

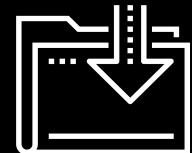


# Intrusion Detection, Snort, and Network Security Monitoring

Cybersecurity

---

Network Security Day 2



# Class Objectives

---

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



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 network security monitoring tools to trace the path of network attacks.



Collect and analyze indicators of attack and indicators of compromise using NSM tools.



Apply knowledge of NSM, Snort rules, and Security Onion to establish situational awareness within a network.

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?

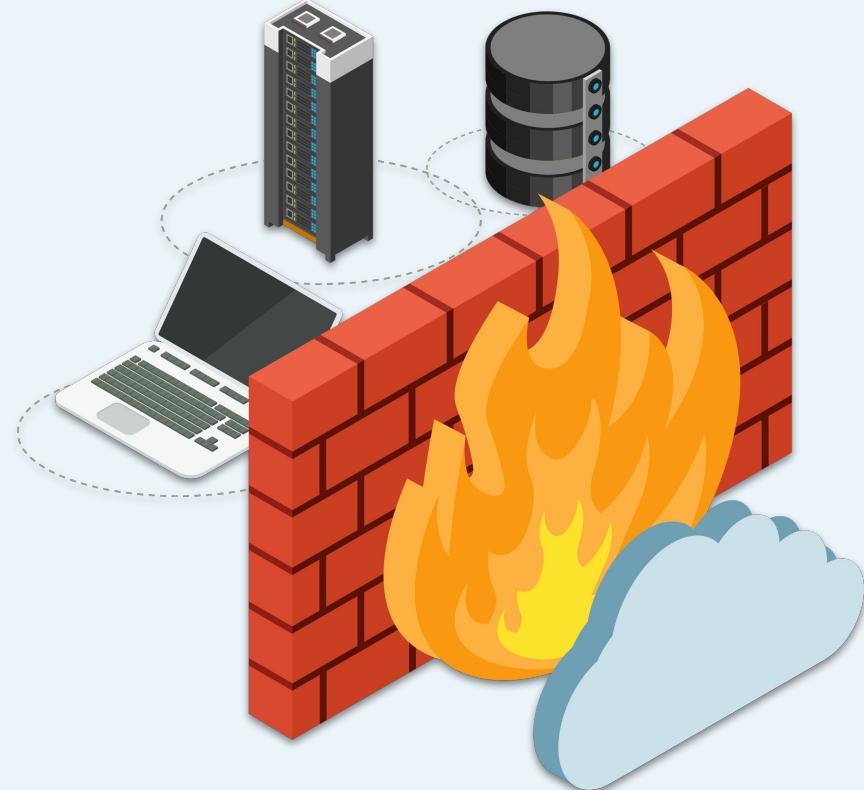


# Network Security Recap

---

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 easily 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.



# Today's Class

---

We will build upon the defense in depth methodology by using **intrusion detection systems (IDS)**.

We will learn how to use **network security monitoring (NSM)** and the **Snort IDS engine** to:



Analyze indicators of attack (IOA) and indicators of compromise (IOC).



Perform network forensics.



Acquire intelligence and situational awareness of our networks.

# Today's Class

---

## First half of the day

### We will:

- Introduce intrusion detection and prevention systems.
- Learn how to physically interconnect IDS systems and how to read, write, and interpret Snort rules.

## Second half of the day

### We will:

Introduce Security Onion and the role NSM tools play in network security.

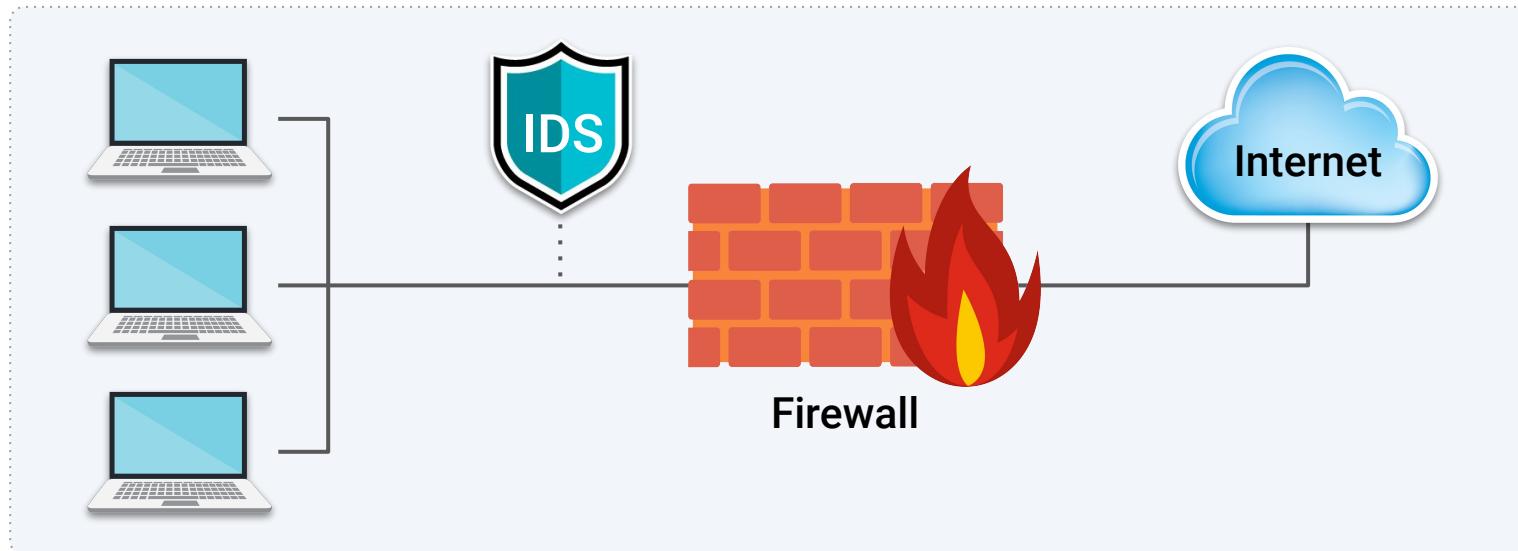
# Introduction to Intrusion Detection and Snort

**Intrusion detection systems (IDS)** are tools that can both analyze traffic and look for malicious signatures.

# Intrusion Detection Systems

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

- An IDS is **passive**.
- It does not respond to attacks, it only logs and documents information for future analysis.
- It helps organizations establish situational awareness of attackers, allowing them to harden defenses.



