I.R

OPERATION CHIMERA

INCIDENT RESPONSE // SECURITY BLUE TEAM

CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.

Useful Links:

[1]
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Anything we've missed? Please let us know, so we can add it in here, and create a useful resource for security professionals worldwide!

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

https://paypal.me/KDMentoring

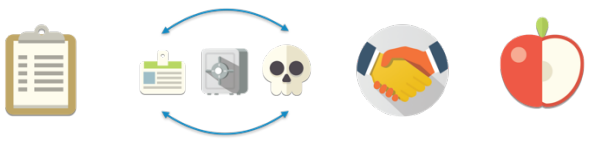
OPERATION CHIMERA - INCIDENT RESPONSE

This module is designed to give a look into the world of Incident Response. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "Incident Response" channel within the "Operation Chimera" category in the SBT Discord server.

WHAT IS INCIDENT RESPONSE?

Incident Response is the pro-active approach to cyber defense, as well as the procedures and actions that are used when a security incident has occurred, and an elevated response is taken to address it. The following stages of Incident Response Triage are based on the industry framework, NIST SP 800-61r2:

- **Preparation –** This stage is about ensuring effective cyber defences are in place, and an Incident Response capability has been established within the organisation.
- **Detection and Analysis –** Ensuring that monitoring solutions are in place and can help to identify potential incidents as they happen. This includes maintaining Firewalls, IDPS, SIEM, and EDR. Analysis is comparing standard behavior to reported behavior, to ensure that discovered activity isn't a false positive.
- **Containment, Eradication, Recovery–** Knowing how to contain an infection or incident appropriately is very important to limit the damage. Evidence and IOCs must be collected carefully to ensure it complies with all applicable laws and regulations. Eradication and Recovery is the process of removing malicious presence to prevent further damage. Recovery is the process of remediating systems and fixing any damage caused.
- **Lessons Learned –** This is the most important part of IR. Learning from the organization's mistakes is the best way to improve and better defend against cyber-attacks and incidents in the future.



I.R

OPERATION CHIMERA

INCIDENT RESPONSE MODULE // SECURITY BLUE TEAM

Image 1 Source:
https://blog.trendmicro.com/pdating-incident-response-for-the-cloud/

Image 2, 3, 4, 5 Source:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

WHY IS IT USEFUL?

Vulnerabilities are announced constantly, and most of them affect software that is used on a mass scale. Examples include security flaws in Google Chrome, Windows operating system, and other programs such as Adobe Flash Player, and Adobe Shockwave Player. Being able to keep on top of these issues, and make sure products are patched as soon as possible (usually after testing, to ensure there's no unwanted effects from the patch), means that hackers have less time to attempt exploitation. By ensuring internet-facing systems are secure, it's harder for attackers to get in, and by ensuring internal systems are secure, it's harder for attackers to move around, and complete the actions they want to.

ASSOCIATED ROLES

The below roles generally contain work that includes aspects of Vulnerability Management:

- **Tier One Security Analyst (Junior)**
  Tier 1 Analysts are responsible for first response to security alerts. They will collect information on the events observed and escalate it up to Tier 2.
- **Tier Two Security Analyst**
  Tier 2 Analysts will provide more critical analysis and use advanced toolsets to investigate the escalated events. If more expert knowledge is required, it will be escalated to Tier 3.
- **Tier Three Security Analyst (Senior)**
  Identifying, reporting on, and helping to remediate vulnerable assets to harden the estate and reduce risk from cyber-attacks.
- **Vulnerability Analyst**
  Understanding how vulnerability exploitation works, Vulnerability Analysts can aid incident response by explaining technical concepts, and replicate attacks to test possible post-actions.
- **Incident Responder (Computer Security Incident Response Team)**
  Incident Responders are responsible for the continuous development of an organizations Incident Response plan and provide emergency support in case of a security incident.

