

Blue Team Level 1 Certification  
(Standard)

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

○ Section Introduction, Report Writing

○ Email Header, Artifacts, and Body Content

○ Analysis Process, Tools, and Results

○ Defensive Measures Taken

○ Artifact Sanitization

○ Activity) Report Writing Exercise

○ Activity Cont.) Report Writing Exercise Answers

□ Activity) End of Section Review, Report Writing

○ PA8) Phishing Response Challenge

3 Topics 1 Quiz

## THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

7 Topics

○ TI2) Threat Actors &amp; 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

Activity Cont.) Report Writing  
Exercise Answers

Blue Team Level 1 Certification (Standard) &gt; PA7) Report Writing &gt; Activity Cont.) Report Writi...

IN PROGRESS

Phishing Analysis  
REPORT WRITING EXERCISE

Below is the report that we would've written given the information included in the investigating analyst's notes. Please note that the required content of phishing reports will vary with different organizations, but the below encompasses all of the information in a format that could be used anywhere. Compare your report to the one below to see how similar they are. People will write their reports differently, so provided you have included all the reports from the investigating analyst's notes, then you've done well!

## CHALLENGE ANSWERS

## Email Description and Artefacts Collected

Sending Address: emailsecalert1@gmail.com

Subject Line: Your Email Will be Locked! Act NOW!

## Recipients:

john.smith@dicksonunited.co.uk

alice.cooper@dicksonunited.co.uk

jacon.long@dicksonunited.co.uk

fred.johnson@dicksonunited.co.uk

pickle.rick@dicksonunited.co.uk

Sending Server IP: 209.85.222.173

Reverse DNS: mail-qk1-f173.google.com (Gmail)

Reply-To: emailsecalert1@gmail.com

Date and Time: 3:21 PM Monday 1st June 2020

Full URL (sanitized): hxxps://outlook-security.emailsecalerts[.]net/index/2020/OWA.php?

Root Domain: hxxps://emailsecalerts[.]net

Looking at the reported email in the Outlook email client, this message is impersonating an Outlook security alert using branding such as Outlook logos. The email is informing recipients that their mailboxes will be closed unless they confirm their identity, where they are directed to click on a button, likely leading to a credential harvester based on the context of the email.

## Artifact Analysis

Checking the email gateway shows that there have been no outgoing emails to the sending address, therefore no recipients have replied to the sender.

A reverse DNS search on the sending server IP shows that this email has definitely originated from Gmail, and not Microsoft.

URL2PNG analysis shows that the full URL is an Outlook credential harvester, asking users to enter in their email and password.

MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

SI2) Logging

6 Topics2 Quizzes

SI3) Aggregation

2 Topics1 Quiz

SI4) Correlation

6 Topics1 Quiz

SI5) Using Splunk

5 Topics2 Quizzes

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

5 Topics1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics2 Quizzes

BTL1 EXAM

A VirusTotal search for the domain shows that it has been flagged for malicious and phishing activity, therefore it is known to be malicious within the security community.

Checking the SIEM and EDR no employees have made a network connection to the malicious domain, so no recipients have clicked on the link in the email at this time.

The domain is also attempting to typo squat or appear as a legitimate domain related to email security alerts, trying to make the attack more believable to targets.

### Suggested Defensive Measures

As the sender is using a Gmail address, the most appropriate action would be to block this specific mailbox to prevent any more incoming malicious emails from this sender.

**Requesting an email gateway block for the sending address "emailsecalert1@gmail.com".**

The domain has been recognised as malicious, and there is no business justification for any employees needing to access this site. As it has a malicious reputation on VirusTotal, and analysis has shown that it is hosting a credential harvester, the entire domain can be blocked on the web proxy, preventing employees from connecting to the site. This will also make future phishing attacks using this same domain ineffective.

**Requesting a web proxy block for the domain "hxxps://emailsecalerts[.]net".**

< Previous Topic

Mark Complete ✓  
Back to Lesson