (TTP):

DDoS - a traffic surge might indicate a distributed denial of service (DDoS) attack. As the attacker will leverage a botnet, one is likely to notice unusual geographic distribution of source IP addresses.

Viruses/worms - High CPU or memory usage - a sign of malware infecting a host.

Network reconnaissance - scans against multiple ports or across numerous IP addresses will be highly visible and provide an early warning of adversary behavior.

Some adversary techniques for communicating with the C2 server include:

Port hopping - The C2 application might use any port to communicate and may "hop" between different ports.

Fast flux DNS - This technique rapidly changes the IP address associated with a domain. It allows the adversary to defeat IP-based blacklists, but the communication patterns established by the changes might be detectable.

Data exfiltration - Spikes in database reads, high-volume network transfers, excessive hard drive space consumption might all be indicators of a data exfiltration.

- Indicator of compromise (IoC)

IoCs indicate that an asset / network has been successfully attacked or is continuing to be attacked. An IoC can be a malware signature, but could also be something like:

- Unauthorized software and files
- Suspicious emails
- Suspicious Registry and file system changes
- Unknown port and protocol usage
- Excessive bandwidth usage
- Rogue hardware
- Service disruption and defacement
- Suspicious or unauthorized account usage

- Common vulnerability scoring system (CVSS)

Risk management system for various vulnerabilities. It works on the scale from 0 to 10 (no risk to critical risk). Source: https://nvd.nist.gov/vuln-metrics/cvss

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Access Vector:

- Physical
- Local
- Adjacent Network or Network - **A type** access to the network.

Access Complexity:

- High
- Low

Privileges Required:

- None
- Low
- High

User Interaction:

- None
- Required

Scope:

- Changed
- Unchanged

Confidentiality, Integrity and Availability:

- High
- Medium
- Low

• *Threat modeling methodologies*

- How can an attack be performed? What assets are accessible?
- What is the potential impact to the CIA of data?
- How likely is the risk to manifest itself? How exploitable is the flaw? Is it theoretical, or does a working exploit exist?
- What mitigating protections are already in place? How long will it take to put additional controls in place? Are those additional protections cost effective?

- Adversary capability

MITRE identifies the following levels of capability:

- Acquired and augmented - commodity malware and techniques (acquired) or some ability to customize existing tools (augmented).

- Developed - exploit zero-day vulnerabilities; significant human & financial resources.

- Advanced - exploit supply chains, proprietary and open-source products, run campaigns that exploit suppliers and service providers.

- Integrated - non-cyber tools, such as political or military assets.

- Total attack surface

All the points at which an adversary could interact with the system and potentially compromise it.

- Corporate data network — access by external users (VPN, email, Wi-Fi, building security) and internal users (management channels, unlocked workstations).

- Website / cloud — web application used for the front end, but also ways to access the application programmatically via an API.

- Software apps — application's user interface and platform vulnerabilities.

- Attack vector

The attack vector is a specific means of exploiting some point on the attack surface. MITRE identifies three principal categories of attack vector:

- ***Cyber*** — Use of a hardware or software IT system. Examples: email or social media messaging, USB storage, compromised user account, open network application port, rogue device.

- ***Human*** — Use of social engineering to perpetrate an attack through coercion, impersonation, or force. Attackers may use cyber interfaces to human attack vectors, such as email or social media.

- ***Physical*** — Gaining local access to premises in order to effect an intrusion or denial of service attack.

- Impact & Likelihood

Risk is assessed by factoring the likelihood of an event and the impact of the event. Likelihood is measured as a probability or percentage, while impact is expressed as a cost value.

- What does an attacker gain from conducting an attack?
- How effective is the attack vector, has it been exploited before?
- How often does the threat successfully affect other enterprises?
- What is the overall impact?

• *Threat intelligence sharing with supported functions*

- Incident response

Responding to breaches, intrusions and other incidents; then conducting lessons learned sessions and sharing the information with the community.

- Vulnerability management

Software vulnerabilities - how to identify, mitigate and fix them.

- Risk management

Conducting assessment of risks and their relevance. Coming up with solutions aimed at reducing this risk through intelligence based frameworks.

- Security engineering

Adapting to emerging threats - security being the main consideration.

- Detection and monitoring

Watching for anomalous patterns in activity over time.

1.3 Given a scenario, perform vulnerability management activities.

- *Vulnerability identification*

Vulnerability scanner can be a software or hardware solution that is configured with a list of weaknesses and exploits and that can scan hosts for the presence of those.

- Define target attributes
- Identify differences between baseline and status quo
- Make a report

- Asset criticality

Prioritize what assets are most important. Identify vulnerabilities and focus on the critical ones. Both ***physical and virtual hosts*** should be scanned!

- Active vs. passive scanning

Active enumeration involves interaction with and touching of the target's infrastructure. Passive is based on stored, static information without engaging with the target. Or passively connecting traffic using a network sniffer.

- Mapping / enumeration

- *Validation*

- True positive

Alert matches a vulnerability and it does exist on the system. A real detection.

- False positive

Alert matches a vulnerability and it does not exist on the system. A fake detection.

- True negative

No alert is signalled and no matching vulnerability exists. No detection.

- False negative

No alert is signalled but a vulnerability exists. An alert should have fired. No detection where there should have been one. System is vulnerable.

- *Remediation / mitigation*

- Configuration baseline

- Patching

Patches can be regular or critical. For patching multiple Windows machines, use the Microsoft System Center Configuration Manager (SCCM).

- Hardening

Attack surface area is reduced by disabling or removing unused services, devices, protocols, etc. Anything left in default mode or not configured should be viewed as a vulnerability. Least privilege for users.

Gold master - standardized configuration baseline containing a hardened image that can be used to rebuild a compromised host.

- Compensating controls
- Risk acceptance
- Verification of mitigation

- *Scanning parameters and criteria*

- Risks associated with scanning activities

Impairment of the network performance, even up to the point of affecting business.

- Vulnerability feed

Similar to AV signatures, these should be regularly updated.

- SCAP - Security Content Automation Protocol - NIST standard

- **CCE** - Common Configuration Enumeration - for provisioning secure configuration checks. Best practice statements.
- **CPE** - Common Platform Enumeration - for hardware, OS and applications
- **CVE** - Common Vulnerabilities and Exposures - long history, sorted by unique IDs. Source: https://cve.mitre.org/
- **NVD** - National Vulnerability Database
- CVSS [severity],
- XCCDF [checklist results],
- OVAL [testing procedures used by checklists].

- Scope

Defining what the subject of scanning is - range of hosts or subnets? IP address ranges? Different portions of the scope can be scanned in different time windows, not to affect the network performance. Also, scope depends on the compliance requirements (like PCI assets, etc.).

- Credentialed vs. non-credentialed

Credentialed scan is internal and includes various necessary creds and permissions within a network. It can be used to obtain a lot of additional information - and more likely to find vulnerabilities.

Non-credentialed scan is external. Fewer details and vulnerabilities can be gleaned but non-credentialed scanning is more realistic and gives the attacker's perspective - from the outside of the firewall. Non-credentialed includes trying to log in with default credentials.

- Server-based vs. agent-based

Server is in this case an external resource that is used to scan a target. Like Nessus. This can be heavy on the other network traffic.

Agent means using a software application installed on the target that scans that target from within, locally. Does not cause network congestion as external communication is limited. Agent scanning can be used offline too.

- Internal vs. external

- Special considerations

- Types of data

- Technical constraints

- Frequency limitations of scanning arising from cost and network impact.
- Certain devices like printers or VoIP can react unpredictably to scans. They should belong to separate scopes so that if issues arise, it's easier to troubleshoot.
- Opening ports for the purpose of scanning can increase attack surface.

- Workflow

Normally the remediation workflow is: detection - remediation - testing.

- Sensitivity levels

Amount of vulnerabilities and the intensity of scans - safe scan vs unsafe scan (unsafe might result in something breaking).

1. Discovery scan - enumeration and mapping of targets only. No vulnerability scanning. Not in-depth.
2. Fast / Basic scan - unpatched vulnerabilities and common configuration issues.
3. Full / Deep scan - comprehensive scan, might affect system performance. Full rescan of every single host, intrusive.
4. Compliance scan - runs through a compliance checklist and a list requirements (e.g. **PCI-DSS - requires a quarterly scan**).

- Regulatory requirements

- Segmentation

- Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings

• *Inhibitors to remediation*

- Memorandum of understanding (MOU)

Not legally binding. Good will based, signals intent to work together.

- Service-level agreement (SLA)

Legally binding. Sets out the terms for providing a service.

- Organizational governance

Business decisions, bureaucracy and other considerations might impact security.

- Business process interruption

Whenever business is disrupted. Service outages might arise from security updates or scans.

- Degrading functionality

Organization systems working but not performing at the peak of functionality.

- Legacy systems

Old systems that are no longer supported. Should be isolated to their own network.

- Proprietary systems

Systems owned by vendors or third party developers. Not always patched in a timely manner.

1.4 Given a scenario, analyze the output from common vulnerability assessment tools.

- *Web application scanner*

- OWASP Zed Attack Proxy (ZAP)

Open source: https://www.zaproxy.org/

Interception proxy for webs apps. Has a vulnerability scan engine.

- Burp suite

Commercial tool: https://portswigger.net/

Burp Suite is an interception proxy to analyze how a web app communicates. It provides tools for automating the modification of requests and insertion of exploits.

Video: https://www.youtube.com/watch?v=h2duGBZLEek

- Nikto

Open source: https://cirt.net/Nikto2

Web application scanner.

- Arachni

Open source: https://www.arachni-scanner.com/

Another web app scanner. Will scan HTML forms, JavaScript forms, JSON input, XML input, links, and any orphan input elements.

- *Infrastructure vulnerability scanner*

- Nessus

On-premise and for cloud. Commercial software. Free for home users.
Source: https://www.tenable.com/products/nessus

Nessus uses plugins for various OS and various vulnerabilities.

- OpenVAS

Open source: https://www.openvas.org/

OpenVAS is a vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low level Internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

- Qualys

Commercial tool: https://www.qualys.com/

Vulnerability management solution - cloud-based. Qualys sensors can be implemented as agent software, a dedicated appliance, or as a virtual machine. It can work as a network vulnerability scanner or a web application scanner.

• *Software assessment tools and techniques*

- Static analysis
- Dynamic analysis
- Reverse engineering
- Fuzzing

• *Enumeration*

- Nmap

Nmap can do discovery scans to footprint the network.