PREPARATION

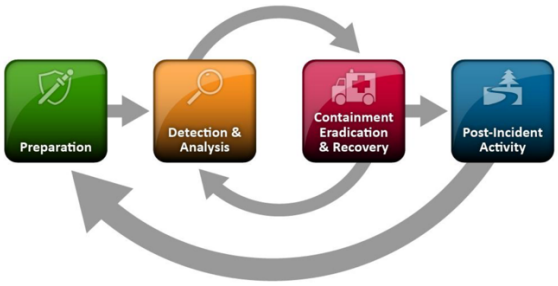


Figure 1: Full Incident Response Lifecycle

Incident Responders need to have the skills, knowledge, and tools to be able to respond to security incidents. This discipline doesn't focus on response, it also includes the continuous development of security defences and countermeasures in order to prevent incidents and breaches from occurring.

Preventing Incidents:

In order to not overwhelm the Incident Response team, security incidents need to be kept to a minimal. This can be achieved by having good security hygiene and keeping up to date with the latest in security developments regarding defences and monitoring solutions. These provide the organisation with automated security, and increased visibility for human analysts to aid post-incident actions.

- Endpoint Security
  This includes products such as anti-virus and malware prevention that work at the host level (computers, servers), on application servers (email gateway, web proxy), and application client level (email clients). Hosts should also have Endpoint Detection and Response (EDR) agents, which can allow for remote control, network isolation, and file download. Systems should be updated with the latest stable updates and security patches, and push log activity such as syslog, to the SIEM collectors, where it is aggregated and correlated into security events.

- Network Security
  Only expected traffic should be allowed inbound and outbound. Physical, Web App, and Host-level firewalls can help control these connections. VPNs also need to be secured to prevent unauthorized access.

- Human Factors
  Staff need to undertake security training, helping to limit chance of an incident. Principle of least privilege should be applied to all users, so that appropriate permissions are placed on accounts, limited the post-actions that can be completed by attackers. Lessons learned from previous incidents should be incorporated into training, to help prevent them from happening again.

Responding to Incidents:

Responding to an incident quickly and efficiently limits the time that attackers have to complete post-actions, such as data exfiltration, system damage, or information harvesting. This half of IR is all about the people, tools, and procedures used in the event of an incident.

- Receiving notification of an incident
  A potential incident could be passed along to the security team from a system owner, a member of the Network Operations Centre, or another employee. It should be easy for people to report an incident, so methods like a form on the intranet, or emergency phone numbers should be used. Minimizing the time from discovery to notification will help security responders get better control of the situation. An incident could also be alerted to human analysts via a SIEM platform. Once information is received, it is important to verify that it is in fact a real incident, and not a false positive. Once confirmed, depending on the severity, the Computer Security Incident Response Team (CSIRT) is activated.

- Assembling key stakeholders
  At this stage, it is crucial that the IR team have a list of key stakeholders, which departments they belong to, and contact information (most importantly phone numbers, which allow for faster contact than emails). People that are likely to be included in this list (for a large corporate company) include Managers and Directors of key departments such as Networks (Operational & Corporate), Endpoints (Servers, Computers), and Infrastructure. Other stakeholders could include the Chief Information Security Officer (CISO), Chief Operations Officer (COO), and all of the security team. Some companies pay for 'retainer incident response teams', which are specialist groups of blue-teamers that act as *teams for hire* when an incident occurs. An example is the Mandiant Response Team, which will come and assist your security team during an incident, providing analysis and suggestions.

- Investigating the incident and affected systems
  The security team should've begun their investigation as soon as the incident was confirmed to be legitimate. This requires tools such as packet sniffers and protocol analyzers (Wireshark is an example), digital forensic workstations for taking and analyzing disk images, dummy systems to be used to detonate malware and/or replicate activity that resulted in the incident, secure storage for preserving log files, backups, evidence collected, laptops for writing reports and storing evidence during the response, and lots more. This allows analysts to figure out what happened, how it happened, and collect evidence to aid with improving defences and potential prosecution.

