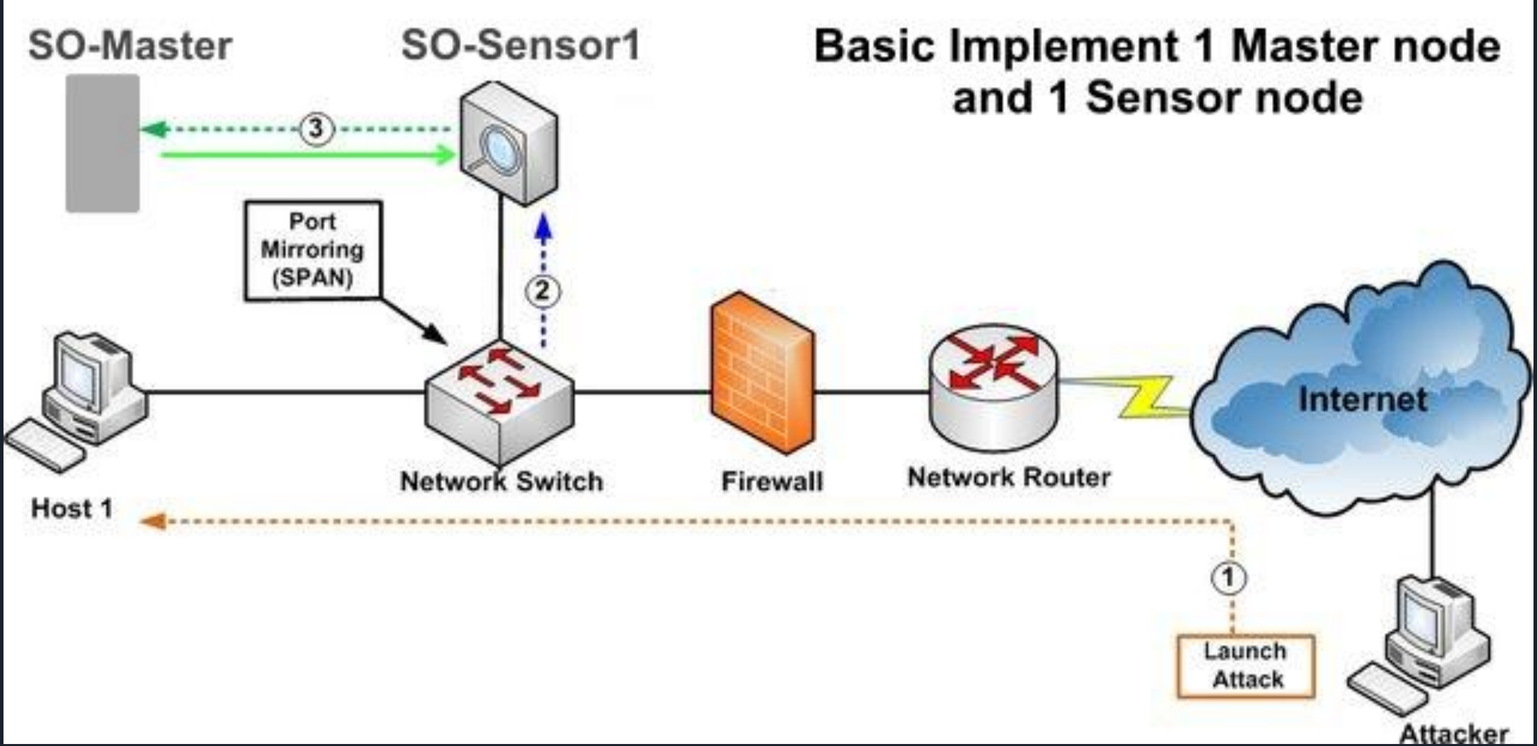
Network Analysis & Detection Intrusion Service

Architecture & Security Team
Packetlove IT Service and Consulting Co.,Ltd.

Why need to analysis packet in your network



What is Security Onion (SO) ?

