Blue Team Level 1 Certification (Standard)

~~Introduction to Security Fundamentals~~
1 Topic

~~Soft Skills~~
7 Topics

~~Security Controls~~
5 Topics | 1 Quiz

~~Networking 101~~
6 Topics | 1 Quiz

~~Management Principles~~
4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

~~PA1) Introduction to Emails and Phishing~~
7 Topics | 1 Quiz

~~PA2) Types of Phishing Emails~~
10 Topics | 2 Quizzes

~~PA3) Tactics and Techniques Used~~
12 Topics | 2 Quizzes

~~PA4) Investigating a Phishing Email~~
8 Topics | 2 Quizzes

~~PA5) Analysing URLs, Attachments, and Artifacts~~
8 Topics | 1 Quiz

PA6) Taking Defensive Actions
12 Topics | 1 Quiz

PA7) Report Writing
7 Topics | 1 Quiz

PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence
7 Topics

TI2) Threat Actors & APTs
6 Topics | 2 Quizzes

TI3) Operational Threat Intelligence
7 Topics | 1 Quiz

TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz

TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz

TI6) Malware and Global Campaigns
6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics
5 Topics

DF2) Forensics Fundamentals
10 Topics | 5 Quizzes

DF3) Digital Evidence Collection
8 Topics | 1 Quiz

DF4) Windows Investigations
3 Topics | 3 Quizzes

DF5) Linux Investigations
4 Topics | 2 Quizzes

Reporting Format

Blue Team Level 1 Certification (Standard) > IR5) Lessons Learned and Reporting > Reporting Fo... IN PROGRESS

The first thing we want to state is that **there is no standard format for incidents reports**. Unfortunately there's not a magical template that will work for all security teams across every organisation in the world. However, it's common to see 4 main sections of a report, which we'll cover in more depth below:

- **Executive Summary**
- **Incident Timeline**
- **Incident Investigation**
- **Appendix**

EXECUTIVE SUMMARY

This is typically where the high-level overview of the incident will go, using non-technical terms to clearly state the business impact. Executives are very busy so it's our job to ensure that this section is easily readable and contains information that is important to this specific audience.

The executive summary should ideally be one page and focus on areas such as business risks, financial costs, and damage occurred and prevented. This is a great place to really highlight the work of the security team and how they have prevented more damage and costs from happening (by containing an incident, preventing data exfiltration, catching an insider threat, etc). Doing this will show the executives that the cost of running the security team is less than suffering successful incidents, showing the value in maintaining (and potentially even growing) the team.

INCIDENT TIMELINE

The timeline will provide the date, time, and short descriptions of all key events throughout the incident. This can either be in the order these actions were taken or discovered, or re-ordered to be in chronological order to make it easier to read exactly what has happened from start to finish. It is common to see security teams use either their local timezone (provided the incident has only affected one geographic location) or Universal Time Coordinated (UTC) if the incident affects users or systems across multiple timezones. Converting multiple timezones to a single one ensure that the timeline is kept neat and easy to read and refer to.

INCIDENT INVESTIGATION

This will be the main bulk of the report, providing step-by-step documentation of actions that were conducted and the associated findings of the incident responders. All stages of the incident response lifecycle should be considered and reported on, with the exception of preparation:

- **Detection and Analysis** – How was the incident discovered? Was it a SIEM alert? A threat hunt? A user or system admin that reported something unusual? How was this activity triaged to ensure it was an incident and not a false positive? Were any checks conducted on the affected system(s) or was network traffic collected and analyzed? Screenshots should be used to show exactly what actions were taken, and what the investigating responders saw when performing analysis.
- **Containment, Eradication, and Recovery** – How was the incident scoped? Remember, this is arguably the most important part of a response, we need to ensure we've found all affected systems to prevent a reinfection at a later date. How did the security team remove the actor(s) from the networks? Were systems restored from known-safe backups? Was anti-virus used to scan all systems, along with manual checks via an EDR solution? Were systems completely decommissioned? And what was the root cause? Correctly identifying this would allow us, as defenders, to address the issue and ensure that a similar incident doesn't occur again.
- **Post-Incident Activity** – What could have been done better? Maybe the security team needs more personnel, or additional tools, or more visibility into networks and systems. This should all be explained here to help drive decision making to help prevent or allow the team to better respond to future incidents. Anything major should be included in the executive summary to ensure that it is seen by the top-level business decision makers.

REPORT APPENDIX

The appendix is used as storage for the report, and will typically include images or figures (graphs, tables) that will be referenced in the main body of the report. An example of content that could be included in this section includes a long list of IP addresses that were scanned to look for malicious indicators. This list or table would be included here as this would take up a lot of space in the 'incident investigation' report.

REPORT TEMPLATES

We can't stress this enough – one template will not work for everyone. We've linked an example incident report template below so you can understand how this document **could** look within an organization. We recommend becoming familiar with the different sections, as you'll be completing a report template for the BTL1 exam soon! (Spoiler; you can look at the report template before starting the exam – this is a good idea to understand what you need to write, and how much detail you need to go into!).

- **Palo Alto –** https://www.paloaltonetworks.com/resources/whitepapers/incident-response-reporting-template

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›