Commands:

- nmap 192.168.1.0/24 - basic syntax of overt scanning for the IP range.
- nmap -sn 192.168.1.0/24 - host discovery scan
- nmap -sL 192.168.1.0/24 - list scan of IPs, do reverse DNS query for hosts on those IPs
- nmap -PS - TCP SYN ping - to check if hosts are alive
- nmap --scan-delay <time> - sparse scanning
- nmap -Tn - scan delay, where n can be from 0 to 5 (slowest >> fastest)
- nmap -sI - idle stealthy scan (redirection)
- nmap -f OR --mtu - fragmentation
- nmap -oN (OR -oX OR -oG) - send output to a file
- nmap -sV - detailed scan
- nmap -A - aggressive scan
- nmap -O - OS identification

Detailed cheat sheet: https://www.tutorialspoint.com/nmap-cheat-sheet

For target practice with scanning: http://scanme.nmap.org/

* Open|filtered status = ports gave no response to the scan; nmap can't determine if a port is open or filtered.

- hping

Hping is an open-source packet generator and analyzer for the TCP/IP protocol. Hping sends TCP/UDP/ICMP/RAW-IP packets. It can be used for firewall testing, TCP/IP auditing, network testing, determining uptime, etc.

- Active vs. passive

- Responder

Used for conducting man in the middle attacks and retrieving password hashes sent between the victim system and the resource.

- *Wireless assessment tools*

- Aircrack-ng

Utilities for testing network security - collects wireless packet data:

- Airmon-ng
- Airodump-ng
- Aireplay-ng
- Aircrack-ng - only effective against WEP-based networks

- Reaver

Brute force attacks against WPS-enabled access points.

- oclHashcat

Relies on the GPU to brute force crack password hashes. Hashcat uses word lists for conducting dictionary attacks against passwords.

- *Cloud infrastructure assessment tools*

- ScoutSuite

https://github.com/nccgroup/ScoutSuite/wiki

It can be used to audit instances and policies on multi cloud platforms like AWS or Azure. Checks & reports on objects like VM instances, S3 buckets, IAM accounts.

- Prowler

https://github.com/toniblyx/prowler

Similar to the above but for AWS only.

- Pacu

https://github.com/RhinoSecurityLabs/pacu

Exploitation framework for testing security of AWS accounts. Can be used to exploit API keys or compromise accounts. It can enumerate users and their permissions.

1.5 Explain the threats and vulnerabilities associated with specialized technology.

• *Mobile*

BYOD - people can bring their own equipment and use it for work purposes. Considered not secure and challenging as devices can have various vulnerabilities.

- Deperimeterization - suddenly the perimeter expands beyond the company. Guy leaves a device behind in a taxi - failed deperimeterization.
- Increased load on the network
- Forensic issues of investigating privately own devices
- Jailbraking poses a huge risk to security of mobile devices
- MDM - Mobile Device Management - tracking and controlling mobile devices
- EMM - Enterprise Mobility Management - identity and app management

• *Internet of Things (IoT)*

Objects that can connect to the Internet by embedded components. Often not secured and running Linux that often does not get updated. IoT should be segmented appropriately and not have access to the whole network.

• *Embedded*

Stripped down computer systems designed for a specific function. They usually have one job to do (like control systems for medical devices, pipelines, ASIC Bitcoin miners, etc). Support and security patches are often very limited. Segmentation again helps with these.

PLC - Programmable Logic Controller

• *Real-time operating system (RTOS)*

Used for time critical tasks. For things that have to have 100% uptime, no reboots, no crashes.

- *System-on-Chip (SoC)*

Processor that integrates multiple logical controllers onto a single chip. Usually small and power efficient.

- *Field programmable gate array (FPGA)*

Can be programmed to perform a specific function - by a customer, not by the manufacturer. Cheaper and more flexible than embedded ASIC.

- *Physical access control*

Premise systems - for physical security.

PACS - security cameras, badges, biometric scanners, etc.

- *Building automation systems*

BAS - battery backups for power, elevators, AC control. All should be segmented. Vulnerabilities include plaintext credentials in the code or vulnerabilities to web interface through code injection.

- *Vehicles and drones*

- CAN bus

CAN bus in a vehicular network can be secured by creating an air-gap between various extra systems like entertainment and the vehicle's CAN bus.

• Workflow and process automation systems

- *Industrial control system*

Availability and integrity > confidentiality

ICS - network for managing embedded devices (power stations, hospitals, etc.). ICS uses fieldbus to link various PLCs together. For human operation, it requires a HMI - Human-Machine Interface.

- *Supervisory control and data acquisition (SCADA)*

Used for managing large scale, multiple site devices spread geographically.

- Modbus

Communications protocol for industrial networks and devices (equivalent to TCP IP for regular computing). Used to change PLC configurations.

1.6 Explain the threats and vulnerabilities associated with operating in the cloud.

- *Cloud service models*

- Software as a Service (SaaS)

SaaS - one of the challenges includes identity and access management - because identification and authorization is handled by the cloud service.

- Platform as a Service (PaaS)

- Infrastructure as a Service (IaaS)

Virtual machines can be deployed in what's called a Trusted Execution Environment (TEE) - a security enclave, which means that other tenants of the cloud platform won't be able to view or modify processes.

- *Cloud deployment models*

- Public
- Private
- Community
- Hybrid

- *Function as a Service (FaaS) / serverless architecture*

In serverless architecture a smart client may require only specific functions, abstracted from the full network infrastructure.

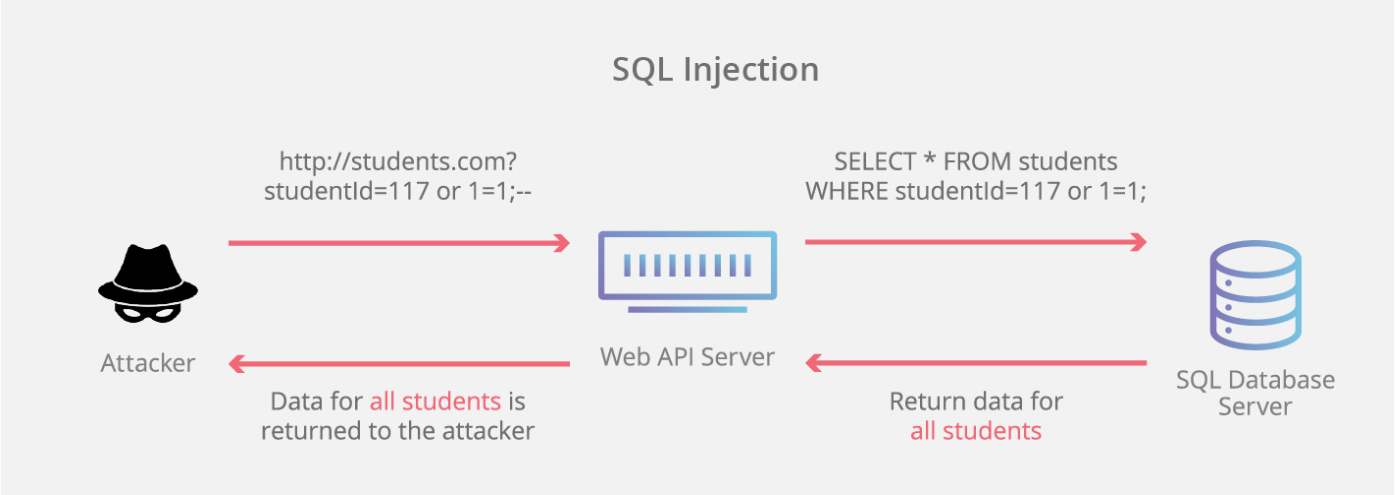
• Infrastructure as code (IaC)
• Insecure application programming interface (API)
• Improper key management
• Unprotected storage
• Logging and monitoring
- Insufficient logging and monitoring
- Inability to access

1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

• *Attack types*

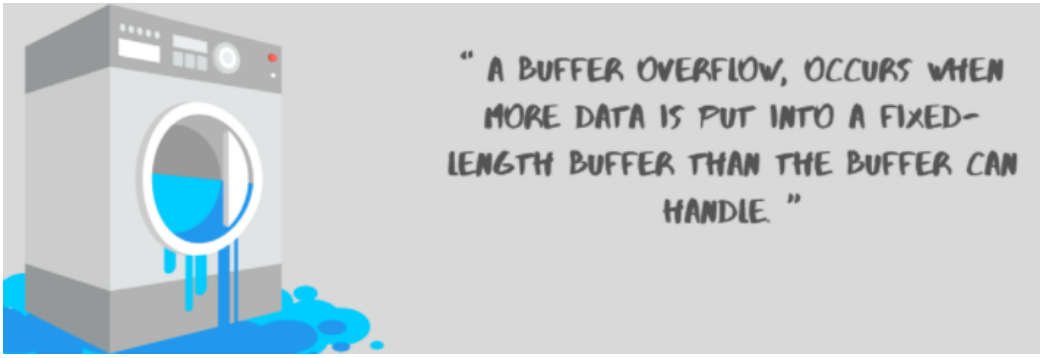
- Extensible markup language (XML) attack

- Structured query language (SQL) injection



- Overflow attack

- Buffer - data goes past the boundary of the destination buffer, corrupts memory and overflows.



- Integer - a computed result is too large to fit into assigned storage space.

- Heap - input is allowed to overwrite memory locations used to store dynamically sized variables.

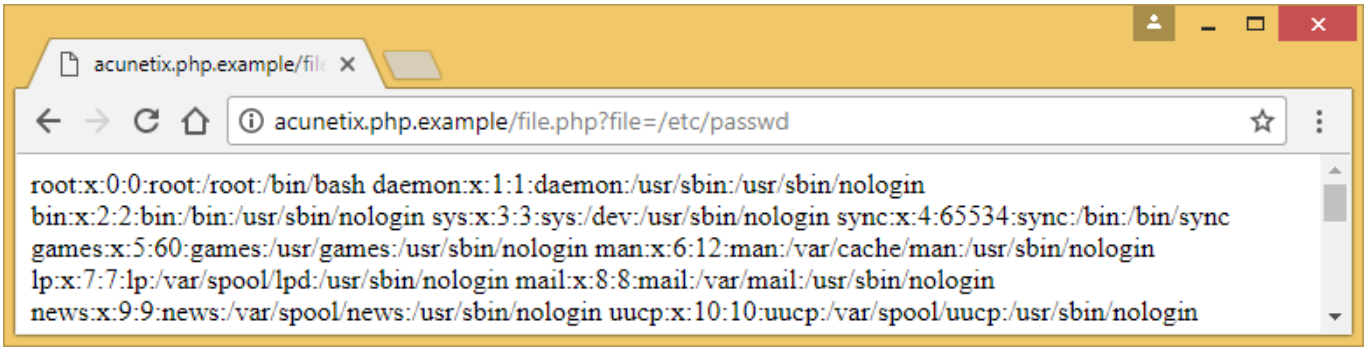
- Remote code execution

This is enabled by vulnerabilities that allow running code on another system. Code can be transported between machines over the Internet and executed remotely.

