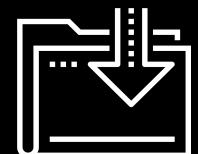




# Intrusion Detection, Snort, and Network Security Monitoring

Cybersecurity  
Network Security Day 2



# Class Objectives

---

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



Define network security monitoring (NSM) and explain its role in defense in depth.



Interpret and define Snort rules and alerts.



Explain how intrusion detection systems work and how they differ from firewalls.



Use Security Onion and its suite of NSM tools to perform network forensics.



Perform collection and analysis of indicators of attack as part of the NSM Detection stage.

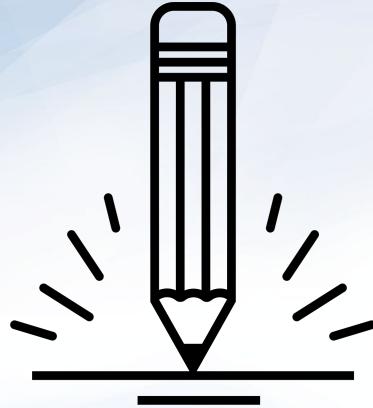


Apply knowledge of NSM, Snort rules, and Security Onion to analyze an indicator of attack and establish an attacker profile.



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



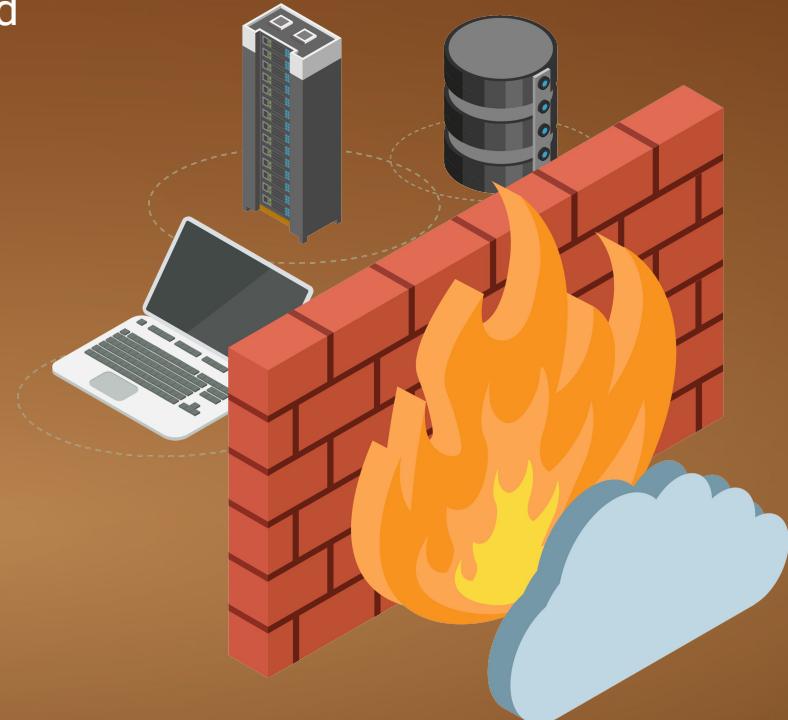
# Overview

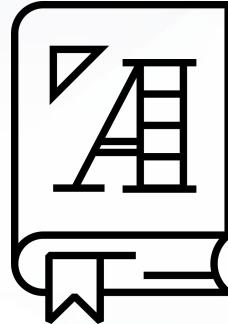
---

Firewalls protect networks by making decisions based on rules. Firewalls are designed to allow traffic from trusted sources and block traffic from untrusted sources.

- Firewalls do have limitations. They can be easily fooled through packet manipulation by clever hackers.
- 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.

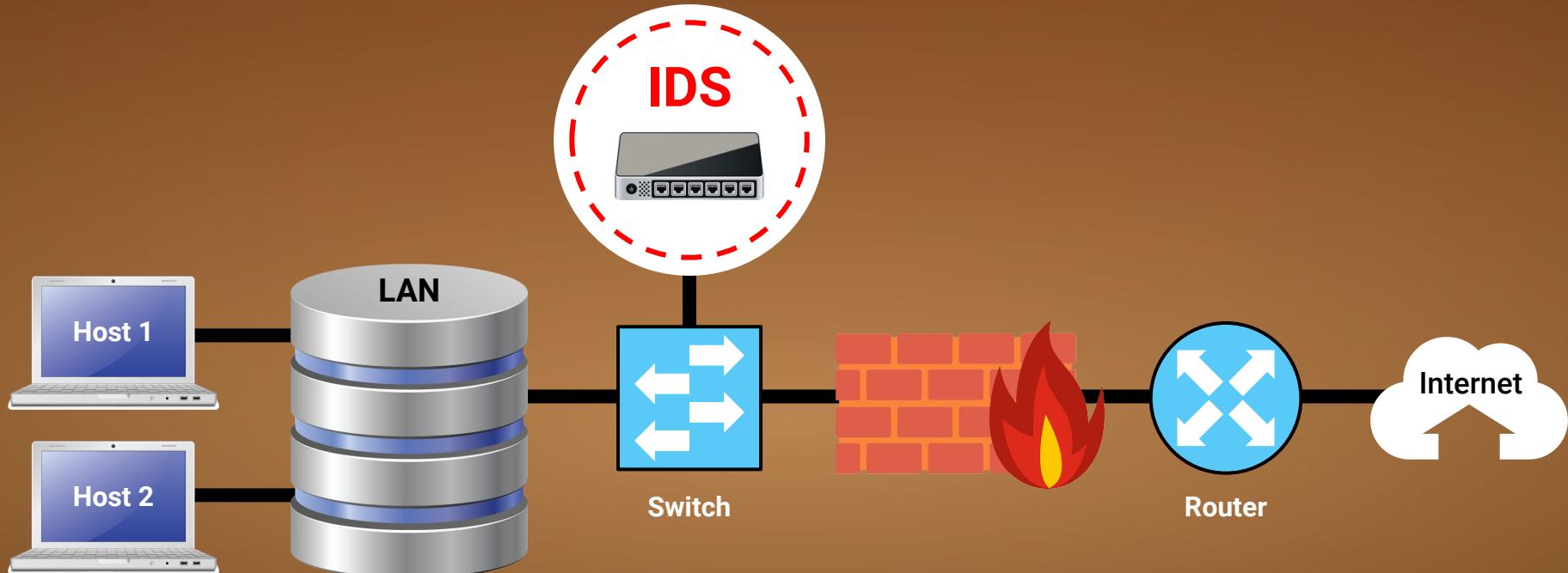




An **intrusion detection system (IDS)** both analyzes traffic and looks for malicious signatures.

# Overview: Intrusion Detection Systems

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).



# Overview: IDS and NSM

---

There are many varieties of intrusion detection systems, but today's class will focus on **Snort**, the world's most popular open-source solution.

- Network security monitoring (NSM) is the process of identifying weaknesses in a network's defense.
- It also provides organizations with situational awareness of their network.

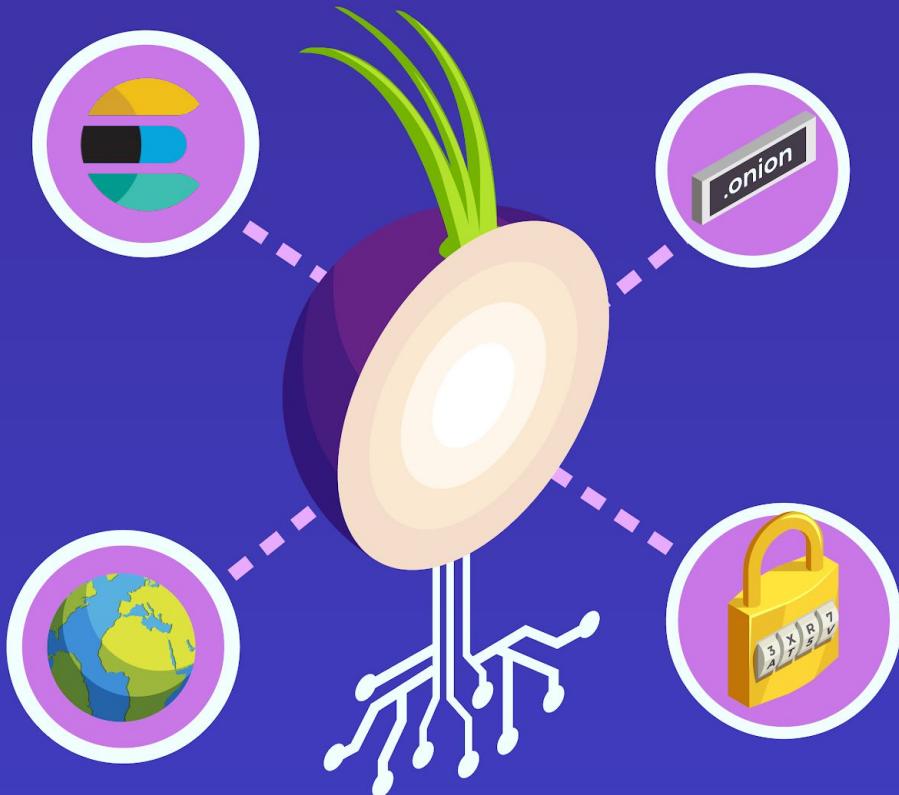


# Security Onion

---

**Security Onion** is a Linux distribution that contains many NSM tools.

Security Onion uses the Snort IDS engine as its event-driven mechanism.