- Security Onion start implement on 2008 by Doug Burks
- Security onion is a network security monitoring (NSM) system that provides full context and forensic visibility into the traffic it monitors
- Designed to make deploying complex open source tools simple via a single package (Snort, Suricata, Squert , Sguil etc.)
- Having the ability to pivot from one tool to the next to seamlessly, provides the most effective collection of network security tools available in a single package
- Allows the choice of IDS engines, analysts consoles, web interfaces
- Support ipv4 and ipv6 for snort and suricata
- Free (Open Source)!!

The security onion - A single entity with many layers.

- The corporate layer
- Policy and human error layers
- The target layer
- The hacker layer
- The threat layer
- The testing layer

What is NSM (Network Security Management) ?

“the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions.”

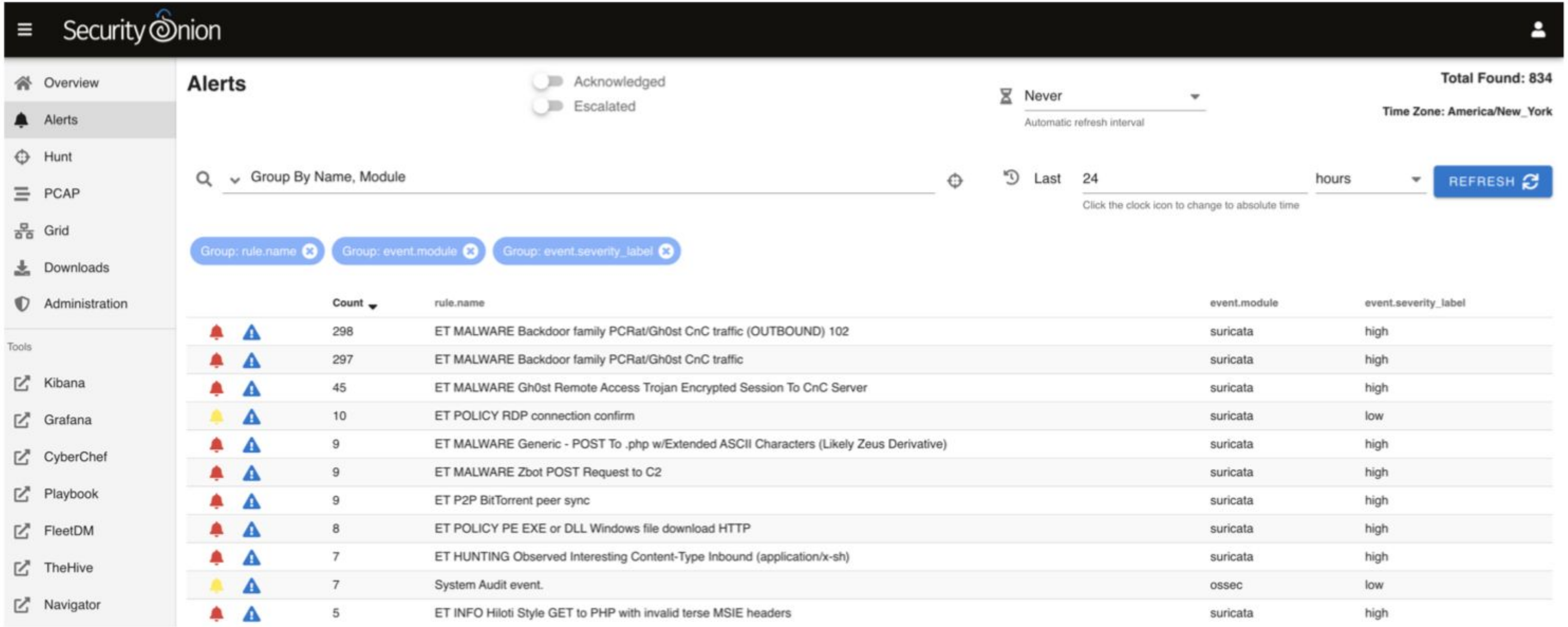
Types of Intrusion Detection Systems

There are two main types of intrusion detection systems (both are explained in more detail later in this guide):

1. **Host-based intrusion detection (HIDS)** – this system will examine events on a computer on your network rather than the traffic that passes around the system.
2. **Network-based intrusion detection (NIDS)** – this system will examine the traffic on your network.

CONSOLE

Security Onion Console (SOC) is the first thing you see when you log into Security Onion. It includes a new *Alerts* interface which allows you to see all of your NIDS and HIDS alerts.



