Enterprise Security Management

Cybersecurity

Network Security Day 3

Class Objectives

By the end of class, you will be able to:

- Analyze indicators of attack for persistent threats.
- Use enterprise security management (ESM) to expand an investigation.
- Use OSSEC endpoint reporting agents as part of a host-based IDS alert system.
- Investigate threats using various analysis tools.
- Escalate alerts to senior incident handlers.

Before we get started, we need to launch an instance of **Security Onion**.

This will generate alert data that we'll use to complete the labs.

Activity: Security Onion Setup

Follow along as we set up Security Onion to generate alert data.

Suggested Time:

10 Minutes

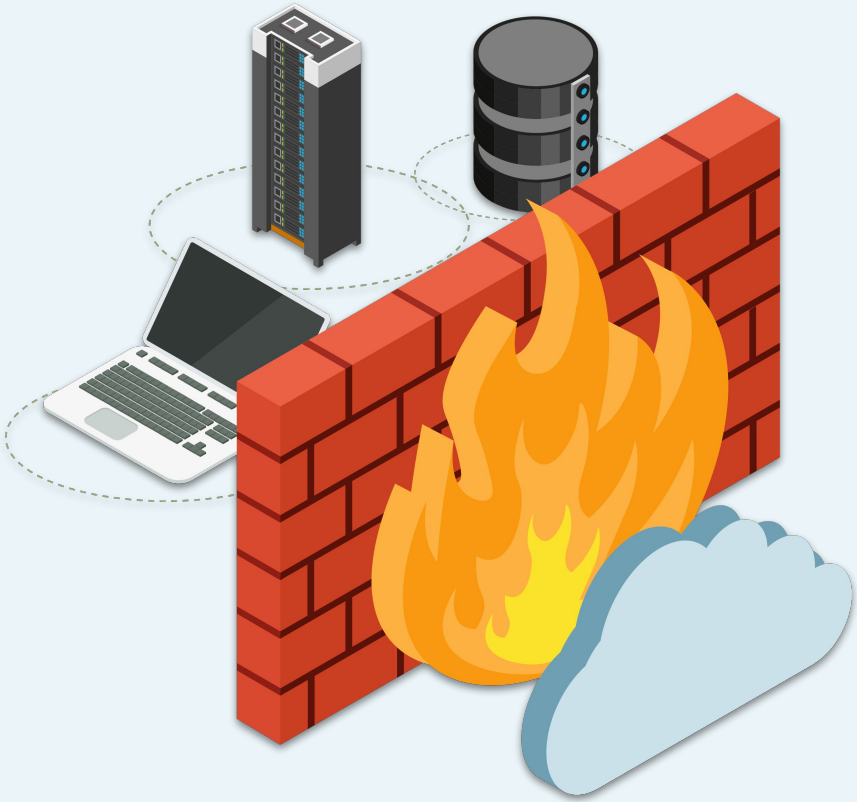
Time’s Up! Let’s Review.

Questions?

