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?

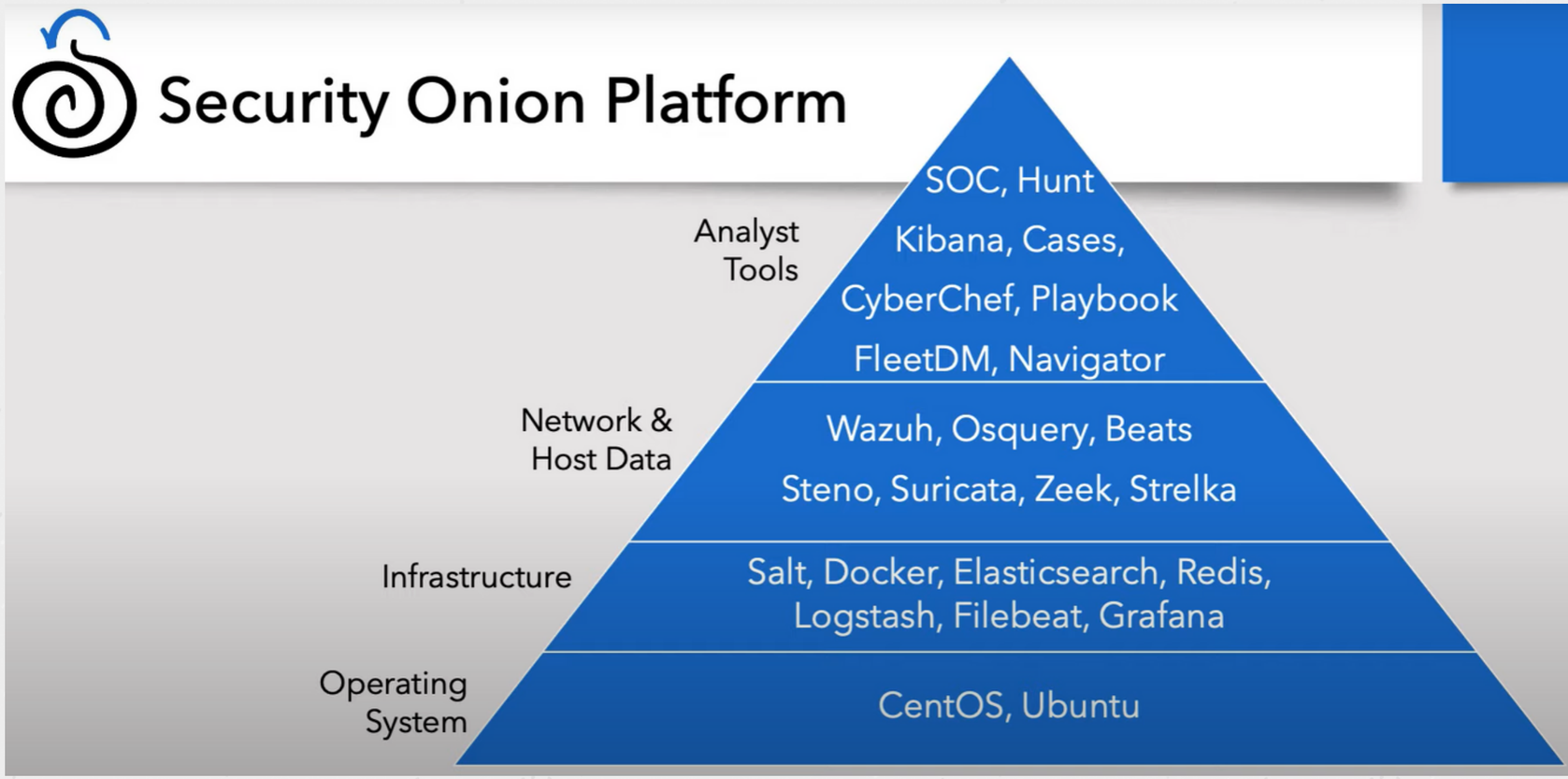
Deployment: AWS, Azure Clouds and Hardware it can be ARM with 512MB ram to Xeon CPU boards 16GB RAM.Hardware is provided by Netgate.

