Security Operations Center: Tools and Processes

Cybersecurity Boot Camp

Incident Response Day 2

Class Objectives

By the end of class today, students will be able to:

- ❏ Explain the difference between SIEMs and SOARs.
- ❏ Investigate pcap files using Wireshark.
- ❏ Walk through the process of investigating an incident.

SIEMs, SOARs, and VMs

SIEMS

Last class, we covered:

- Incident Response
- IR Plan and Playbook Creation
- The Basics of an SOC
- Planning an SOC

The Importance of Virtual Machines

The first resource in an Analyst's toolbox is a virtual machine.

Virtual Machines provide analysts with a platform to view malware, malicious links and other untrustworthy sources.

VMs act as sandboxes, making it difficult for harmful programs to escape and cause damage to the actual computer or file.

Virtual machines are not impervious to viruses,

but they are a good precaution as a layer of security.

We know SIEMs receive logs from a company’s systems, then output statuses and alerts...

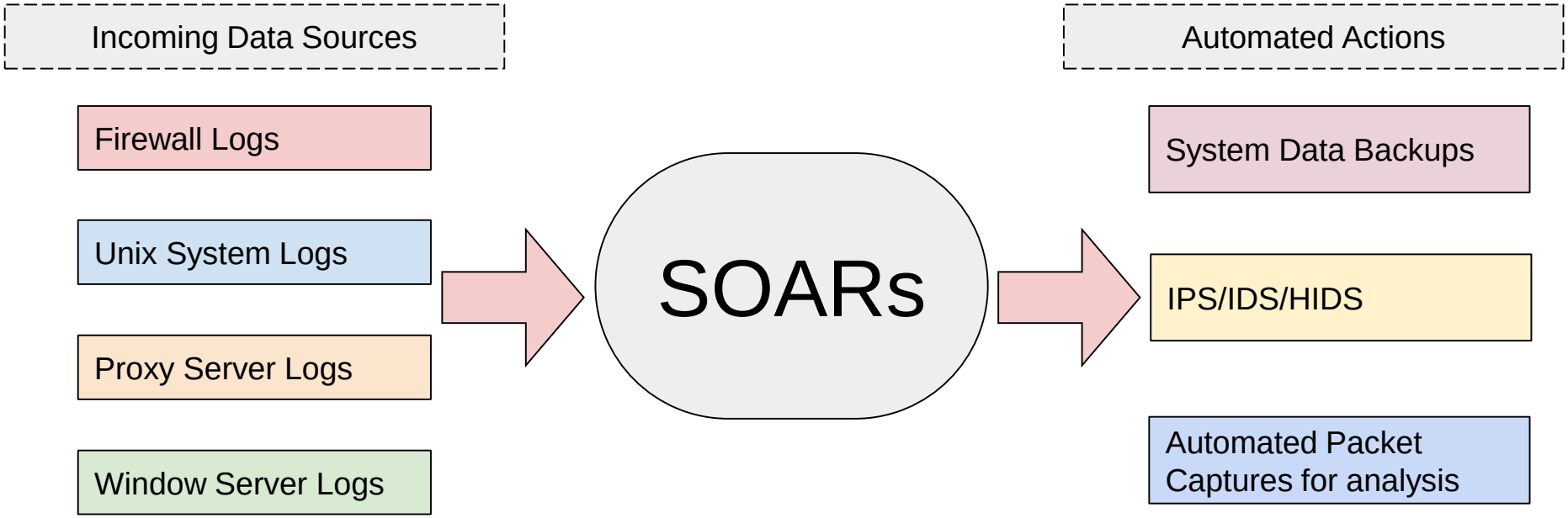
SOARs

Security Orchestration, Automation, and Response is the next generation of SIEMs.

SOARs will not only send alerts, but also take some automated actions on behalf of an analyst.

- Automated actions may include gathering enrichment data like whois data and threat intelligence.
- They may even block an IP in a firewall or quarantine a system.
- The main goal of an IR team is to act on an incident *as quickly as possible*.
    - So, if the SIEM system can gather logs or network information on its own, the analyst can get to work investigating the incident much faster.