Firewall Recap

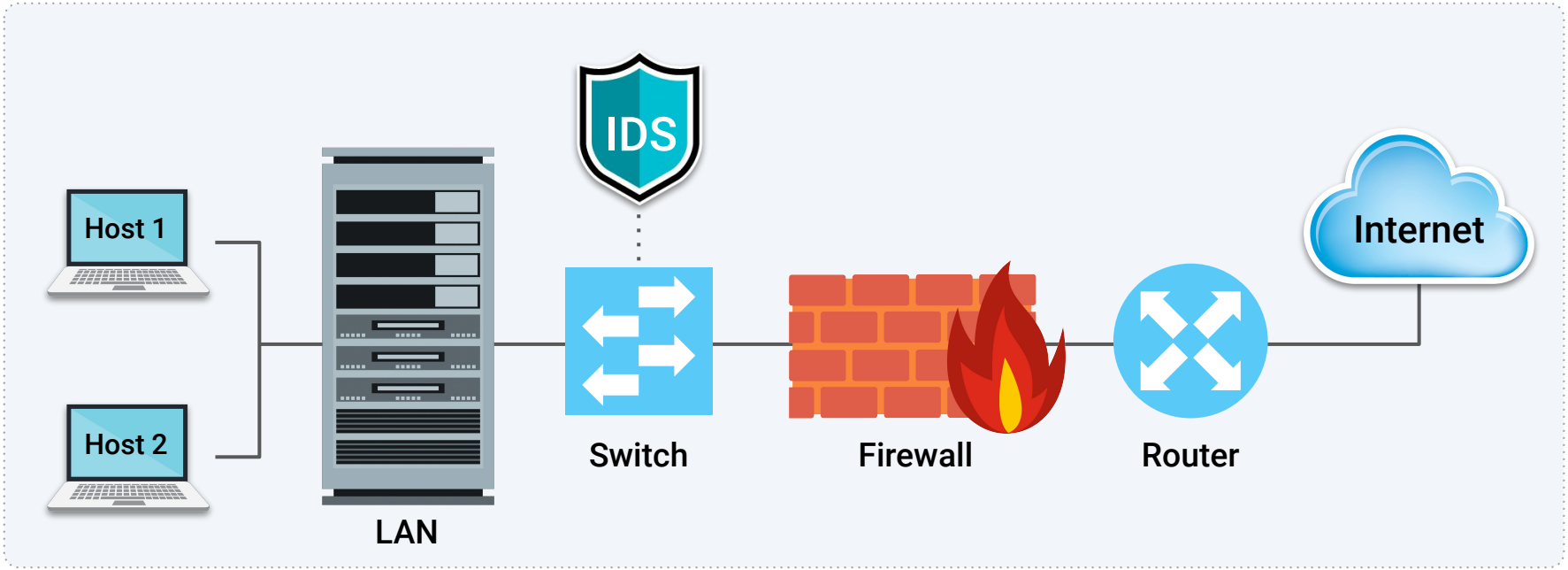
Firewalls protect networks by using rules to make decisions.

- Firewalls are designed to allow traffic from trusted sources and block traffic from untrusted sources.
- Firewalls do have limitations. They can be fooled through packet manipulation by clever attackers.
  - For example, attackers can send malicious data through a firewall by hijacking or impersonating a trusted machine.
- This is why it's crucial to have an effective defense in depth methodology to help protect sensitive data.



IDS Recap

An IDS is like a firewall that reads the data in the packets it inspects, issues alerts, and blocks malicious traffic (if configured to do so).



Snort is the world’s most popular open source network IDS/IPS.

Alert:
C2 Beacon

In the next activity,

you will apply your knowledge of NSM to an attack that targets a command and control (C2) server.

Command and Control (C2)

C2 servers are used to create a specific type of alert for attacks that use persistence as part of their attack campaigns.

- Infected hosts make callbacks to C2 servers.
- These callbacks (referred to as “keep alives”) serve as beacons that keep the back channel open to enable access in and out of the network at all times.