DETECTION AND ANALYSIS

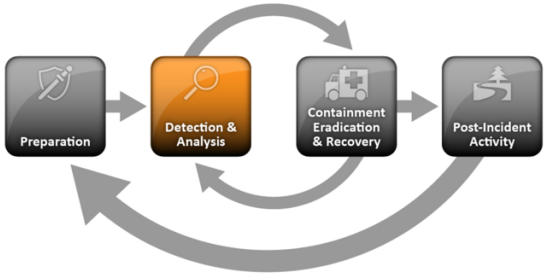


Figure 2: Detection & Analysis Stage

Detection – 1) Attack Vectors

It's important to be able to categorize the type of attack that has occurred, so we know how to respond to it. We can do this by using the following the NIST SP 800-61r2 attack vectors (copy-pasted definitions to keep full detail [1]):

External/Removable Media:	An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
Attrition:	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
Web:	An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a

	site that exploits a browser vulnerability and installs malware.
Email:	An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
Impersonation:	An attack involving replacement of something benign with something malicious— for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage:	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment:	The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
Other:	An attack that does not fit into any of the other categories.

Detection – 2) Signs of an Incident

It can be very hard for an organization to detect an incident, depending on the activity, and how much activity is actually being conducted. Events such as an attacker trying to brute-force a login page on a website would be loud and easy to spot, however stealthy attacks may be almost impossible to identify. For proper analysis, the security team needs to include specialized intrusion detection analysts that have the knowledge to analyze incident-related data. Another issue is that IDPS and other security tools can generate false positives, and false negatives (where an alert should've occurred, but didn't). Combine that with the fact that the potential signs of an incident can be high, as medium-large businesses will likely receive a large volume of security alerts and looking at each one properly takes time.

Precursors – This is a sign that an incident may occur in the future. An example would be a web server that has evidence of someone scanning it with a vulnerability scanner. Now that an attacker has these results, they may attack it in the future. Another example would be a hacking group talking on underground forums about attacking the organisation.

Indicators – This is a sign that an incident may have occurred, or may be occurring now. Antivirus software alerting that a host has been infected with malware, or a system owner finding a text file on a server that contains an unexpected script.

Detection – 3) Sources of Precursors and Indicators

Precursors and Indicators of Compromise (IOCs) can be used to help identify malicious activity. These can be retrieved from vendor and government security alerts, threat intelligence platforms, intelligence exchanges, information sharing associations, and even other organizations.

Intrusion Detection and Protection Systems – Most IDPS systems use signatures to identify suspicious or malicious activity. Once activity is detected, the system will record information such as the time, type of attack, source and destination, and any other information that is available, before generating an alert for analysts to investigate. IDPS software is known to generate false positives, which is when activity generates alerts when it shouldn't.

Security Information and Event Monitoring – SIEM solutions are similar to IDPS, however these products generate alerts based on the analysis of aggregated log data.
Antivirus and Antispam Software – Antivirus uses signatures to detect and remove known malware from protected systems. Antispam works the same way, but is usually used on an email gateway, dropping emails that are known to be spam or malicious, so they are not successfully delivered to employees.

Analysis – 1) Analyzing an Incident

We can't trust every alert, whether this is generated from an IDPS or SIEM, or a user reporting some suspicious behavior. Software can generate false positives, and humans can misunderstand something. A server crashing could be the result of malware, but it could also just be an issue with the system itself, and is not malicious in any way. The Incident Response team should analyze and confirm or deny each potential incident, as doing so prevents any from being missed out, which could have damaging consequences. Below are a few NIST recommended techniques for making analysis easier:

- **Profiling, Baselines, and Expected Behavior.** This is the practice of determining a baseline standard, which is essentially what the organization classes *'normal'* activity. This way unexpected behavior can easily be spotted, as it differs from the baseline.
- **Event Correlation.** Different security tools may have recorded different pieces of information. It's important to bring them all together to give a complete picture of an attack.
- **Using Packet Sniffers to Collect Additional Data.** If an attack is happening, using a packet sniffer to collect network traffic could help analysts to determine the exact activity that is happening, and then respond to it appropriately.

