How to Investigate a SIEM Alert? BY P3NGU1N

Detection

🎯 In which channel can you take ownership of the alert?

ANSWER: Main Channel

🎯 Once you have completed the analysis of an alert, in which channel can you close the alert?

ANSWER: Investigation Channel

Case Creation and Playbook Initiation

Note: The following questions refer to the alert with " **EventID: 257 - SOC282 - Phishing Alert - Deceptive Mail Detected** ". Try to answer the questions by solving the alert and following the steps mentioned in the course.

🎯 What is the "type" of the alert?

ANSWER: Exchange

🎯 When was the alert generated?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

ANSWER: May, 13, 2024, 09:22 AM

🎯 What is the email's SMTP address?

ANSWER: 103.80.134.63

🎯 What is the source address?

ANSWER: free@coffeeshooop.com

🎯 What is the destination address?

ANSWER: felix@letsdefend.io

Email Analysis

Note: The following questions refer to the alert with " **EventID: 257 - SOC282 - Phishing Alert - Deceptive Mail Detected** ". Try to answer the questions by solving the alert and following the steps mentioned in the course.

🎯 **Question:** What is the name of the attachment?

Answer Format: filename.extension

ANSWER: free-coffee.zip

🎯 What is the subject of the email?

ANSWER: Free Coffee Voucher

🎯 When was the email sent?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

ANSWER: May, 13, 2024, 09:22 AM

Network and Log Analysis

Note: The following questions refer to the alert with " **EventID: 257 - SOC282 - Phishing Alert - Deceptive Mail Detected** ". Try to answer the questions by solving the alert and following the steps mentioned in the course.

🎯 **Question:** What is the IP address of the Felix host?
ANSWER: 172.16.20.151

🎯 When exactly did Felix download the malicious file?

Answer Format: As written in the alert details.

Sample Answer: Apr, 20, 2023, 09:42 AM

ANSWER: May, 13, 2024, 12:59 PM

🎯 What is the C2 address?

ANSWER: 37.120.233.226

🎯 What's the name of the process that communicated with C2?

Answer Format: processname.extension

ANSWER: coffee.exe

🎯 What port did the malware use to communicate?

ANSWER: 3451

Endpoint Analysis

Note: The following questions refer to the alert with " **EventID: 257 - SOC282 - Phishing Alert - Deceptive Mail Detected** ". Try to answer the questions by solving the alert and following the steps mentioned in the course.

🎯 **Question**: What is the Process ID (PID) of the "coffee.exe"?
ANSWER: 6697

🎯 What is the "image hash" of the malicious process?

ANSWER:
CD903AD2211CF7D166646D75E57FB866000F4A3B870B5EC759929BE2FD81D334

🎯 How many child processes does "cmd.exe" have?

ANSWER: 7

Result

🎯 On the monitoring page, through which channel can you access the official incident report of an alert?

ANSWER: Closed Alerts