# IDS Types

---

There are two types of IDS:

01

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

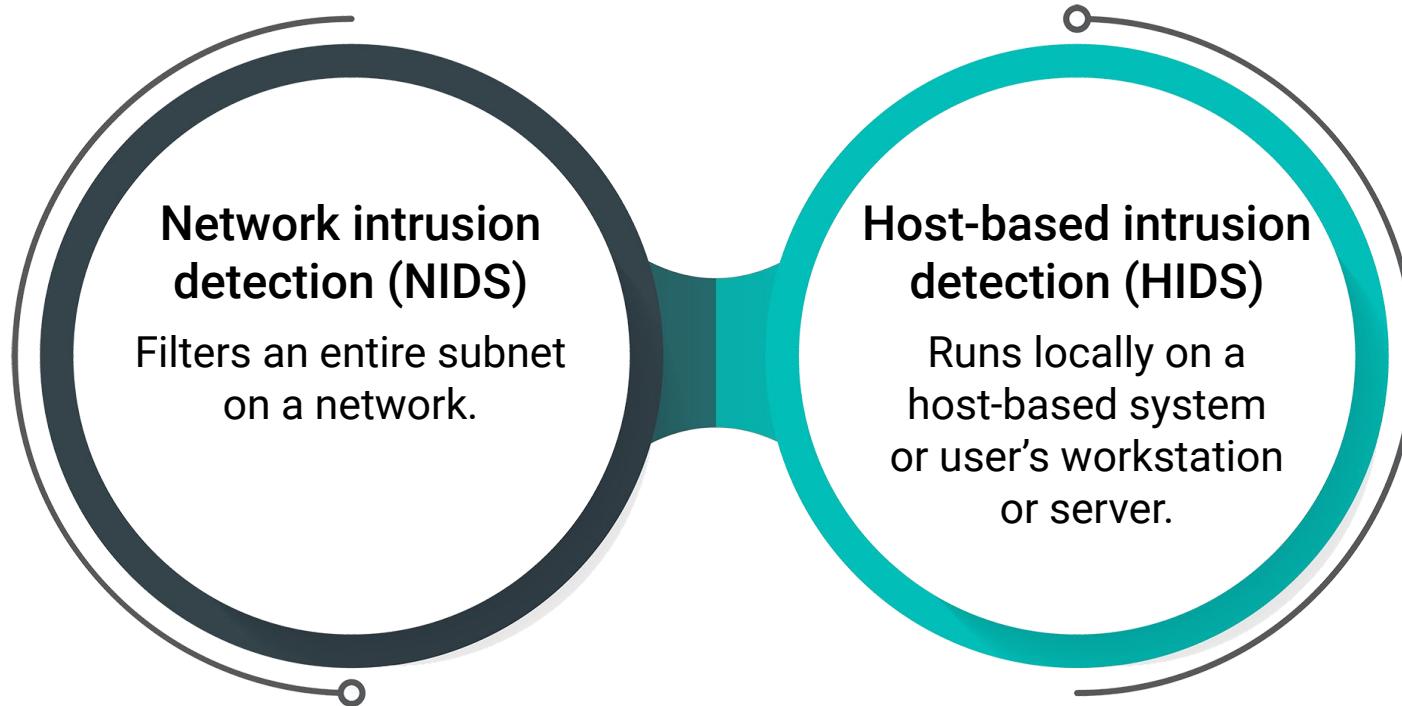
**Compares patterns of traffic against a well-known baseline.**

- 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

---

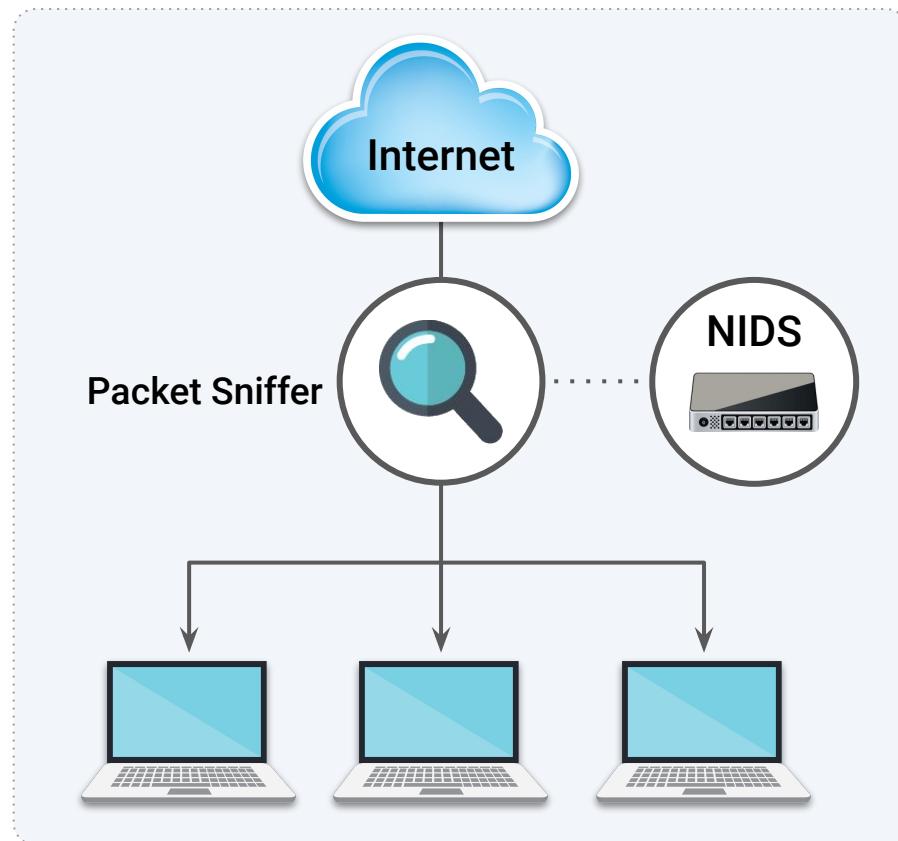
Intrusion detection systems have two basic architectures:



# Intrusion Detection Architecture

**NIDS** filters an entire subnet on a network.

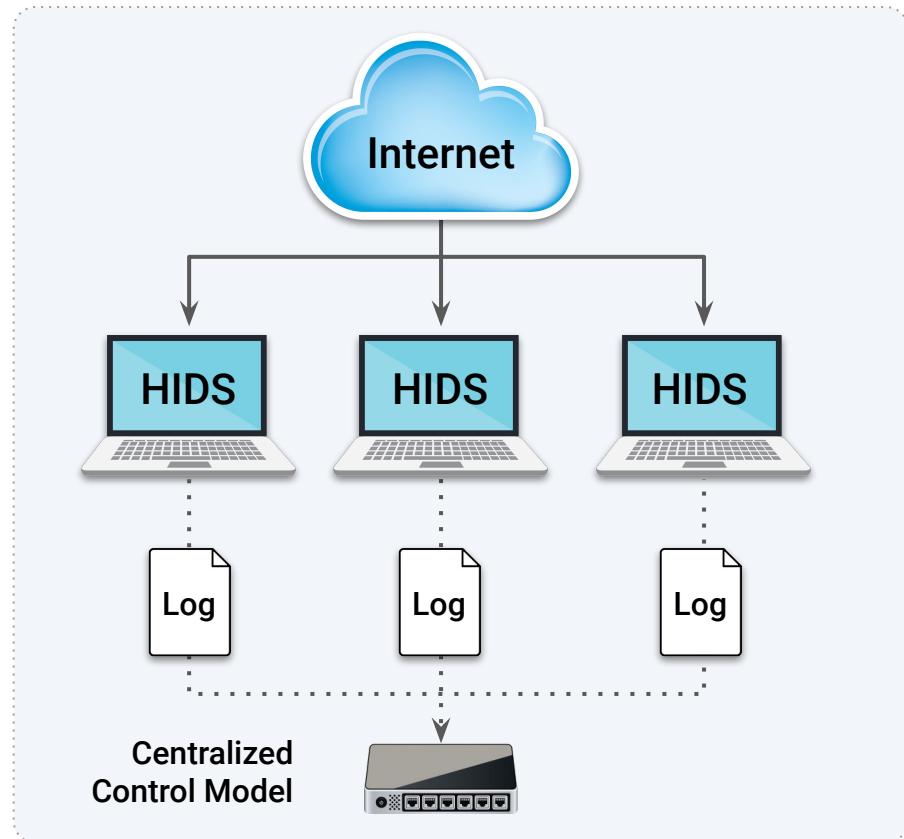
- Matches all traffic to a known library of attack signatures.
- Passively examines network traffic at points that it's deployed.
- Relatively easy to deploy and difficult to detect by attackers.



# Intrusion Detection Architecture

**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.

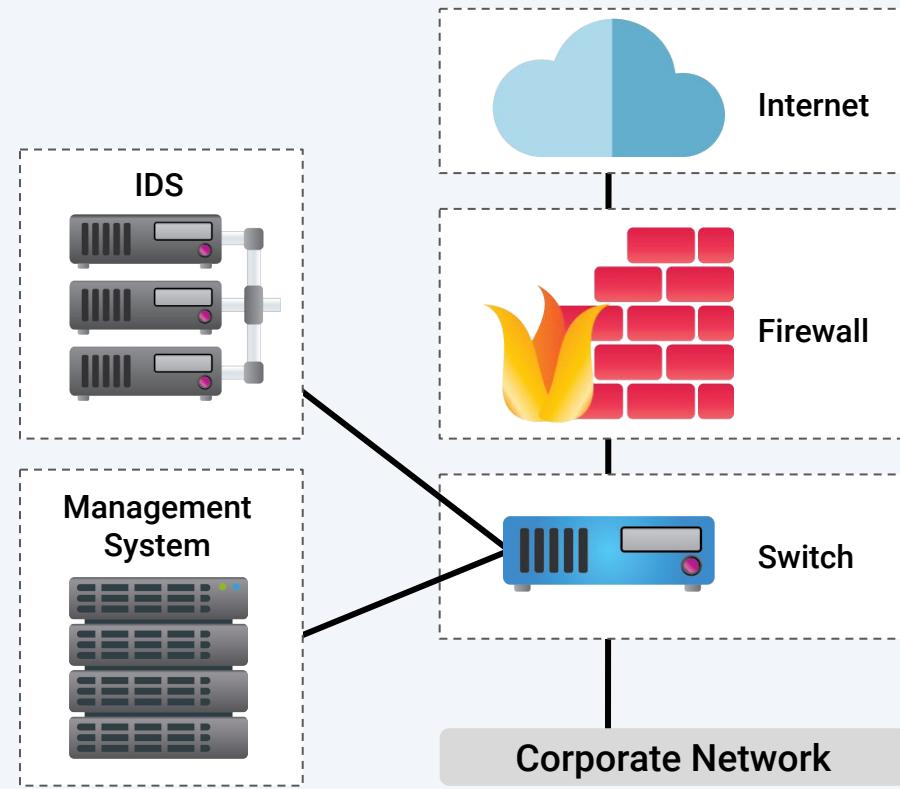
IPS can react to packets by blocking malicious traffic, preventing it from being delivered to a host on the network.

# 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

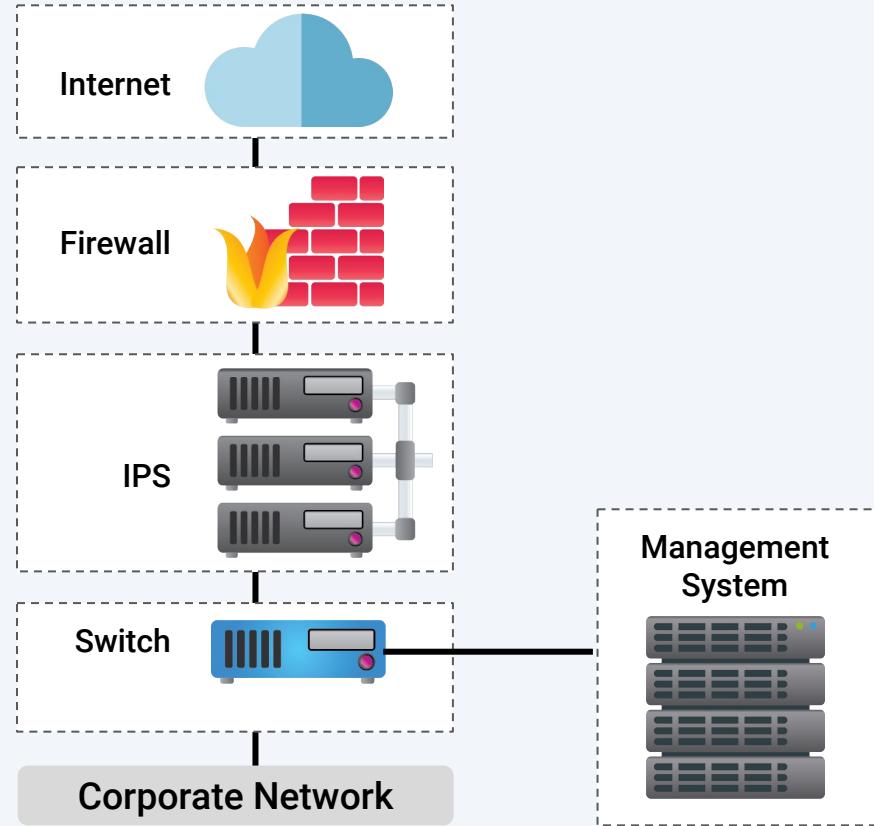


# IDS vs. IPS

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



# IDS Alerts

---

An **alert** is a message that is sent to an analyst's console as an IOA.

An IDS system generates alerts when it detects malicious traffic that matches a signature.