Alerts

Acknowledged

Escalated

Never
Automatic refresh interval

Total Found: 834

Time Zone: America/New_York

Group By Name, Module

Last 24 hours
Click the clock icon to change to absolute time

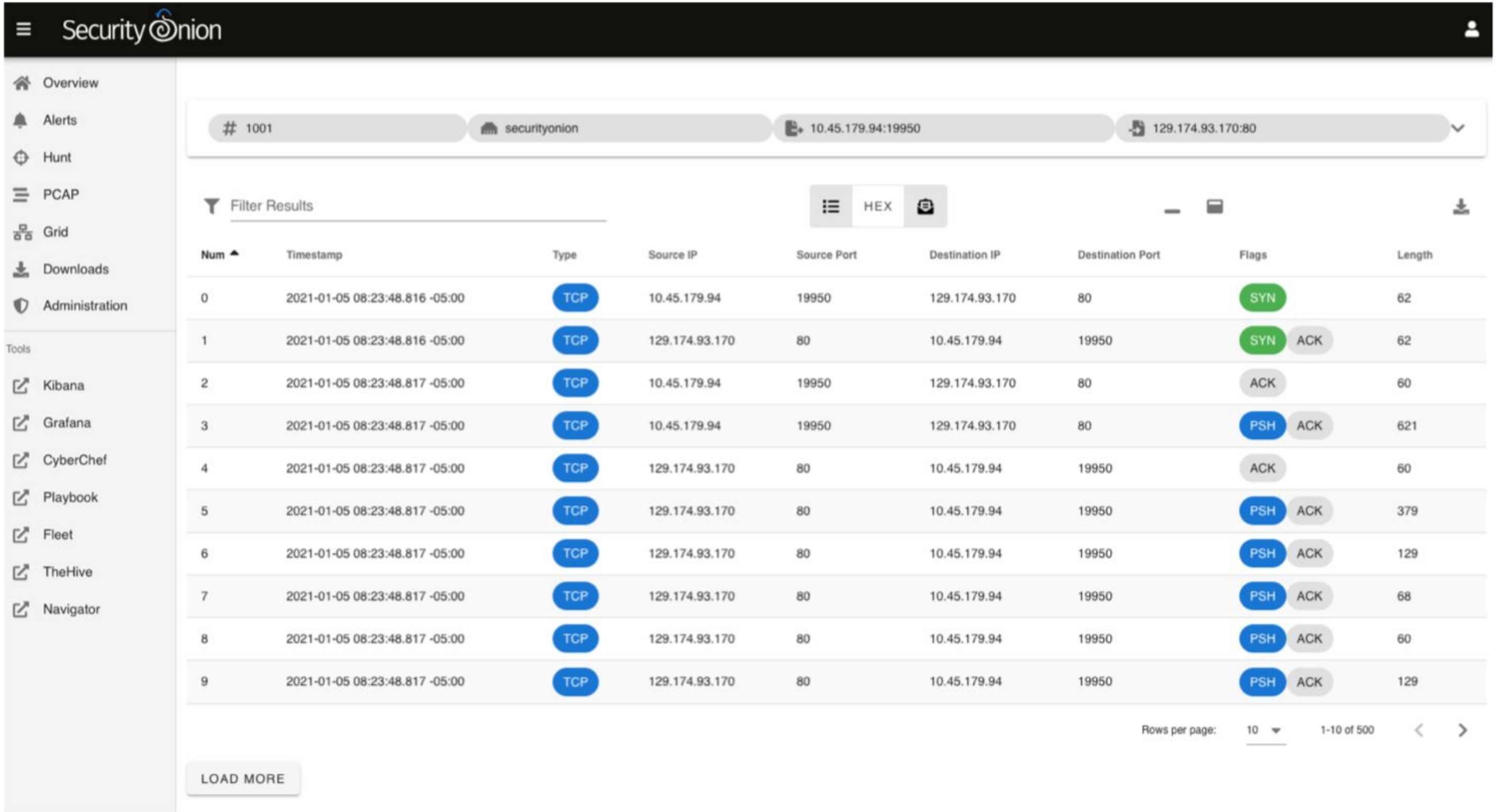
Group: rule.name ⓧ Group: event.module ⓧ Group: event.severity_label ⓧ

