

Blue Team Level 1 Certification
(Standard)

Based Artifacts

☐ Reactive Measures: Blocking Web-Based Artifacts☐ Reactive Measures: Blocking File-Based Artifacts☒ Reactive Measures: Informing Threat Intelligence Team☒ Activity) End of Section Review, Defensive Measures☐ 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

☐ DF6) Volatility

3 Topics 1 Quiz

☐ DF7) Autopsy

4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN☐ SI1) Introduction to SIEM

7 Topics 1 Quiz

☐ SI2) Logging

6 Topics 2 Quizzes

☐ SI3) Aggregation

2 Topics 1 Quiz

☐ SI4) Correlation

6 Topics 1 Quiz

☐ SI5) Using Splunk

5 Topics 2 Quizzes

Reactive Measures: Informing Threat Intelligence Team

Blue Team Level 1 Certification (Standard) > PA6) Taking Defensive Actions > Reactive Measure...

IN PROGRESS

Phishing Analysis INFORMING THREAT INTEL TEAM



In some cases, it is necessary for the investigating analyst to inform the threat intelligence team, if the organization has one in-house. This is typically conducted when there is an on-going and sustained phishing campaign against the organization, the phishing emails are extremely targeted towards the organization, or the attack is complex and the sharing of intelligence could benefit other organizations and help them to defend themselves. We will cover all three of these scenarios below.

SUSTAINED CAMPAIGN

If an organization is being bombarded by a continuous stream of phishing emails, there is an increased risk that an employee will open one and potentially compromise the company. Depending on the maturity of the threat intelligence team and the tools they have at their disposal, they may be able to predict how the campaign will continue and take actions to outsmart the attacks. If a pattern emerges based on the sending addresses used to push the malicious emails to employees, or with the domain names used to host malicious content, proactive blocking actions can be taken to stop future phishing emails before they're even sent.

TARGETED ATTACK

If a phishing attack or campaign is specifically targeted towards the organization, or even worse, spear-phishing specific employees, it is definitely time to let the threat intelligence team know. They can work with the victim(s) to provide specific support regarding being targeted, and can also conduct public exposure assessments to determine how much information is available publicly online about the target(s).

SOPHISTICATED ATTACK

If an attack is extremely sophisticated, gathering and sharing indicators of compromise (IOCs) with intelligence sharing partners, government, and even publicly can be a great move to help other organizations protect themselves and have the organization earn a good reputation amongst others for their approach.

CONCLUSION

Whilst it's not always beneficial to inform the threat intelligence team about phishing emails, in certain circumstances, they are able to provide more context, perform threat exposure checks, and share intelligence with

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics1 Quiz

IR2) Preparation Phase

10 Topics2 Quizzes

IR3) Detection and Analysis Phase

7 Topics4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

other organizations to help other network defenders prepare for, or take proactive measures to protect themselves.

< Previous Topic

Mark Complete ✓
Back to Lesson

Privacy & Cookies Policy