# IDS Alerts

---

Indicators can be either:

## Indicator of Attack

**IOA 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.

## Indicator of Compromise

**IOC 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.

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

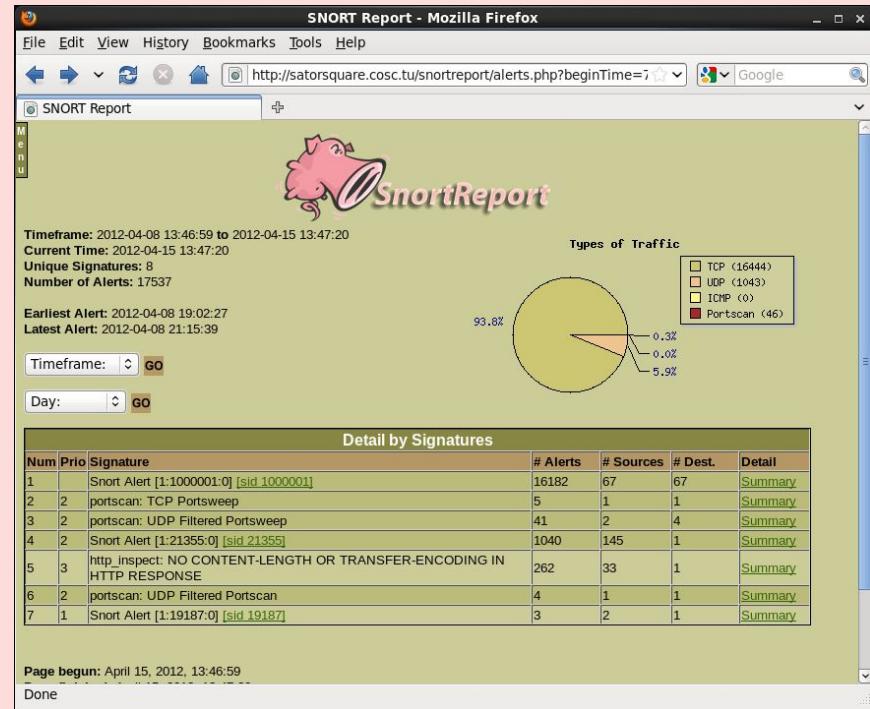


# Snort

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

It 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:

<b>Sniffer mode</b>	Reads network packets and displays them on screen.
<b>Packet logger mode</b>	Performs packet captures by logging all traffic to disk.
<b>Network IDS mode</b>	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

Generating an alert when traffic matches a rule pattern and logging the matching packet for later inspection.

# Snort Rules

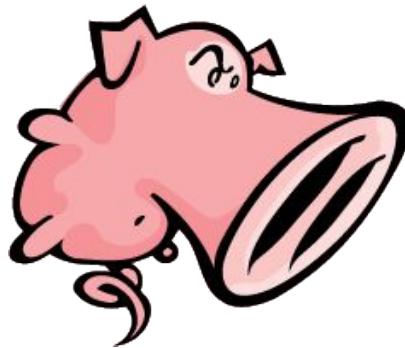
---

Rules can direct Snort to monitor the following information:

<b>OSI layer</b>	We can watch for IP and TCP data.
<b>Source and destination address</b>	Where the traffic is flowing from and to.
<b>Byte sequences</b>	Patterns contained in data packets that might indicate malware, etc.