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

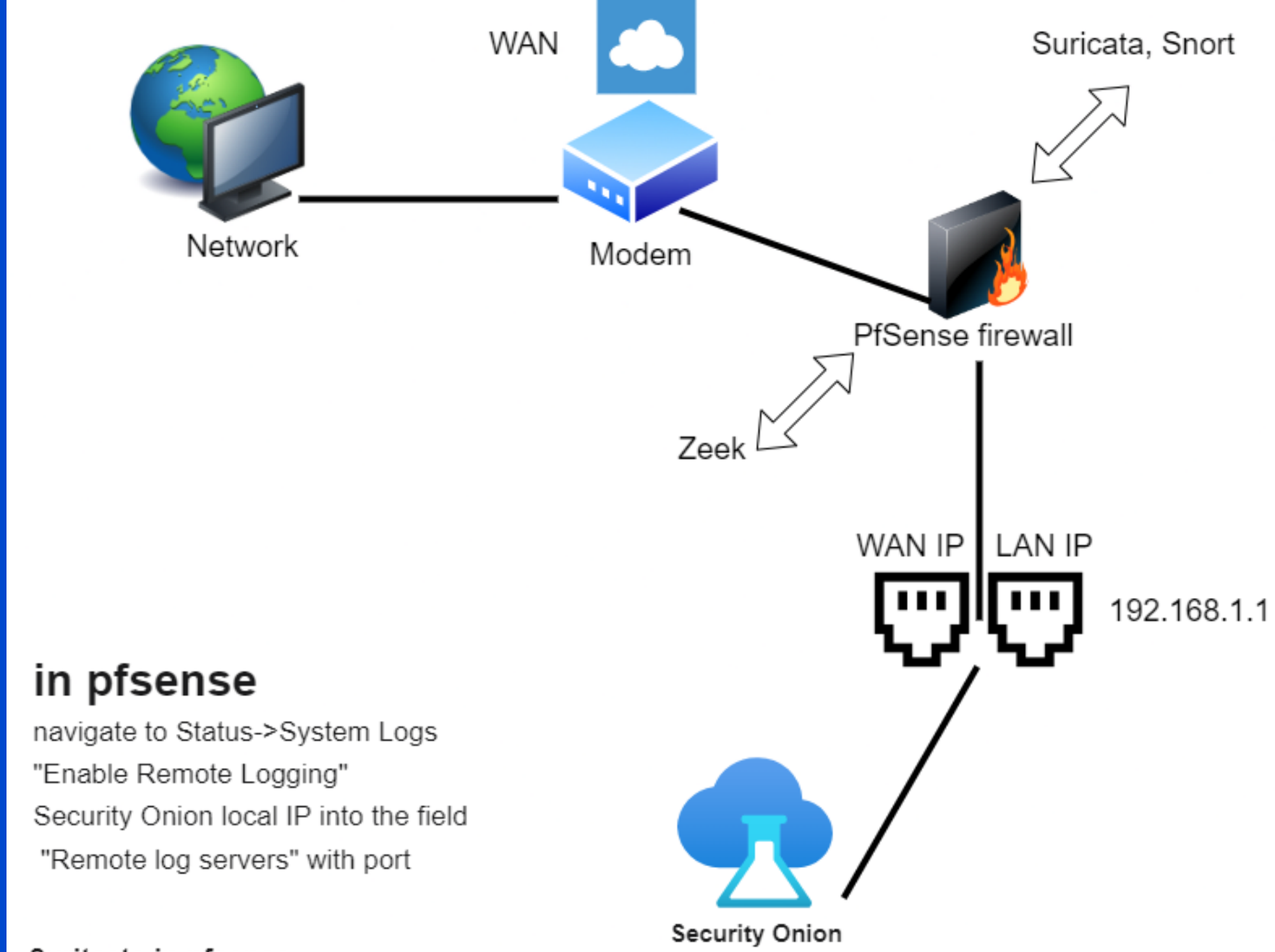
Real-time alerting via email or SNMP trap

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

Suritcata-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.