- Directory traversal

This is a HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory. It can also be encoded, so not necessarily in plain text.

https://www.acunetix.com/websitesecurity/directory-traversal/



Mitigation: input validation.

- Privilege escalation

Gaining admin or root permissions when normally not being entitled to.

- Vertical - escalating from user to admin
- Horizontal - user accesses resources of peer users, not those with higher permissions

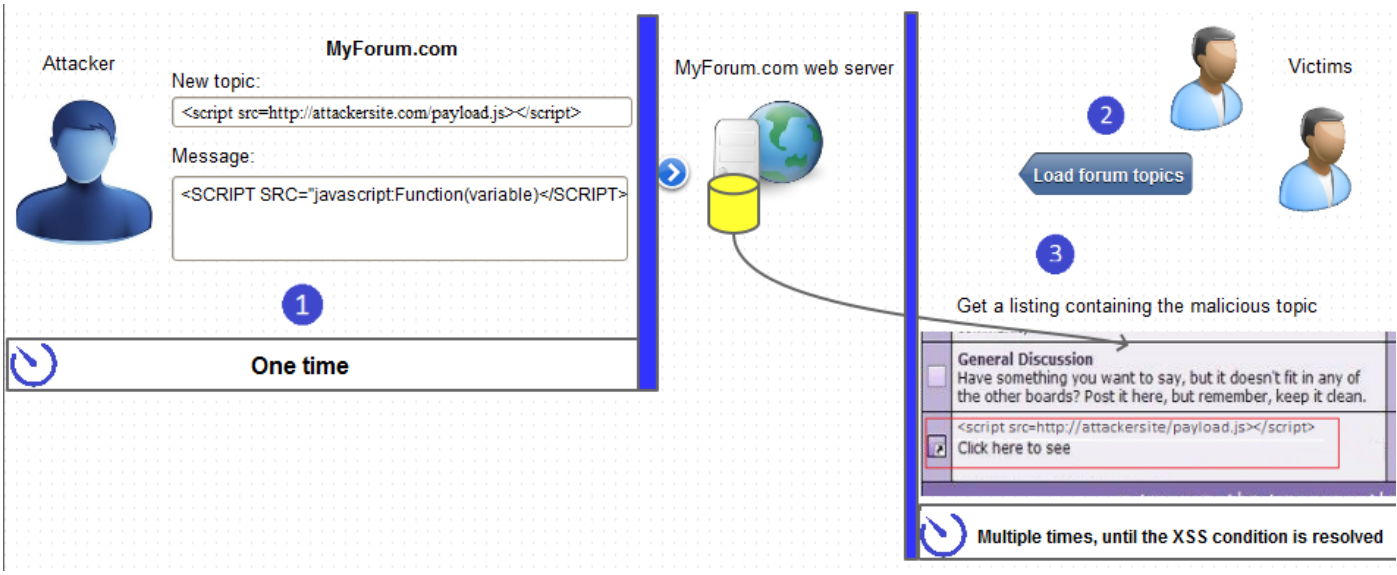
- Password spraying
- Credential stuffing
- Impersonation
- On-path attack (previously known as man-in-the-middle attack)
- Session hijacking

- Rootkit

Malware that modifies system files at the kernel level to conceal itself.

- Cross-site scripting

Uses crafted URLs to perform code injection against a trusted website. The trusted website returns a page containing the malicious code to the user and the code is then executed in the user's browser.



- Reflected

This is XSS that is once off - it does not persist.

Mitigation: WAF; use appropriate response headers; avoid suspicious links.

- Persistent

Code is inserted into a back end database used by the site.

- Document object model (DOM)

Exploits client side web browser.

- *Vulnerabilities*

- Improper error handling

Default error messages can leak sensitive information.

- Dereferencing

Removal of the relationship between a pointer and the things it points to.

- Insecure object reference

- Race condition

Multiple threads attempt to write a variable at the same memory location (and they “race” to it). Can be the case of an attacker trying to conduct an action ahead of the legitimate process that was to take place.

- Broken authentication
- Sensitive data exposure
- Insecure components
- Insufficient logging and monitoring
- Weak or default configurations
- Use of insecure functions
  - strcpy

2.0 Software and Systems Security

2.1 Given a scenario, apply security solutions for infrastructure management.

- *Cloud vs. on-premises*
- *Asset management*

- Asset tagging

Each of these will have IAM credentials: endpoints, peripherals, servers, software. All of these will be given certain labels and unique IDs for the purpose of classification.

- *Segmentation*

Networks can be separated into multiple separate sub-networks or zones.

- Physical

Two networks could be operating in parallel but not connected. Everything is connected up and divided up by physical equipment - switches.

- Virtual

As above, but segmentation does not rely on switches but VLANs. Only one switch is needed - everything else can be segmented virtually.

- Jumpbox

Hardened server or device that provides access to other hosts in the DMZ. It creates segmentation between a user's laptop and the rest of the network users connect to.

- System isolation

DMZ - demilitarized zone - segment isolated by firewalls. It is a semi-trusted zone and it prevents outsiders from seeing within a private part of the network.

Bastion host - hardened services located in the DMZ.

- Air gap

Physical separation of a network from other networks. There is no outside connection at all. Air gaps demand cross network transfers. USB and similar devices create a vector of attack for air-gapped networks.

- *Network architecture*

- Physical

All the physical components, from cabling to wireless devices. Physical security measures add to the network architecture security.

- Software-defined

Software Defined Networking (SDN) includes APIs and virtualized solutions.

Software applications are responsible for deciding how to best route data (control layer) and also for moving the packets around (data layer).

- Virtual private cloud (VPC)

- Virtual private network (VPN)

Secure tunnels connecting two endpoints over an unsecure network.

- Serverless

- *Change management*

- *Virtualization*

Host computer with a hypervisor that can install and manage virtual machines.

VM sprawl - VM provisioning without proper change control procedures.

- Virtual desktop infrastructure (VDI)

Virtualization implementation that separates a computing environment from an end user's physical computer. The host device does not matter - once it's capable of running a virtual image. No local processing however - if a server / network is down, cannot use the system.

- *Containerization*

Allows for an isolated execution environment for an application. Containers are isolated and can't communicate with each other. But if a host OS is compromised, so are the containers.

Containerization separates applications from the OS and underlying hardware by extracting the OS kernel and enabling security separation from OS and from hardware.

- *Identity and access management*

- Privilege management

Discretionary Access Control (DAC) - each resource has an access control list (ACL) managed by whoever the owner is.

- Multi-factor authentication (MFA)

Two different factors of credentials: from physical tokens, digital security certificates, SMS or apps, biometrics, geolocation.

- Single sign-on (SSO)

"One password to rule them all". But the disadvantage is the one single point of failure, should this password be compromised.

- Federation

Shared login capability across multiple sites ("sign in with Google"). It's a trust relationship between two different networks. ***This is not a single sign on!***

Relying Parties (RP) - provide services to members of a federation. Identity Provider (IdP) provides identities and manages them.

- Role-based

Permissions depend on what predefined role a user has. Should follow the principles of least privilege and separation of duties. RBAC - Role Based Access Control.

- Attribute-based

Attribute Based Access Control - dividing users into groups with defined attributes.

- Mandatory

Mandatory Access Control (MAC) - everything has a clearance level and is labelled.

- Manual review

Checking manually if permissions are accurate for certain users - if people get moved to various roles or sacked, this should be reflected by changes to their permissions. Manual reviews also include recertification of accounts, permissions, configurations and clearance.

• Cloud access security broker (CASB)

• *Honeypot*

Active defence mechanism - deceives the attacker by luring him with a decoy. It could be a fake unpatched server or database, designed to make the attacker reveal their methods. Honeypots can be connected together to form a honeynet.

• *Monitoring and logging*

Audit logs - for tracing user actions and detecting attempted intrusions.

Red flags:
- Multiple failed logins
- Unscheduled changes to systems
- Errors and gaps in logs

• Encryption

• *Certificate management*

- **Sigcheck** - third party utility to verify root certificates by comparing them against a trust list.

- **OpenSSL** -
- **Certutil** - Windows utility for certificate management

Certificate life cycle: creation; storage; dissemination; suspension; revocation.

• *Active defense*

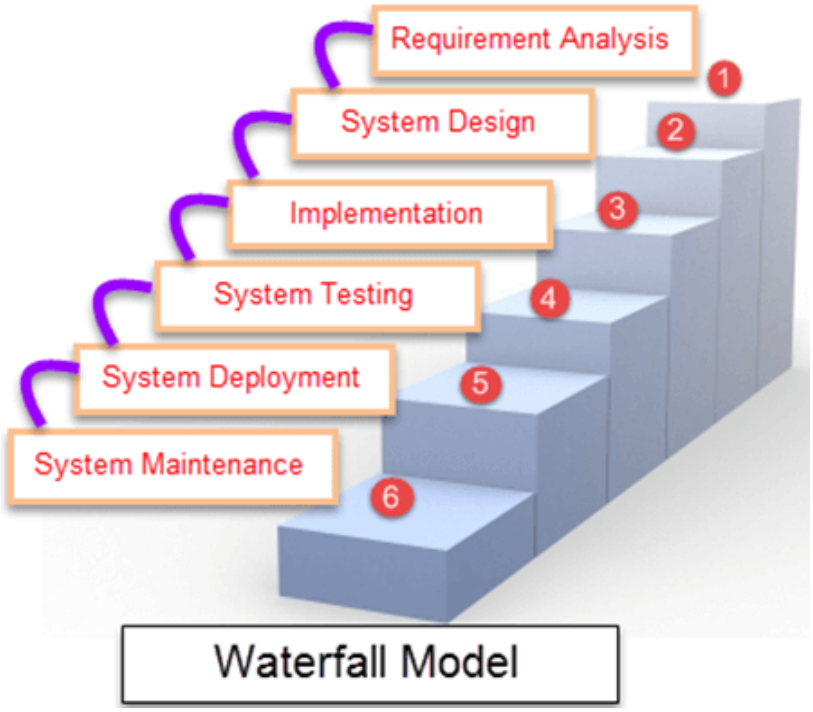
Hack back - usually only nation state agencies. They counterattack the adversary. For example, a DDoS against the IP address that launched an attack in the first place. This might be illegal, depending on jurisdictions.