Analysis – 2) Prioritization

If multiple incidents occur at the same time, it is crucial to prioritize them properly and assign appropriate resources to each response. Doing them on a first-come first-serve basis could mean the security team is dealing with a low-impact incident, whilst a damaging malware attack is spreading through the networks. The three main factors used to decide prioritization included in NIST SP 800-61r2 are:

Table 3-2. Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Table 3-3. Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table 3-4. Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Analysis – 3) Notification

These are the stakeholders that may be contacted during an incident, depending on the severity.

- Chief Information Security Officer
- Networking/Infrastructure teams
- Human Resources department
- Public Affairs department
- Legal department
- External incident response teams (retainers)
- US-CERT / UK-CERT
- Law enforcement

CONTAINMENT, ERADICATION, RECOVERY

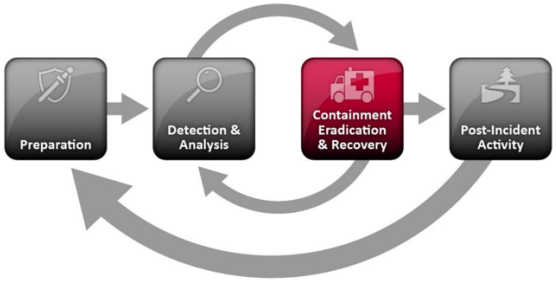


Figure 3: Containment, Eradication, & Recovery Stage

This stage is about containing the threat to prevent more damage, completely removing it from all affected systems, and fixing any damage that has occurred as a result of the attack.

Containment:

This is the process of 'trapping' the malicious actor or threat, so they are unable to spread. This could be achieved by powering off the affected systems, isolating it from the network so it can't communicate with any other machines, or disabling features that are being utilized to spread (such as Windows SMB during the WannaCry ransomworm). In some cases, security teams may redirect the attacker to a sandbox or honeypot, where they can monitor the activity to gather tactics used, and evidence for prosecution. An organization should create different 'Containment Strategies' tailored towards different incident types, so that the most appropriate one can be used. Advanced malware may be able to detect when it is contained and take measures to destroy itself so it can't be analyzed by security professionals.

Eradication and Recovery:

To fully remove all components of an incident, we can take actions such as deleting or disabling compromised user accounts, removing malicious files, and patching vulnerabilities. It is incredibly important to identify every single affected host, so that no threats are left behind after this stage.

During the Recovery phase, system owners work to get operations back to the normal baseline. Depending on the damage done, it could be simple work such as restoring systems to previous images or backups, or rebuilding systems from scratch could be required. Firewall, EDR and IDPS rules/signatures will be updated at this point, so similar activity can be detected and prevented in the future.

LESSONS LEARNED

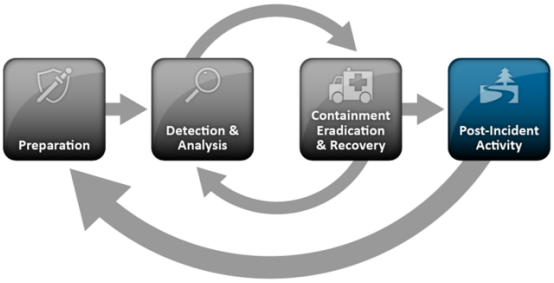


Figure 4: Post-Incident Activity Stage

This is one of the most important sections. By reflecting on the past, security teams are able to implement more effective defences, reducing the risk and probability of future attacks. Here are some questions that will usually be asked in the meeting:

- Exactly what happened?
- How well did the incident response plan work? How could it be improved?
- How could we protect against this type of attack in the future?
- Are any additional tools or resources needed to mitigate future attacks?

Not only do these meetings help improve the security posture of the company by reviewing toolsets and improving policies and procedures, but it also promotes intelligence sharing with other organizations, helping their Incident Response Teams improve their preparation phase.

MODULE CHALLENGE

If you think you're ready for the module challenge, head over to the website and click on the 'Challenge Brief' under the Incident Response module! Good luck.