SOARS



SOAR systems often use Python scripts to automate these processes.
Analysts that know Python are able to review and modify these scripts.

Many companies contribute to the vast SIEMs marketplace...

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2018)

Wireshark Tips and Tricks

Activity: Wireshark Tips and Tricks

In this activity, you will customize your Wireshark setup.

Activities/Wireshark

Suggested Time:
20 minutes

Take a Break!

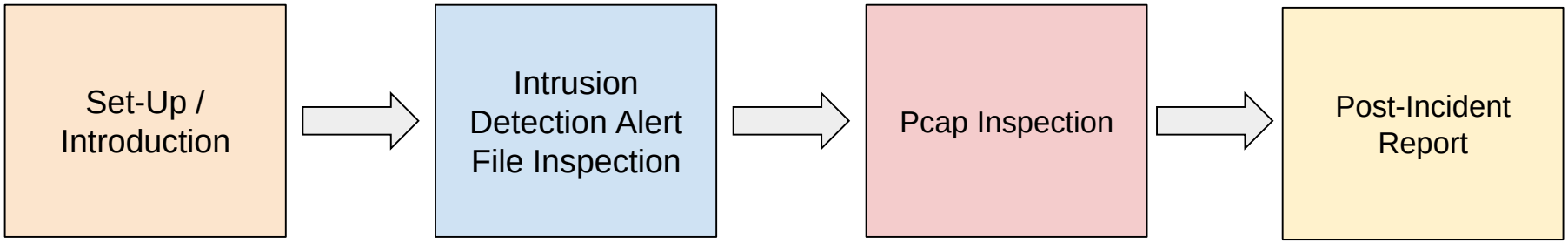
Incident Walkthrough

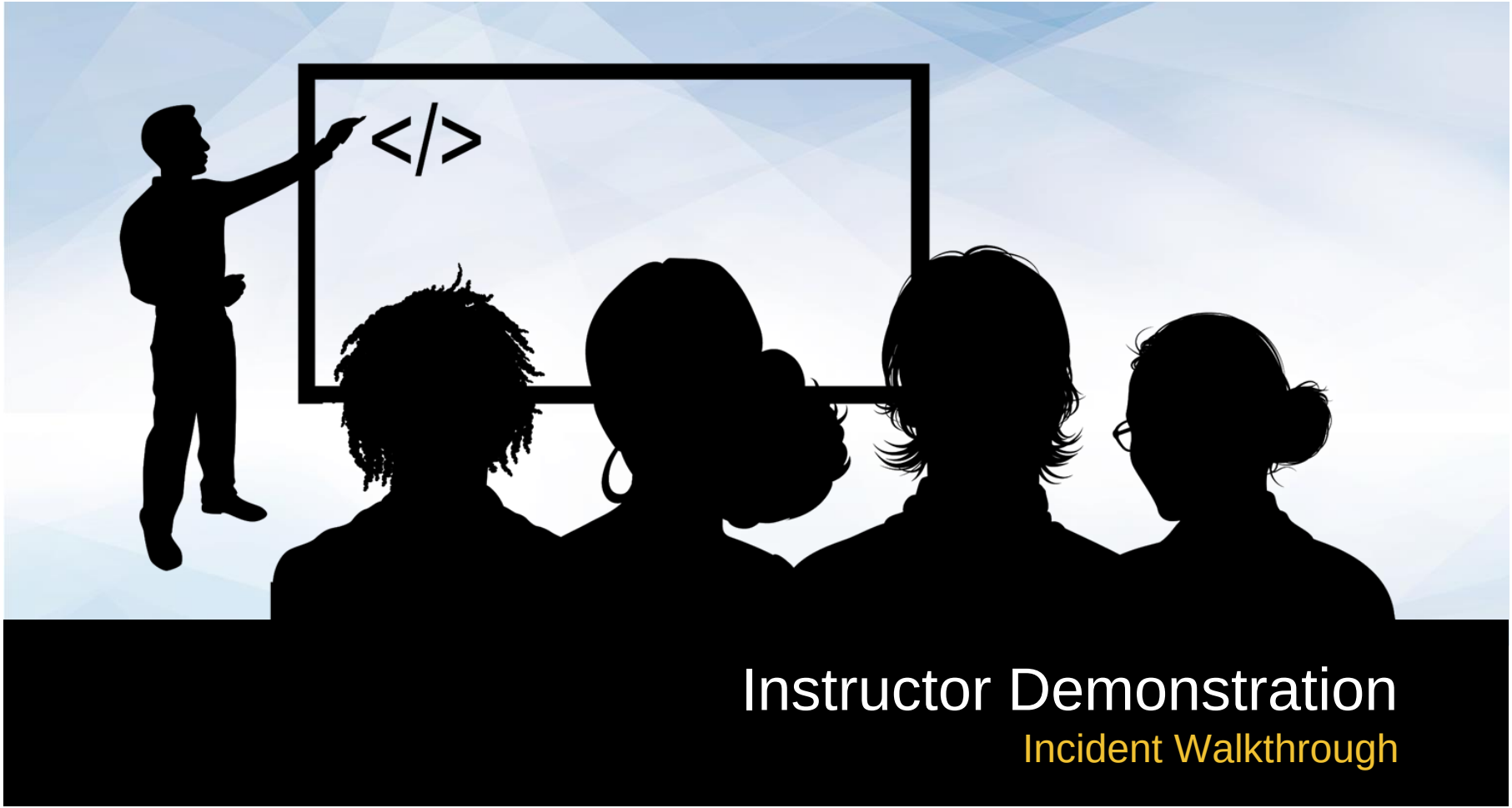
This exercise uses live malware.
Make sure you're using your virtual machines!