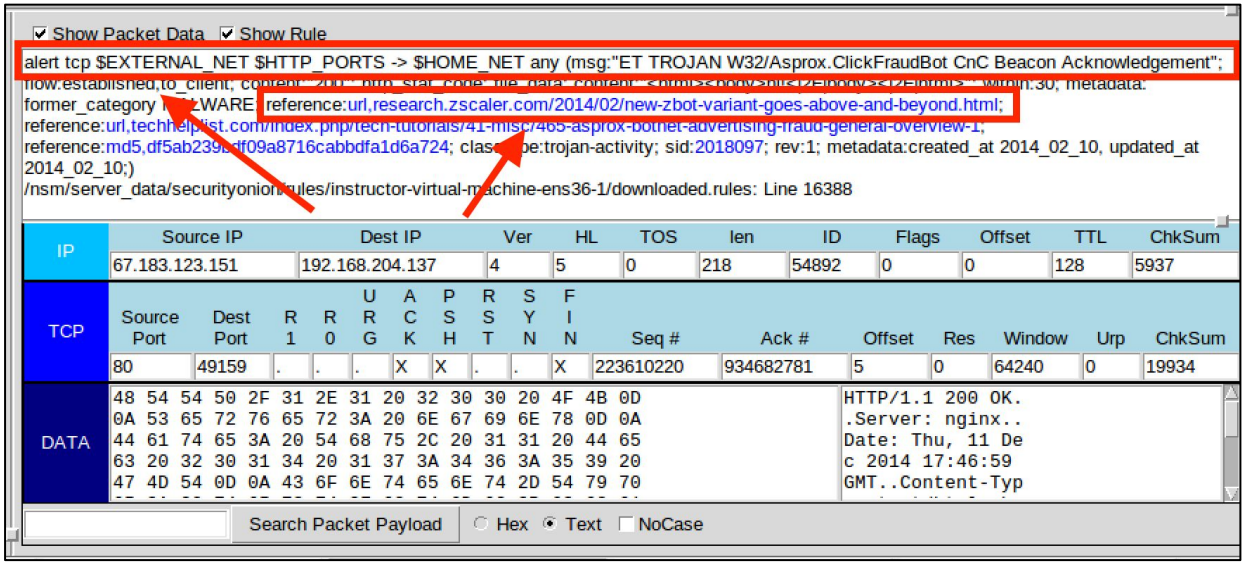
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Event Message
RT	1	instructor-virtualbox-eth1-1	3.1573	2020-03-05 19:02:50	67.18...	80	192.168.204.137	49159	ET TROJAN W32/Asprox.ClickFraudBot CnC Beac...
RT	2	instructor-virtualbox-eth1-1	3.1586	2020-03-05 19:02:50	70.32...	8080	192.168.204.137	49173	ET TROJAN W32/Asprox.ClickFraudBot CnC Beac...
RT	9	instructor-virtualbox-eth1-1	3.1598	2020-03-05 19:02:50	46.16...	80	192.168.204.137	49182	ET TROJAN Win32/Zemot Fake Search Page
RT	1	instructor-virtualbox-eth1-1	3.1608	2020-03-05 19:02:52	128.1...	80	192.168.204.137	49646	ET CURRENT_EVENTS DRIVEBY Nuclear EK La...
RT	13	instructor-virtualbox-eth1-1	3.1609	2020-03-05 19:02:52	128.1...	80	192.168.204.137	49646	ET CURRENT_EVENTS Nuclear EK Landing Jan 1...

Alert identified as a C2 beacon acknowledgement.

Command and Control (C2)

Writers of Snort rules can include a reference URL in the Snort rule option.

- Snort rules can include links to help network defenders establish TTPs regarding their attackers.
- With this information, network defenders can form mitigation strategies to help improve their security posture.



Activity: C2 Beacon

In this activity, you will establish an attacker profile that includes the TTPs used by the adversary in an emerging threat: a C2 beacon acknowledgement.

Suggested Time:

20 Minutes

Time’s Up! Let’s Review.

Questions?

Now that we've learned about the benefits of using firewalls and NSM, we'll cover the more all-encompassing enterprise security monitoring (ESM), which includes endpoint telemetry.

OSSEC

Firewalls and NSMs cannot access encrypted traffic. In most cases, malware will be transmitted from attacker to victim in an encrypted state to hide its presence and intent. This also serves as a method of obfuscation to bypass IDS detection engines.

- Malware cannot activate in the encrypted state.
- It must be decrypted before it can launch.
- This can only happen after it's been installed on the victim's machine.

This is where ESM and, more specifically, endpoint telemetry become relevant.

