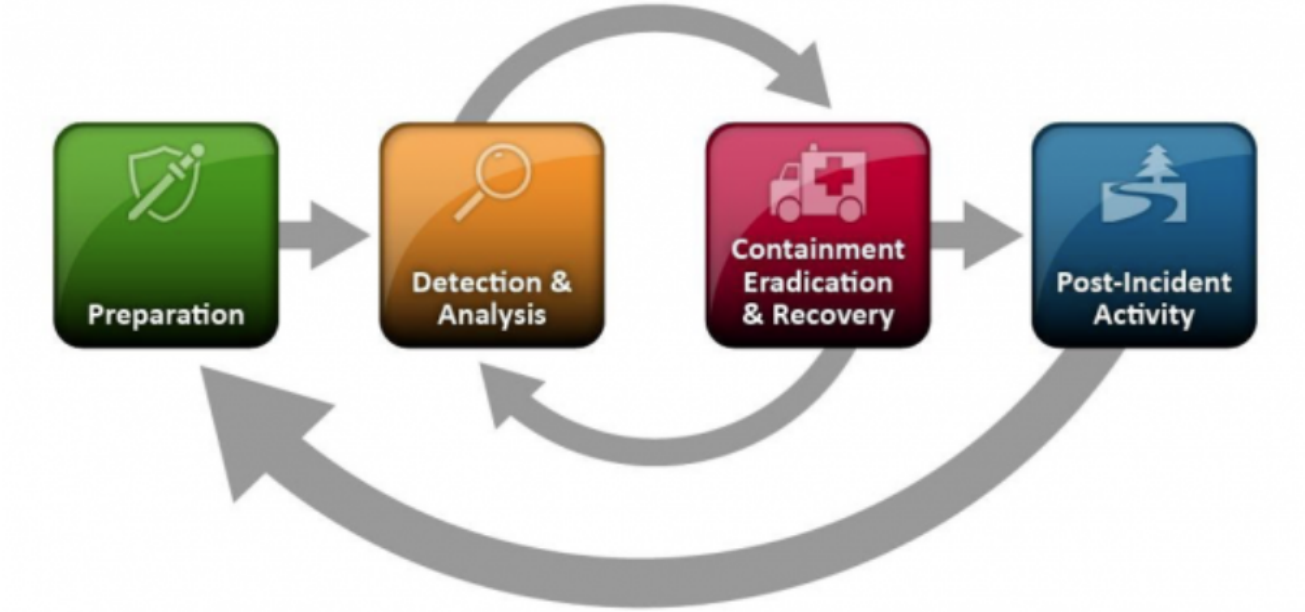
Incident Response

“Incident response is the methodology an organization uses to respond to and manage a cyber attack.“

- A Security event is anything that could have a security implication, such as causing damage or disruption.
- Security incidents are security events that have resulted in damage to the organization.

Incident Response Lifecycle

- Many organizations have procedures for handling computer-security incidents, and this is known as having an Incident Response Plan (IRP).
- Many of these plans are based on the NIST SP 800 61r2 guidelines.



Preparation

- While there is no perfect preparation phase of the incident response process, it is the first line of defense of an attack that could have catastrophic damage.
- Having an incident response plan (IRP) can make all the difference when responding to a security incident.
- Having a well-documented plan for IT and security staff can ensure that the response process is clear and defined, preventing confusion which costs the organization valuable time.
- Incident response plans need to be constantly updated and training should be maintained constantly to ensure all employees that could be involved with incident response are capable of performing their duties.

We can split this section into three main phases:

- Developing response plans for different incident types and running simulated scenarios to evaluate how the incident response team responds, training them for the real thing.
- Ensure that all resources needed by the incident response team are approved and ready to use, such as: laptops, notebooks, software tools, forensic equipment, training, and the ability to abandon normal responsibilities when an incident occurs.
- Continually train and evaluate the performance of incident response team members to ensure they are capable of completing their duties defined in the response plans.

Asset inventory and Risk Assessments

- If we want to protect systems, we need to know what assets our organization actually has, so keeping an up-to-date asset inventory can help to monitor production systems, test environments, and other devices that fall under our protection.
- The purpose of this practice is to store key information associated with a device, such as a system owner, the operating system version, the software installed, what IP address it's using (if it is assigned a static IP address), and more. -> This allows IT teams to manage assets, track what systems need to be updated, and assist with technical support.
- Using risk assessment, we can identify systems that are of high value to the business, and therefore require more protection than others. -> if two incidents occur at the same time, prioritization needs to be clear so that time and resources are focused in the right place
- If a security function is unsure of risk to different systems and assets, a good place to start is by looking at the Business Impact Plan and Business Continuity Plan, both of which should clearly outline the critical systems for business operations.

