

Welcome to Network Monitoring and Detection Lab IDS!

Today we will overview the concept of how to monitor network and get to know what's happening on your network

I will cover the following topics:

- The concept of monitoring your network
- How to monitor your network using various tools
- How to detect malicious activity on your network



PfSense

PfSense is a free network firewall distribution, based on FreeBSD OS and includes numerous third party free software packages intended to expand firewall functionality.

PfSense hardware can be installed on common hardware or in the cloud. This variety in installation options, together with project's openness and modern UI, makes pfSense one of the top software-based firewalls in the world.

What Is PfSense features?

Deployment: AWS, Azure Clouds and Hardware it can be ARM with 512MB ram to Xeon CPU boards 16GB RAM. Hardware is provided by Netgate.

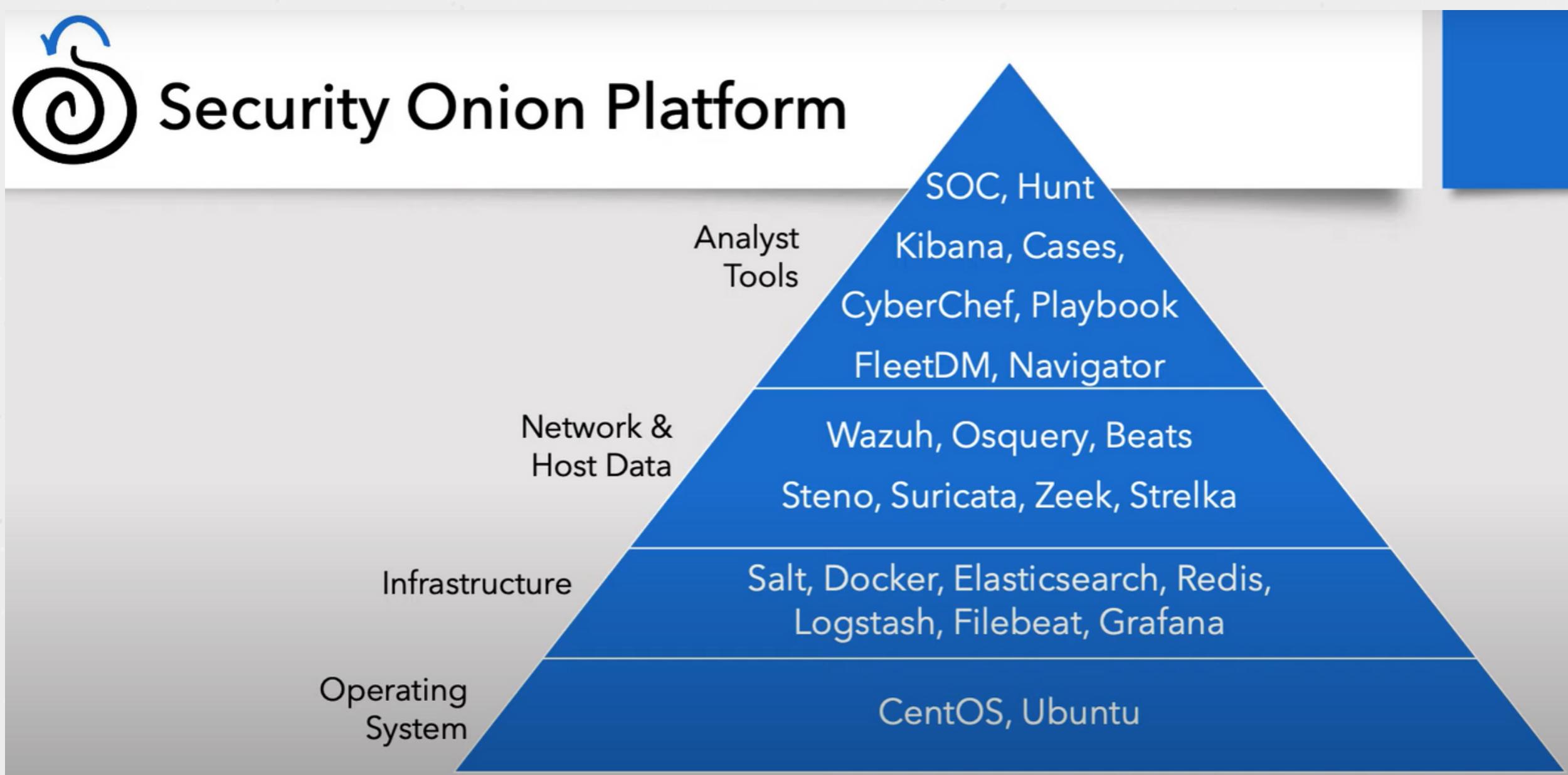
Dashboard: PfSense supports Routing and many protocols like OSPF, BGP, RIP and also support Static routing. Packages like Suricata, Zeek, squid, Snort.