OSSEC

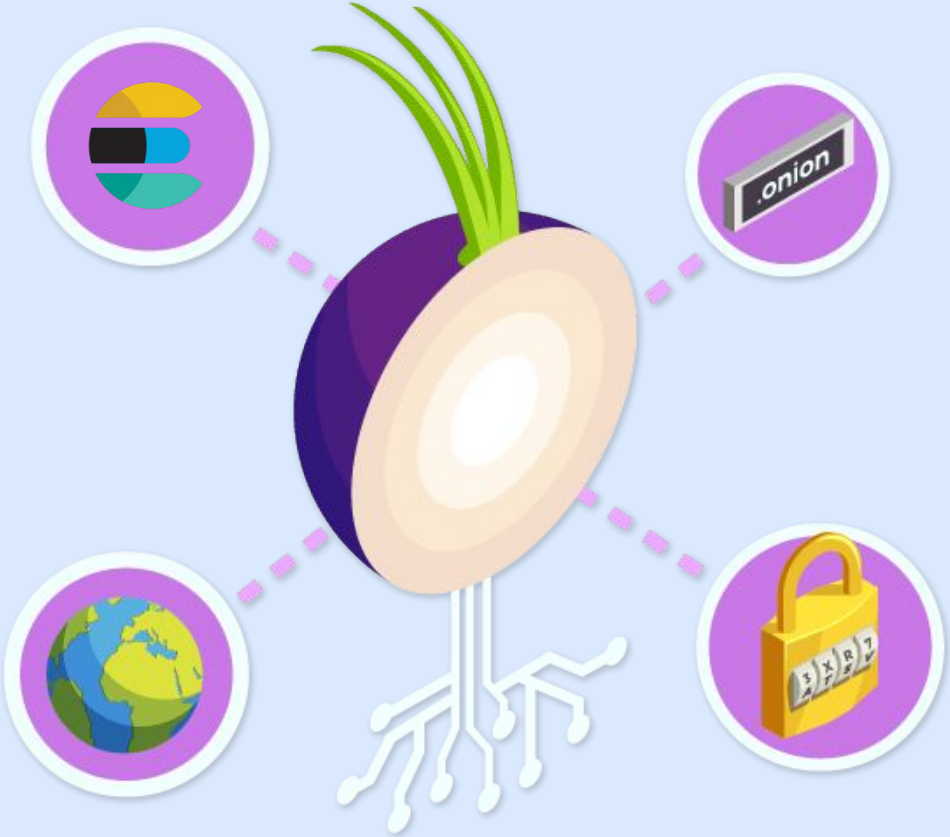
ESMs use OSSEC to provide visibility at the host level, where malware infection takes place after it's decrypted.

- OSSEC is the industry's most widely used host-based IDS (HIDS).
- It has many configuration options and can be tailored to the needs of any organization.

Endpoint telemetry is essentially a host-based monitoring of system data.

OSSEC agents are deployed to hosts and collect syslog data.

- This data generates alerts that are sent to the centralized server, Security Onion.
- Security administrators can then use Security Onion to form a detailed understanding of the situation and reconstruct a crime.



Elastic Stack

OSSEC monitors syslog data, but security admins use three other important tools to fully analyze packet captures.

(elastic.co)

Elastic Stack

These tools are collectively known as **Elastic (ELK) Stack**, the engine that operates within Security Onion.

The heart of Elastic Stack, a distributed, restful search and analytics engine capable of addressing thousands of data points seen within network traffic.