There are four approaches to risk:

- Transfer the risk (such as purchasing insurance)
- Accept the risk (a decision that is made to not spend any resources as the impact would be low and the cost too high)
- Mitigate the risk (apply security and other controls to protect the asset and reduce the risk)
- Avoid the risk (an asset that is at too high a risk may simply be taken offline so it can’t be exploited)

Prevention

DMZ

- In computer networks, a DMZ (demilitarized zone) is a physical or logical subnet that separates an internet local area network (aka LAN) from other untrusted networks (usually the internet).
- External-facing servers, resources, and services that are located in the DMZ are directly accessible from the internet, however, this layer will keep the internal LAN unreachable, providing an additional layer of security to the LAN as it restricts a hacker’s ability to directly access internal server and data via the internet.
- Protect sensitive organizational systems and resources.
- Isolate and keep potential target systems separate from internal networks.

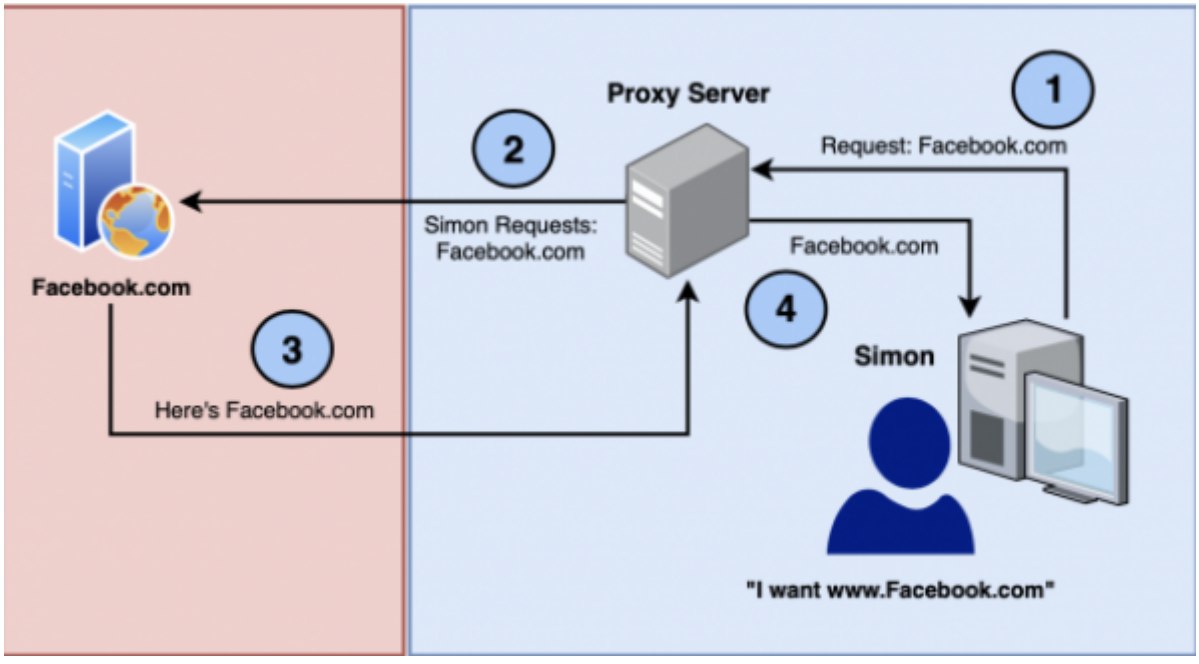
- Reduce and control access to those systems outside the organization.

Host Defenses

- Host Intrusion Detection and Prevention -> installed on an endpoint that allows for the detection of suspicious or malicious activity using rules which are checked against activity to see if it matches any known malicious patterns.
- Anti-Virus Software -> This is a fundamental security control that works to detect and remove known malware that is present on the system.
- Centralized Logging -> Endpoints can be configured to send logs to a centralized location, a SIEM platform, where this data is aggregated, normalized, and matched against a number of rules designed to detect and flag suspicious or unusual activity so it can be investigated by security analysts.
- Endpoint Detection & Response -> These solutions will typically allow analysts to conduct investigations straight from the platform and see exactly what processes are running on monitored systems, and conduct in-depth investigations to analyze the suspicious activity.
- Local Firewall -> The software will allow administrators to decide what ports should be open, and allow or deny connections coming in or going out of the system.
- Windows Group Policies

Network Defenses

- Network Intrusion Detection and Prevention
- Firewalls -> Firewalls are used to separate parts of a network to create private zones by restricting the traffic that can come in or go out.
- Event Monitoring
- Web Proxy -> Requests for internet resources are sent from the requesting client to the web proxy, then sent on behalf of the proxy to the destination, the request is fulfilled and the resource is sent back to the proxy, where it sends it to the requesting client.