Incident Walkthrough Demo

Questions we'll answer as a group:

- ☐ How can we confirm that a computer was infected with malware?
- ☐ How can we identify which computers were involved in the incident?
- ☐ Can we identify when and how the computer was infected?
- ☐ Can we identify source and destination IP addresses and ports used in the attack?
- ☐ Can we identify the exact malware that was used in the attack?
- ☐ Can we create a firewall rule to prevent this attack in the future?





Instructor Demonstration

Incident Walkthrough

Incident Review

- ☐ How can we confirm that a computer was infected with malware?
- ☐ How can we identify the computers involved in the incident?
- ☐ Can we identify the source and destination IP Address and Ports used?

Incident Review

- ☐ How can we confirm that a computer was infected with malware?

By extracting the malware from the pcap file and using Virus Total to verify.

- ☐ How can we identify which computers were involved in the incident?

- ☐ Can we identify the source and destination IP Address and Ports used?

Incident Review

- ☐ How can we confirm that a computer was infected with malware?

By extracting the malware from the pcap file and using Virus Total to verify

- ☐ How can we identify which computers were involved in the incident?

We can see the MAC address, host name and operating system of the infected computer by searching the pcap for DHCP traffic OR by searching for the string ‘Host Name”

- ☐ Can we identify the source and destination IP Address and Ports used?

Incident Review

- ☐ How can we confirm that a computer was infected with malware?

By extracting the malware from the pcap file and using virus total to verify

- ☐ How can we identify which computers were involved in the incident?

We can see the MAC address, host name and operating system of the infected computer by searching the pcap for DHCP traffic OR by searching for the string ‘Host Name”

- ☐ Can we identify the source and destination IP Address and Ports used?

We can See the **source 192.168.1.96** and **destination 104.27.158.125** in the Snort Alerts.

Incident Review

- ☐ Can we identify when and how the computer was infected?

We can see the date and time for the original HTTP request in the pcap.

- ☐ Can we identify the exact malware that was used in the attack?

- ☐ Can we create a firewall rule to prevent this traffic?

Incident Review

- ☐ Can we identify when and how the computer was infected?