High Availability, Firewall & NAT, DHCP Services, NTP Configuration, VPN



Security Onion is a free and open source intrusion detection system (IDS), security monitoring, and log management solution.

With its witty slogan, "Peel back the layers of security in your enterprise," it offers full packet capture, both network-based and host-based intrusion detection systems (NIDS and HIDS, respectively), but also includes powerful indexing, search, visualization and analysis tools to make sense of those mountains of data.



Security Onion's features include:

Network-based packet capture (including SYN/FIN/ACK traffic)

Host-based packet capture (including ICMP/IGMP/IGRP, ARP/RARP traffic)

Full HTTP filtering capability

Real-time alerting via email or SNMP trap

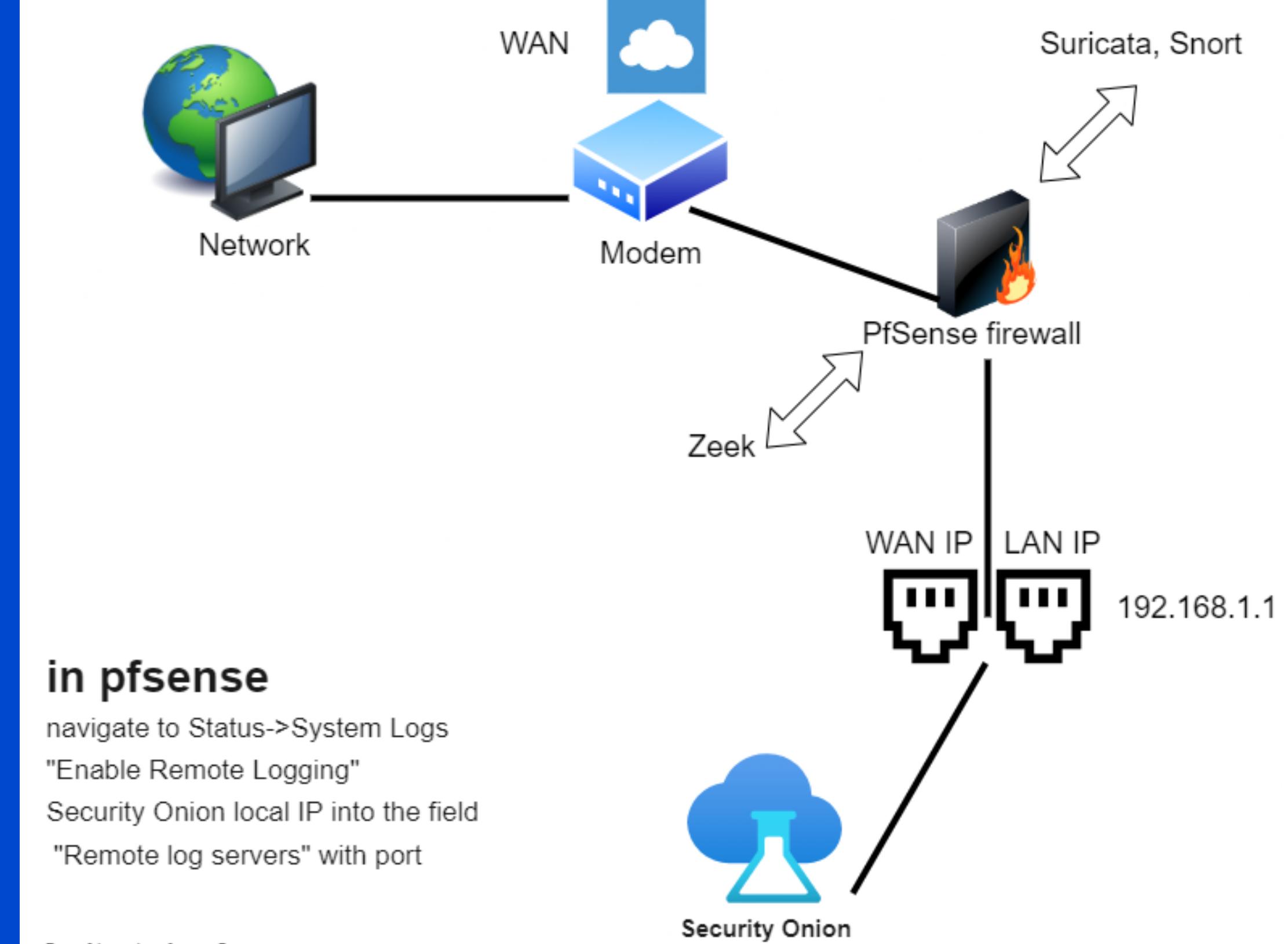
Intrusion detection based on TCP stream activity