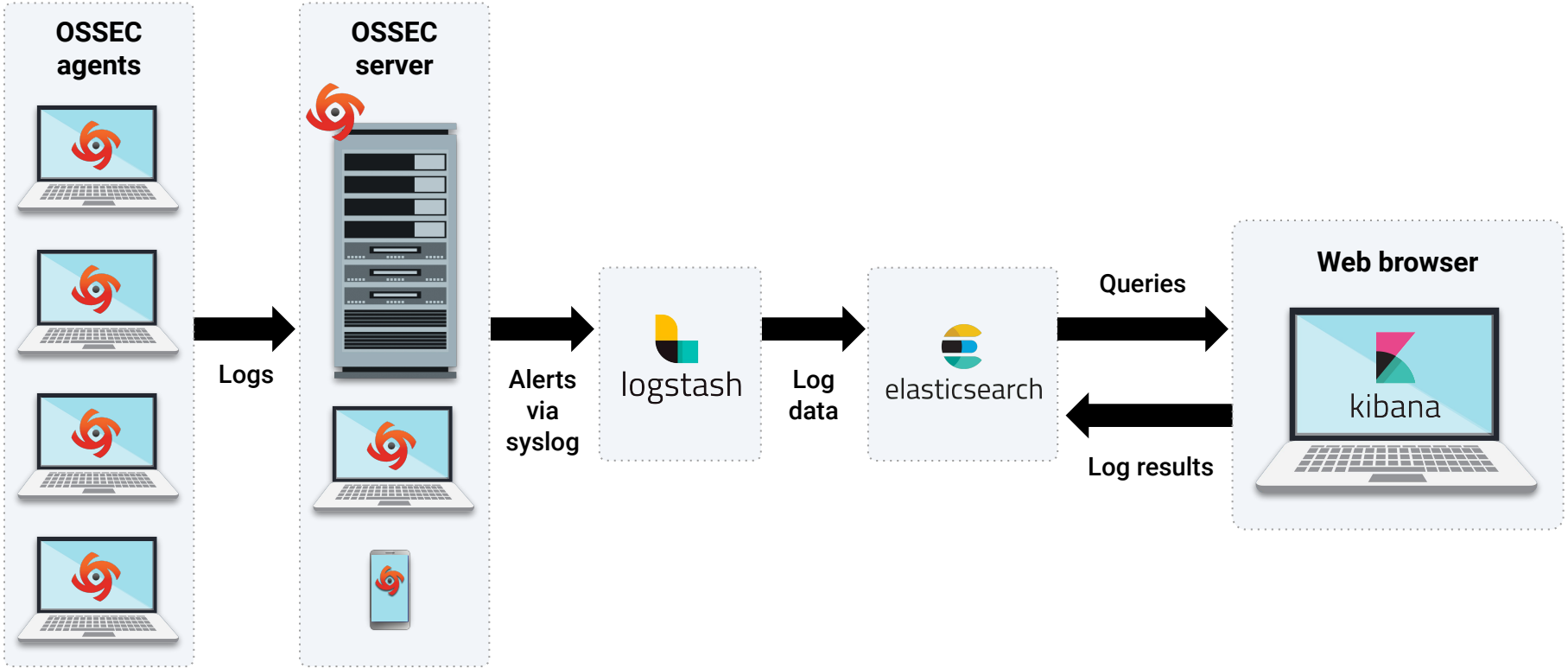
Helps security administrators locate the expected and uncover the unexpected.

Open source, server-side data processing pipeline built into Security Onion.

Ingests data from many sources at the same time by transforming it and sending it to designated log files, referred to as stashes.

A browser-based visualization interface. It uses thousands of data points from the Elastic Stack as its core engine.