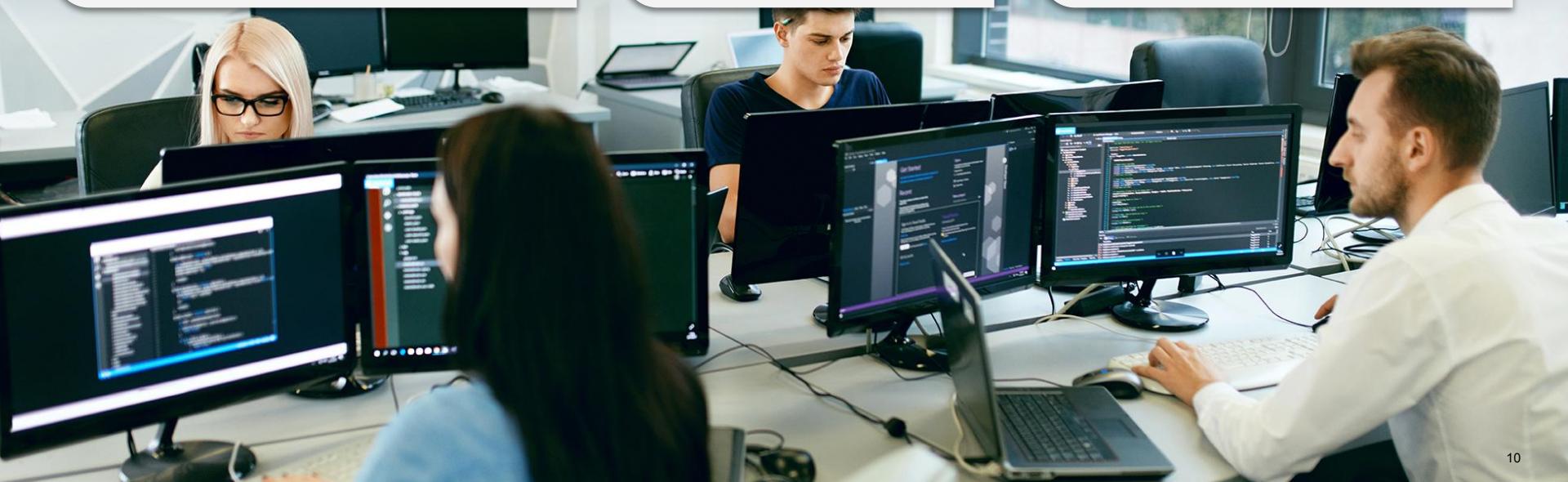
# Network Security

Knowledge of computer networking is essential for the following technical roles:

**Security analysts** are responsible for protecting all sensitive information within a company. Their main job is to analyze a company's security measures and determine how effective they are.

**SOC analysts** provide situational awareness through the detection, containment, and remediation of IT threats.

**Network forensics** capture, record and analyze network events in order to discover the source of security attacks or other incidents.

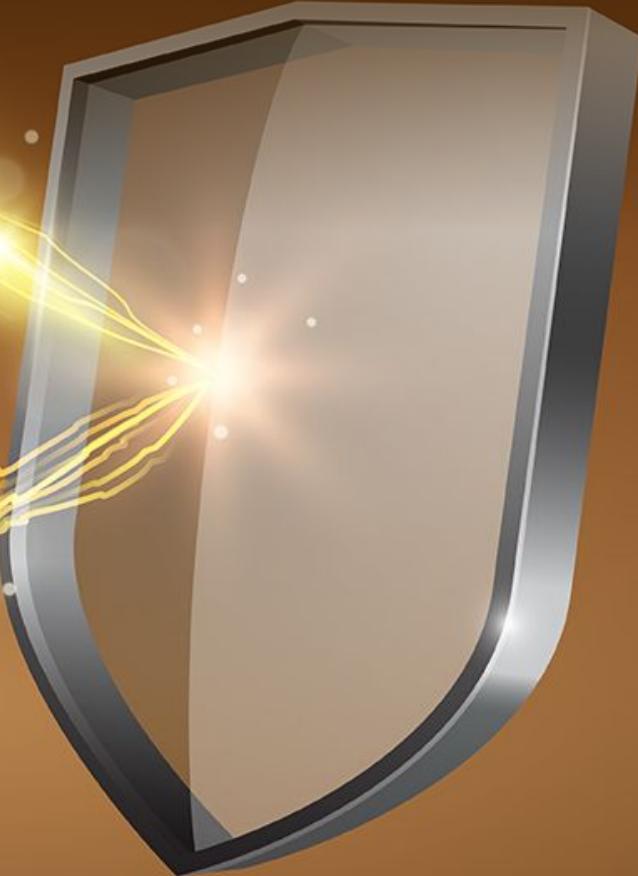


# Introduction to Intrusion Detection and Snort

# Intrusion Detection Systems

Unlike firewalls, an IDS detects and alerts of an attack.

- IDS are *passive*. They do not respond to attacks, they only log and document information for future analysis.
- IDS helps organizations enforce the cyber kill chain by establishing situational awareness of attackers, allowing them to harden defenses.



# IDS Types

---

There are two types of IDS:

01

## Signature-based IDS

A signature-based IDS compares patterns of traffic to predefined signatures.

- Good for identifying well-known attacks.
- Can be updated as new attack signatures are released.
- Vulnerable to attacks through packet manipulation.
- Unable to detect zero-day attacks.

02

## Anomaly-based IDS

An anomaly-based IDS compares patterns of traffic against a well-known baseline.

- Good for detecting suspicious traffic that deviates from well-known baselines.
- Excellent at detecting when attackers probe and sweep a network.
- Prone to false alerts.
- Assumes network behavior does not deviate from well-known baselines.

# Intrusion Detection Architecture

---

Intrusion detection systems have two basic architectures:

A large, bold, white "NIDS" text centered on a solid brown rectangular background.

NIDS

**Network intrusion detection (NIDS)**  
filters an entire subnet on a network.

A large, bold, white "HIDS" text centered on a solid brown rectangular background.