2.2 Explain software assurance best practices.

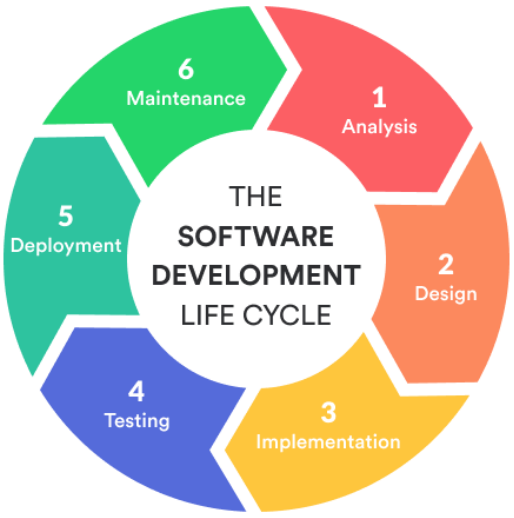
• Platforms
- Mobile
- Web application
- Client/server
- Embedded
- System-on-chip (SoC)
- Firmware

• *Software development life cycle (SDLC) integration*

The Waterfall Model - SDLC phases cascade down, one must be finished before the next phase is started. Drawbacks - long cycle, delays, customer can’t respond as software gets developed. Security might be treated as an afterthought.



The Agile Model - incremental and non-linear development, with room left for changing priorities and expectations.



The phases of the SDLC model:

1. Requirement gathering and analysis
2. Design
3. Implementation or coding
4. Testing
5. Deployment
6. Maintenance

• DevSecOps
• Software assessment methods
- User acceptance testing
- Stress test application
- Security regression testing
- Code review

• Secure coding best practices

- Input validation

Every time any input is accepted into a web app, it should be validated. It means that characters considered unsafe are not accepted into the input fields - therefore preventing various attacks like SQL injections or XSS.

- Output encoding
- Session management
- Authentication
- Data protection
- Parameterized queries
• Static analysis tools
• Dynamic analysis tools
• Formal methods for verification of critical software
• Service-oriented architecture
- Security Assertions Markup Language (SAML)
- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)
- Microservices

2.3 Explain hardware assurance best practices.

• *Hardware root of trust*

Secure boot - a feature in UEFI that establishes the root of trust in the firmware.

- Trusted platform module (TPM)
- Hardware security module (HSM)
• eFuse

• Unified Extensible Firmware Interface (UEFI)
• Trusted foundry
• Secure processing
- Trusted execution
- Secure enclave
- Processor security extensions
- Atomic execution
• Anti-tamper

- *Self-encrypting drive*

SED remains unlocked if a laptop is restarted without shutting off power.

• Trusted firmware updates

- *Measured boot and attestation*

Measured boot is a security feature preventing rootkit and bootkit infections. It logs the boot process to a computer's UEFI and to a trusted server (attestation server). A computer must have a TPM and UEFI to use a measured boot.

• Bus encryption

3.0 Security Operations and Monitoring

3.1 Given a scenario, analyze data as part of security monitoring activities.

- *Heuristics*

- *Trend analysis*

Detecting patterns in data. It's important to see what the baseline is and what the anomalies are. It's not possible to identify a trend from just looking at singular events.

- Frequency based - how often, in what intervals
- Volume based - size of events - how much, how many?
- Statistical deviation analysis - averaging and stats, looks for outliers

• *Endpoint*

- Malware

- Reverse engineering

The objective is to read the code and find out who wrote it. Sandboxing is a key requirement for malware analysis. Other things include: code detonation; software fingerprinting against existing hashes; decompilers and disassemblers.

First two bytes of a binary headery that indicate a file type - **Magic Numbers**.

- Memory

- System and application behavior

Known-good behavior & Anomalous behavior - establish a baseline and understand what is normal system behaviour. Then match it against anomalies and outliers.

- Exploit techniques

- **Dropper / downloader** - small file, piece of malware that once deployed on a system, proceeds to download the rest of the malicious code.
- **Shellcode** - lightweight code designed to run an exploit on the target.
- **Code injection** - malicious code with ID number of a legitimate process
- **Living Off the Land** - using standard system tools to perform intrusions.

- File system

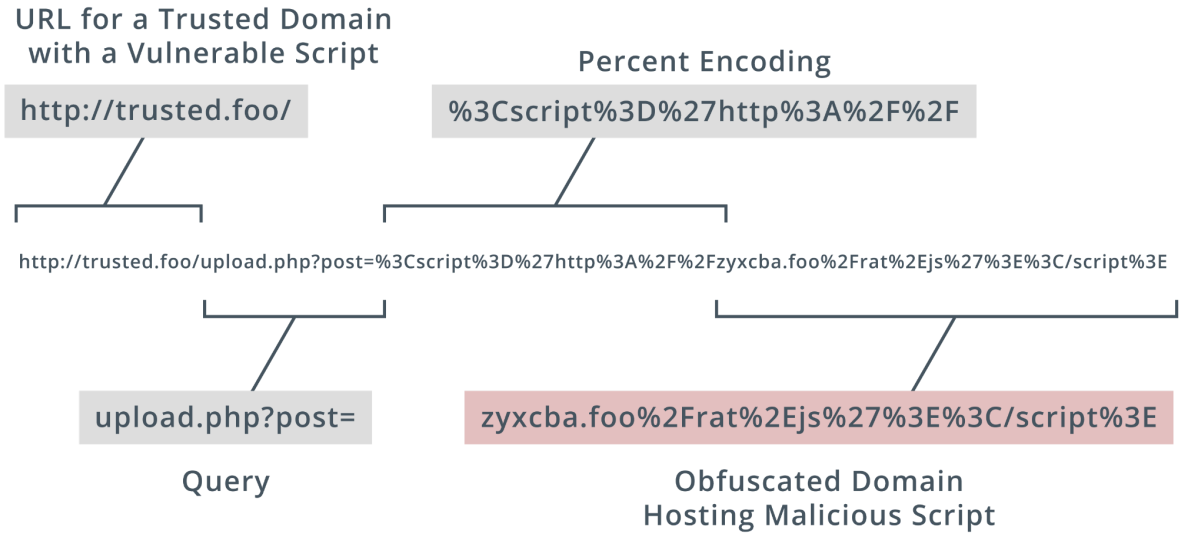
- User and entity behavior analytics (UEBA)

Attempts to determine which users are behaving oddly. Normally the exhibited behaviour is compared to what users would normally do - so if their account is hacked, the behaviour pattern won't match. Also works for insider threats.

- *Network*

- Uniform Resource Locator (URL) and domain name system (DNS) analysis

- GET - HTTP request to retrieve a resource
- POST - sending data to the server for processing by the requested resource
- PUT - upload a resource to a server
- DELETE - remove a file
- HEAD - retrieves headers only, not the body. Used for banner grabbing.



200 - GET or POST request successful
201 - PUT request successful
3xx - redirect occurred by the server

4xx - error in the client request

- ❏ 400 requested could not be parsed
- ❏ 401 authentication creds not supplied
- ❏ 403 insufficient permissions
- ❏ 404 non existent resource

5xx - server side issues

- 500 general error
- 502 bad gateway
- 503 overloading of a server
- 504 gateway timeout

Reserved ASCII characters are used as delimiters within the URL syntax and should only be used unencoded for those purposes:

: / ? # [ ] @ ! $ & ' ( ) * + , ; =

Percent encoding allows a user-agent to submit any safe or unsafe character (or binary data) to the server within the URL. Percent encoding can be misused to obfuscate the nature of a URL (encoding unreserved characters) and submit malicious input as a script or binary or to perform directory traversal.

- Domain generation algorithm (DGA)

To avoid using hard-coded IP ranges, malware has switched to domains that are dynamically generated using an algorithm. This works through dynamic DNS (DDNS) services, typically using fraudulent credentials and payment methods or using bulletproof hosting, where the service provider does not act against illicit activity.

```
uqodupegbo.ddns.net
xisenuun.ddns.net
omexithamisi.ddns.net
uxtoleite.ddns.net
uglaweedipwaho.ddns.net
ahtilenearo.ddns.net
niesivaxumo.ddns.net
iricilec.ddns.net
uqadvoduurgeuhi.ddns.net
ehwepikeisi.ddns.net
```

When the malware needs to initiate a C&C connection, it tries a selection of the domains it has created.

DGA can be combined with techniques to continually change the IP address that a domain name resolves to. This continually-changing architecture is referred to as a **fast flux network**.

- Flow analysis

The analysis of network traffic stats sampled by a flow collector - collects metadata and statistics on the traffic and not the traffic itself. Examples:

- NetFlow - Cisco product, network flow goes into a database

- Zeek (Bro) - passive network monitor
- MRTG - open source grapher tool

- Packet and protocol analysis

- Malware

• *Log review*

- Event logs

- Syslog

Syslog server is a centralized log management solution. By looking through the logs on the syslog server, the technician could determine which service failed on which server, since all the logs are retained on the syslog server from all of the network devices and servers.

Syslog severity levels:

0 - Emergency: System is unstable
1 - Alert: Correct action must be taken immediately
2 - Critical: Critical condition/hard failure
3 - Error: Error condition detected
4 - Warning: Warning condition/message
5 - Notice: Normal condition
6 - Informational: Informational messages
7 - Debug: Debug level messages

- Firewall logs
- Web application firewall (WAF)
- Proxy
- Intrusion detection system (IDS) / Intrusion prevention system (IPS)

• Impact analysis
- Organization impact vs. localized impact
- Immediate vs. total

• *Security information and event management (SIEM) review*

Can be hardware, software or external outsourced services.

- Rule writing
- Known-bad Internet protocol (IP)
- Dashboard

• *Query writing*

Correlation - focuses on relationships between individual data points, but requires normalisation of the data first.