# Snort Rules

---



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

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

# 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 any -> 10.199.12.8 21
```

**tcp**

Applies rule to all TCP packets.

**any**

Applies the rule to packets from any port.

**21**

Applies the rule to traffic to destination port 21.

## Rule Option

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

**{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 IDS.

Suggested Time:

---

10 Minutes



Time's Up! Let's Review.

# Questions?



# Networking Security Monitoring and Security Onion

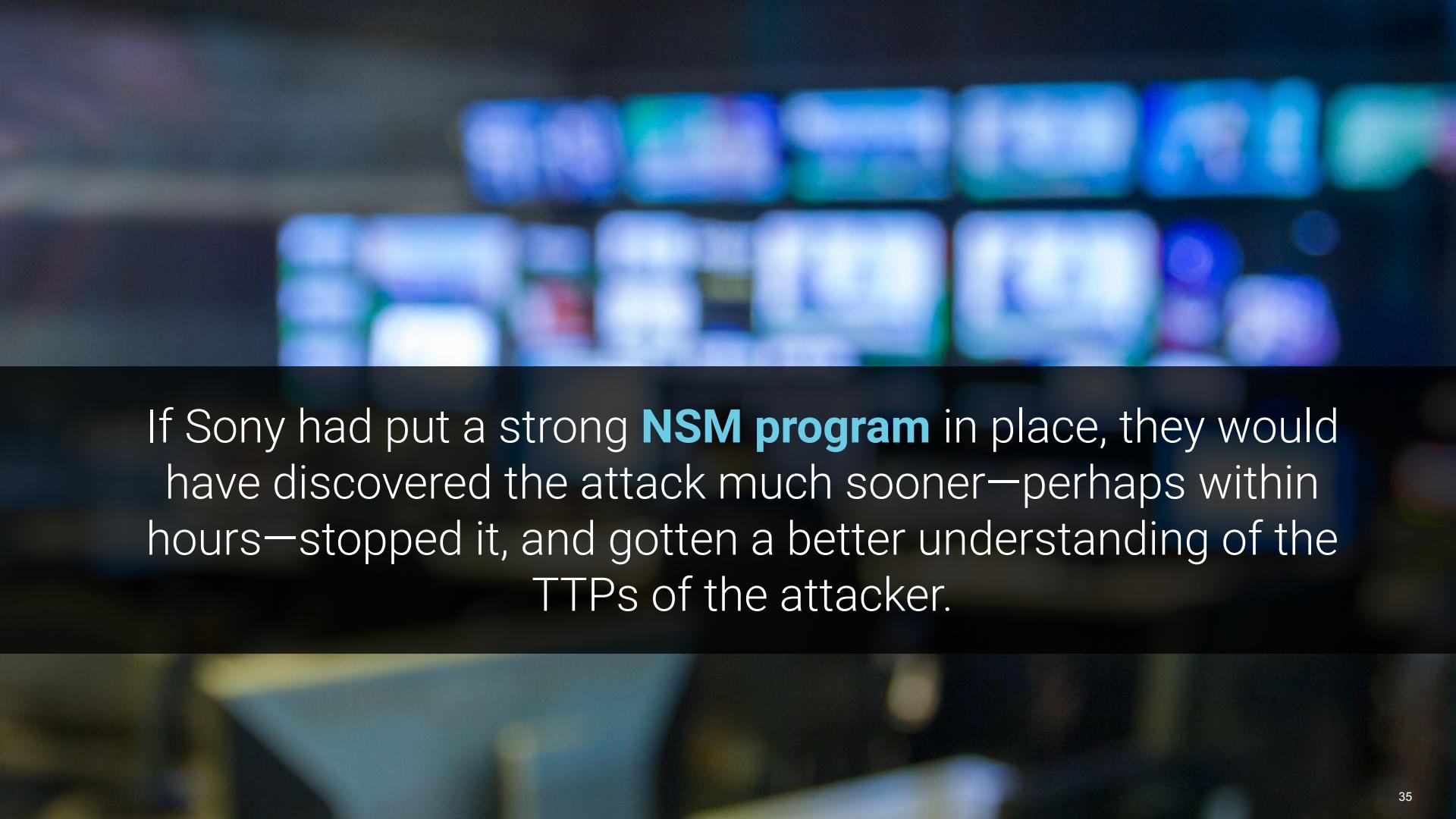
# Network Security Monitoring Case Study

On November 24, 2014, a group of attackers 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.

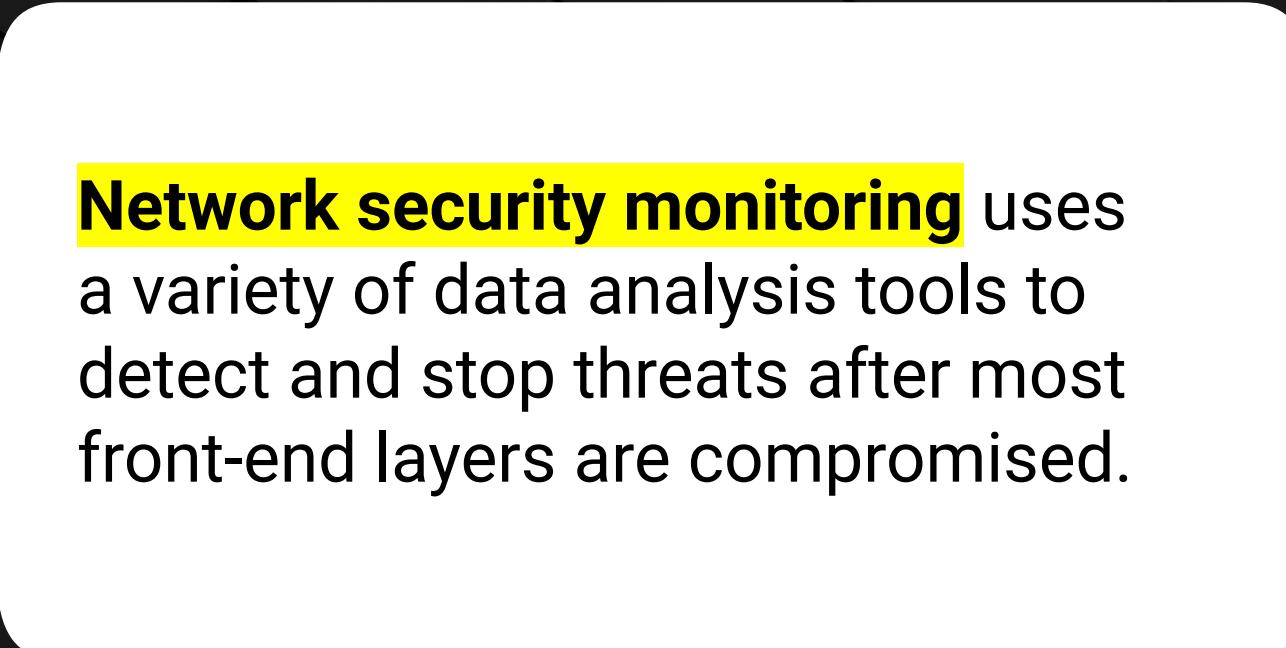
It was discovered that assailants had lurked on Sony's network for 17 months.

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





If Sony had put a strong **NSM program** in place, 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** uses a variety of data analysis tools to detect and stop threats after most front-end layers are compromised.

# Network Security Monitoring

---



NSM is threat-centric. It focuses on the adversary, not the vulnerability.



NSM focuses on the visibility of an attack, not the response to the attack.



NSM also reveals statistical data related to specific IOAs and IOCs from attacks.

# NSM Strengths

NSM allows organizations to:



**Track adversaries** through a network and determine intent.



**Be reactive** through incident response and network forensics.



**Acquire intelligence** and situational awareness.



**Provide insights** about advanced persistent threats.



**Be proactive** by identifying vulnerabilities.



**Uncover** and track malware.

# NSM Weaknesses

NSM has its limitations:



**Cannot read** encrypted traffic.



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



Powerful hardware and CPU requirements mean **higher costs**.



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



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

# NSM Stages and Processes

---

NSM operates in two stages, each involving two processes:

01

Detection

An alert is generated in the Sguil analyst console.

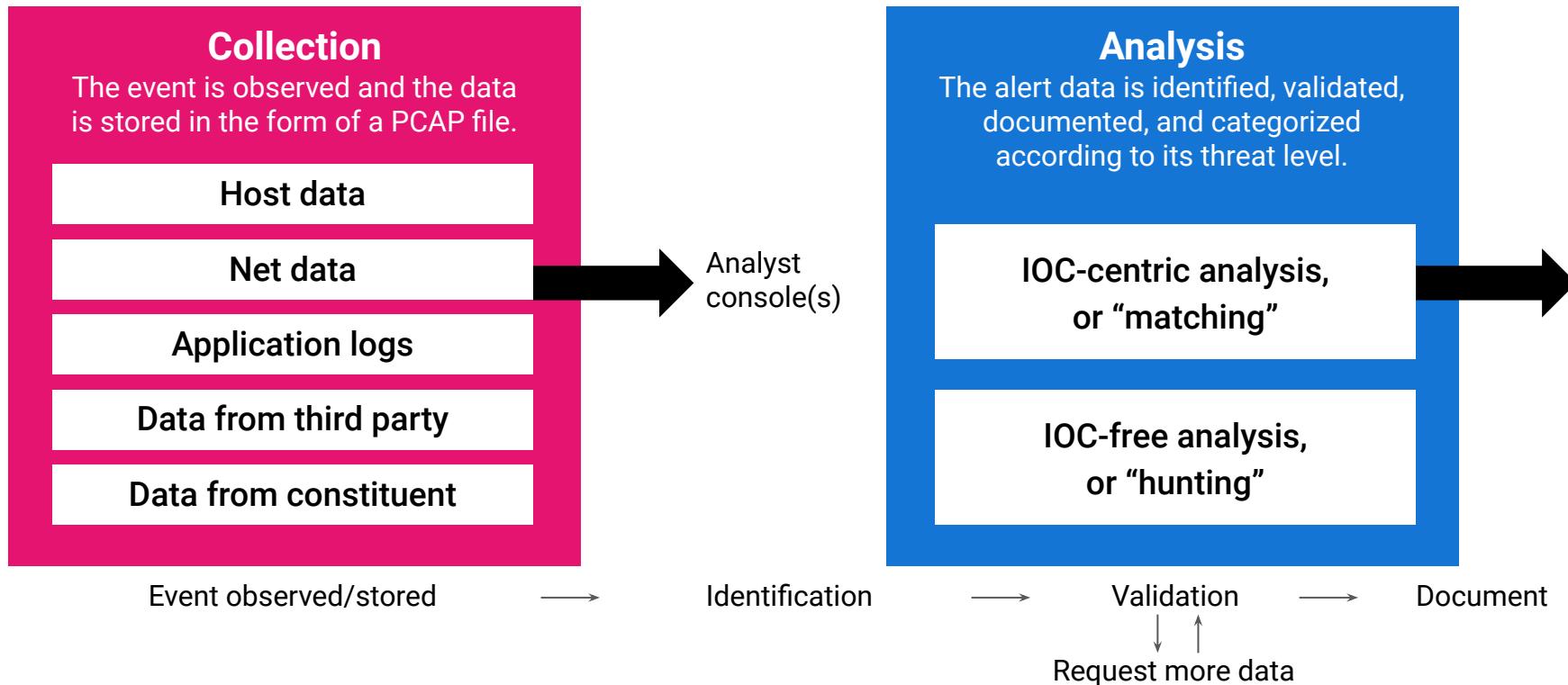