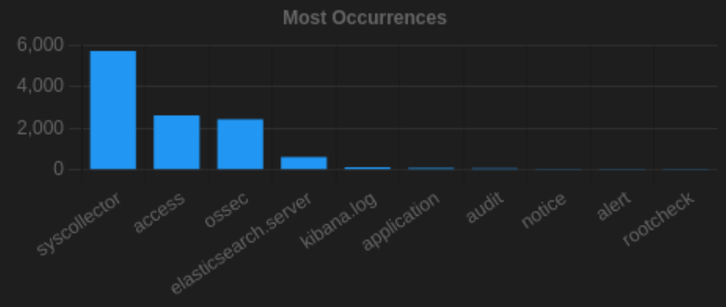
Security Onion

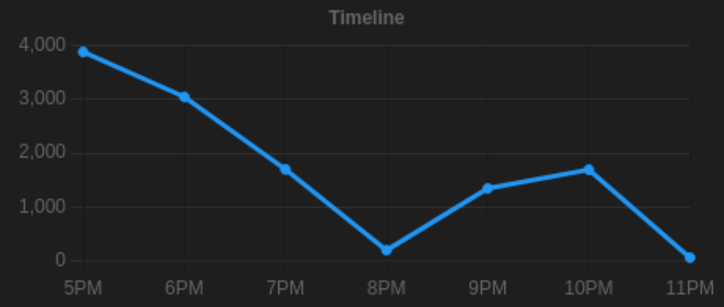
- Overview
- Alerts
- Dashboards
- Hunt
- Cases
- PCAP
- Grid
- Downloads
- Administration
  - Users