Regular Expressions (regex): https://regexr.com/

- String search, - Script, - Piping

Lecture on searching and piping:
https://www.udemy.com/course/comptiacsaplus/learn/lecture/21163412#overview

Lecture on script tools:
https://www.udemy.com/course/comptiacsaplus/learn/lecture/21163420#overview

• *E-mail analysis*

- Malicious payload

- Domain Keys Identified Mail (DKIM)

Cryptographic authentication for mail using a public key published as a DNS record. It can be used (or replace) SPF.

- Domain-based Message Authentication, Reporting & Conformance (DMARC)

- Sender Policy Framework (SPF)

DNS record that identifies hosts authorized to send mail for the domain.

A TXT record for SPF defines the mail servers that are allowed to send mail for your domain. A single domain can have only one TXT record for SPF. However, the TXT record for a domain can specify multiple servers and domains that are allowed to send mail for the domain.

- Phishing

Fraudulent emails that impersonate a legitimate sender in order to deceive the victim and make them disclose confidential information. More targeted phishing is spear-phishing.

S/MIME - Secure / Multipurpose Internet Mail Extensions - allows to encrypt emails and to digitally sign emails to verify the legitimate sender of the message, making it effective against phishing.

- Forwarding

A phishing email is formatted to look like it has come as part of a reply or a previous email thread.

- Digital signature

- Email signature block

Signature blocks can be a giveaway of a phishing email due to poor formatting or unusual block structure.

- Embedded links

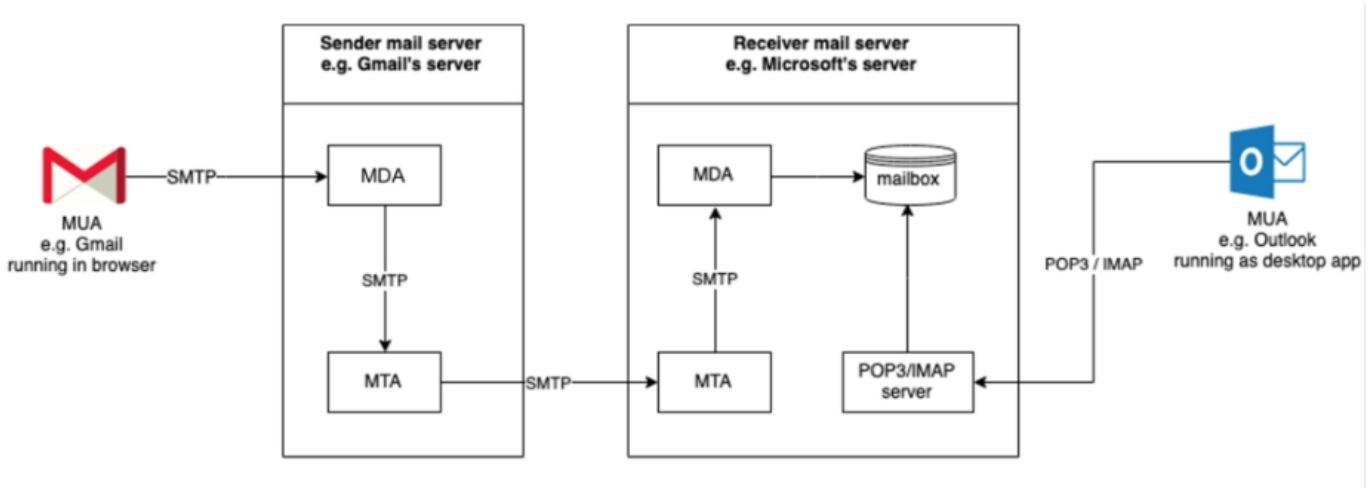
Links can be used to direct users to spoofed destinations.

- Impersonation

The attacker assumes the identity of a legitimate person who could be a real employee of the company (see the CEO fraud). Usually linked to business email compromise (BEC), where a takeover of the real email account takes place and is used to impersonate the victim. This cannot be detected the same way a spoofed email can be - as the sender is using a truly legitimate email (but compromised).

- Header

Record of email servers involved in transferring the email from the sender to the recipient.



Video: https://www.youtube.com/watch?v=nK5QpGSBR8c

Questions:

- *Which of the following techniques would allow an attacker to get a full listing of your internal DNS information if your DNS server is not properly secured?*

Zone transfers. A DNS zone transfer provides a full listing of DNS information. If an internal DNS server is improperly secured, an attacker can gather this information by performing a zone transfer.

- *A company's NetFlow collection system can handle up to 2 Gbps. Due to excessive load, this has begun to approach full utilization at various times of the day. If the security team does not have additional money in their budget to purchase a more capable collector, which of the following options could they use to collect useful data?*

Enable sampling of the data. Sampling can help them capture network flows that could be useful without collecting everything passing through the sensor. This reduces the bottleneck of 2 Gbps and still provides useful information.

3.2 Given a scenario, implement configuration changes to existing controls to improve security.

• Permissions

• *Allow list (previously known as whitelisting)*

Implied deny rule - deny everything by default unless it’s on a whitelist.

- *Blocklist (previously known as blacklisting)*

Blocking certain types of traffic or resources. Everything is allowed, unless it’s on the blacklist.

• Firewall
• Intrusion prevention system (IPS) rules
• Data loss prevention (DLP)

- *Endpoint detection and response (EDR)*

Submit malware samples to VirusTotal: https://www.virustotal.com/gui/home/upload

Yara - multi platform program for identifying and classifying malware samples. This is done through applying Yara rules.

• Network access control (NAC)
• Sinkholing
• Malware signatures
- Development/rule writing
• Sandboxing
• Port security

3.4 Compare and contrast automation concepts and technologies.

• Workflow orchestration
- Security Orchestration, Automation, and Response (SOAR)
• Scripting
• Application programming interface (API) integration
• Automated malware signature creation
• Data enrichment
• Threat feed combination
• Machine learning
• Use of automation protocols and standards
- Security Content Automation Protocol (SCAP)

- *Continuous integration*

Developers should commit and test updates often, even a couple of times a day. This is to reduce potential conflicts of code committed by two or more devs and to resolve code issues quickly and on the fly.

- *Continuous deployment / delivery*

Continuous deployment - focused on making changes to the prod environment - app and platform updates are committed to production rapidly.

Continuous delivery - focused on testing - app and platform requirements are frequently tested and validated for immediate availability.

4.0 Incident Response

4.1 Explain the importance of the incident response process

- *Communication plan*

- Limiting communication to trusted parties

Includes: law enforcement, information sharing partners (ISAC), vendors and manufacturers, actual or potential victims, media

- Disclosing based on regulatory / legislative requirements

Depending on what type of data leaked and what jurisdiction it falls under.

- Preventing inadvertent release of information

Avoid media attention, contain the news to the CSIRT team only. Employ public relations team to properly release info.

- Using a secure method of communication

- ❏ Using end to end encryption apps - Signal or Whatsapp, off the record comms
- ❏ External encrypted emails
- ❏ Accurate contact list

- Reporting requirements

GDPR - within 72h from the breach

5 types of breaches:

1. **Data exfiltration** —An attacker breaks into systems and transfers data to another system. This is the most serious type of breach.

2. **Insider data exfiltration** —As above, but the attack is perpetrated by an employee or ex-employee with privileges on the system.

3. **Device theft / loss** —A device storing data is lost or stolen. The device may be protected by encryption or strong authentication, in which case a breach may be suspected, but not proven.

4. **Accidental data breach** —Human error or a misconfiguration leads to data being made public or sent to unauthorized recipients.

5. **Integrity / availability** —Attacks that compromise the availability (destruction of systems-processing data) and integrity (a virus corrupting backups) are also likely to require regulatory notification and reporting, however.

• *Response coordination with relevant entities*

- Legal

Legal officers tasked with dealing with LE, as well as evaluating the incidents from the compliance perspective.

- Human resources

It is vital that contact with suspected insider threats is mediated through HR, so that no breaches of employment law or employment contracts are made.

- Public relations

For handling negative PR, talking to the media, etc.

- Internal and external

Internal = usually a rapid response team. External = advisory bodies and regulators.

- Law enforcement

External stakeholder. LE agencies depend on the jurisdiction. Decisions to involve LE must be taken by senior executives as it's likely to cause a lasting business disruption. They will take legal action against the attacker if apprehended.

- Senior leadership

Typically involves a crisis management team. They will make key decisions and escalate them through the chain of command. Everything must be appropriately approved and agreed on.

- Regulatory bodies

For advice and various regulatory matters.

- *Factors contributing to data criticality*

- Personally identifiable information (PII)

Names, DOBs, addresses, social security numbers and so on. Anything linked to the subject that can enable their identification.

- Personal health information (PHI)

Health records, patient and medical insurance data, lab tests, etc. PHI cannot be changed once leaked, the way financial info can. HIPAA regulations apply.

- Sensitive personal information (SPI)

As defined by GDPR, SPI includes religious beliefs, political opinions, trade union membership, gender, sexual orientation, racial or ethnic origin, genetic data, and health information

- High value asset

HVA is a critical information system. Critical = if the confidentiality, integrity, or availability of the asset is compromised, it impacts mission essential functions of the organization. An incident involving an HVA must be considered high priority.

- Financial information

Anything related to payments and financial transactions. Most commonly this is card numbers. PCI DSS regulations apply - ***Requirement 11***.

- Intellectual property

IP can include copyright works, patents, and trademarks.

- Corporate information

Contracts, legal information, data on sales, salaries and products.

4.2 Given a scenario, apply the appropriate incident response procedure.

- *Preparation*

Before any incident response takes place, one should conduct a data criticality and prioritization analysis, to focus on what needs to be the number one for protection.

NIST incident response life cycle:

1. **Preparation** — hardening systems, writing policies and procedures, and setting up confidential lines of communication, creating incident response resources and procedures. ***Training, testing, documentation.***

2. **Detection and Analysis** — if an incident has taken place, assess how severe it might be (triage), followed by notification of the incident to stakeholders.

3. **Containment** — Limit the scope and magnitude of the incident, secure data while limiting the immediate impact on customers and business partners.

4. **Eradication and Recovery** — the cause of the incident can be removed, and the system brought back to a secure state.

5. **Post-incident Activity** — Lessons learned and documenting the incident response. The outputs from this phase feed back into a new preparation phase in the cycle.

- Training

This depends on the role performed. Training also applies to end users - for example faux phishing campaigns. Lessons learned - key part of training, used to improve the security posture. Training includes soft skills and relationships.

- Testing

Practical exercises, simulating real incidents. Tabletop Exercise (TTX) - theoretical aspects hashed out at a table, discussions on what would be done. No hands on.