Intrusion detection based on HTTP requests per second per port number

Intrusion detection based on port number usage statistics



Integrating Security Onion with pfSense



in pfSense

navigate to Status->System Logs
"Enable Remote Logging"
Security Onion local IP into the field
"Remote log servers" with port

Suricata-in pfSense

- Interfaces: For each interface you have configured, edit and repeat steps for each interface
- In each "Interface" Settings -> under Alert Settings check Send Alerts to System Log
- "Log Facility" should be "LOCAL1" & "Log Priority" should be "NOTICE"
- Further down under "EVE Output Settings", check "EVE JSON Log"
- "EVE Output Type" set to "SYSLOG" "EVE Syslog Output Facility"
- set to "AUTH" and "EVE Syslog Output Priority" set to "notice"



When would you use security onion?

- As a learning tool: In evaluation mode. Used to configure network interfaces
- PCAP forensics: PCAP files (packet capture — basically all files transmitted across a network) can be used for packet-sniffing and data network characteristic analysis
- As a production server: Both standalone and distributed
- Analyst VM: As a virtual machine to allow analysts to perform digital forensics
- To populate SIEM: As a connection to an external SIEM system.



Specify a query in Onion Query Language (OQL)

Overview

Alerts

Dashboards

Hunt

Cases

PCAP

Grid

Downloads

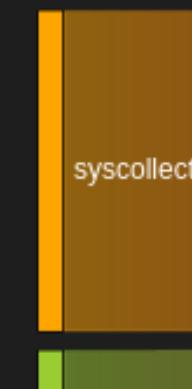
Administration

Users

Tools

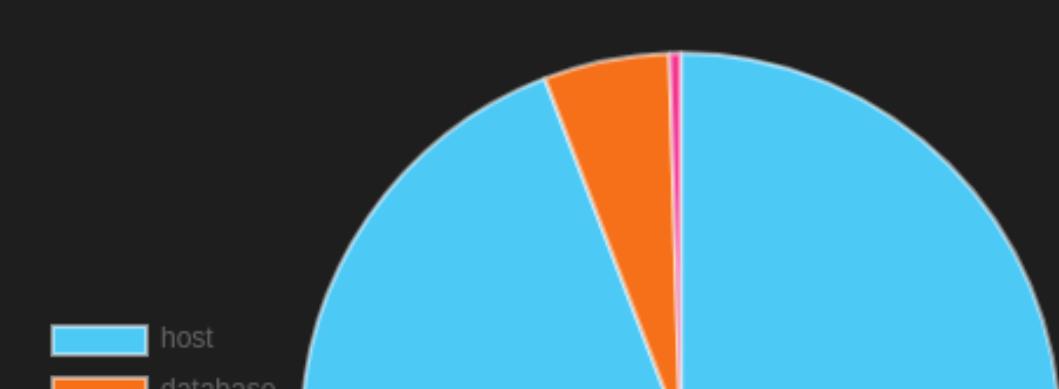
Kibana

event.dataset, event.category

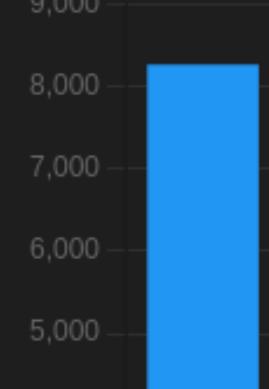
Fetch Limit
10

Filter Results

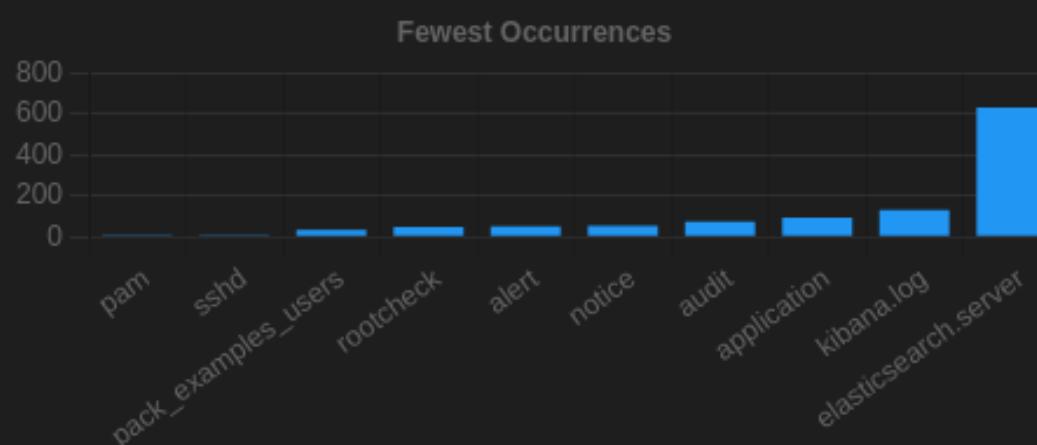
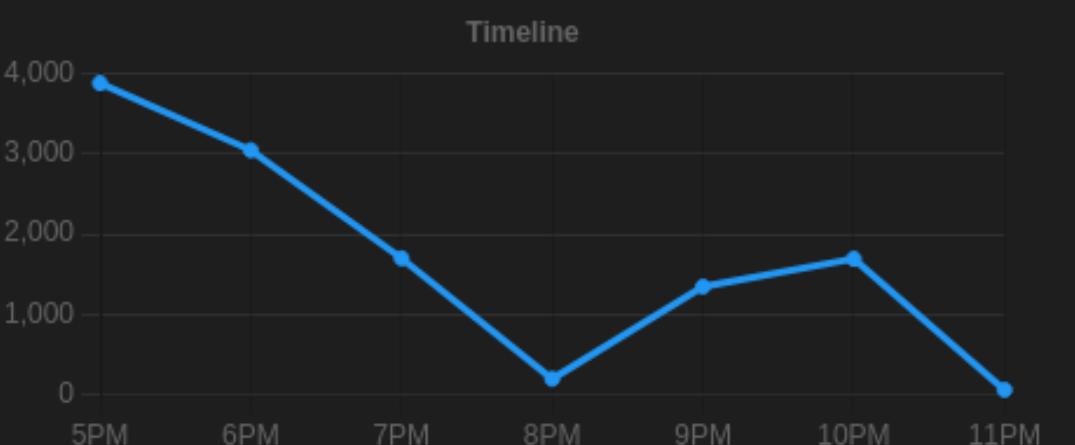
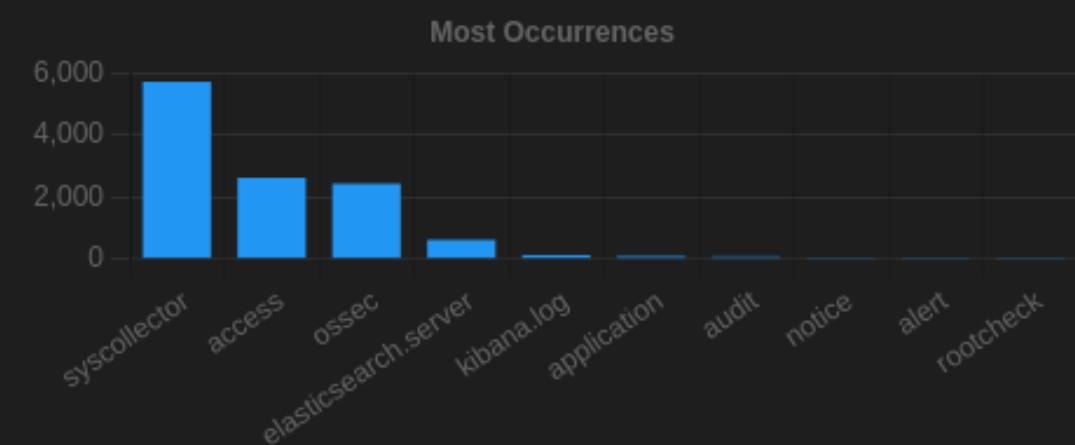
event.category