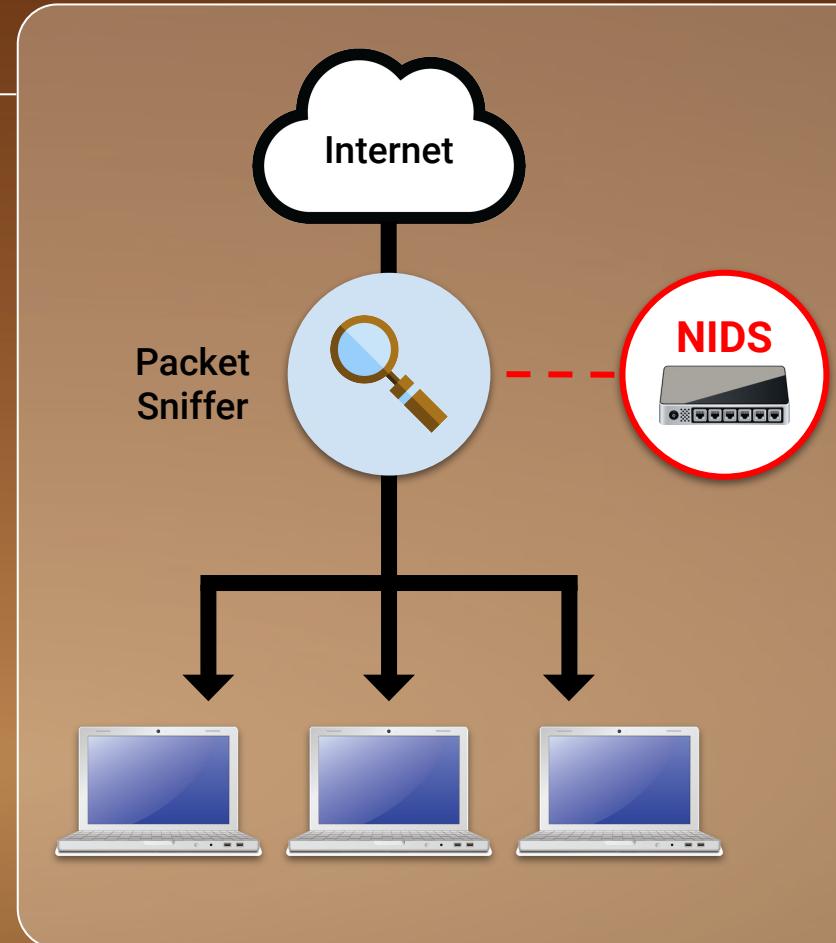
HIDS

**Host-based intrusion detection (HIDS)**  
runs locally on a host-based system  
or user's workstation or server.

# Intrusion Detection Architecture

**Network intrusion detection (NIDS)**  
filters an entire subnet on a network.

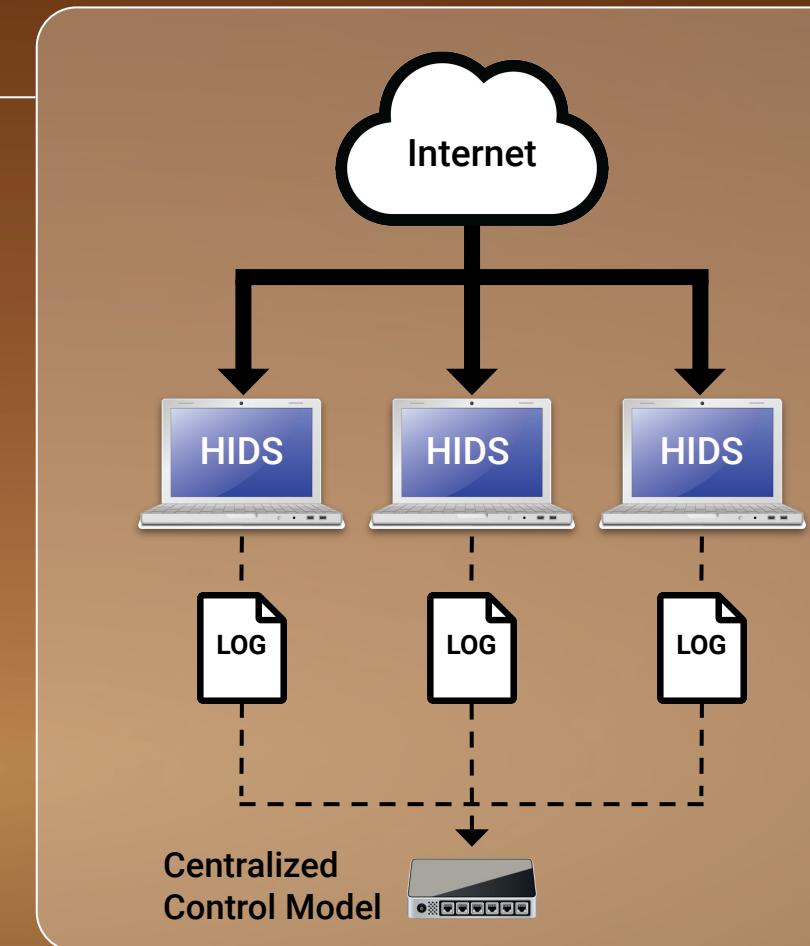
- Matches all traffic to a known library of attack signatures.
- Passively examines network traffic at points that it's deployed.
- Relatively easy to deploy and difficult to detect by attackers.



# Intrusion Detection Architecture

**Host-based intrusion detection (HIDS)** runs locally on a host based system or user's workstation or server.

- Acts as a second line of defense against malicious traffic that successfully gets past a NIDS.
- Examines entire file systems on a host, compares them to previous snapshots or baselines, and generates an alert if there are significant differences between the two.



# Intrusion Prevention System



An **Intrusion Prevention System (IPS)** can do everything an IDS can, but can **also** respond to attacks.

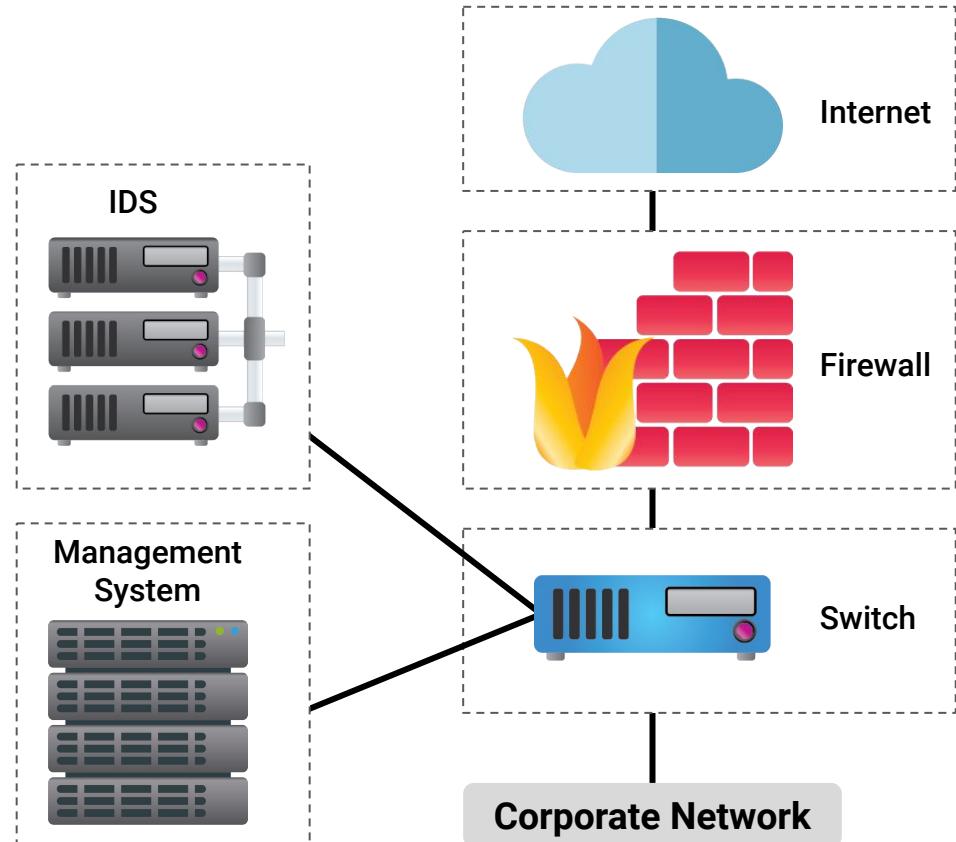
IPS can react to packets by blocking malicious traffic, preventing it from being delivered to a host on the network.

# IDS vs. IPS

IDS connects via a network tap or mirrored SPAN port.

- **Network TAP** (Test Access Port) is a hardware device that provides access to a network. Network taps transit both inbound and outbound data streams on separate channels at the same time, so all data will arrive at the monitoring device in real time.
- **SPAN** (Switched Port Analyzer), also known as **port mirroring**, sends a mirror image of all network data to another physical port, where the packets can be captured and analyzed.
- IDS requires an administrator to react to an alert by examining what was flagged.

## Intrusion Detection System (IDS)

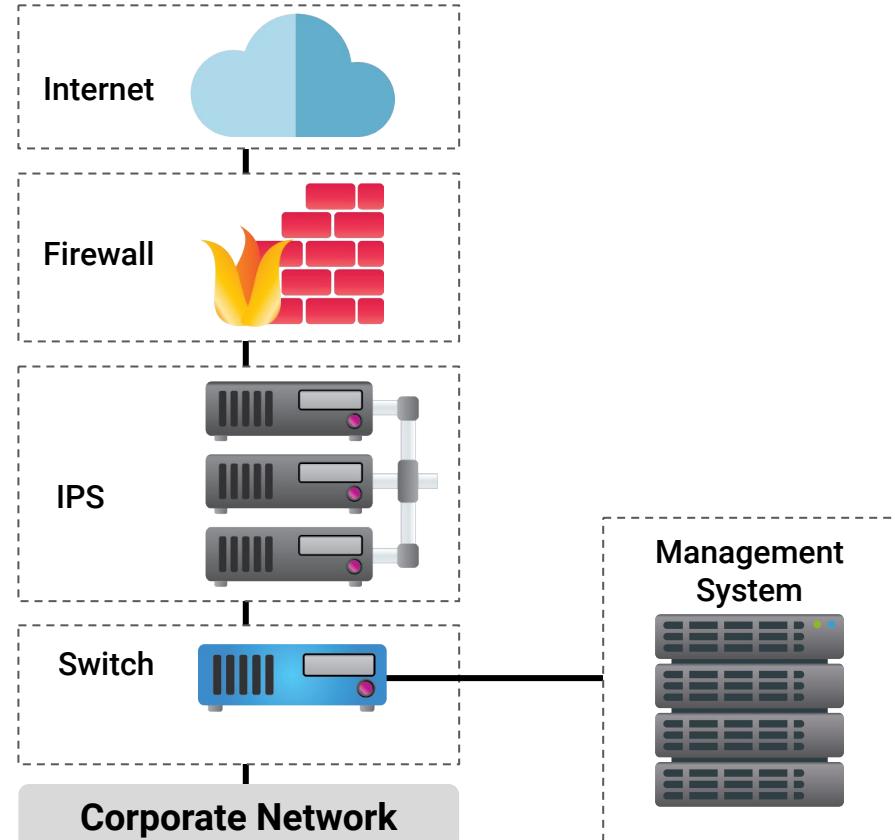


# IDS vs. IPS

IPS connects **inline** with the flow of data, typically between the firewall and network switch.

- Requires more robust hardware due to the amount of traffic flowing through it.
- IPS will automatically take action by blocking and logging a threat, thus it doesn't require administrative intervention.

## Intrusion Prevention System (IPS)



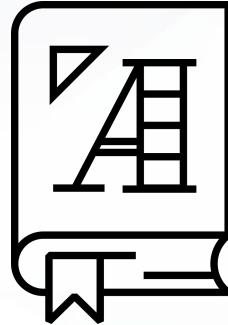
# IDS Alerts

---



An IDS system generates alerts when a **Snort rule** detects malicious traffic that matches a signature.

```
alert ip any any -> any any {msg: "IP Packet Detected";}
```



An **alert** is a message that is sent to an analyst's console as an indicator of attack (IOA).

# IDS Alerts

---

**Indicators** can be either:



# IDS Alerts

---

01

## Indicator of Attack (IOA)

Indicators of attack indicate attacks happening in real time.

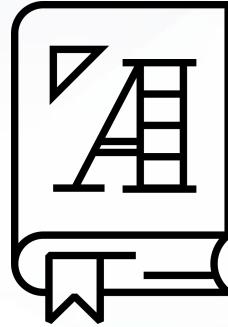
- Proactive approach to intrusion attempts.
- Indicate that an attack is currently in progress but a full breach has not been determined.
- Focus on revealing the intent and end goal of an attacker, regardless of the exploit or malware used in the attack.