		Count	rule.name	event.module	event.severity_label
🔔	⚠	298	ET MALWARE Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102	suricata	high
🔔	⚠	297	ET MALWARE Backdoor family PCRat/Gh0st CnC traffic	suricata	high
🔔	⚠	45	ET MALWARE Gh0st Remote Access Trojan Encrypted Session To CnC Server	suricata	high
🔔	⚠	10	ET POLICY RDP connection confirm	suricata	low
🔔	⚠	9	ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	suricata	high
🔔	⚠	9	ET MALWARE Zbot POST Request to C2	suricata	high
🔔	⚠	9	ET P2P BitTorrent peer sync	suricata	high
🔔	⚠	8	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
🔔	⚠	7	ET HUNTING Observed Interesting Content-Type Inbound (application/x-sh)	suricata	high
🔔	⚠	7	System Audit event.	ossec	low
🔔	⚠	5	ET INFO Hiloti Style GET to PHP with invalid terse MSIE headers	suricata	high

Security Onion Console (SOC) also includes a new *Hunt* interface for threat hunting which allows you to query not only your NIDS/HIDS alerts but also *Zeek* logs and system logs.

PACKET CAPTURE

Security Onion Console (SOC) also includes an interface for full packet capture (*PCAP*) retrieval.

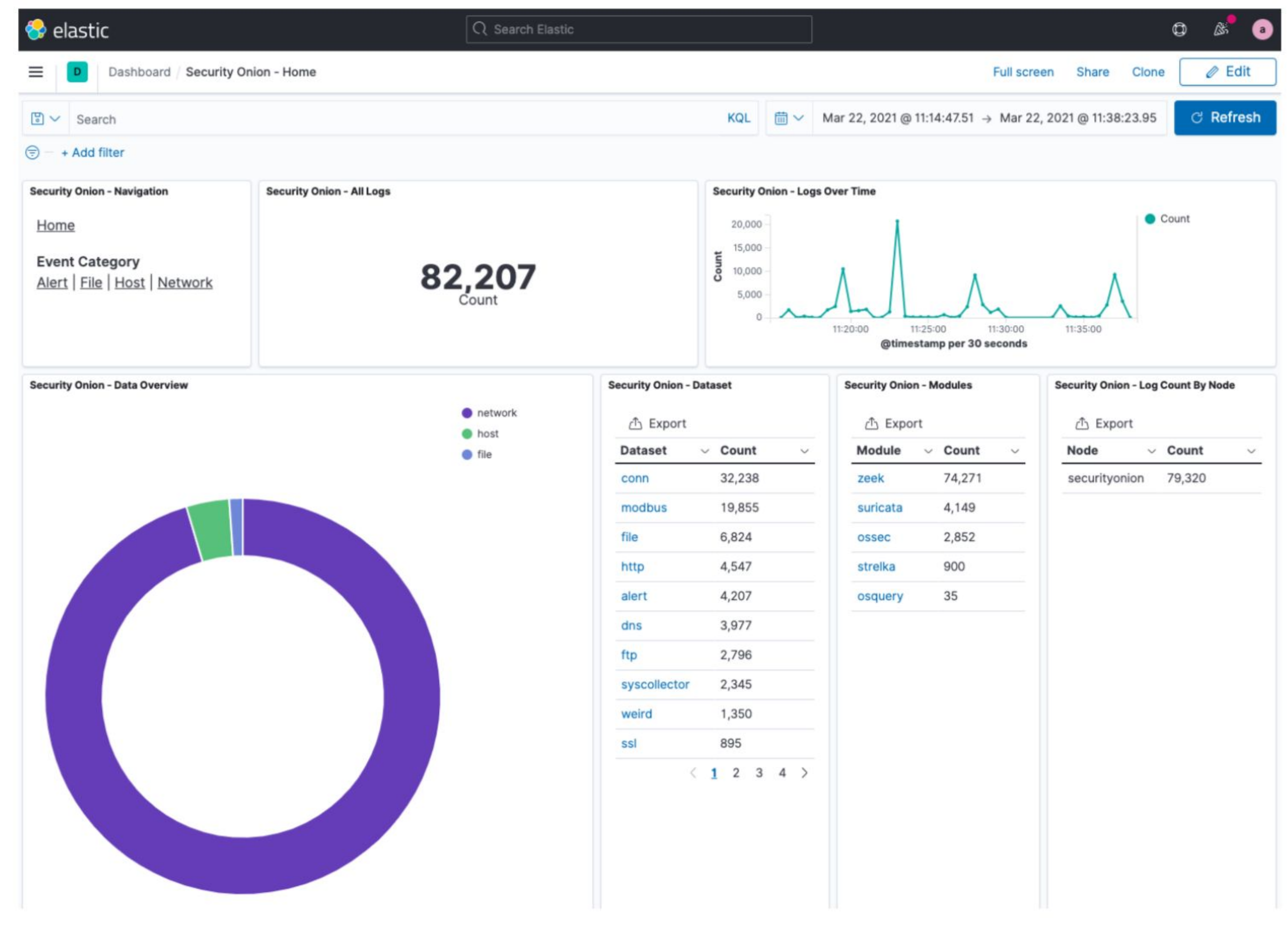


1001 | securityonion | 10.45.179.94:19950 | 129.174.93.170:80

Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags	Length
0	2021-01-05 08:23:48.816 -05:00	TCP	10.45.179.94	19950	129.174.93.170	80	SYN	62
1	2021-01-05 08:23:48.816 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	SYN ACK	62
2	2021-01-05 08:23:48.817 -05:00	TCP	10.45.179.94	19950	129.174.93.170	80	ACK	60
3	2021-01-05 08:23:48.817 -05:00	TCP	10.45.179.94	19950	129.174.93.170	80	PSH ACK	621
4	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	ACK	60
5	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	PSH ACK	379
6	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	PSH ACK	129
7	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	PSH ACK	68
8	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	PSH ACK	60
9	2021-01-05 08:23:48.817 -05:00	TCP	129.174.93.170	80	10.45.179.94	19950	PSH ACK	129

Rows per page: 10 1-10 of 500

DASHBOARD CONSOLE



Mar 22, 2021 @ 11:14:47.51 → Mar 22, 2021 @ 11:38:23.95

Security Onion - Navigation

Home

Event Category

Alert | File | Host | Network

Security Onion - All Logs

82,207

Count

Security Onion - Dataset

Dataset	Count
conn	32,238
modbus	19,855
file	6,824
http	4,547
alert	4,207
dns	3,977
ftp	2,796
syscollector	2,345
weird	1,350
ssl	895

