

29% COMPLETE 86/287 Steps

< Previous Topic

Mark Complete

Blue Team Level 1 Certification (Standard)

7 Topics 4 Quizzes

IR(4) Containment, Eradication, and Recovery Phase

5 Topics 1 Quiz

IR(5) Lessons Learned and Reporting

7 Topics

Section Introduction, Lessons Learned and Reporting

What Went Well?

What Can be Improved?

Importance of Documentation

Incident Response Metrics

Reporting Format

Reporting Considerations

Blue Team Level 1 Certification (Standard) > IR(5) Lessons Learned and Reporting > Reporting C...

IN PROGRESS

Incident Response Domain

REPORTING CONSIDERATIONS

SBT

BLUE TEAM

LEVEL

1

There are a number of things we need to consider when writing a report or similar documentation post-incident. We will be looking at the following considerations in this lesson:

- Report Audience
- Incident Investigation
- Screenshots and Captions



REPORT AUDIENCE

As mentioned in the previous lesson, incident reports will typically have a number of different audiences, especially Executive Board members, IT staff, and the wider security team. We need to ensure that each section is tailored to the intended audience, making sure it has the appropriate level of detail and technical jargon.

- Executive Summary** – This should be short, sweet, and talk about the whole incident at a high-level. This means technical terms and phrases should be avoided and the incident should be explained using business risks. For example, if an incident occurred where the company’s website was defaced, the executive summary should talk about how the incident was discovered, how it was resolved, and how this could’ve affected the business if it wasn’t addressed quickly (loss of sales, reputation damage, loss of customer trust, etc). It’s also important to remember that Executives are extremely busy, and they will likely not read any more than the executive summary – we need to make this as impactful as possible.
- Rest of the Report** – The remainder of the report will typically be aimed at technical staff so this should include a lot of detail, annotated screenshots, and should use technical language where appropriate.



INCIDENT INVESTIGATION

This section needs to be detailed. Really detailed. Any points you make need to be backed up with evidence, otherwise it is just speculation (try not to do this – if there’s no proof, you can’t prove it actually happened). For example, let’s pretend we’re investigating a system that was compromised by a phishing email that contained a Microsoft Word document with a malicious macro which downloads malware to the system. We can state a phishing email was the initial access vector, but we need to provide evidence. This could include a screenshot of the email, a screenshot of the malicious macro contents, a screenshot of the SIEM logs showing the outbound beaconing and download of the malware, etc. Try to follow the below approach: **Make a Point > Provide Evidence**.

For security teams it’s helpful to also include the [MITRE ATT&CK](#) tactics that were used. Continuing with the above example regarding phishing, the following would be applicable:

Home > Techniques > Enterprise > Phishing

Phishing

Sub-techniques (3)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of *Valid Accounts*. Phishing may also be conducted via third-party services, like social media platforms.

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003

Tactic: Initial Access

Platforms: Linux, Office 365, SaaS, Windows, macOS

Data Sources: Anti-virus, Detonation chamber, Email gateway, File monitoring, Mail server, Network intrusion detection system, Packet capture, SSL/TLS inspection, Web proxy

CAPEC ID: CAPEC-98

Version: 2.0

Created: 02 March 2020

Last Modified: 18 October 2020

User Execution: Malicious File

Other sub-techniques of User Execution (2)

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from *Spearphishing Attachment*. Adversaries may use several types of files that require a user to execute them, including *.doc*, *.pdf*, *.xls*, *.rtf*, *.scr*, *.exe*, *.lnk*, *.pif*, and *.cpl*.

Adversaries may employ various forms of *Masquerading* on the file to increase the likelihood that a user will open it.

While *Malicious File* frequently occurs shortly after *Initial Access* it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user’s desktop hoping that a user will click on it. This activity may also be seen shortly after *Internal Spearphishing*.

ID: T1204.002

Sub-technique of: T1204

Tactic: Execution

Platforms: Linux, Windows, macOS

Permissions Required: User

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Version: 1.0

Created: 11 March 2020

Last Modified: 11 March 2020

Therefore, when explaining these stages of the incident in our report, we would mention T1566 for phishing initial access, and T1204.002 for code execution using a malicious file (attached to the phishing email).



SCREENSHOTS & CAPTIONS

Screenshots are a great way to provide evidence, remember the saying “a picture speaks a thousands words”? Well it really does apply with security reports (not just incident handling, but also penetration testing!). Above we mentioned the ‘Make a Point > Provide Evidence’ process, and screenshots are a perfect way to do this. If you’re talking about a port scan conducted from one internal system to another and you have PCAPs available, then screenshot Wireshark with a filter showing the scanning activity! If you’re stating that an adversary moved between systems using password re-use then provide screenshots of login events from the SIEM, local access logs, or anything else that shows this activity.

All images should also be captioned with a short sentence or two, summarising what is being shown in the screenshot. The helps people to quickly digest the information in case they don’t fully understand what they’re looking at (such as output from a tool they’ve never used before).

< Previous Topic

Mark Complete ✓

Back to Lesson