02

## Indicator of Compromise (IOC)

Indicators of compromise indicate previous malicious activity.

- Indicate that an attack has occurred, resulting in a breach.
- Used to establish an adversary's techniques, tactics, and procedures (TTPs).
- Expose all the vulnerabilities used in an attack, giving network defenders the opportunity to revamp their defense as part of their mitigation strategy.



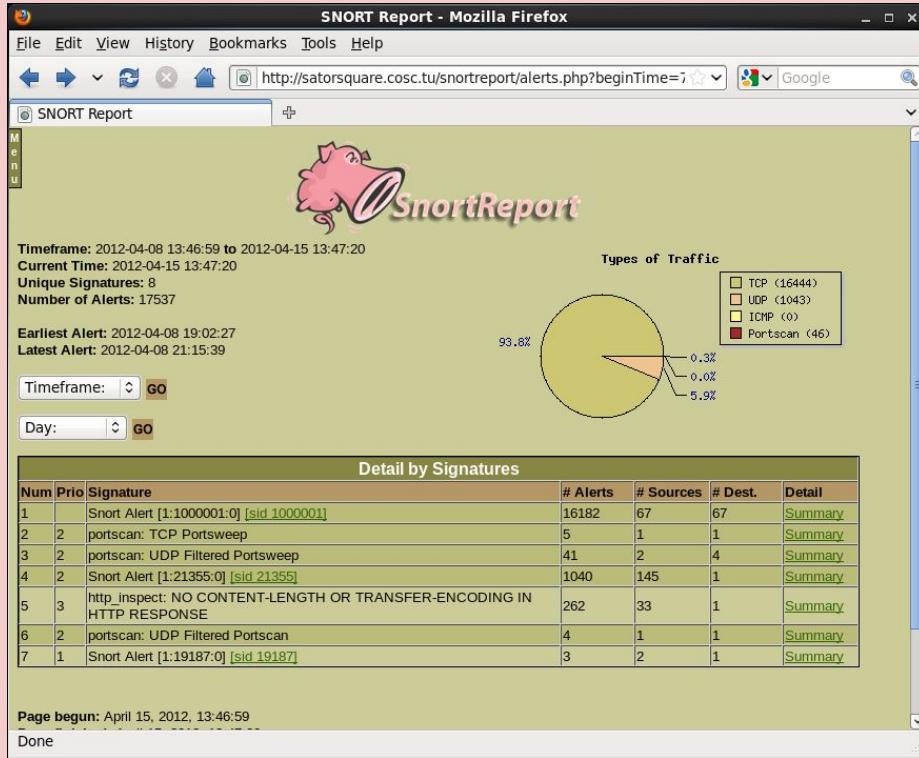
**Snort** is a free, open source  
network IDS/IPS.

# Snort

Snort can perform real-time traffic analysis and can log packets on a network.

Snort adds additional layers of defense that can be applied at various layers of the defense in depth model, including:

- Perimeter IDS and IPS architecture
- Network IDS and IPS architecture
- Host IDS and IPS architecture



# Snort Configuration Modes

---

Snort can operate in three modes:

01

## **Sniffer Mode**

Reads network packets and displays them on screen.

02

## **Packet Logger Mode**

Performs packet captures by logging all traffic to disk.

03

## **Network IDS Mode**

Monitors network traffic, analyzes it, and performs specific actions based on administratively defined rules.

# Snort Rules

Snort uses rules to detect and prevent intrusions. It operates by:



01

Reading a configuration file.

02

Loading the rules and plugins.

03

Capturing packets and monitoring traffic for patterns specified in rules.

04

When traffic matches a rule pattern, generating an alert and logging the matching packet for later inspection.

# Snort Rules

---

Rules can direct Snort to monitor the following information:

01

## OSI Layer

We can watch for IP and TCP data.

02

## Source and Destination Address

Where the traffic is flowing from and to.

03

## Byte Sequences

Patterns contained in data packets that might indicate malware, etc.

# Snort Rules

---

```
alert ip any any -> any any {msg: "IP Packet Detected";}
```

This rule logs the message **“IP Packet Detected”** when it detects an IP packet.

# Snort Rules

## Rule Header

**alert**

Action Snort will take when triggered.

**any**

Applies to packets coming from any source IP address.

**10.199.12.8**

The destination IP address.

```
alert tcp any 21 -> 10.199.12.8 any
```

**tcp**

Applies rule to all TCP packets.

**21**

Applies to packets from port 21.

## Rule Option

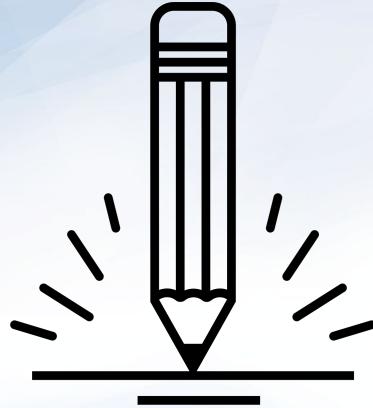
```
{msg: "TCP Packet Detected";}
```

**any**

The destination IP address.

```
{msg: "TCP Packet Detected";}
```

The message printed with the alert.



## Activity: IDS and Snort

Today, you will play the role of an SOC analyst for the California Department of Motor Vehicles (DMV).

In this activity, you will strengthen your knowledge of concepts related to Snort and intrusion detection systems.

**Suggested Time:**  
**10 Minutes**





**Time's Up! Let's Review.**

# Networking Security Monitoring and Security Onion

# Network Security Monitoring Case Study

---

On November 24, 2014, a hacker group released confidential information from Sony Pictures that contained personally identifiable information (PII) for all employees, including full names, home addresses, social security numbers, and financial information.

It was discovered that assailants had lurked on Sony's network for 17 months.

- A number of executives and upper management were fired.
- PII of all employees was exposed.
- Sony suffered massive damage to its reputation.
- Sony had to pay massive fines for violating federal regulations.



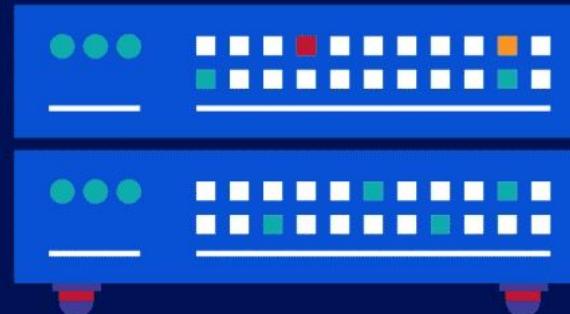


If Sony had a strong **network security monitoring** program, they would have discovered the attack much sooner—perhaps within hours—stopped it, and gotten a better understanding of the TTPs of the attacker.

# Network Security Monitoring

---

Network security monitoring  
use a variety of data analysis  
tools to detect and stop threats  
after most front-end layers are  
compromised.



# NSM Strengths

---

NSM allows organizations to:



Track adversaries through a network and determine intent.



Acquire intelligence and situational awareness.



Be proactive by identifying vulnerabilities.



Be reactive through incident response and network forensics.



Provide insights about advanced persistent threats.



Uncover and track malware.



# NSM Weaknesses

NSM has its limitations:



Cannot read encrypted traffic.



Powerful hardware and CPU requirements mean higher costs.



Difficulty reading radio transmissions, meaning attackers can use mobile radio communications to obfuscate attacks.



NSM is an invasive process that monitors and records all network data.



Placement of an NSM can be limited at certain areas of the network.



# NSM Stages and Processes

---

NSM operates in two stages, each involving two processes:

01

Detection

An alert is generated in the Squil analyst console.

02

Response

A security team responds to a security incident.

# NSM Stages and Processes

## Detection

An alert is generated in the Squil analyst console.

### Collection

The event is observed and the data is stored in the form of a PCAP file.

Host data

Net data

Application logs

Data from third party

Data from constituent

Analyst  
console(s)

### Analysis

The alert data is identified, validated, documented, and categorized according to its threat level.