02

Response

A security team responds to a security incident.

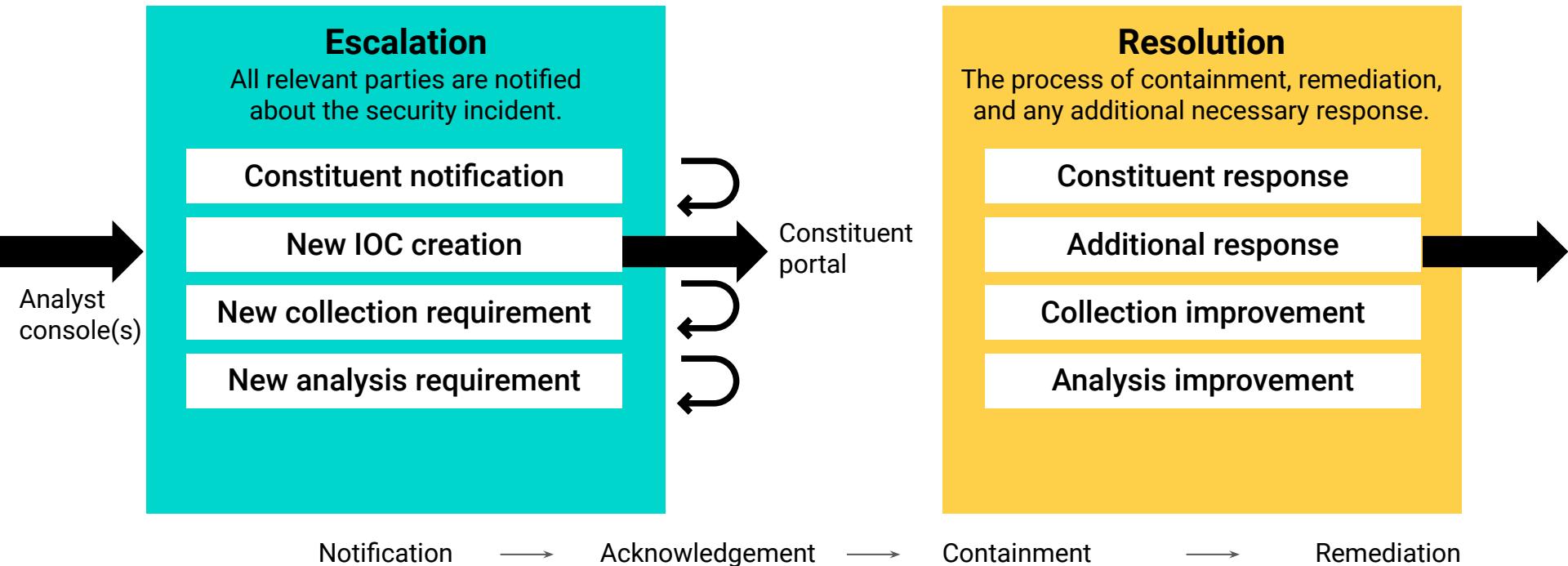
# NSM Stages and Processes

**Detection:** An alert is generated in the Sguil analyst console.



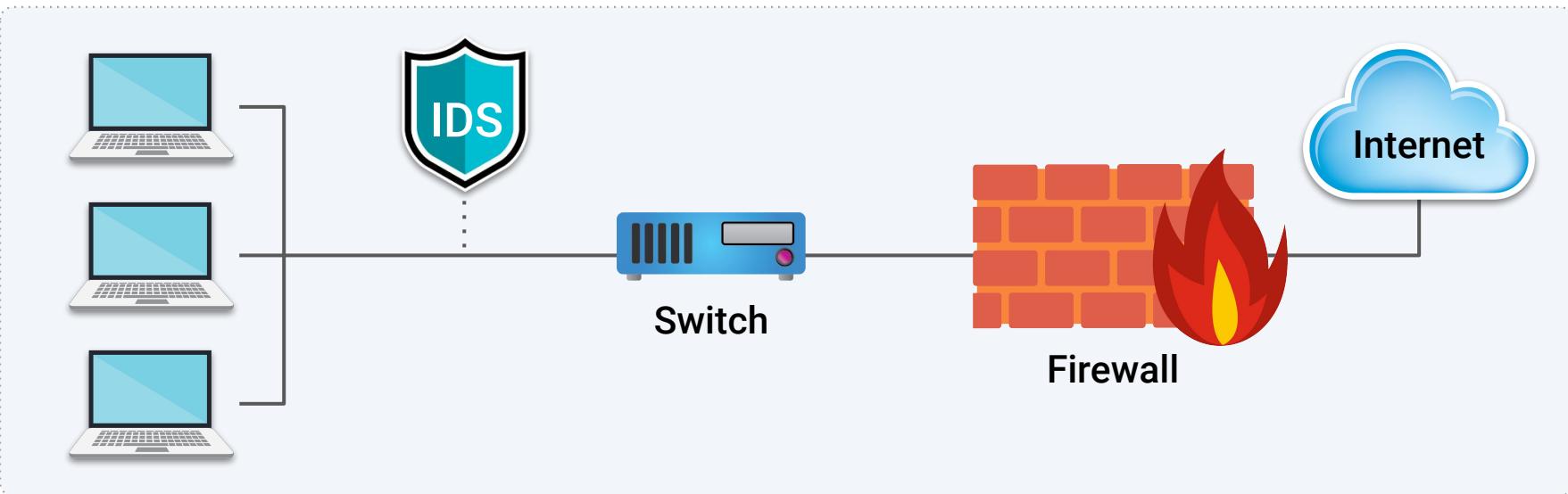
# NSM Stages and Processes

**Response:** A security team responds to a security incident.



# Intrusion Detection Systems

Intrusion detection systems are generally placed at strategic points in a network  
~~Where traffic is most likely to pass~~



# 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

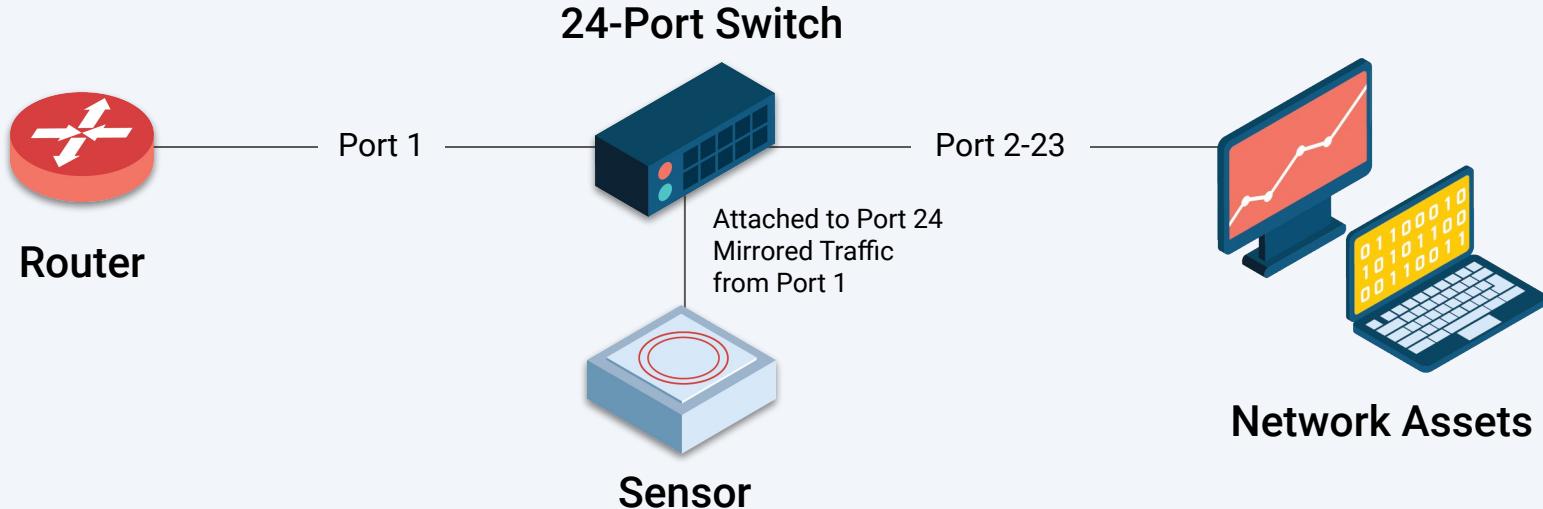
Network TAP

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

## SPAN or mirrored port

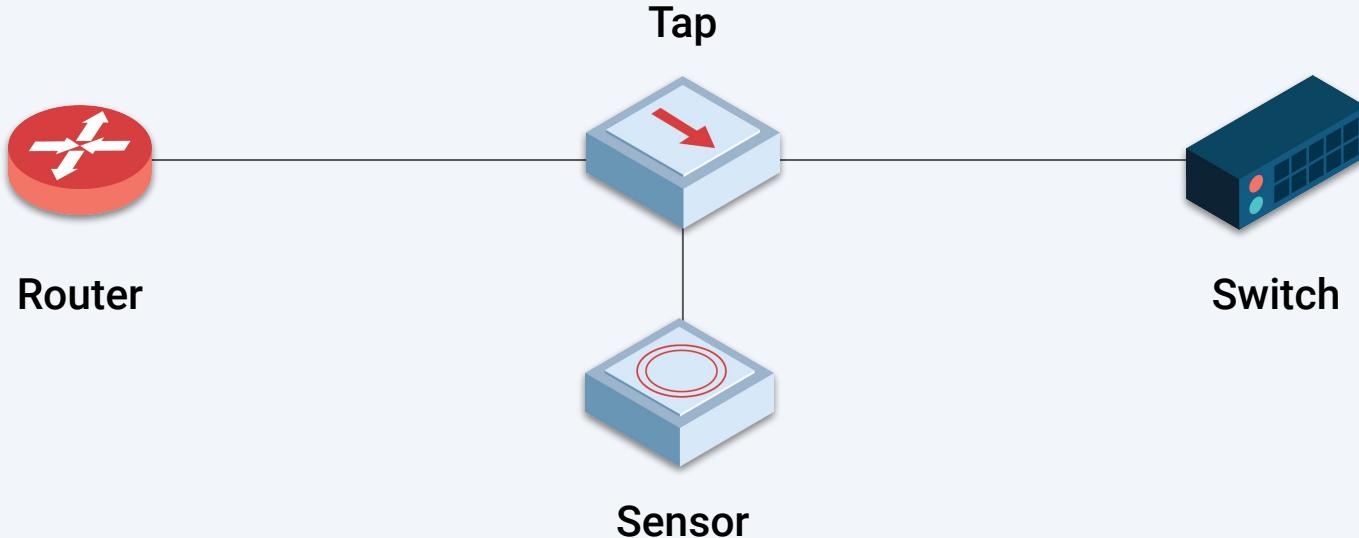
A SPAN port is a function of an enterprise-level switch allowing you to mirror one or more physical switch ports to another port. A mirror image of all data flows across both ports equally. This allows the IDS to perform packet captures on all inbound and outbound traffic within a network.



# NSM Sensor Connectivity

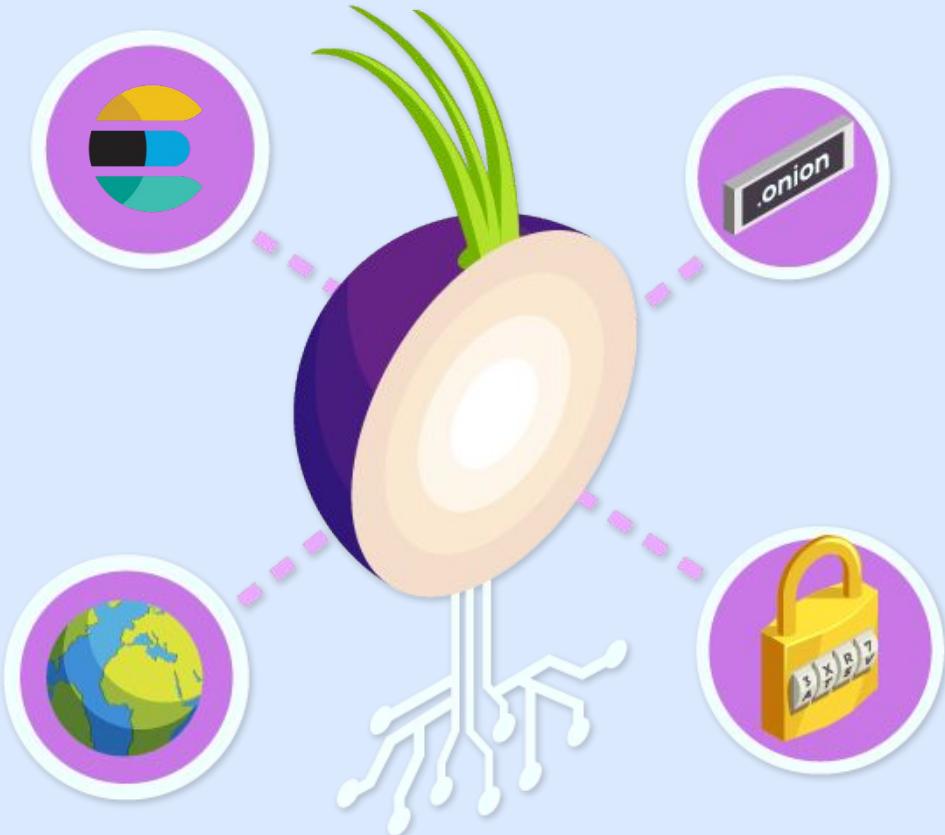
## Network TAP

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.



Today we'll work with **Security Onion**, an NSM 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:

## Alert panel

Displays detailed alert data, including:

- Source and destination IP
- Source and destination port
- Alert ID and severity
- Event message (message generated by Snort rule option)

## Snort rule

The Snort rule that generated the alert, obtained from the IDS engine.

## Packet data

PCAP file showing header and payload information of the data.

## IP resolution

Displays reverse DNS lookup information.

# 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

## ST (status)

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.

## Alert ID

A randomly generated numerical ID created by Sguil.

## Source IP

IP address of the source identified by the alert.

## Event message

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 and packet data.