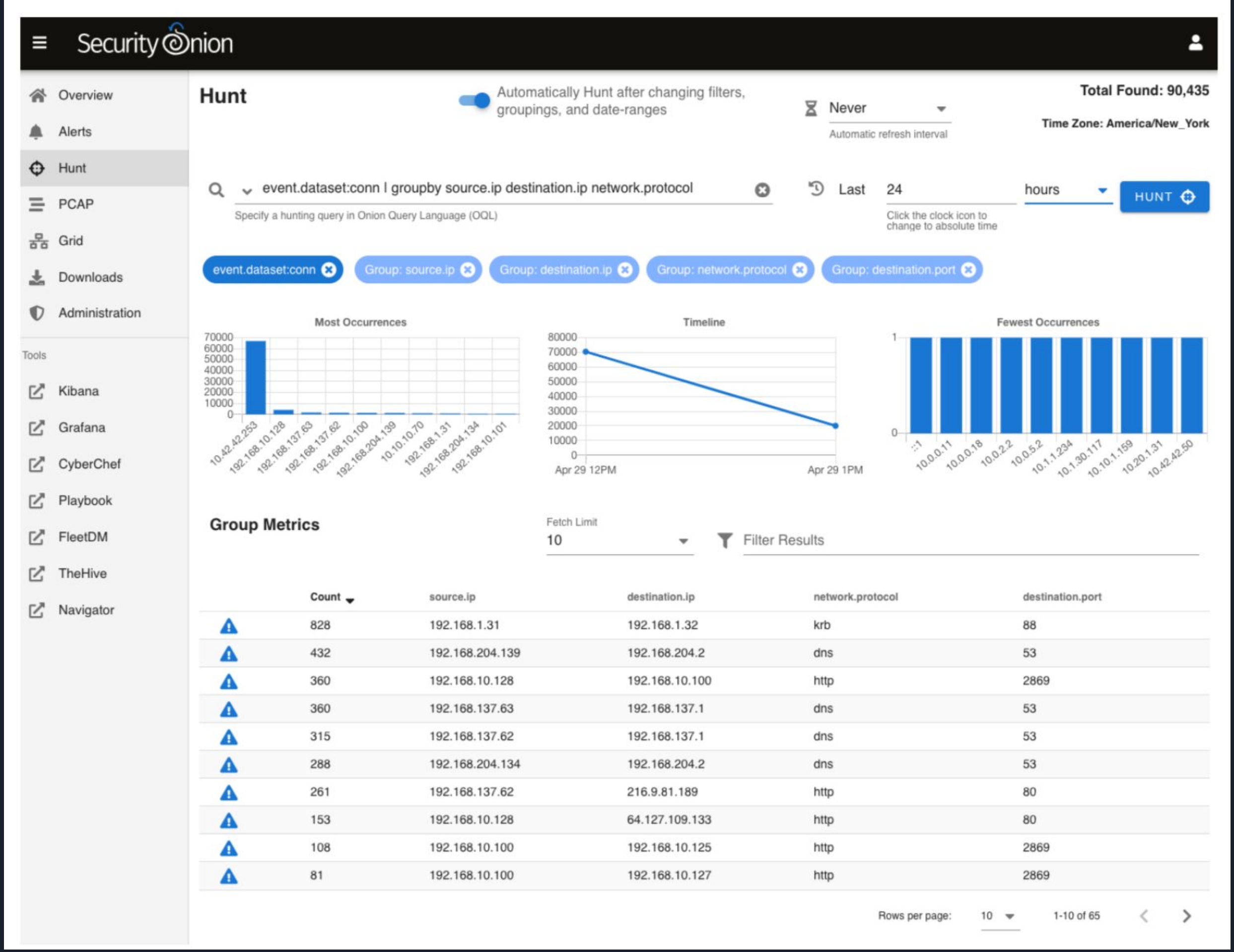
Security Onion - Modules

Module	Count
zeek	74,271
suricata	4,149
ossec	2,852
strelka	900
osquery	35

Security Onion - Log Count By Node

Node	Count
securityonion	79,320

CONSOLE FOR HUNT AND SEE ATTACK SOURCE



Hunt

Automatically Hunt after changing filters, groupings, and date-ranges

Never
Automatic refresh interval

Total Found: 90,435

Time Zone: America/New_York

event.dataset:conn | groupby source.ip destination.ip network.protocol

Specify a hunting query in Onion Query Language (OQL)

Last 24 hours

Click the clock icon to change to absolute time

event.dataset:conn · Group: source.ip · Group: destination.ip · Group: network.protocol · Group: destination.port