Email Defenses

- SPF, DKIM, DMARC
- Marking External Emails
- Spam Filter
- Sandboxing -> emails that include file attachments are extracted and analyzed, and files are detonated (run) in a virtual environment, where everything is monitored to see actually what happens when a file is executed.
- Data Loss Prevention
- Security Awareness Training

Human Defenses

- Security Awareness Training
- Security Policies
- Incentives
- Phishing Simulations
- Whistleblowing

Detection and Analysis

- For the detection sub-phase, many SOCs, internal security teams, and organizations have tools such as intrusion detection and prevention systems (IDPs), antivirus/antispam/antimalware software, and log monitoring solutions set up to alert the appropriate team when incidents are detected.
- Analysis can often be one of the most complex steps in the IR lifecycle because it involves finding how the initial attack took place and how it moves throughout the network. Many organizations utilize network profiles and baselines, knowledge bases, and policies for log retention, in order to make this phase easier for the incident responder.
- Baselining refers to the recording and profiling of what is considered to be “normal” on a system or in a network.
- This baseline can be consistently compared to the current state of the network to identify any anomalies which could potentially suggest a security or performance issue -> anomaly-based detection.

DeepBlueCLI
DeepBlueCLI is a PowerShell script that was created by SANS to aid with the investigation and triage of Windows Event logs. This tool can be provided with exported .evtx log files, or can be run on a live system to analyze the local log files.

CMD commands
ipconfig /all

tasklist
This command will check running processes and programs and print a list to the terminal.
wmic process get description, executablepath
This command will display running processes and the associated binary file that was executed to create the process.
net user
This command will print a list of all system users to the terminal.
net localgroup administrators
This command will list all users that are in the administrators user group.
sc query | more
This command will list all services and detailed information about each one.
netstat -ab
This command will list open ports on a system, which could show the presence of a backdoor.

PowerShell Commands
Get-NetIPConfiguration and Get-NetIPAddress
Similar to ifconfig in CMD, we can use the two above commands to get network-related information from the system.
Get-LocalUser
Using the above command we can list all local users on the system.
Get-LocalUser -Name BTLO | select
We can provide a specific user to the command to only get information about them.
Get-Service | Where Status -eq "Running" | Out-GridView
The above command let's us quickly identify running services on the system.
Get-Process | Format-Table -View priority
Another great command is the ability to group running processes by their priority value.
Get-Process -Id 'idhere' | Select
We can collect specific information from a service by including the name in the command (-Name 'namehere') or the Id.
Get-ScheduledTask
Similar to Services, Scheduled Tasks are often abused and utilized a common persistence technique. With the above command we can list tasks that are set to run after certain conditions are met.
Get-ScheduledTask -TaskName 'PutANameHere' | Select
We can dig deeper by specifying the task we're interested in, and retrieving all properties for it.

Containment, Eradication, Recovery

Incident Containment
The first sub-phase is containment

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability

- Time and resources needed
- Effectiveness
- Duration of the solution
  Depending on the type of incident, there are several responses we can take to contain the incident, preventing it from spreading to additional systems and potentially causing more damage.

Perimeter Containment

- Block inbound traffic and outbound traffic.
- IDS/IPS Filters to identify further malicious traffic and take automated actions, such as blocking active connections.
- Web Application Firewall policies, to detect and take action against web attacks.
- Null route DNS, to prevent DNS resolutions so internal hosts cannot find the IP address of a given domain name and establish a connection

Network Containment

- Switch-based VLAN isolation, to restrict network access.
- Router-based segment isolation, to restrict network access.
- Port blocking, to prevent connections on specific ports.
- IP or MAC Address blocking, to restrict network access.
- Access Control Lists (ACLs), to provide rules that restrict what hosts on the network can and cannot do.

Endpoint Containment

- Disconnecting the infected system from any network connections (turning WiFi off, pulling ethernet cable).
- Powering off the infected system.
- Blocking rules in the local firewall.
- Host intrusion prevention system (HIPS) actions, such as device isolation.