IOC-centric analysis,  
or “matching”

IOC-free analysis,  
or “hunting”

Event observed/stored



Identification



Validation



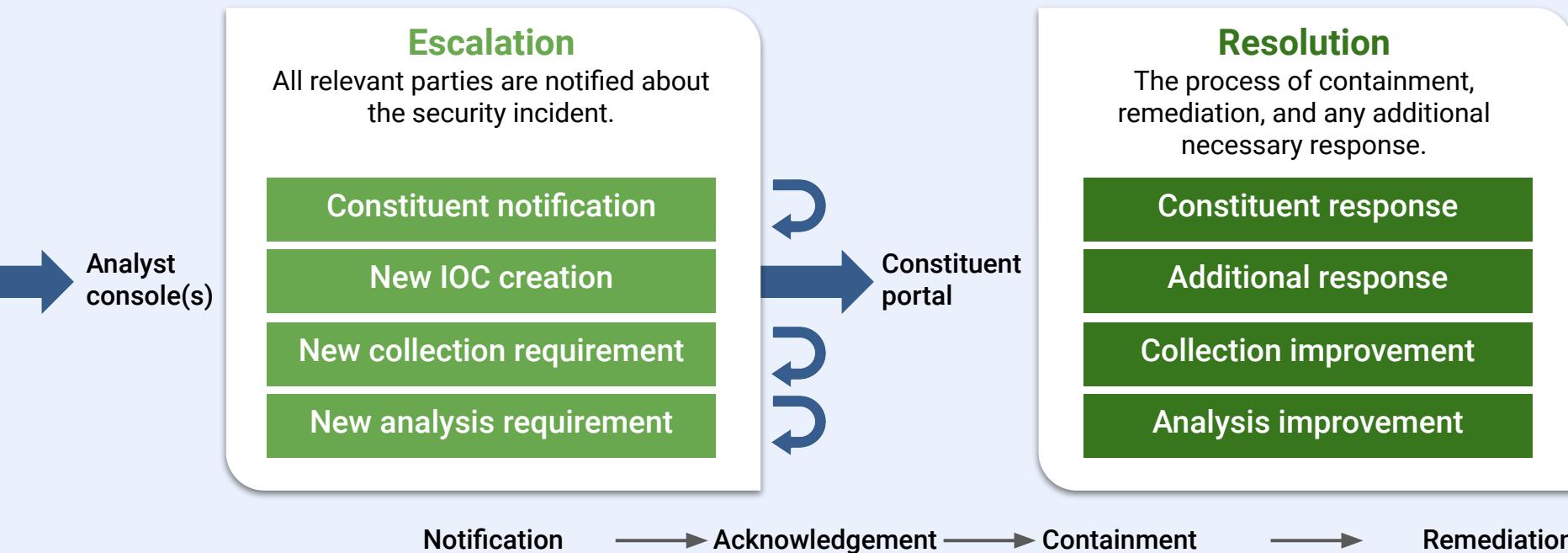
Document

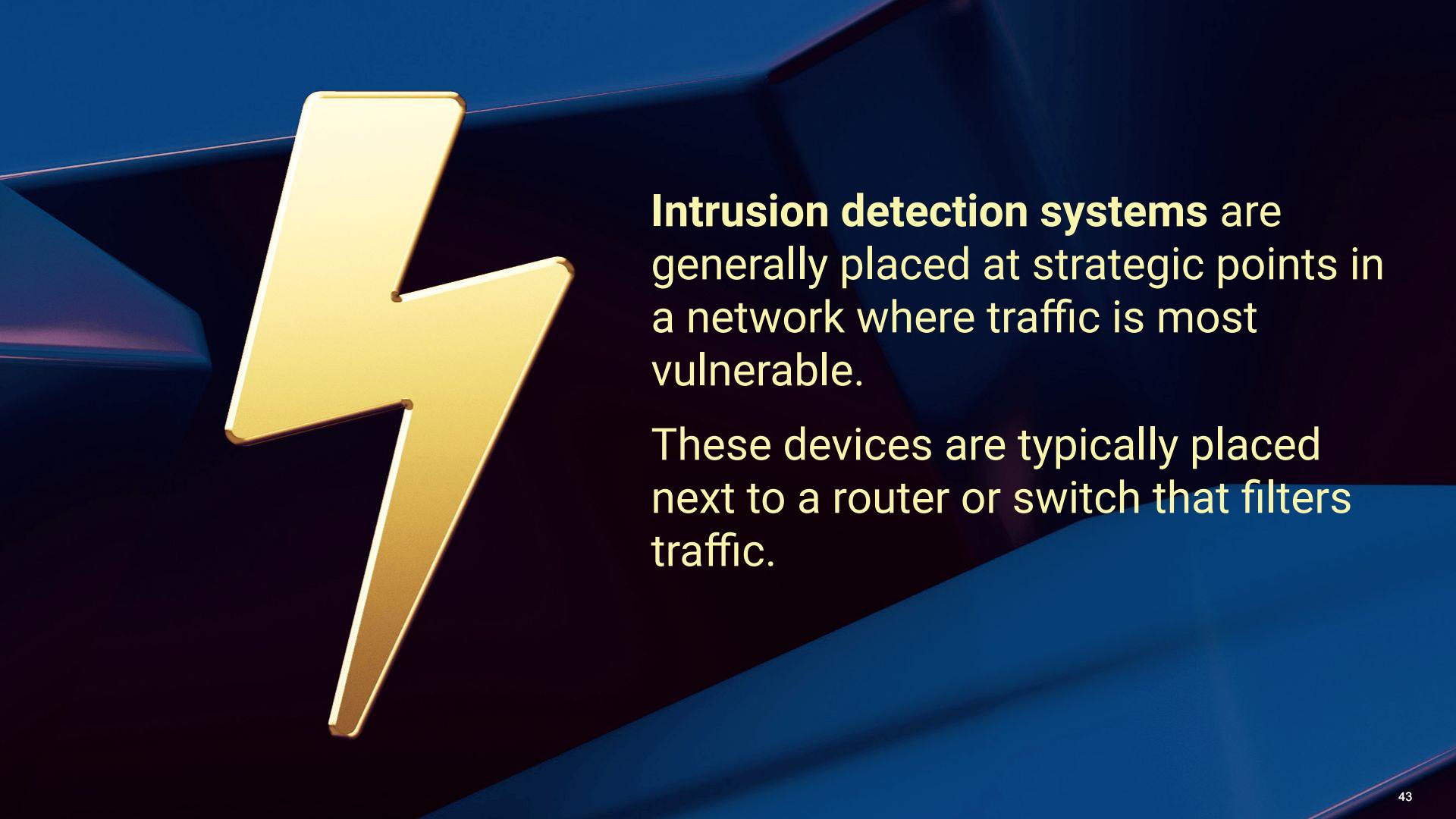
Request more data

# NSM Stages and Processes

## Response

A security team responds to a security incident.





**Intrusion detection systems** are generally placed at strategic points in a network where traffic is most vulnerable.

These devices are typically placed next to a router or switch that filters traffic.

# NSM Sensor Connectivity

---

IDS can be physically connected to a network in two ways:

01

## SPAN or Mirrored Port

A SPAN port is a function of an enterprise-level switch that allows you to mirror one or more physical switch ports to another port.

A mirror image of all data will flow across both ports equally.

02

## Network TAP

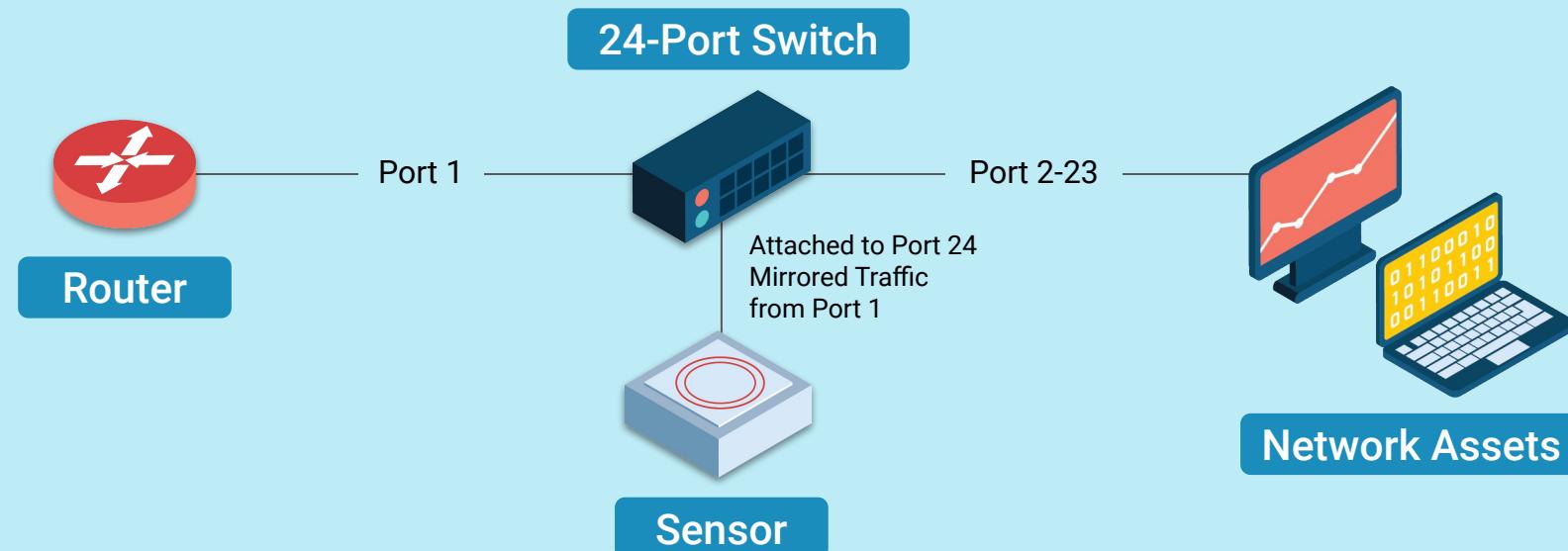
The most common type of TAP is an aggregated TAP, in which a cable connects the TAP monitor port with the NIC on the sensor. This specific placement allows traffic to be monitored between the router and switch.

# NSM Sensor Connectivity

01

## SPAN or Mirrored Port

A SPAN port is a function of an enterprise-level switch allowing you to mirror one or more physical switch ports to another port. A mirror image of all data flows across both ports equally. This allows the IDS to perform packet captures on all inbound and outbound traffic within a network.