event.module



Basic Metrics

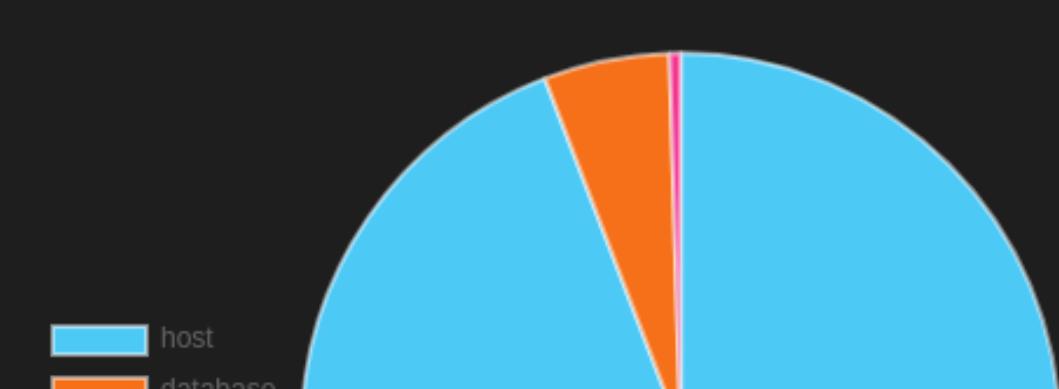


Group Metrics

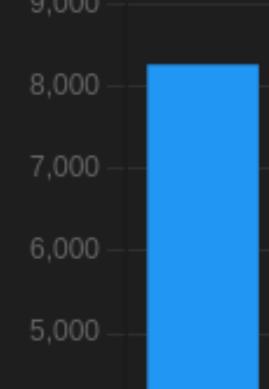
Fetch Limit
10

Filter Results

event.category



event.module



elastic

Find apps, content, and more. Ex: Discover

Dashboard Security Onion - Zeek - Notices

Full screen Share Clone Ed DETECTION PLAYBOOKS

Last 24 hours Refresher Activity Issues Create New Play

event.dataset:notice AND event.module:zeek

Security Onion - Alert Data Security Onion - All Logs Count 55

Security Onion - Zeek - Notice Export Notice Count 55

captureLoss::Too_Little_Traffic Only observed 0 TCP ACKs and was expecting at least 1.