Pentest - practical testing, simulated intrusion that actually takes place. There is a specific goal in mind. Rules of engagement are pre-determined before.

- Documentation of procedures

A playbook - a set of standard operating procedures.
https://www.incidentresponse.com/playbooks/
Procedures include things like:

Call List - incident response contacts of people who should be called in the event of an incident. Includes secondary and tertiary contacts and means for contacting them.

Incident Form - details of what, when, who, how, etc.

• *Detection and analysis*

OODA Loop - Observe, Orient, Decide, Act

Defense capabilities:

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

- Characteristics contributing to severity level classification

Divided into: functional impact, economic impact, recoverability effort, data (information) impact rating.

Impact can be divided further into:

- Organisational - wide range of users in the org, large scale impact
- Localised - single department, small user group, small amount of systems
- Immediate - direct costs incurred
- Total - cost and damage during the incident + long term effects

- Downtime

Incidents can degrade the availability of systems or assets. See DDOS attacks.

- Recovery time

Higher recovery time means a more serious incident and higher priority one.

- Data integrity

Where data is modified and loses integrity. Can't trust it anymore.

- Economic

Short term and long term costs incurred as result of the incident.

- System process criticality

Essential business functions are threatened.

- Reverse engineering

When malware is linked to an adversary group.

- Data correlation

Incident characteristics indicate it could be correlated to a threat actor, like an APT.

- *Containment*

Containment means limiting the magnitude and impact of the incident by securing assets.

1. Ensure safety and security of staff
2. Prevent ongoing breach or intrusion
3. Identify if the attack is the primary or secondary attack
4. Avoid alerting attackers (APTs can “burn down the house”)
5. Preserve any forensic evidence

- Segmentation

Creating segments within the network by using networking mechanisms, routing, subnets, VLANs or firewalls. Sandbox - separate the system from the rest of the environment. Honeypots and honeynets can be sandboxes to lure in attackers and make them uncover their methods. Traffic can also be rerouted elsewhere.

- Isolation

An affected component gets removed out of the environment. Air gap - cutting off connection to such systems, by physically removing connections or removing accounts and their access rights. This is considered the strongest possible response to an incident.

- *Eradication and recovery*

Eradication - complete destruction / removal of the factor that caused an incident.

Recovery - bringing systems back to good working order. Might include new devices.

- Vulnerability mitigation

Perform vulnerability scans and attempt to protect systems against future attacks.

- Sanitization

Overall efforts to dispose of obsolete records, including physical storage media. This includes a **Cryptographic Erase** (CE) - sanitizing a **self-encrypting drive** by erasing the media encryption key (usually for SSDs).

Zero fill - overwrite a drive with zeroes. For older magnetic drives. Not reliable for SSDs.

Command in Windows c:/ fs:NTFS /p:1 (p = amount of passes of sets of zeroes).

Secure Erase (SE) - specific erase software used.

- Reconstruction / reimaging

Replacement of the affected system with a brand new one, from a known good image. However, some malware might be resilient to formatting the drive - so this does not always work.

- Secure disposal

Physical destruction of the media - mechanical shredding, incineration, degaussing.

- Patching

Updates and fixes to a system. Scan, patch, scan again.

- Restoration of permissions

Permissions should be reviewed and confirmed that everybody has correct ones. If necessary, passwords should be changed and managed accordingly.

- Reconstitution of resources

Restoring a system that cannot be sanitized using manual removal or reinstallation. Usually applies to single settings or single files. Starts with scanning for malware

presence, followed by termination of suspected processes, disabling autostart, replacement of resources with trusted content from trusted media. Then reboot and analyze for malware. If malware persists, analyze USBs and firmware for malware.

- Restoration of capabilities and services

If no malware was detected, reconstitution is successful and the system can return to production.

- Verification of logging / communication to security monitoring

Verify that logging works. Attackers might have turned off logging. Logs should be audited and searched for any changes performed by the attacker.

System hardening:

- Turn off all unused components and subsystems
- Disable unused accounts (guest, admin, etc.)
- Implement patch management
- Restrict host access to peripherals (disable USB ports, DVD tray, etc)
- Restrict shell commands (only admins should use shell, not normal users) - least privilege principle

• *Post-incident activities*

Post incident reports should be tailored to a specific audience and their needs. Executive summary especially targets non technical executives.

- Evidence retention

Preservation of evidence in cases of a legal or regulatory impact. Necessary for prosecution and court cases. But retention often means cost.

- Lessons learned report

Insights into what and how to do to improve security posture.

1. Who was the adversary?
2. What was the motive and what did they try to do?
3. When did the incident happen? When was it detected?
4. Where did it happen?
5. How did it happen?
6. How could we have stopped it? What can we do about it?

NB: Lessons learned is about improving the security posture, not assigning blame.

- Change control process

Aims to document emergency changes that bypassed normal configuration management / change control process and to return to them post-incident. Changes that require too long to be approved won't be effective.

- Incident response plan update

Aims to identify plan deficiencies and make changes to any future IR plans

- Incident summary report

Key information, for a specific audience. Might be for the PR department or for system administrators.

- IoC generation

Indicators of compromise include: network and host artifacts, addresses, hashes, tools, TTPs, etc. It enriches filters and query statements and enables building new ones.

- Monitoring

Continuous monitoring for old and new methods of attack.

4.3 Given an incident, analyze potential indicators of compromise.

- *Network-related*

- Bandwidth consumption

Value of bytes sent / received or a percentage of the link utilization.

- Beaconing

A network node attempts to link to another node (C2 server for malware). Beaconing can be used legitimately too - by systems doing automatic updates or by wireless access points that beacon the whole time.

Infected hosts beacon out to C2 servers at intervals to show they are still active as part of a botnet.

DGA - Domain generation algorithm

Fast flux DNS

- Irregular peer-to-peer communication

SMB - Server Message Block - sometimes abused by attackers. Communication happening between 2 clients on a network where normally they don't communicate or only communicate with a server is an indicator of compromise.

Lateral movement - can be identified by analysing irregular peer to peer communication. Often followed by pivoting - using one infected machine to attack the next. Pivot is often followed or preceded by privilege escalation.

- Rogue device on the network

Anything that has not been authorised and is connected to a network - from switches and network taps, VMs, to simple USB sticks.

Network tap - physical device attached to cabling that records packets passing over a network segment.

Wireless Access Point (WAP) - rogue ones used to conduct man in the middle attacks.

Rogue server - aimed at tricking users to divert traffic.

Personal devices plugged into the network should also be considered as rogue, unless otherwise stated in the BYOD policy.

Mitigation techniques:

- Visual inspection of ports and switches
- Network mapping and host discovery - enumeration of devices and OS types
- Wireless monitoring - wireless sniffing for unknown SSIDs
- Packet sniffing and traffic flow
- NAC and intrusion detection - devices without a digital certificate should be stopped from getting on the network

- Scan / sweep

Port scan - shows the status of TCP and UDP ports (tool - nmap)

Fingerprinting - identifies OS type based on the types of responses received

Footprinting - similar to the above but directed at multiple machines, not just one

Sweep - a scan directed at multiple IP addresses. Could be done to check on an entire network to see who has port 80 open, etc.

Authorized network scans should be conducted from a restricted range of hosts.

Indicators of a scan or sweep - discrepancy between SYN and ACK packets. Usually scanning only sends SYN packets and does not require ACK, since it's not a valid handshake.

- Unusual traffic spike

DDoS often causes these spikes. Indicators: HTTP 503 errors or excessive TIME_WAIT connections in a load balancer.

Outbound traffic in excess - compromised hosts that form part of somebody else's botnet.

Slashdot effect - a website crashes due to becoming too popular too quickly

Mitigations to DDoS:

1. Real time log analysis to identify suspicious traffic and to sinkhole it
2. Geolocation and IP reputation - e.g. ignore traffic coming from abroad
3. Close slower connections by reducing timeouts
4. Use caching and backend infrastructure to offload to other servers
5. Commercial providers like Cloudflare or Akamai

- Common protocol over non-standard port

Refresher - Common and known ports:
https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-ports.html

TCP:
https://www.udemy.com/course/comptiacsaplus/learn/lecture/21182030#overview

UDP:
https://www.udemy.com/course/comptiacsaplus/learn/lecture/21182044#overview

Well known ports - 0 to 1023
Registered ports - 1024 to 49151
Dynamic ports - 49152 to 65535 - unknown dynamic ports open for long periods of time can indicate malicious activity, as these ports are meant for short term usage.

IOCs: Using non standard ports for something that already has another port assigned to it.

Mitigation:

1. Configuring firewalls to allow whitelisted ports only.
2. Limiting the ports that are allowed to be used on any given host type.
3. Configuring detection rules to detect mismatched protocol usage over a standard port.

Reverse shell:
https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/

- *Host-related*

- Processor consumption

- Memory consumption

Fileless malware - only exists in system memory. It can be detected through behaviour analysis as opposed to file signatures. Memory dump and examination is also a valid technique of analysis.

Check how much consumption is being used for a single process - potential IOC.

- Drive capacity consumption

Malware uses a staging area on the drive, where data is awaiting exfiltration. Often it might be compressed or encrypted. Malware can also be hidden in alternate data streams.

- Unauthorized software

Not only malware. Legitimate software can be rogue as well - unauthorised downloads of free software or things like Filezilla or Apache, etc. Software includes virtual machines.

- Malicious process

Legitimate processes exhibit abnormal behaviour - a sign they were compromised by malicious code.

Sfc - system file checker (Windows)

Process Monitor and Process Explorer - for live monitoring

Tasklist - cmd line version of Task Manager

Process Identification (PID) - in Linux for identifying a process

systemd(1) - process no.1

- Unauthorized change

Installing software or changing configuration or adding unauthorized hardware (external HDD or USB drive).

- Unauthorized privilege

Privilege escalation - more permissions than a user needs. Getting to root or admin privileges are the usual objectives of attackers.

Can be detected by monitoring users who access resources they should normally not access; failed log-on attempts; newly created accounts; guest accounts; off-hours usage.

- Data exfiltration

HTTP or HTTPS - through an online service like Google Drive or Dropbox

HTTP request to a database - through SQL injection or PHP requests to database

DNS - txt files or MX records - anything other than the standard A record

FTP - file transfers or a P2P service

VPN or SSH - private tunneled connection

Mitigation - encryption of data both at rest and in transit.

- Abnormal OS process behavior

Knowing a baseline is important to see what is normal and what is an anomaly.