The second sub-phase is eradication & recovery

- this phase is the act of returning your systems back to normal.
- Actions for eradication could consist of rebuilding machines from known good backups, deleting a malware, or resetting credentials on compromised accounts.
- Actions for recovery consist of restoring those systems to their pre-attack state. -> This could also include eliminating any vulnerabilities that were exploited in the attack, as well as changing passwords, installing patches, tightening network security, etc.
- Identify the root cause

Lessons Learned

- Exactly what happened and when did it happen?
- Who performed well?
- Were any new tools or processes used that provided benefit?
- Review the metrics that have been collected from the incident.
- Review the communication between different company departments.
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can be taken?
- What indicators should be watched for in the future?
- What additional tools or resources are needed to mitigate future incidents?

This is the perfect time to discuss with management the need for resources to strengthen the response to future incidents:

- More budget for security personnel such as Forensic Analysts, Incident Responders, Incident Commanders, etc.
- More budget for personnel in other departments, such as Legal, Public Relations, Communications, or Human Resources.
- More budget for tools that can assist with incident response activities.
- Review of documentation such as run-books, policies, and procedures.

Metrics are numerical values used for quantitative assessment, allowing us to assess, compare, and track performance. Regarding incident response, it can highlight areas where the team has responded efficiently or ineffectively. These metrics can also help to identify trends in incidents that the organization is facing so they can be addressed, using metrics to support a business case to receive more budget or personnel.

Impact Metrics

- Service Level Agreement (SLA)
- Service Level Objective (SLO)
- Escalation Rate

Time-Based Metrics

- Mean Time to Detect (MTTD)
- Mean Time to Response (MTTR)
- Incidents Over Time

- Remediation Time

Incident Type Metrics
Cumulative Number of Incidents Per Types
Alerts Created per Incident
Cost per Incident (CPI)

Reporting Format:

- Executive Summary
- Incident Timeline
- Incident Investigation
- Appendix

MITRE ATT&CK Framework

The MITRE ATT&CK™ framework is a comprehensive collection of tactics and techniques used by adversaries, which can be utilized by both blue and red team members to improve the security posture of an organization.

Initial Access

hese techniques are used to describe ways that adversaries could get their first foothold in a network

Execution

These techniques are used to describe ways that adversaries will execute malicious code for a number of purposes.

Persistence

Once an adversary has access to a system they need to attempt to maintain their foothold by hiding from the defenders and utilising multiple methods to regain access to the compromised host.

Privilege Escalation

These techniques are used to describe ways that adversaries will attempt to gain higher privileges, such as moving from a standard user to an administrator, or from an admin to a domain admin.

Defense Evasion

These techniques are used to describe ways that adversaries will work to evade or disable security defenses such as antivirus, endpoint detection and response, logging, and human analysts to ensure they can remain in the network for as long as possible.

Credential Access

These techniques are used to describe ways that adversaries will work to steal credentials such as passwords and usernames from compromised systems using methods such as credential dumping (retrieving credentials that are stored in memory while the system is powered on) or deploying a key logger to monitor what keyboard buttons are pressed.

Discovery

These techniques are used to describe ways that adversaries will collect more information about the network they're in and other systems that are present.

Lateral Movement

An adversary commonly has to exploit multiple machines within a network to reach their primary objective, the movement between these hosts is called 'Lateral movement'.

Collection

These techniques are used to describe ways that adversaries will identify important files or information, collect them, and prepare them for data exfiltration.

Command and Control

Command and Control consist of techniques and methods adversaries use to communicate with systems they have compromised on the targets networks.

Exfiltration

The Exfiltration phase consists of techniques used to steal data from the compromised network and systems, and ways of avoiding detection when completing this. This can include the compression, encryption or encoding of files when removing them from the network and typically involves transferring it over a command-and-control communication channel.

Impact

These techniques are used to describe the actions that adversaries may use to disrupt availability or compromise integrity by manipulating business and operational processes, such as tampering or destroying data.

ATT&CK Navigator

For Threat Hunting

Threat Hunting is the process of identifying threat actors that have already made it past the perimeter and are now operating inside an environment undetected.

For Adversary Emulation

Adversary Emulation is different from a standard penetration test and requires a lot more time and knowledge. Why? because the aim is to accurately imitate advanced threat actors attacking the organization by copying all of their known tactics and techniques. Organizations with mature security

teams would likely conduct these events, and have the red or purple team members imitate the techniques of threat actors that are likely to target the organization based on previous attacks, motives, and industries the actor's target.

For Threat Detection

Threat Detection is all about ensuring that the monitoring and detection capabilities of the defenders are as accurate as they can be. From tuning false positives to writing new rulesets, security teams are constantly adapting the way they detect malicious actors from a mountain of data.