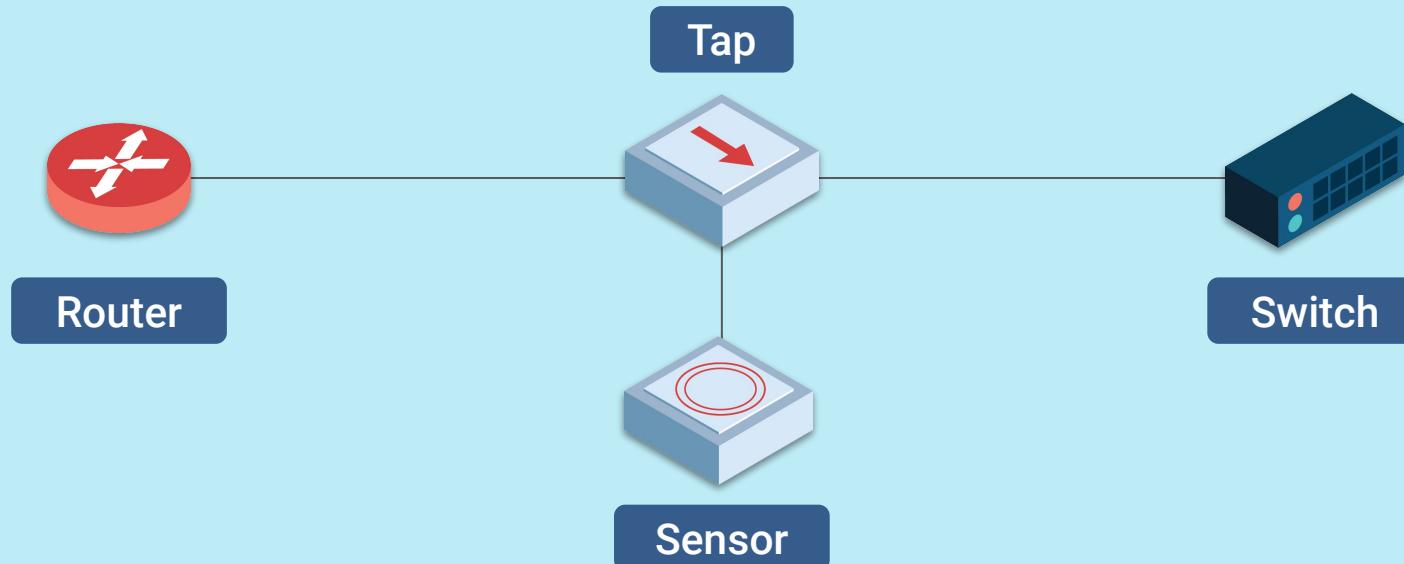
# NSM Sensor Connectivity

02

## Network Tap

The most common type of TAP

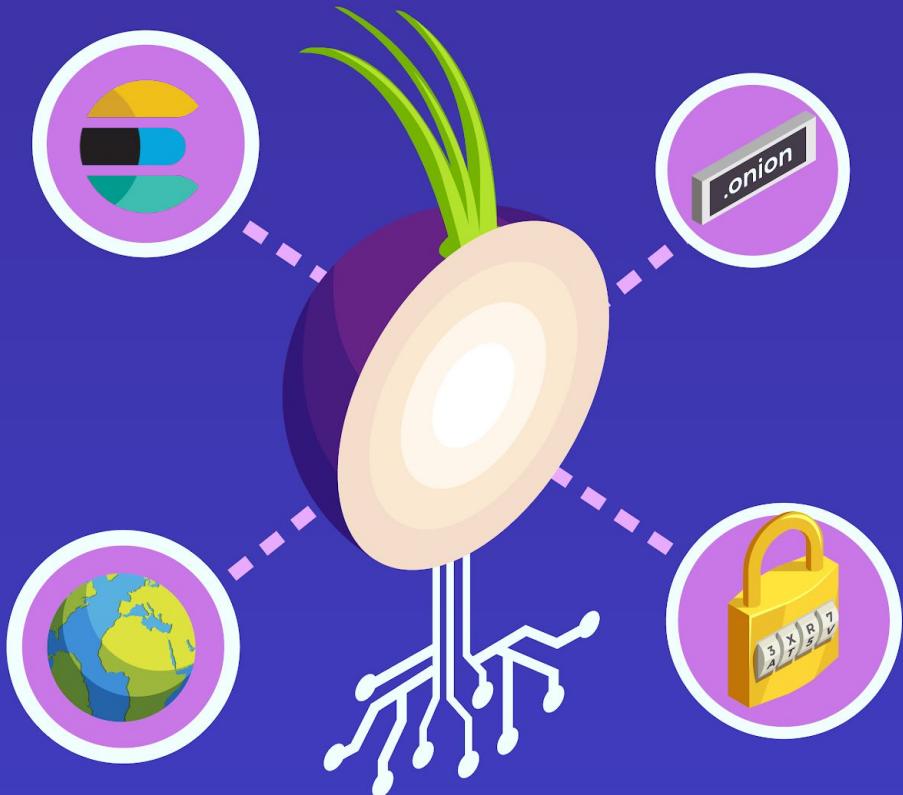
is an aggregated TAP, in which a cable connects the TAP monitor port with the NIC on the sensor. This specific placement allows traffic to be monitored between the router and switch.



# Security Onion

Today we'll work with Security Onion, a network security monitoring platform that provides context, intelligence, and situational awareness of a network.

Security Onion is an Ubuntu-based, open source Linux distribution that contains many NSM tools used to protect networks from attacks.



# Security Onion and NSM

We'll also use a few NSM tools for incident detection and response:

01

## Sguil

Pulls alert data from Snort, allowing us to more thoroughly analyze alerts.

02

## Transcript

Provides a view of PCAP transcripts that are rendered with TCP flow.

03

## NetworkMiner

Performs advanced network traffic analysis through extraction of artifacts contained in PCAP files.

# Sguil

---

Sguil has six key functions that help with analysis:

- 01      Performs simple aggregation of alert data records.
- 02      Makes available certain types of metadata.
- 03      Allows queries and review of alert data.
- 04      Allows queries and review of session data.
- 05      Allows easy transitions between alert or session data and full content data.
- 06      Counts and classifies events, enabling escalation and other incident response decisions.

# Sguil

---

Sguil has four main sections:

01

Alert Panel

02

Snort Rule

03

Packet Data

04

IP Resolution

# Sguil Alert Panel

SGUIL-0.9.0 - Connected To localhost										
RealTime Events   Escalated Events										
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	337	instructor-virtualbox-ossec	1.1	2019-08-10 17:55:30	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] File added to the system.
RT	449	instructor-virtualbox-ossec	1.2	2019-08-10 17:55:30	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity checksum changed.
RT	3	instructor-virtualbox-ossec	1.3	2019-08-10 17:55:31	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Interface entered in promiscuous(sniffing) mode.
RT	2	instructor-virtualbox-ossec	1.86	2019-08-10 17:55:46	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Host-based anomaly detection event (rootcheck).
RT	7	instructor-virtualbox-ossec	1.87	2019-08-10 17:55:55	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New group added to the system
RT	7	instructor-virtualbox-ossec	1.89	2019-08-10 17:55:55	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New user added to the system
RT	9	instructor-virtualbox-ossec	1.101	2019-08-10 17:58:31	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Dpkg (Debian Package) half configured.
RT	5	instructor-virtualbox-ossec	1.105	2019-08-10 17:58:39	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New dpkg (Debian Package) installed.
RT	15	instructor-virtualbox-ossec	1.115	2019-08-10 18:04:53	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
RT	1	instructor-virtualbox-ossec	1.116	2019-08-10 18:04:53	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!
RT	3	instructor-virtualbox-emp0s3-1	3.1	2019-08-10 18:07:40	217.160.0.187	80	10.0.2.15	49664	6	GPL ATTACK_RESPONSE id check returned root

<b>ST or Status</b>	Colors indicate severity levels of real-time"or "RT" events.  Red Critical, possible data breach in progress. Must be resolved immediately. Orange Moderate, high potential for data breach. Requires immediate review. Yellow General, low potential for data breach. Requires review.
<b>Alert ID</b>	A randomly generated numerical ID created by Sguil.
<b>Source IP</b>	IP address of the source identified by the alert.
<b>Event Message</b>	The message generated by the Snort rule option.

# Sguil Snort Rule and Packet Data

The screenshot shows the Sguil interface with two main sections: 'Snort Rule' at the top and 'Packet Data' below it.