Elastic Stack



Elastic Stack

01 OSSEC generates an alert.

02 OSSEC sends alert data gathered from syslog to Security Onion's OSSEC server.

03 The OSSEC-generated syslog alert is written to Logstash for storage.

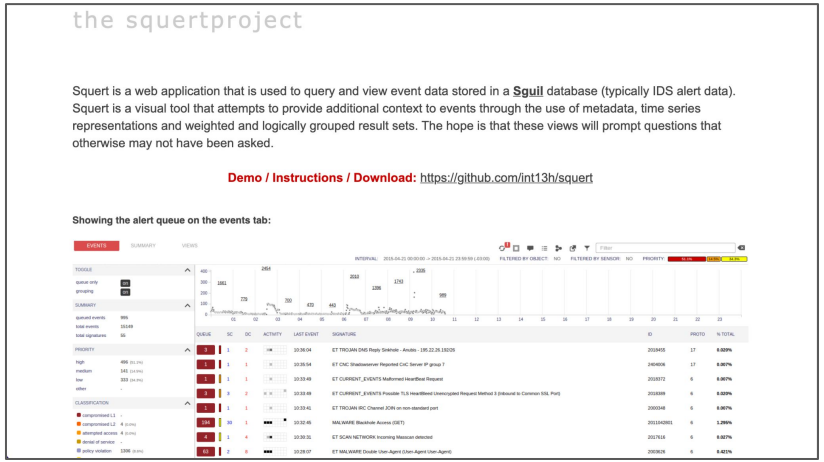
04 Log data is ingested into the Elasticsearch analytics engine, which parses hundreds of thousands of data points to prepare for data presentation.

05 Users interact with data through the Kibana web interface.

ESM Tools

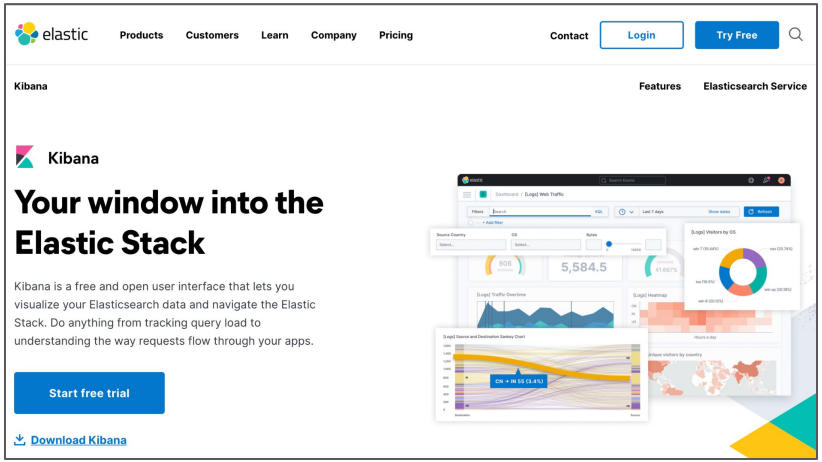
We will use these ESM tools to investigate a network security breach.