**Snort rule:** The top portion displays the Snort NIDS engine's alert data. A red arrow points from the text "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;)" to the packet list below. Another red arrow points from the word "SNORT ALERT" to the alert message.

**Packet data:** The lower portion shows network traffic analysis. A red box highlights the source and destination ports (80, 49664) in the TCP header. A red arrow points from the "DATA" section to the hex dump of the payload. Another red arrow points from the payload hex dump to the corresponding ASCII text representation. The ASCII text includes headers like "HTTP/1.1 200 OK.", "Content-Type: text/html", and "Connection: keep-alive".

## 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 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 displays the following fields:

Src IP:	217.160.0.187
Src Name:	217-160-0-187.elastic-ssl.ui-r.com
Dst IP:	10.0.2.15
Dst Name:	Unknown

Below these fields is a "Whois Query" section with three radio button options: None (disabled), Src IP (selected), and Dst IP. The "Src IP" option is selected. To the right of the "Whois Query" section, there is a large block of Whois data for the IP address 217.160.0.187. Red arrows point from the text "reverse DNS" in the first bullet point to the "Src Name" field and from the text "country of origin" in the second bullet point to the "country" field in the Whois data. The Whois data includes the following entries:

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

At the bottom of the Whois data, there is a note: "abuse mailbox: abuse@oneandone.net".



# Activity: Security Onion and NSM

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

Suggested Time:

---

20 Minutes



Time's Up! Let's Review.

# Questions?





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 guided tour,  
we'll use Sguil as the starting point  
for learning other NSM tools for  
security investigations.



## Instructor Demonstration

---

### Security Onion—Sguil

# Questions?



# 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.

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

The screenshot shows the NetworkMiner 2.0 interface. The main window displays a table of files extracted from network traffic. The columns are D.port, Protocol, Filename, Extension, Size, and Details. The table lists various files including certificates (nr-data.net.cer, GeoTrust SSL CA - G2.cer, GeoTrust Global CA.cer), HTML files (index.html[2].ocsp-response, index.html), JavaScript files (almond.min.js.javascript, meetup.jquery\_ui.css, client.min.js.javascript, infoWidget.min.js.javascript, groupMetadata.min.js.javascript, mt-twoButtonCTA testimonial.css), CSS files (print.css, meetup-modem.css, whitney.css), and images (thumb\_156167702.jpeg, thumb\_151699612.jpeg.PNG). The 'Details' column shows file types like cer, html, javascript, css, and jpeg. The 'Size' column shows file sizes in bytes. The 'Case Panel' on the right shows a list of files with their MD5 hashes, including snort.log.... and f301c2...