We can see the date and time for the original HTTP request in the pcap.

- ☐ Can we identify the exact malware that was used in the attack?

Snort correctly identified the **Pushdo Trojan**.

- ☐ Can we create a firewall rule to prevent this traffic?

Incident Review

- ☐ Can we identify when and how the computer was infected?

We can see the date and time for the original HTTP request in the pcap.

- ☐ Can we identify the exact malware that was used in the attack?

Snort correctly identified the Pushdo Trojan.

- ☐ Can we create a firewall rule to prevent this traffic?

Tools > Firewall ACL Rules

This function is not actually configuring a firewall, but Wireshark is providing potential firewall rules to block traffic for the packet you have selected.

Activity: Post-Wireshark Activity

In this activity, you will investigate a malware attack using a Snort alert file and network pcap.

Activities/WireSharkFollowUp

Suggested Time:
20 Minutes

Wireshark Follow-Up

Examine the Snort file and answer the following questions:

What activity is Snort reporting on? (Provide some alert headlines.)

What is the date and time of the alert?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What activity is Snort reporting on? (Provide some alert headlines.)

- “Likely Evil EXE download from dotted Quad by MSXMLHTTP”
- “ET Malware Windows executable sent when remote host claims to send an image”
- “ET Trojan [PTsecurity] Trickbot Data Exfiltration”

What is the date and time of the alert?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What activity is Snort reporting on? (Provide some alert headlines.)

- “Likely Evil EXE download from dotted Quad by MSXMLHTTP”
- “ET Malware Windows executable sent when remote host claims to send an image”
- “ET Trojan [PTsecurity] Trickbot Data Exfiltration”

What is the date and time of the alert?

2019-02-23 19:27

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What is the external IP address that Snort is flagging for malicious activity?

What is the internal IP address that Snort is flagging for malicious activity?

What is the source port of the activity?

What is the destination port of the activity?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What is the external IP address that Snort is flagging for malicious activity?

209.141.55.226

What is the internal IP address that Snort is flagging for malicious activity?

What is the source port of the activity?

What is the destination port of the activity?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What is the external IP address that Snort is flagging for malicious activity?

209.141.55.226

What is the internal IP address that Snort is flagging for malicious activity?

10.2.23.231

What is the source port of the activity?

What is the destination port of the activity?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What is the external IP address that Snort is flagging for malicious activity?

209.141.55.226

What is the internal IP address that Snort is flagging for malicious activity?

10.2.23.231

What is the source port of the activity?

80

What is the destination port of the activity?

Wireshark Follow-Up

Examine the snort file and answer the following questions:

What is the external IP address that Snort is flagging for malicious activity?

209.141.55.226

What is the internal IP address that Snort is flagging for malicious activity?

10.2.23.231

What is the source port of the activity?

80

What is the destination port of the activity?

49195

Wireshark Follow-Up

Pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort alert.

What is the MAC Address if the internal computer?

What is the host name of the infected machine?

Wireshark Follow-Up

Pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort alert.

Http.request and ip.addr eq 209.141.55.226 and ip.addr eq 10.2.23.231

What is the MAC Address if the internal computer?

What is the host name of the infected machine?

Wireshark Follow-Up

Pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort alert.

Http.request and ip.addr eq 209.141.55.226 and ip.addr eq 10.2.23.231

What is the MAC Address if the internal computer?

While inspected this packet, under the ‘Ethernet II’ section, we can see that this is likely a Windows machine with the name HewlettP and the MAC Address: (00:11:0a:9f:c0:2d)

What is the host name of the infected machine?

Wireshark Follow-Up

Pcap File

Filter the pcap file to show the conversation between the two machines that were identified in the Snort alert.

Http.request and ip.addr eq 209.141.55.226 and ip.addr eq 10.2.23.231

What is the MAC Address if the internal computer?

While inspecting this packet, under the ‘Ethernet II’ section, we can see that this is likely a Windows machine with the name HewlettP and the MAC Address: (00:11:0a:9f:c0:2d)

What is the host name of the infected machine?