Squert



http://www.squertproject.org/

Kibana

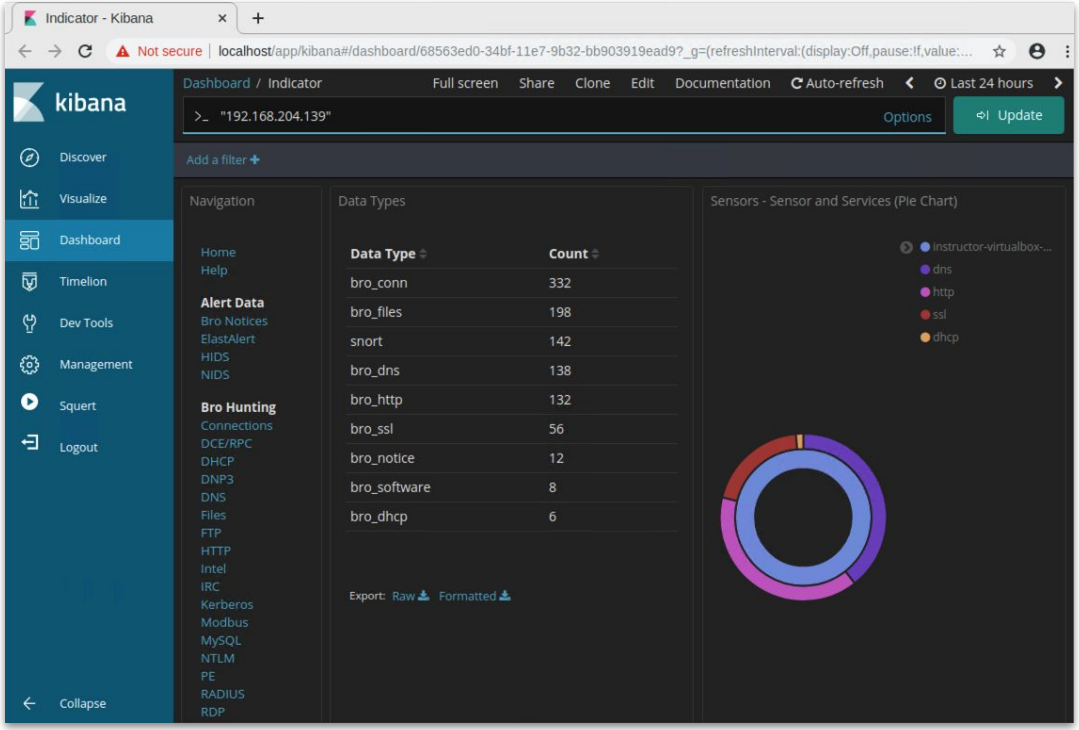


https://www.elastic.co/kibana/

Investigation, Analysis, and Escalation Demo

We'll act as a junior analyst working in a Security Operations Center.

- Junior analysts belong to a multi-tier group of analysts.
- Junior analysts typically perform the initial triage of alerts and then escalate these events to senior incident responders.



Instructor Demonstration

Investigation, Analysis, and Escalation

Demonstration Recap

In this demonstration, we conducted investigations using various threat hunting techniques. We focused on a few of the many ways to start an investigation.

ESM includes endpoint telemetry, host-based monitoring of system data that uses OSSEC collection agents to gather syslog data.

To investigate network-based IDS alerts, security administrators must use enterprise security monitoring, which includes visibility into endpoint OSSEC agents.

IDS alerts are snapshots in time. They raise questions that need answers. With the use of Security Onion, security admins can use PCAPs to reconstruct a crime.

Activity: Investigation, Analysis, and Escalation

In this activity, you will use Squert and Kibana to investigate, analyze, and escalate indicators of attack.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

Threat Hunting

Threat intelligence is important at every level of government and public sector organizations, which use it to determine acceptable risk and develop security controls that inform budgets.

Threat Intelligence: Know Thy Enemy

Understanding what motivates attacks against your organization will help you determine the security measures necessary to defend against them.