**Snort Rule:** This section displays the Snort rule that triggered the alert. The rule is:

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_23);
```

**Packet Data:** This section shows a detailed view of the network traffic. It includes:

- Header:** Shows the IP, TCP, and DATA headers for the selected packet. The TCP header is highlighted with a red box.
- Payload:** The raw hex and ASCII data of the packet payload. A red box highlights the ASCII output, which contains an HTTP response.
- Event Message:** The text "SNORT ALERT" is displayed above the payload area.
- HTTP Response:** The ASCII output shows an HTTP/1.1 200 OK response with various headers. A red box highlights the "Content-Type: text/html" header.

## Snort Rule

In the top portion of this window is the Snort NIDS engine that generated alert data when traffic matched one of its rules.

- Alert data is an indicator of attack. An analyst may have to determine if it represents benign or malicious activity.
- Alert data from the Snort NIDS stores entries in the Event Messages column that begin with text like "ET" (for Emerging Threats, an IDS rule source).

## Packet Data

The lower, more colorful part of this window is the portion of Sguil that performs network packet analysis.

- The packet analyzer presents a detailed view of the data capture that includes packet header information and data streams presented in hex and text form.

# Sguil's IP Resolution

This section of Sguil's analyst console provides reverse DNS lookup information.

- This information is used to reveal identifying information about the attacker, including domain name registries and IP addresses.
- Other information may include country of origin, and possibly the names, email addresses, and/or phone numbers of the DNS registrants.

The screenshot shows the Sguil IP Resolution interface. At the top, there are tabs for IP Resolution, Agent Status, Snort Statistics, System Msgs, and User Msgs. The IP Resolution tab is selected. Below the tabs, there are two checked checkboxes: Reverse DNS and Enable External DNS. The main area contains four input fields: Src IP (217.160.0.187), Src Name (217-160-0-187.elastic-ssl.ui-r.com), Dst IP (10.0.2.15), and Dst Name (Unknown). A red arrow points from the Src Name field down to the Whois Query section. Another red arrow points from the Dst IP field down to the detailed WHOIS results. The Whois Query section has three radio button options: None (unchecked), Src IP (checked), and Dst IP (unchecked). The detailed WHOIS results for the IP 217.160.0.187 are as follows:

inetnum:	217.160.0.0 - 217.160.1.255
netname:	SCHLUND-CUSTOMERS
descr:	1&1 Internet AG
country:	DE