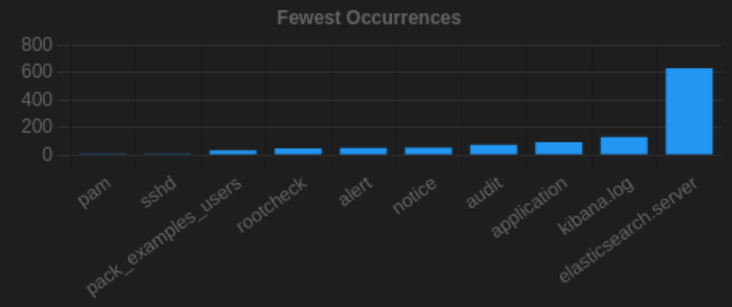
Tools

- Kibana
- Grafana
- CyberChef
- Playbook
- FleetDM
- Navigator

Basic Metrics



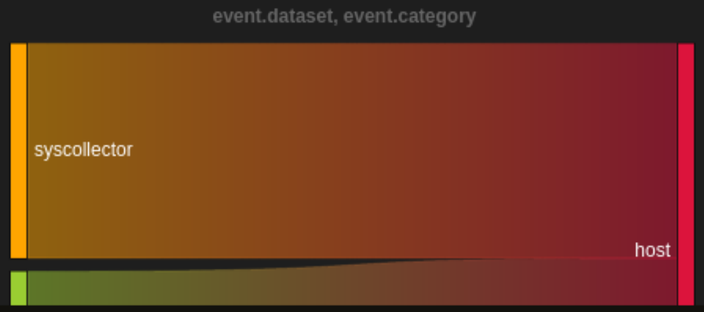


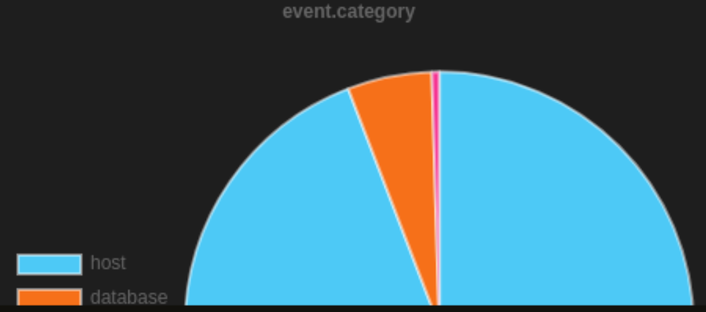


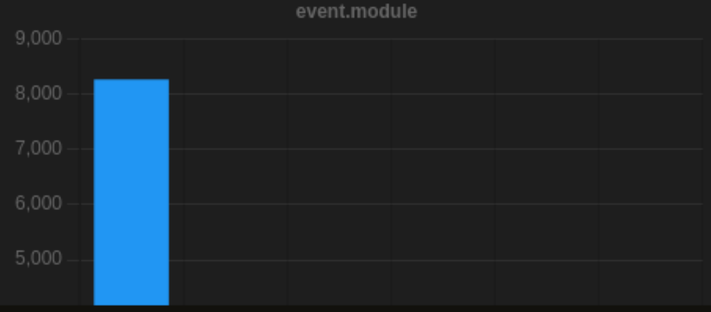
Group Metrics

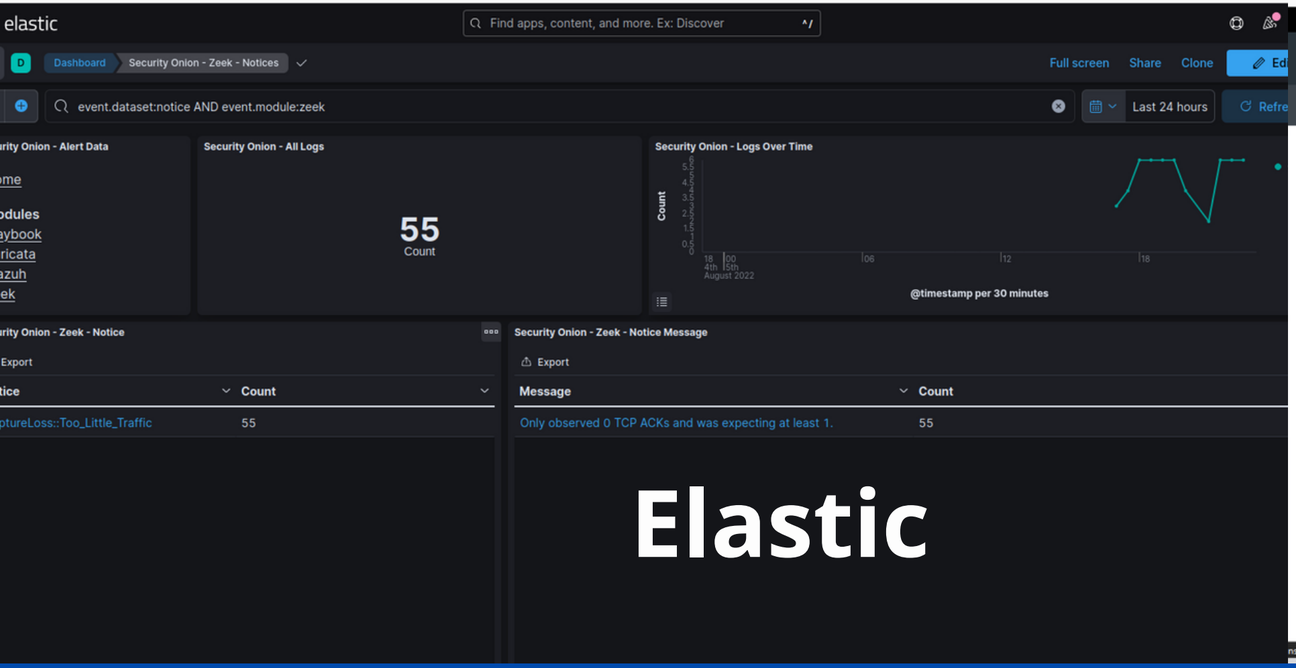
Fetch Limit: 10

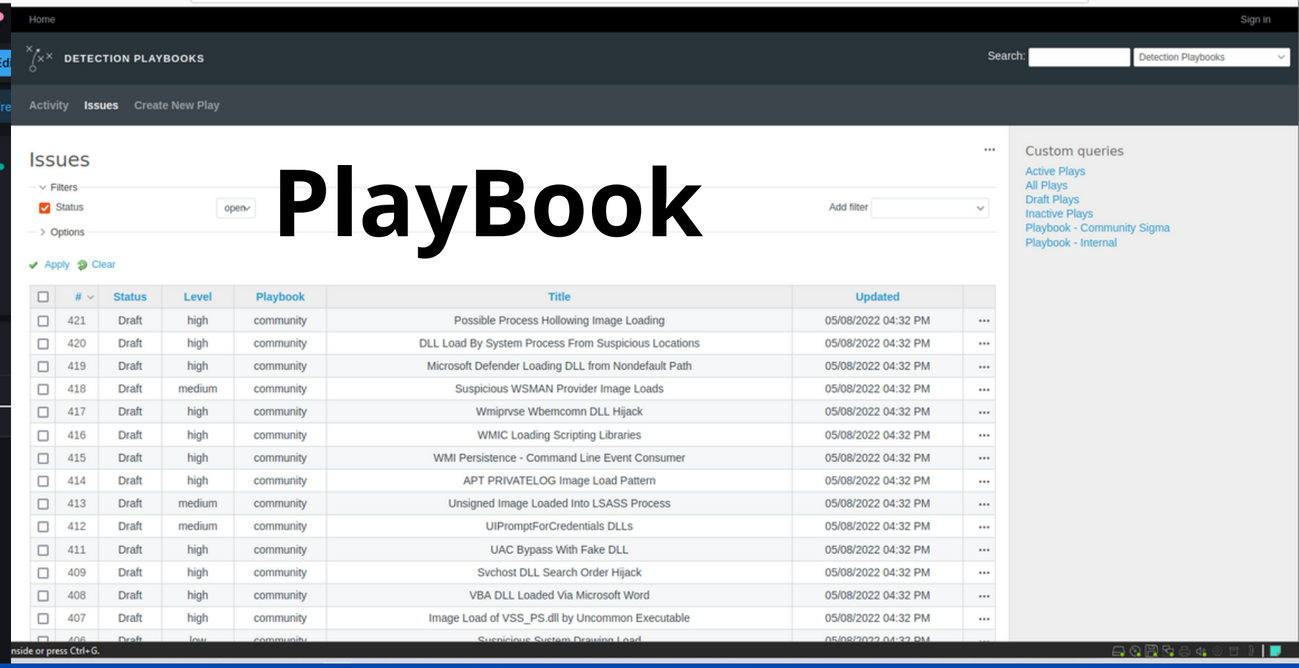
Filter Results

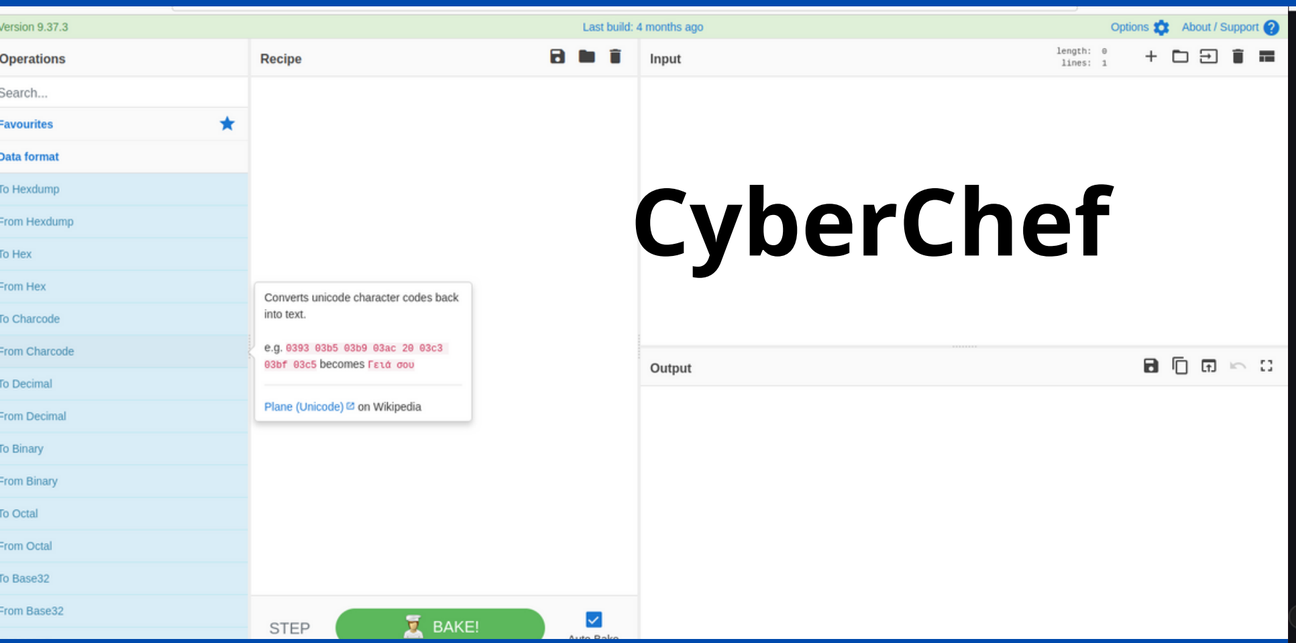


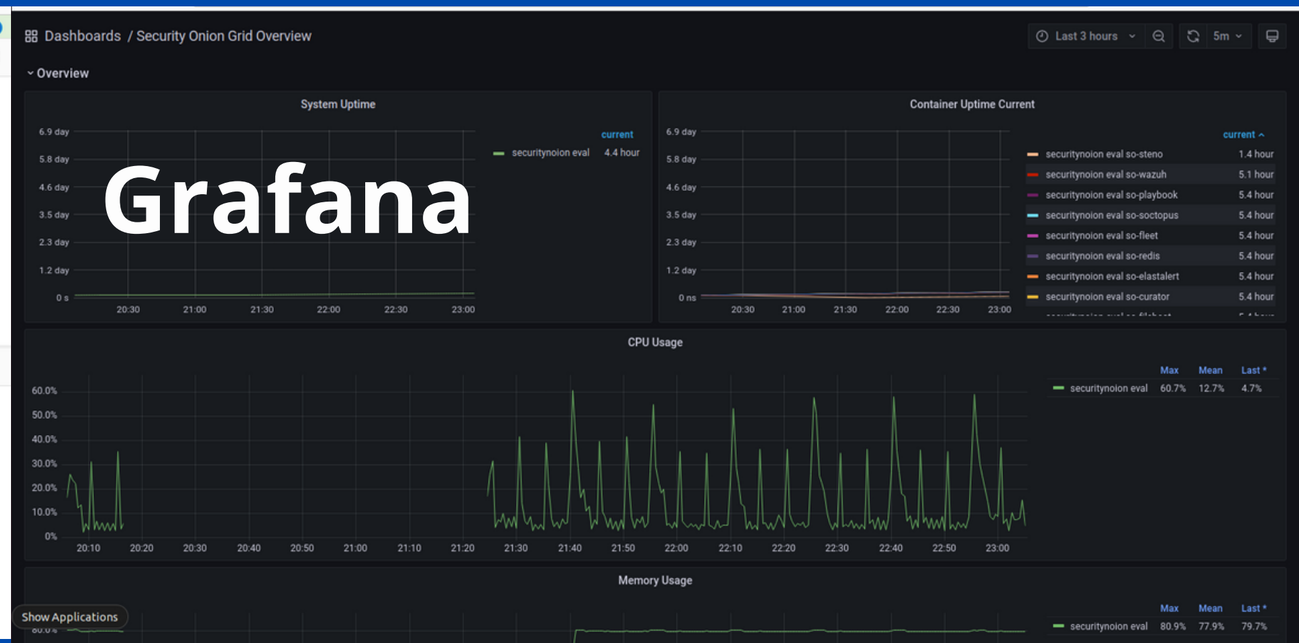




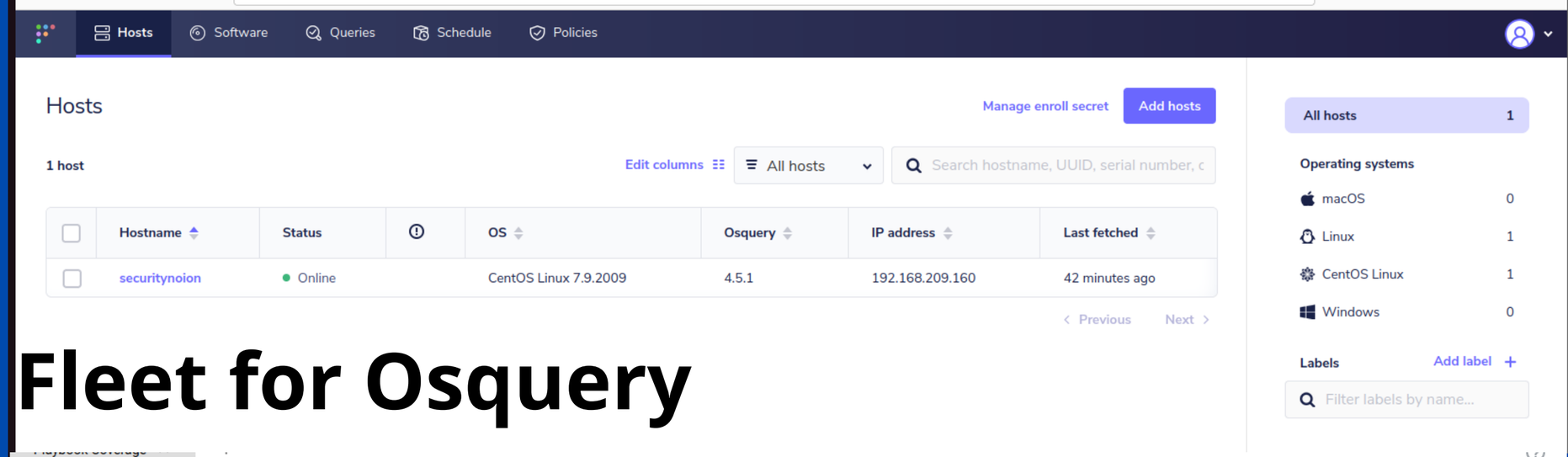

elastic