- File system change or anomaly

Malware might attempt to change file extensions of files to hide.

- Registry change or anomaly

Part of building persistence includes changes made to the registry.

Registry entries for system's drivers and services are here:

HKLM\SYSTEM\CurrentControlSet\Services

- Unauthorized scheduled task

Scheduled tasks that were scheduled by the attacker - can be viewed in Task Scheduler.

- *Application-related*

- Anomalous activity

Anything out of the ordinary on web apps, databases, DNS services and any other applications. These can include log entries, resource consumption or strange user accounts and activity.

- Unexpected outbound communication
- Unexpected output
- Defacement of service

- Introduction of new accounts

Rogue accounts add to persistence and help maintain access for attackers. There should be defined admin account creation approvals and change management workflows, user creation logs, granted privileges tracking, etc.

- Unexpected output

A golden ticket attack against Active Directory; it allows an attacker to create a Kerberos authentication ticket from a compromised service account, called krbtgt. By using the NTLM hash of the compromised account an attacker can create fraudulent golden tickets. These tickets appear pre-authorized to perform whatever action the attackers want without any real authentication.

- Unexpected outbound communication

Pass the Hash - network based attack method of stealing hashes of user credentials and trying to authenticate to the same network on which they were generated. This enables presenting the hash to network protocols without actually knowing the password. This can be used to elevate privilege.

Pass the Hash attack can be used to harvest cached credentials of users logged in through Single Sign On.

Mimikatz - scans system memory for cached passwords and finds hashes to pass.

- Service interruption

- Have security services been turned off?
- Which process launched the malicious process?
- Is it a DDoS attack?
- Excessive bandwidth usage - this might not be malicious though.

Running services can be checked in Task Manager, Services.msc or *net start*

- Application log

- DNS event logs
- HTTP access logs
- FTP access logs
- SQL event logs

4.4 Given a scenario, utilize basic digital forensics techniques.

- *Network*

- Wireshark

http://www.wireshark.org/

Open source GUI based packet capture software. It can be used for live capture or to capture a file (output in .pcap format).

- tcpdump

Command line packet capture for Linux.

Basic syntax of commands: *tcpdump -i eth*

-n show addresses in numeric format (not host names)
-nn show address and port in numeric format
-e include the data link Ethernet header

- *Endpoint*

- Disk

Places on the disk (removable media) where potential evidence can be located include:

Registry, autorun keys, MFT, event logs, INDX files, change logs, volume shadow copies, user artifacts, Recycle Bin, hibernation files / memory dumps, temporary directories, app logs, removable devices.

Extraction methods:

- Manual - interaction with the UI while recording the process on video.
- Logical - copying the current data or acquiring it from cloud accounts.
- File system - systems must be decrypted first though.
- Call data - mobile phone and text data.

- Memory

Acquired through memory dump tools; useful when examining suspected fileless malware infections.

- *Mobile*

Mobile forensics is conducted using commercial tools like Cellebrite or Encase.

• Cloud

• *Virtualization*

Forensic examination of VM requires suspending them and taking a snapshot.

• *Legal hold*

Refers to holding and preservation of evidence relevant to a court case. It means that certain resources (servers or individual machines) may be removed and taken possession of by LE until the court case is concluded.

• *Procedures*

Identification - secure the scene, prevent evidence contamination, identify the scope.

Collection - forensically obtain evidence based on appropriate authority.

Analysis - forensically copy evidence and analyse it.

Reporting - make a report with findings and conclusions

• *Hashing*

MD5 - old and weak algorithm (128 bit)

SHA - comes in two variants, SHA-1 (160 bit) and SHA-2 (256 or 512 bit).

- Changes to binaries

Hashing can be used to prove file integrity.

• *Carving*

Technique used to extract files from unallocated space; cluster-based (file start near FAT / NTFS cluster boundary), sector-based (de-clustered files), byte-based (file in a file).

When a file is deleted, it's only deleting the reference in the table. The space where the file was stored becomes free. The file is not permanently removed but only de-indexed.

- *Data acquisition*

Based on forensically sound tools and methods of obtaining evidence.

Order of volatility:

1. Short term - CPU registers, cache memory
2. RAM - and anything that vanishes when power is turned off
3. Mass storage - HDD, USB, SSD
4. Remote logging and monitoring data
5. Physical exhibits
6. Archives - backup tapes, DVDs, long term storage

5.0 Compliance and Assessment

5.1 Understand the importance of data privacy and protection.

- *Privacy vs. security*

- *Non-technical controls*

- Classification

- Unclassified (public) — no restrictions on viewing the data.
- Classified (private / internal use only / official use only)—Viewing is restricted to authorized persons within the owner organization or to third parties under a non-disclosure agreement (NDA).

- Confidential (or restricted)—The information is highly sensitive, for viewing only by approved persons within the organization (and possibly by trusted third parties under NDA).

- Secret—The information is too valuable to allow any risk of its capture. Viewing is severely restricted.

- Top-Secret— the highest level of classification.

Data classification is normally subject to a **separate data classification policy**.

- Ownership

- **Data owner** — A senior executive responsible for maintaining the confidentiality, integrity, and availability of the data.

- **Data steward** — responsible for data quality and that data is labeled and identified appropriately, as well as collected and stored in a format and with values that comply with applicable laws and regulations.

- **Data custodian** — responsible for managing the system on which the data assets are stored (typically a system admin). This includes responsibility for enforcing access control, encryption, and backup / recovery measures.

- **Privacy officer** — responsible for oversight of any PII / SPI / PHI assets managed by the company. The privacy officer ensures that the data complies with legal and regulatory frameworks.

- Retention & Retention standards

Files and records that change frequently might need retaining for version control. Short term retention is also important in recovering from security incidents.

Data may need to be stored to meet legal requirements or to follow company policies or industry standards (long term retention).

Backups and archives help meet data retention requirements. A retention policy can either be based on redundancy (the number of copies of each file that should be retained) or on a recovery window (the number of days into the past that should be retained).

The recovery window is determined by the **recovery point objective (RPO)**, which is determined through business continuity planning.

Once the retention period for data has expired, the data must be disposed of through the secure erasure process.

- Data types

- personally identifiable information (PII)
- sensitive personal information (SPI)
- personal health information (PHI) - *[if more than 500 people are affected by a breach, one must notify the US Department of Health]*
- financial information

Microsoft's data loss prevention (DLP) solution defines over 70 sensitive information types.

Further possible types: intellectual property (IP), accounts, fulfilment / operational, and security monitoring data types. Data can also be structured or unstructured.

- Confidentiality

- Legal requirements

EU's General Data Protection Regulation (GDPR) states that personal data cannot be collected, processed, or retained without the individual's informed consent. Data must be collected and processed only for the stated purpose.

GDPR gives data subjects rights to withdraw consent, and to inspect, amend, or erase data held about them.

California Consumer Privacy Act (CCPA)

US federal privacy-related standards or laws other than GDPR and the CCPA:

- SOX—The Sarbanes-Oxley Act (SOX) - requirements for the storage and retention of documents relating to an organization's financial and business operations. It is relevant for **any publicly traded company** with a market value of at least $75 million.

- GLBA—The Gramm-Leach-Bliley Act (GLBA) - protects the privacy of an individual's financial information held by financial institutions and others, such as tax preparation companies.

- **FISMA—The Federal Information Security Management Act (FISMA)** requires federal organizations to adopt information assurance controls. It mandates the documentation of system information, the use of risk assessment, the use of security controls, and the adoption of continuous monitoring.

- COSO—The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides guidance on a variety of governance-related topics including fraud, controls, finance, and ethics.

- **HIPAA—The Health Insurance Portability and Accountability Act (HIPAA)** data relating to healthcare in the United States. Protects the privacy of patient medical information through restricted access to medical records and regulations for sharing medical records.

- Data sovereignty

Data sovereignty refers to a jurisdiction preventing or restricting processing and storage from taking place on systems that do not physically reside within that jurisdiction. E.g. moving offices to another jurisdiction without privacy regulations in order to misuse gathered data violates the data sovereignty principle.

GDPR - Data subjects can consent to allow data transfer but there must be a meaningful option for them to refuse consent. In the US, companies can self-certify that the protections they offer are adequate under the Privacy Shield scheme.

- Data minimization

Data minimization - data should only be processed and stored if that is necessary to perform the purpose for which it is collected. It implies tracking how long a data point has been stored for since it was collected and whether continued retention supports a legitimate processing function.

The minimization principle forbids the use of real data records in a test environment.

The data required for the stated purpose should be collected in a single transaction to which the data subject can give clear consent. Collecting additional data later would not be compliant with this principle.

- Purpose limitation

Data can only be collected for a defined purpose, with explicit consent given. Purpose limitation will restrict the ability to transfer data to third parties. Tracking

consent statements and keeping data usage in compliance with the consent is also required.

- Non-disclosure agreement (NDA)

- **Service level agreement (SLA)** — A contractual agreement setting out the detailed terms under which a service is provided.

- **Interconnection security agreement (ISA)** — Any federal agency interconnecting its IT system to a third party must create an ISA to govern the relationship.

- **Non-disclosure agreement (NDA)** — Legal basis for protecting information assets.

- **Data sharing and use agreement** — they specify terms for the way a dataset can be analyzed and shared. Also define the use of reidentification techniques to protect anonymized data.

• *Technical controls*

- Encryption

Data at Rest - the data is in persistent storage media (financial information stored in databases, etc.) It is usually possible to encrypt the data, using techniques such as whole disk encryption, database encryption, and file- or folder-level encryption.

Data in Transit (or Data in Motion) - data is transmitted over a network - website traffic, remote access traffic, sync between cloud repositories, etc. Data can be protected by a transport encryption protocol, such as TLS or IPsec.

Data in Use - non-persistent data is present in volatile memory, such as system RAM or CPU registers and cache. Examples: documents open in a word processor, database data that is currently being modified, event logs, etc. When a user works with data, that data usually needs to be decrypted and may stay decrypted for an entire work session, which puts it at risk.

- Data loss prevention (DLP)

Data loss prevention (DLP) - data is not viewed or transferred without a proper authorization.

- Policy server— configure classification, confidentiality, and privacy rules and policies, log incidents, and compile reports

- Endpoint agents— enforce policy on client computers, even when they are not connected to the network.

- Network agents— scan communications at network borders and interface with web and messaging servers to enforce policy.

The transfer of content to removable media or by email, instant messaging, or social media can be blocked if it does not conform to a predefined policy.