Security Onion - Zeek - Notice Message Export Message Count 55

Only observed 0 TCP ACKs and was expecting at least 1.

Security Onion - Logs Over Time Count @timestamp per 30 minutes

Issues

Filters Status Options

Apply Clear

Add filter

PlayBook

#	Status	Level	Playbook	Title	Updated
421	Draft	high	community	Possible Process Hollowing Image Loading	05/08/2022 04:32 PM
420	Draft	high	community	DLL Load By System Process From Suspicious Locations	05/08/2022 04:32 PM
419	Draft	high	community	Microsoft Defender Loading DLL from Nondefault Path	05/08/2022 04:32 PM
418	Draft	medium	community	Suspicious WSMAN Provider Image Loads	05/08/2022 04:32 PM
417	Draft	high	community	Wmiprvse Wbemcomm DLL Hijack	05/08/2022 04:32 PM
416	Draft	high	community	WMIC Loading Scripting Libraries	05/08/2022 04:32 PM
415	Draft	high	community	WMI Persistence - Command Line Event Consumer	05/08/2022 04:32 PM
414	Draft	high	community	APT PRIVATELOG Image Load Pattern	05/08/2022 04:32 PM
413	Draft	medium	community	Unsigned Image Loaded Into LSASS Process	05/08/2022 04:32 PM
412	Draft	medium	community	UIPromptForCredentials DLLs	05/08/2022 04:32 PM
411	Draft	high	community	UAC Bypass With Fake DLL	05/08/2022 04:32 PM
409	Draft	high	community	Svhost DLL Search Order Hijack	05/08/2022 04:32 PM
408	Draft	high	community	VBA DLL Loaded Vía Microsoft Word	05/08/2022 04:32 PM
407	Draft	high	community	Image Load of VSS_PS.dll by Uncommon Executable	05/08/2022 04:32 PM
406	Draft	low	community	Suspicious System Drawing Load	05/08/2022 04:32 PM

Custom queries

- Active Plays
- All Plays
- Draft Plays
- Inactive Plays
- Playbook - Community Sigma
- Playbook - Internal

version 9.37.3

Last build: 4 months ago

Operations Recipe Input

length: 0 lines: 1

Options About / Support

Search...

Favourites

Data format

To Hexdump

From Hexdump

To Hex

From Hex

To Charcode

From Charcode

To Decimal

From Decimal

To Binary

From Binary

To Octal

From Octal

To Base32

From Base32

Converts unicode character codes back into text.

e.g. 0393 03b5 03b9 03ac 20 03c3
03bf 03c5 becomes フaidou

Plane (Unicode) on Wikipedia

Output

BAKE!

STEP Auto BAKE

CyberChef



Intrusion detection
Enterprise security
monitoring
Log management

Fleet for Osquery

Attack Navigator

Hosts

1 host

Hostname	Status	OS	Osquery	IP address	Last fetched
securitynoion	Online	CentOS Linux 7.9.2009	4.5.1	192.168.209.160	42 minutes ago

Manage enroll secret Add hosts

All hosts 1

Operating systems

- macOS 0
- Linux 1
- CentOS Linux 1
- Windows 0

Labels

Add label +

Filter labels by name...