D.port	Protocol	Filename	Extension	Size	Details
TCP 53130	TlsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C
TCP 53138	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb.symcd.com/
TCP 53139	HttpGetChunked	index.html	html	86 958 B	www.meetup.com
TCP 53142	HttpGetNormal	almond.min.js.javascript	javascript	2 758 B	static2.meetupsta
TCP 53140	HttpGetNormal	meetup.jquery_ui.css	css	6 725 B	static2.meetupsta
TCP 53144	HttpGetNormal	client.min.js.javascript	javascript	3 692 B	static2.meetupsta
TCP 53145	HttpGetNormal	infoWidget.min.js.javascript	javascript	20 639 B	static2.meetupsta
TCP 53151	HttpGetNormal	groupMetadata.min.js.javascript	javascript	2 409 B	static1.meetupsta
TCP 53149	HttpGetNormal	mt-twoButtonCTA testimonial.css	css	445 B	static1.meetupsta
TCP 53147	HttpGetNormal	print.css	css	2 171 B	static1.meetupsta
TCP 53141	HttpGetNormal	meetup-modem.css	css	223 971 B	static2.meetupsta
TCP 53139	HttpGetNormal	index.html.6D1A30C1.css	css	5 582 B	www.meetup.com
TCP 53146	HttpGetNormal	whitney.css	css	83 455 B	static1.meetupsta
TCP 53150	HttpGetNormal	ghome.min.js.javascript	javascript	102 378 B	static1.meetupsta
TCP 53148	HttpGetNormal	chapterbase.css	css	165 101 B	static1.base.meetupsta
TCP 53143	HttpGetNormal	Meetup.Base jquery.min.js.javascript	javascript	414 355 B	static2.meetupsta
TCP 53152	HttpGetNormal	thumb_156167702.jpeg	jpeg	2 611 B	photos3.meetupsta
TCP 53156	HttpGetNormal	thumb_151699612.jpeg.PNG	PNG	2 571 B	photos3.meetupsta



## Instructor Demonstration

---

Security Onion—NetworkMiner

# Summary

---

NSM allows organizations to:

-  Track adversaries through a network and determine their intent.
-  Acquire intelligence and situational awareness.
-  Be proactive by identifying vulnerabilities.
-  Be reactive through incident response and network forensics.
-  Provide insights related to advanced persistent threats (APTs).
-  Uncover and track malware.



# 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:

---

20 Minutes



Time's Up! Let's Review.

# Questions?



*The  
End*