Group Metrics

Fetch Limit
10

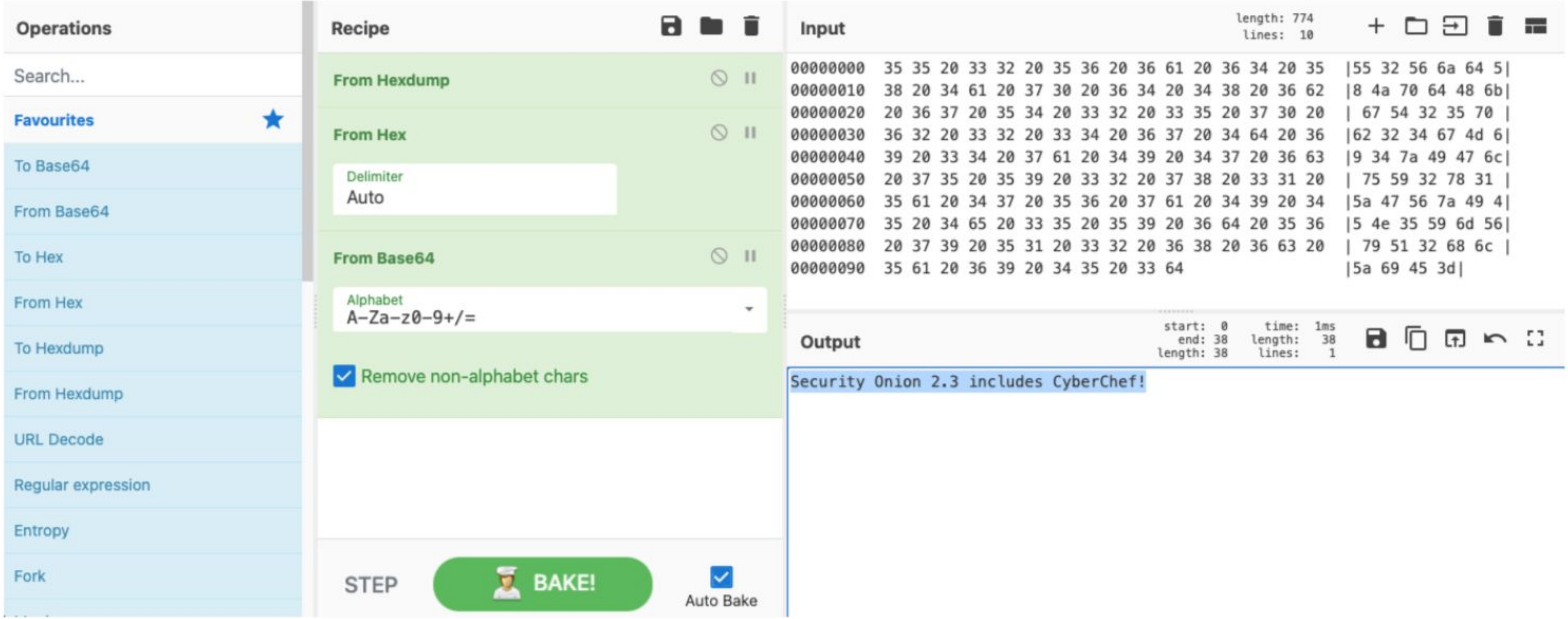
Filter Results

	Count	source.ip	destination.ip	network.protocol	destination.port
⚠	828	192.168.1.31	192.168.1.32	krb	88
⚠	432	192.168.204.139	192.168.204.2	dns	53
⚠	360	192.168.10.128	192.168.10.100	http	2869
⚠	360	192.168.137.63	192.168.137.1	dns	53
⚠	315	192.168.137.62	192.168.137.1	dns	53
⚠	288	192.168.204.134	192.168.204.2	dns	53
⚠	261	192.168.137.62	216.9.81.189	http	80
⚠	153	192.168.10.128	64.127.109.133	http	80
⚠	108	192.168.10.100	192.168.10.125	http	2869
⚠	81	192.168.10.100	192.168.10.127	http	2869

Rows per page: 10 1-10 of 65

CYBERCHEF

CyberChef allows you decode, decompress, and analyze artifacts.



Recipe:

- From Hexdump
- From Hex — Delimiter: Auto
- From Base64 — Alphabet: A-Za-z0-9+/= — ☑ Remove non-alphabet chars

☑ Auto Bake

Input (length: 774, lines: 10):