admin-c:	IPAD-RIPE
tech-c:	IPOP-RIPE
remarks:	INFRA-AW
remarks:	in case of abuse or spam, please mailto: abuse@oneandone.net
status:	ASSIGNED PA
mnt-by:	AS8560-MNT
created:	2015-09-14T12:43:21Z
last-modified:	2015-09-14T12:43:21Z
source:	RIPE # Filtered
role:	IP Administration
address:	1&1 Internet SE
admin-c:	RME9-RIPE
admin-c:	JR2342-RIPE
tech-c:	RME9-RIPE
tech-c:	JR2342-RIPE
nic-hdl:	IPAD-RIPE



## **Activity:** Security Onion and NSM

In this activity, you will reinforce your knowledge of Security Onion and network security monitoring.

**Suggested Time:**  
**10 Minutes**





**Time's Up! Let's Review.**



Countdown timer

15:00

(with alarm)

Break



# Alert: FTP File Extraction

# Security Onion Demo Setup

---

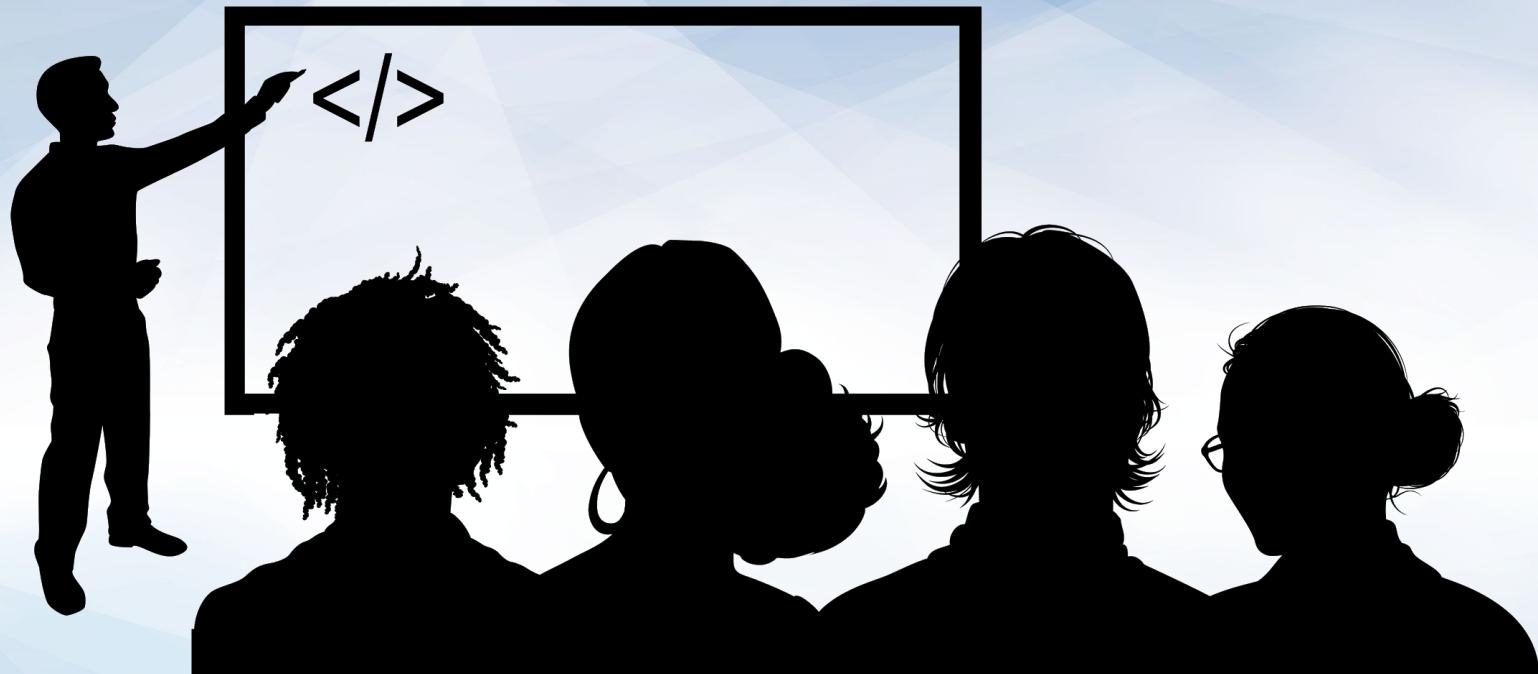
Sometimes, an alert requires an analyst to do some data mining.

- A security analyst must have a thorough understanding of how NSM tools are integrated.
- These skills help speed up incident and response efforts.





In the next walkthrough,  
we'll use Sguil as the starting  
point for learning other NSM  
tools for security  
investigations.



Instructor Demonstration  
Security Onion - Sguil

# Security Onion and NetworkMiner Demo

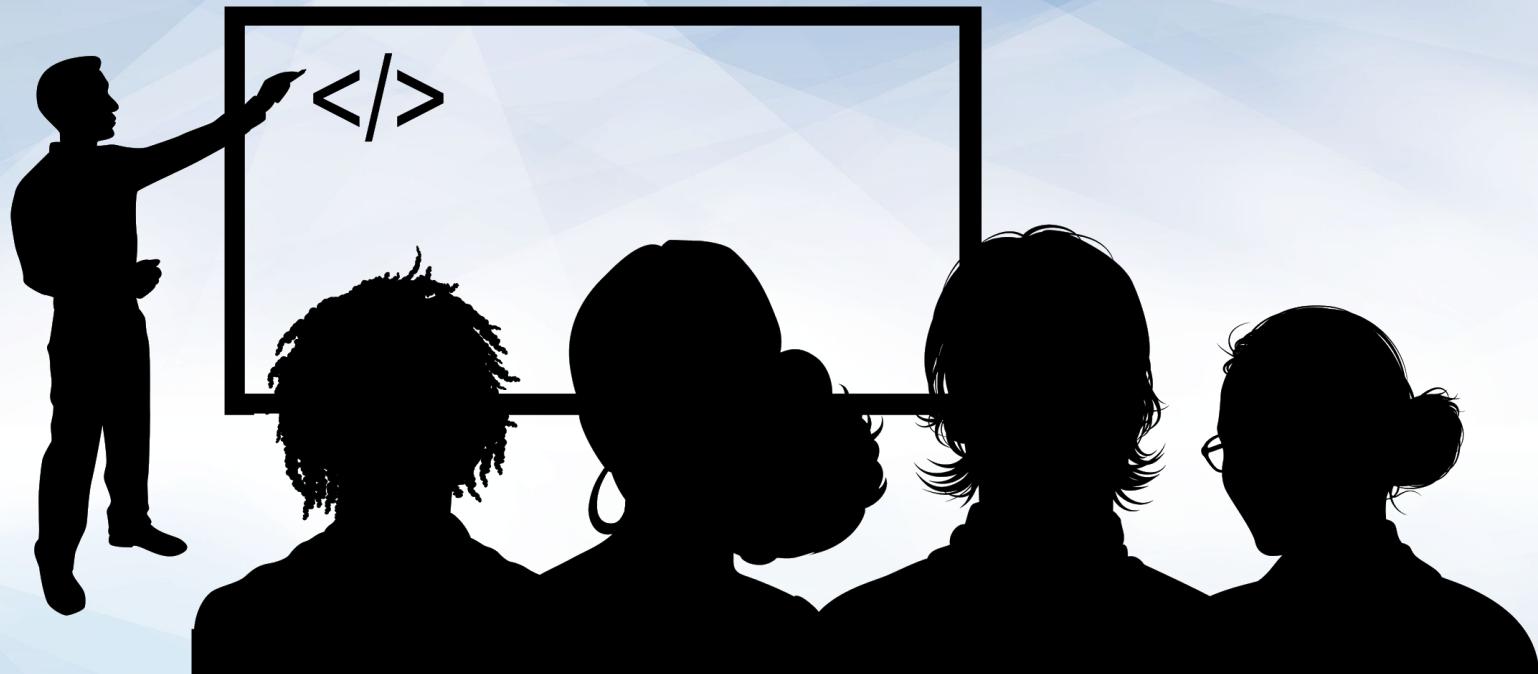
---

Now that we now know there was a drive-by attack, we must search for any files that were downloaded to the host.

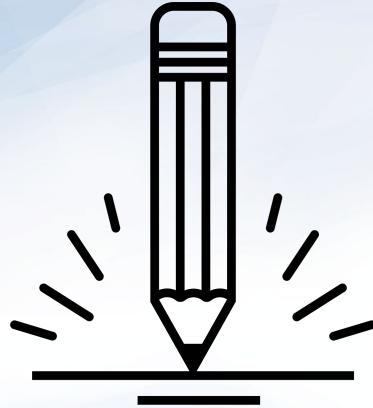
We'll use a forensics tool called **NetworkMiner** to extract any files that were installed on the user's machine, and put together an attacker profile.

- Network Miner is an NSM tool that performs advanced Network Traffic Analysis (NTA) of extracted artifacts, presented through an intuitive interface.





Instructor Demonstration  
Security Onion - NetworkMiner



## **Activity: Alert - FTP File Extraction**

In this activity, you will examine an alert to determine if any systems were breached and if any data was supplanted or exfiltrated from the network.

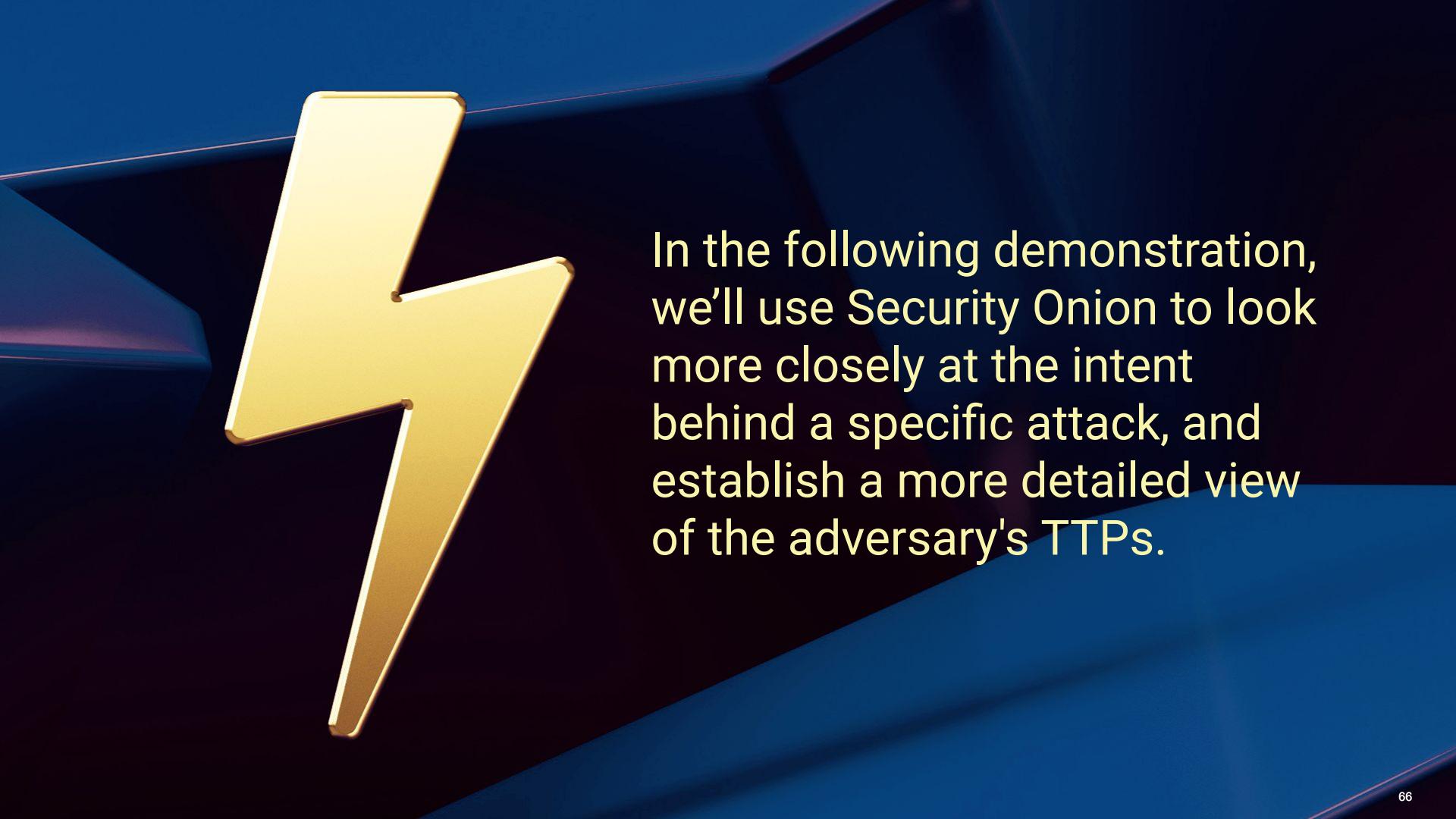
**Suggested Time:**  
**10 Minutes**



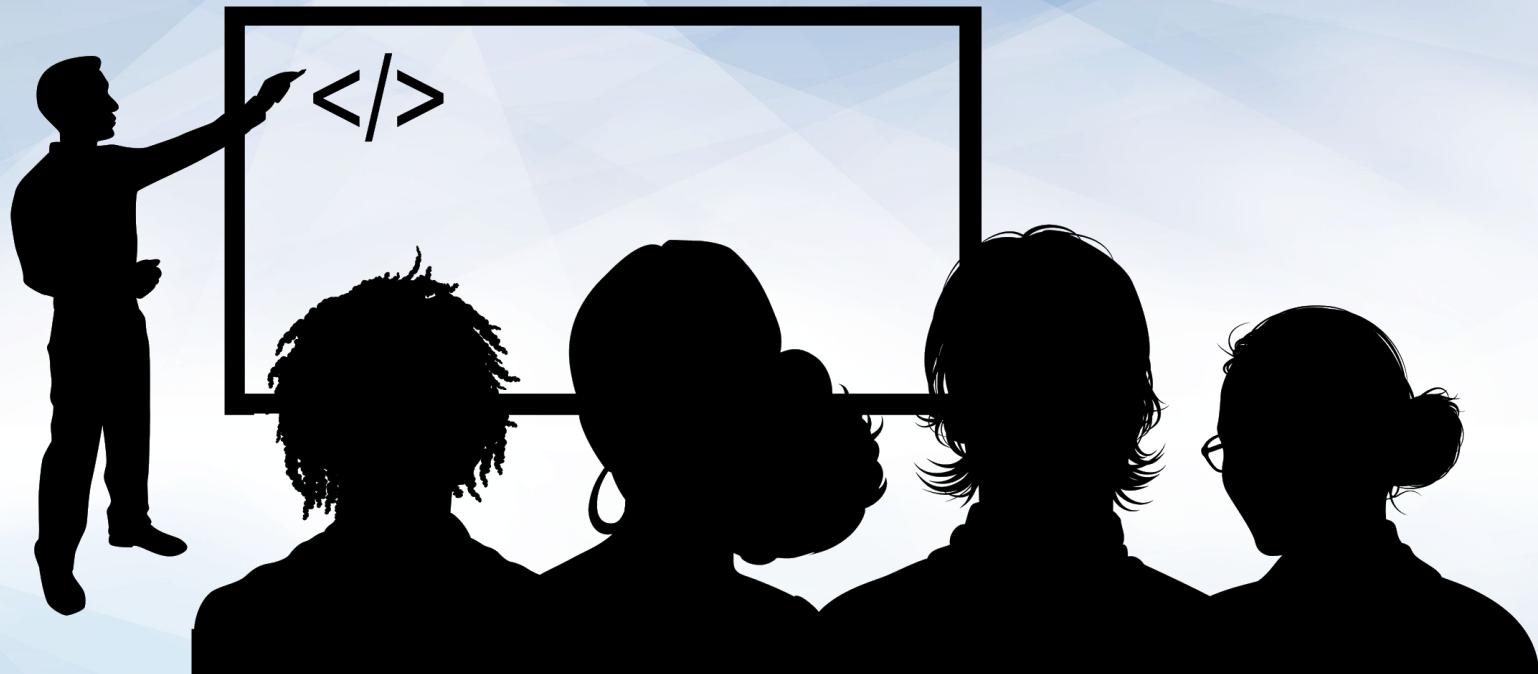


**Time's Up! Let's Review.**

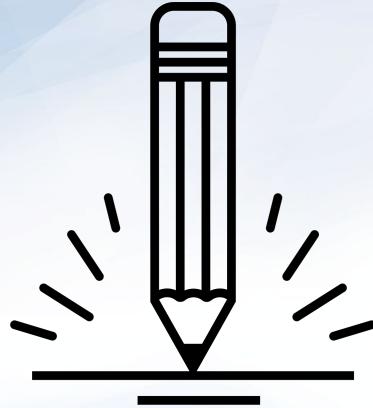
# Alert: ET INFO Executable Download



In the following demonstration, we'll use Security Onion to look more closely at the intent behind a specific attack, and establish a more detailed view of the adversary's TTPs.



Instructor Demonstration  
Security Onion - NetworkMiner



## **Activity:** Alert - ET INFO Executable Download

In this activity, you'll discover the intent of an attack and prepare a report that includes the attacker's TTPs.

**Suggested Time:**  
**10 Minutes**



# Questions?

*The  
End*