

Blue Team Level 1 Certification
(Standard)

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

Section Introduction: Defensive Measures

Preventative Measures: Marking External Emails

Preventative Measures: Email Security Technology

Preventative Measures: Spam Filter

Preventative Measures: Attachment Filtering

Preventative Measures: Attachment Sandboxing

Preventative Measures: Security Awareness Training

Reactive Measures: Immediate Response Process

Reactive Measures: Blocking Email-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

Reactive Measures: Immediate Response Process

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

IN PROGRESS

Phishing Analysis IMMEDIATE RESPONSE PROCESS



Immediate response are the steps the investigating analyst should take once they have identified a phishing email, from detection through to concluding their investigation report. These steps will work to triage the attack, and take measures to address the risk generated by malicious emails being successfully delivered to employee mailboxes.

The steps are:

1. Retrieve an original copy of the phishing email
2. Gather artifacts from the phishing email
3. Inform the recipients that received the email
4. Investigate malicious artifacts to collect indicators of compromise that can be blocked to protect the organization
5. Take defensive measures
6. Complete the investigation report, documenting all of the above steps

1) Retrieve an Original of the Suspicious Email:

An original version of the email can be obtained via a number of methods, such as; through security technology on the email gateway or the gateway itself, pulling the email directly from the email solution, such as Microsoft Exchange servers, or having an employee forward the email to a security-owned mailbox.

2) Gather Artifacts From the Original Email:

We have already covered the artifacts we need to collect, and why they're important. These are used later in the investigation process to perform artifact analysis and take defensive measures.

3) Inform Email Recipients:

A crucial part of the immediate response to a phishing attack is to notify any individuals that have received the email. This helps to reduce the chance of them opening and interacting with the email.

Typically organizations will have an email template that they can send to recipients once they have been identified. The investigating analyst would check on the email gateway to see which mailboxes the phishing email has been delivered to, and then add the recipients into BCC of the email template, and include the following details:

- **The date and time the email was sent** (allows the recipients to find the email easier by looking at the times of emails that they have received)
- **The subject line of the malicious email** (allows the recipients to find the email easier by looking at the subject lines of emails that they have received)
- **Clear instructions on what to do with the email** (this will depend on how the organization deals with phishing emails. This could either be instructing the recipients to delete the email or forward it to a security-owned mailbox)
- **Contact details for if the recipient is unsure what to do** (typically a security-owned mailbox, so the user can get support from the security team)

4) Artifact Analysis and Investigation:

We have already covered how to investigate email, web, and file-based artifacts to collect more information and determine how malicious they are. Tools that should be used include enterprise-grade sandboxing, HIPS, DNMIC

determine how malicious they are. Tools that should be used include Enterprise-grade sandboxing, Cuckoo Sandbox, VirusTotal, IPVoid, WannaBrowser, a virtual machine, and more.

5) Take Defensive Measures:

Defensive measures are the actions taken by the security team to reduce the risk generated by the phishing attack. This potentially includes blocking email, web, and file-based artifacts. If a malicious email includes a URL that takes the user to a credential harvester, blocking this URL on a web proxy would prevent employees from connecting to the webpage, completely mitigating the risk of them entering their credentials. We will cover blocking email, web, and file-based artifacts in the next three lessons.

6) Complete Investigation Report:

We will cover this in detail in a later section. Your investigation report will include notes about all of the steps you have completed during the immediate response process. This provides an audit trail to show that the email was identified, investigated, and defensive measures were taken to protect the organization from this attack.

[Previous Topic](#)

[Mark Complete](#) ✓
Back to Lesson

[Next Topic](#)

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

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response