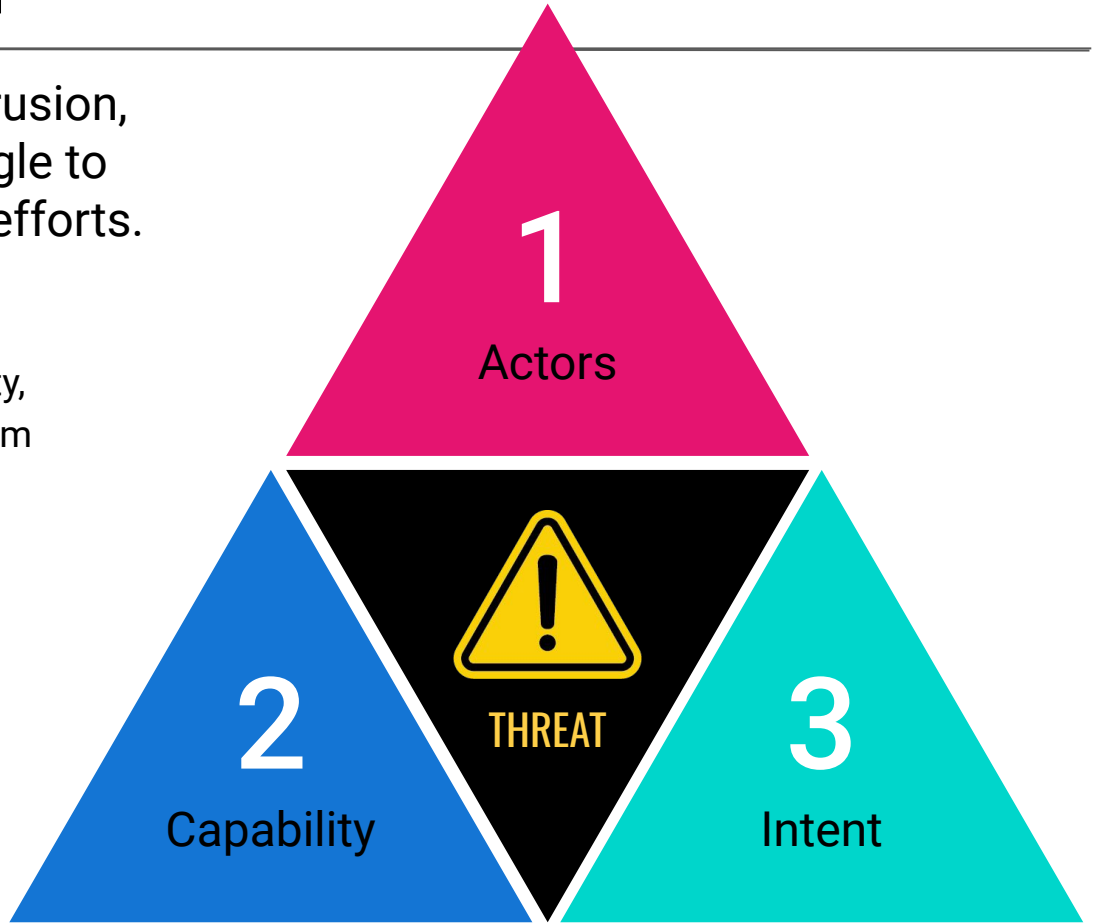
Hacktivist organizations	are politically motivated.
Criminal hackers	are financially motivated.
Cyber espionage campaigns	are typically associated with nation states; steal corporate secrets.

Computer and Incident Response Teams (CIRTs) are responsible for establishing **threat intelligence cards**, which document the TTPs used by an adversary to infiltrate a network.

Threat Intelligence Card

When handling a large-scale intrusion, incident responders often struggle to organize intelligence-gathering efforts.

- Threat intelligence cards are shared among the cyber defense community, allowing organizations to benefit from the lessons learned by others.
- The triad of actors, capability, and intent informs situationally aware decision making, enhanced network defense operations, and effective tactical assessments.



Cyber Kill Chain Framework

One aspect of that framework, called the Cyber Kill Chain, defines seven steps that an adversary must complete before being able to act on their objectives.

Advantages	Examples
Reconnaissance	Information gathering stage against targeted victim. Information sources include: DNS registration websites, LinkedIn, Facebook, Twitter, etc.
Weaponization	After collecting information regarding infrastructure and employees, adversaries have the capability to establish attack vectors and technical profiles of targets such as: logical and administrative security controls, infil/exfil points, etc.
Delivery	The delivery of the weaponized payload, via email, website, USB, etc.
Exploitation	Actively compromise adversary's applications and servers while averting the physical, logical, and administrative controls. Exploiting employees through social engineering. This stage prepares for escalation during the installation phase.
Installation	A.k.a., the persistence preparation phase. Activities include malicious software installation, backdoor implants, persistence mechanism, ie. Cron Jobs, AutoRun keys, services, log file deletion, and timestamp manipulation.
Command & Control (C2)	A command channel, most typically Internet Relay Chat (IRC) , used for remote control of a victim's computer.
Actions on Objectives	After achieving the equivalent of "Hands on Keyboard" access to a victim's systems, adversaries are now able to act their objectives.

Activity: Threat Hunting – Cyber Threat Intelligence

In this activity, you will strengthen your knowledge of concepts related to intelligence gathering and incidence response as part of the ESM process.

Use any tool you've learned to hunt for a malicious threat and create a threat intelligence card.

Suggested Time:

45 Minutes

Time’s Up! Let’s Review.

Questions?


The End