Reconnaissance 10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access 9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Inter-Process Communication (0/2)
- Native API
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship

Execution 12 techniques

- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Exploitation for Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

Persistence 19 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/15)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create or Modify System Process (0/4)
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- External Remote Services
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Implant Internal Image
- Scheduled Task Job (0/6)
- Malicious Automation Process (0/4)
- Office

Privilege Escalation 13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/15)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Exploit for Credential Access
- Deploy Container
- Forced Authentication
- Domain Policy Modification (0/2)
- Input Capture (0/4)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Network Sniffing
- OS Credential Dumping (0/8)
- Hijack Execution Flow (0/11)
- Impair Defenses (0/9)
- Scheduled Task Job (0/6)
- Indicator Removal on Host (0/6)
- Valid Accounts (0/4)
- Office

Defense Evasion 40 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Cloud Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Peripheral Device
- Protocol Tunneling
- Data Staged (0/2)
- Remote Access Software
- Email Collection (0/3)

Credential Access 15 techniques

- Adversary-in-the-Middle (0/2)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploit for Credential Access
- Deploy Container
- Forced Authentication
- Forge Web Credentials (0/2)
- Domain Policy Modification (0/2)
- Input Capture (0/4)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Network Sniffing
- OS Credential Dumping (0/8)
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Implant Internal Image
- Scheduled Task Job (0/6)
- Indicator Removal on Host (0/6)
- Valid Accounts (0/4)
- Office

Discovery 29 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Brute Force
- Credentials from Password Stores
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Credential Access
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Defense Evasion
- File and Directory Permissions Modification
- Network Sniffing
- OS Credential Dumping
- Hijack Execution Flow
- Process Injection
- Implant Internal Image
- Scheduled Task Job
- Indicator Removal on Host
- Valid Accounts
- Office

Lateral Movement 9 techniques

- Adversary-in-the-Middle (0/2)
- Brute Force
- Credentials from Password Stores
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification

Collection 17 techniques

- Account Discovery
- Application Window Discovery
- Brute Force
- Credentials from Password Stores
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Credential Access
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Defense Evasion
- File and Directory Permissions Modification
- Network Sniffing
- OS Credential Dumping
- Hijack Execution Flow
- Process Injection
- Implant Internal Image
- Scheduled Task Job
- Indicator Removal on Host
- Valid Accounts
- Office

Command and Control 16 techniques

- Adversary-in-the-Middle (0/2)
- Brute Force
- Credentials from Password Stores
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Credential Access
- Deploy Container
- Forced Authentication
- Forge Web Credentials
- Domain Policy Modification
- Input Capture
- Execution Guardrails
- Exploit for Defense Evasion
- File and Directory Permissions Modification
- Network Sniffing
- OS Credential Dumping
- Hijack Execution Flow
- Process Injection
- Implant Internal Image
- Scheduled Task Job
- Indicator Removal on Host
- Valid Accounts
- Office

Exfiltration 9 techniques

- Application Layer Protocol (0/4)
- Archive Collected Data (0/3)
- Communication Through Removable Media
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Dynamic Resolution (0/3)
- Exfiltration Over Other Network Medium (0/1)
- Encrypted Channel (0/2)
- Fallback Channels
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- File and Directory Discovery
- Taint Shared Content
- Use Alternate Authentication Material (0/4)
- Data from Local System
- Data from Network Shared Drive
- Non-Standard Port
- Protocol Tunneling
- Data Staged (0/2)
- Remote Access Software
- Email Collection (0/3)

Final Thoughts

What's the best way to protect your business?

It's a question we all ask ourselves, but it's difficult to answer. There are so many factors that go into choosing the right security solution for your company: things like budget, size of the data you store, and what types of threats you want to protect against.

So how can you be sure that your IDS/IPS system will be able to protect your sensitive data? One approach is to look at research reports. These reports can give you an idea of where your organization stands against some of the most common attacks out there. They also help identify specific vulnerabilities that can be addressed by a particular product or service.

If you're looking for an IDS/IPS system for your organization, then make sure it has been tested and proven effective in protecting against specific attacks. Look for products that have been evaluated by independent researchers and have received positive reviews from customers who use them in their own businesses. The more information out there about a particular product or service, the better!

The best IDS/IPS system is the one that works best for