Find apps, content, and more. Ex: Discover
Dashboard
Security Onion - Zeek - Notices
Full screen
Share
Clone
event.dataset:notice AND event.module:zeek
Last 24 hours
Security Onion - Alert Data
Security Onion - All Logs
55
Count
Security Onion - Logs Over Time
@timestamp per 30 minutes
Security Onion - Zeek - Notice
Export
Count
tureLoss::Too_Little_Traffic
55
Security Onion - Zeek - Notice Message
Export
Message
Count
Only observed 0 TCP ACKs and was expecting at least 1.
55
Elastic


Home
Sign in
DETECTION PLAYBOOKS
Search:
Detection Playbooks
Activity
Issues
Create New Play
Issues
Filters
Status
open
Options
Add filter
Apply
Clear
Custom queries
Active Plays
All Plays
Draft Plays
Inactive Plays
Playbook - Community Sigma
Playbook - Internal
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 Wbemcomn 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 Svchost DLL Search Order Hijack 05/08/2022 04:32 PM
408 Draft high community VBA DLL Loaded Via 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
PlayBook


Version 9.37.3
Last build: 4 months ago
Options
About / Support
Operations
Recipe
Input
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 Γειά σου
Plane (Unicode) on Wikipedia
Output
STEP
BAKE!
CyberChef


Dashboards / Security Onion Grid Overview
Last 3 hours
5m
Overview
System Uptime
Container Uptime Current
CPU Usage
Memory Usage
Show Applications
securitynoion eval
Grafana

Intrusion detection
Enterprise security monitoring
Log management



Fleet for Osquery

Attack Navigator

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