- Filter Wireshark for bootp which gives you DHCP traffic
- In the packet info, under the Bootstrap Protocol there is an Option: (xx)Host Name
- This machine’s host name is Ferguson-Win-PC

Wireshark Follow-Up

Pcap File

Can you confirm the date and time this issue occurred?

How can you confirm if the Snort alert is accurate?

Can you safely verify whether or no malware was downloaded?

Wireshark Follow-Up

Pcap File

Can you confirm the date and time this issue occurred?

Confirmed: pcap shows 2019-02-23 14:27 UTC

How can you confirm if the Snort alert is accurate?

Can you safely verify whether or no malware was downloaded?

Wireshark Follow-Up

Pcap File

Can you confirm the date and time this issue occurred?

Confirmed: pcap shows 2019-02-23 14:27 UTC

How can you confirm if the Snort alert is accurate?

Following the TCP stream shows binary data with !This program cannot be run in DOS mode.

Shows the file named troll1.jpg.

Can you safely verify whether or no malware was downloaded?

Wireshark Follow-Up

Pcap File

Can you confirm the date and time this issue occurred?

Confirmed: pcap shows 2019-02-23 14:27 UTC

How can you confirm if the Snort alert is accurate?

Following the TCP stream shows binary data with “!This program cannot be run in DOS mode.”

Shows the file named troll1.jpg.

Can you safely verify whether or no malware was downloaded?

Using File > Export Objects > HTTP, choose the troll1.jpg file out of the list and save it.

Run md5sum troll1.jpg to hash the file.

Visit Virus Total and paste in the hash to verify malware.

Wireshark Follow-Up

Pcap File

Would you categorize this alert as a False Positive or a True Positive?

If this issue needs to be mitigated, what steps should be taken with the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Wireshark Follow-Up

Pcap File

Would you categorize this alert as a False Positive or a True Positive?

Malware was verified to be download, so its a **True Positive**.

If this issue needs to be mitigated, what steps should be taken with the infected machine?

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Wireshark Follow-Up

Pcap File

Would you categorize this alert as a False Positive or a True Positive?

Malware was verified to be download, so its a **True Positive**.

If this issue needs to be mitigated, what steps should be taken with the infected machine?

The machine should be restored to a backup prior to this incident.

What steps should be taken in regards to network security?

Would you categorize this issue as a Web, Email or Network attack?

Wireshark Follow-Up

Pcap File

Would you categorize this alert as a False Positive or a True Positive?

Malware was verified to be download, so its a **True Positive**.

If this issue needs to be mitigated, what steps should be taken with the infected machine?

The machine should be restored to a backup prior to this incident.

What steps should be taken in regards to network security?

We can use Wireshark to create a firewall rule:

- Block #IPv4 malicious address.
- Iptables --append INPUT --in-interface etho --source 209.141.55.226/32 --jump DROP

Would you categorize this issue as a Web, Email or Network attack?

Wireshark Follow-Up

Pcap File

Would you categorize this alert as a False Positive or a True Positive?

Malware was verified to be download, so its a **True Positive**.

If this issue needs to be mitigated, what steps should be taken with the infected machine?

The machine should be restored to a backup prior to this incident.

What steps should be taken in regards to network security?

We can use Wireshark to create a firewall rule:

- Block #IPv4 malicious address.
- Iptables --append INPUT --in-interface etho --source 209.141.55.226/32 --jump DROP

Would you categorize this issue as a Web, Email or Network attack?

This attack was propagated by visiting a malicious web link, so it’s a Web Attack.

Activity: Incident Response Post-Mortem

In this activity, you will find a recent news article about a security incident that was handled poorly and fill in a post-mortem template

Activities/IR_PostMortem

Suggested Time:
20 Minutes

Class Objectives

By the end of class today, students will be able to:

- ☑ Explain the difference between SIEMs and SOARs.
- ☑ Investigate pcap files using Wireshark.
- ☑ Walk through the process of investigating an incident.