An exact data match (EDM) is a pattern matching technique that uses a structured database of string values to detect matches.

- Data masking

Data masking - the contents of a field are redacted, by substituting all character strings with "x" for example. For example, in a telephone number, the dialing prefix might be retained, but the subscriber number redacted.

- De-identification

Personal or financial data is collected to perform a transaction but does not need to be retained thereafter. Example: a company uses a customer's credit card number to take payment for an order. When storing the order details, it only keeps the final 4 digits of the card as part of the transaction log, rather than the full card number.

- Tokenization

Tokenization - all or parts of data in a field is replaced with a randomly generated token. An authorized query or app can retrieve the original value from the vault, if necessary, so tokenization is a reversible technique. Tokenization is used as a substitute for encryption.

- Digital rights management (DRM) & Watermarking

Prevents distributing unauthorized copies of content. There are both hardware and software approaches to DRM:

- Authorized players—Content can be locked to a particular type of device, such as a games console or a TV from an authorized vendor. The device will use a cryptographic key to identify itself as an authenticated playback device.

- Authorized viewers—A DRM file can also be locked to a particular type of software running on a general computing host, such as a customized PDF viewer or video player that prevent copying by other applications running on the same device.

Watermark could be a visible mark using an identifying feature of the customer, or it could be a digital / forensic watermark, encoded in the file.

- Geographic access requirements

Data centers for processing and storage must ensure that information is not illegally transferred from a particular privacy jurisdiction without consent.

Cloud-based file and database services can apply constraint-based access controls to validate the user's geographic location before authorizing access. This is in the case of remote employees logging in from other jurisdictions.

- Access controls

The ACL - access control list of accounts allowed to access the resource with defined permissions. Each record in the ACL is called an access control entry (ACE).

File permissions

Windows - ***icacls*** - command line utility for displaying and modifying permissions

Linux - ***chmod*** - modifies permissions for files; ***chown*** - modifies ownership of files

5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- *Business impact analysis*

  - ❏ **MTD** - Maximum Tolerable Downtime - the point after which the impact of an incident becomes unacceptable.
  - ❏ Mission critical assets and resources
  - ❏ Backups and backups of backups must be planned accordingly
  - ❏ **RTO** - Recovery Time Objective - how fast does a backup kick in
  - ❏ **WRT** - Work Recovery Time - restoration of systems
  - ❏ **RPO** - Recovery Point Objective - tolerance of temporary data loss, time between the last backup and the restoration - how much data was lost

• *Risk identification process*

Enterprise Risk Management (ERM) - the process of evaluating, measuring and mitigating risk. There are multiple reasons for having an ERM, from avoiding financial loss, legal liability, to maintaining a positive public image and satisfying the stakeholders' requirements.

NIST identifies 4 components of the ERM process:

1. Frame - overall goal for the degree of risk that can be tolerated.
2. Assess - identify risk to which systems and processes are exposed.
3. Respond - mitigate each risk, deploy controls.
4. Monitor - examine the situation on an ongoing basis.

• *Risk calculation*

Probability - the chance of a threat being realized - how likely, percentage-wise?
Magnitude - the impact of a successful exploit or a risk event materialising.

Probability * Magnitude = Risk

1. Quantitative Risk Calculation - specific values to the elements of risk.

AV (Asset Value) x EF (Exposure Factor) = SLE (Single Loss Expectancy)

SLE (Single Loss Expectancy) x ARO (Annual Rate of Occurrence) = ALE (Annual Loss Expectancy)

2. Qualitative Risk Calculation - scenario based, people's opinions on risk. For example impact measurements: low, medium, high, etc.

3. Semi-Quantitative Risk Calculation - mixed approach to measure intangible stuff - how much is staff morale or good PR worth?

• *Communication of risk factors*

Risk register - a document showing risk assessment results for the stakeholders to understand the risks. States things like the impact and likelihood, description of risk, controls, risk owners, etc.

• *Risk prioritization*

- Risk mitigation - overall process of reducing risk.Depends on what the risk appetite is. Involves adding controls.
- Risk deterrence / reduction - making the risk events less likely and less impactful or costly.
- Risk avoidance - avoiding the risk completely, for instance by withdrawing a product from the market. Involves changing plans.
- Risk transference - offloading risk to a third party. See car insurance example - there are equivalent insurance policies against hacks, incidents, etc.
- Risk acceptance / retention - some risks are unavoidable and should be monitored, but cannot be mitigated against. Involves low and unlikely risks.

- Security controls

Return on security investment (ROSI) - a percentage value determined by calculating a new annual loss expectancy (ALE), based on the reduction in loss that will be created by the security control introduced.

- Engineering Tradeoffs

When a risk mitigation solution has its own risks / costs. This is based on risk appetite - risk vs convenience.

• *Systems assessment*

- Business continuity
- Legal liabilities
- Reputational aspect

Includes conducting a full inventory check on all assets, people, intangible assets (reputation, etc.), procedures and policies.

• *Documented compensating controls*

Compensating controls - something put in place of the controls recommended by the standards, due to some important business reason or use case. For example, for devices or systems that don’t support a 16 character password - use the 8 character but apply 2FA, etc.

Exception Management - for documenting the deviations from the standard. Its goal is to document what is impacted and how. Often used for older systems that cannot comply with current standards.

- *Training and exercises*

- Red team

Red team simulates the attacker and attempts to penetrate the network.

- Blue team

The defender team; aims to detect and prevent the actions of the red team.

- White team

White team sets the parameters for the exercise and controls its flow. They act as judges when determining failure / success of both red and blue teams. They are responsible for the 'lessons learned' report and recommendations.

- Tabletop exercise

This is a facilitator led training event, theoretical, set in reality but based on discussions and scenarios illustrating various aspects of responding to emergencies. No practical info though - like how long really things take, etc.

Penetration test - active tools are used to simulate an attack on a system. Aimed to discover vulnerabilities and weaknesses, but also to test if controls work. Pentest must be properly scoped and resourced, with specific areas of concern and targets clearly identified.

Main criteria for a pentest: Scope, Timing and Authorization.

- *Supply chain assessment*

- Vendor due diligence

Efforts directed at evaluating risks involved in partnership with potential vendors. Verify things like due diligence on suppliers and contractors, product support lifecycle (will the vendor still be around to help).

Trusted Foundry - microprocessor manufacturing utility - US military (Department of Defense)

- Hardware source authenticity

Hardware is procured tamper-free, from reputable suppliers. Purchasing from second hand or aftermarket sources creates a risk of buying counterfeit or compromised devices.

ROT - Root of Trust - cryptographic module embedded in a computer system, endorses trusted execution and attests to boot settings. TPM is a Root of Trust - TPM has hardware based storage of digital certificates, keys, hashed passwords and other identification information. TPM is used with full disk encryption.

HSM - Hardware Security Module - appliance for generating and storing cryptographic keys, more secure than a software based solution.

UEFI - Unified Extensible Firmware Interface (replacement for BIOS) - system firmware providing support for 64-bit CPUs at boot, GUI and boot security. Has **secure boot**, prevents unwanted processes from executing during boot and it protects against hijacking the computer by a malicious OS.

Attestation - data presented in the report is valid by digitally signing it using the TPM's private key.

eFUSE - electronic fuse that "blows" when tampered with.

A field programmable gate array (**FPGA**) is an anti-tamper mechanism that makes use of a type of programmable controller and a physically unclonable function (PUF).

5.3 Explain the importance of frameworks, policies, procedures, and controls.

- *Frameworks*

❏ ITIL
❏ COBIT
❏ TOGAF
❏ ISO 20000

- Risk-based

They use risk assessment to prioritize security controls. If regulatory compliance is not a priority, mandatory solutions are best replaced with something relevant to the organisation's risk appetite.

NIST Cybersecurity Framework

- Core: Identify, Protect, Detect, Respond, Recover
- Tiers - from least to most mature:
    - Partial, Risk Informed, Repeatable, Adaptive
- Profiles: capturing a baseline in terms of the above framework and where we want to be as an organisation.

- Prescriptive

They stipulate control selection and deployment - they are mandatory.

Maturity model - for assessing formality, optimization and usage to address any gaps. New companies are usually reactive in their posture. Maturity means more of a proactive approach - policies get defined, quantitative management, risk registers appear and so on. Optimizing is at the top of this maturity structure.

• *Policies and procedures*

- Code of conduct / ethics - behaviour of end users, employees in specific roles. Formalised work ethics.

- Acceptable use policy (AUP) - all users on the network and how they use company equipment and resources. What activity is allowed and not allowed, etc.

- Password policy - complexity rules, timelines of when passwords must be changed (but nowadays not enforced), not allowing password reuse, challenge questions, 2FA, password manager use.

- Data ownership

- Data retention

After the determined period of time for data retention expires, removing data from hard drives should take place in the following way:

- purging the drives
- validating that the purge was effective
- documenting the sanitization

- Account management

Account lifecycle (provision =>; active use =>; decommission)

Identity and access management IAM - how users and devices are granted access to company resources.

Account types:

- Personnel - for individual employees
- Endpoint - approved devices that can connect to the network, identified by digital certificates
- Server - usually mission critical systems that provide resources
- Software - applications, uniquely identified. Specific apps that are allowed
- Roles - permission and privilege based classification

- Continuous monitoring

- Work product retention

- *Control types*

- Managerial: security assessment, planning, risk identification, evaluation of controls

- Operational: practices and procedures that follow security requirements. E.g - separation of duties - having more than one person required to complete a task.

- Technical: systems/devices/software/settings etc. that enforce CIA requirements

- Preventative: proactive measures to prevent incidents, e.g. firewalls, training

- Detective: detects and captures information on incidents, e.g. alarms, notifications

- Responsive: responds to breach and restores initial behaviours of systems, e.g. backups

- Corrective: remediates incident or limits damage, e.g. patching, antimalware

- *Audits and assessments*

Quality Control (actions during building something) and Quality Assurance (checking for the desired level of quality).

- Verification - is the program correctly written?
- Validation - is the system fit for purpose? Does it meet the use case needs?
- Assessment - checking something against a list of requirements and an absolute standard. See a checklist.
- Evaluation - judgement and comparative measures.
- Audit - comparing an organisation against a regulated baseline and known standards.

- Regulatory

PCI DSS (internal & external vulnerability scanning by professional or ASV - approved scanning vendor).

- Compliance

HIPAA, GLBA, SOX, FERPA, FISMA, data breach notification laws.