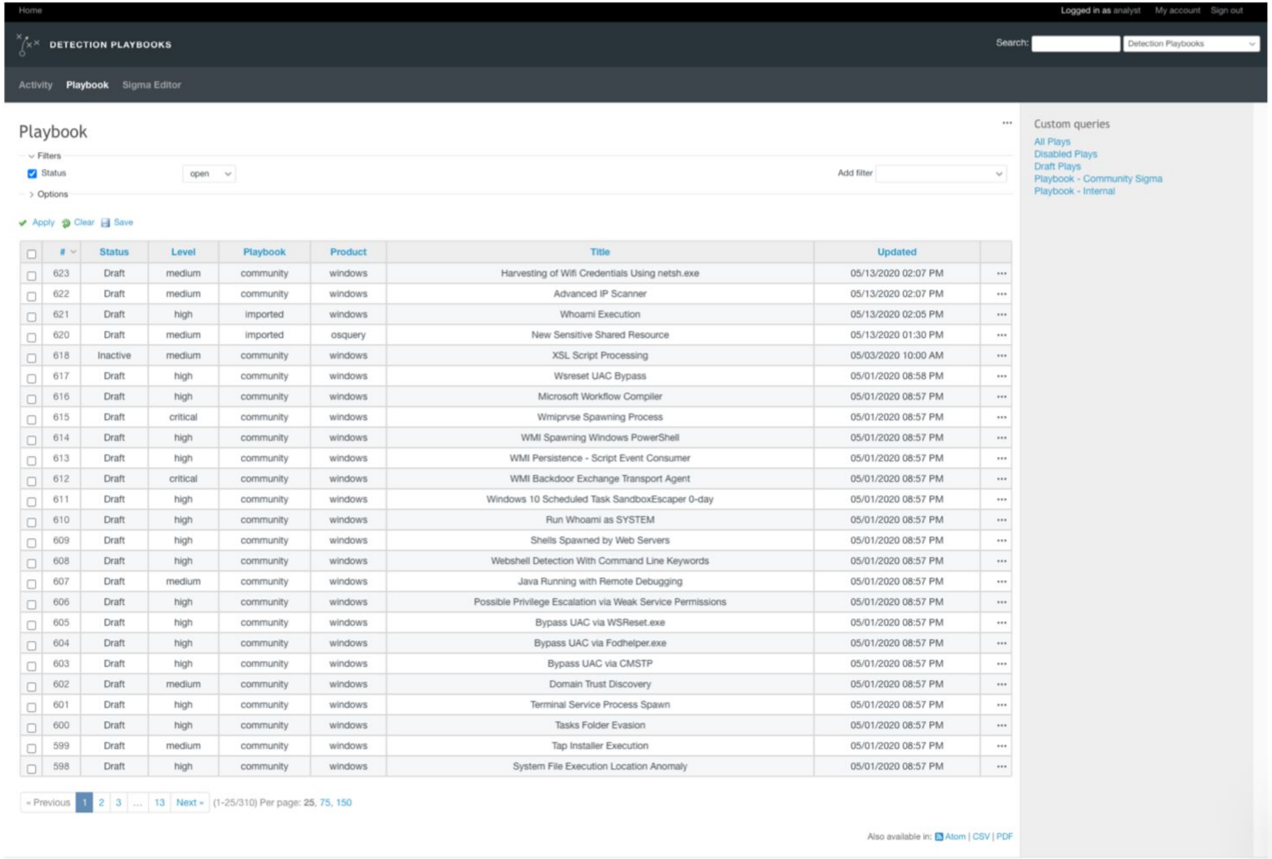
```
00000000  35 35 20 33 32 20 35 36 20 36 61 20 36 34 20 35  |55 32 56 6a 64 5|
00000010  38 20 34 61 20 37 30 20 36 34 20 34 38 20 36 62  |8 4a 70 64 48 6b|
00000020  20 36 37 20 35 34 20 33 32 20 33 35 20 37 30 20  | 67 54 32 35 70 |
00000030  36 32 20 33 32 20 33 34 20 36 37 20 34 64 20 36  |62 32 34 67 4d 6|
00000040  39 20 33 34 20 37 61 20 34 39 20 34 37 20 36 63  |9 34 7a 49 47 6c|
00000050  20 37 35 20 35 39 20 33 32 20 37 38 20 33 31 20  | 75 59 32 78 31 |
00000060  35 61 20 34 37 20 35 36 20 37 61 20 34 39 20 34  |5a 47 56 7a 49 4|
00000070  35 20 34 65 20 33 35 20 35 39 20 36 64 20 35 36  |5 4e 35 59 6d 56|
00000080  20 37 39 20 35 31 20 33 32 20 36 38 20 36 63 20  | 79 51 32 68 6c |
00000090  35 61 20 36 39 20 34 35 20 33 64                 |5a 69 45 3d|
```

Output (start: 0, end: 38, length: 38; time: 1ms, length: 38, lines: 1):

```
Security Onion 2.3 includes CyberChef!
```

PLAYBOOK

Playbook is a web application that allows you to create a Detection Playbook, which itself consists of individual plays. These plays are fully self-contained and describe the different aspects around the particular detection strategy.



Playbook

Filters

☑ Status open

Add filter

Options

✓ Apply Clear Save

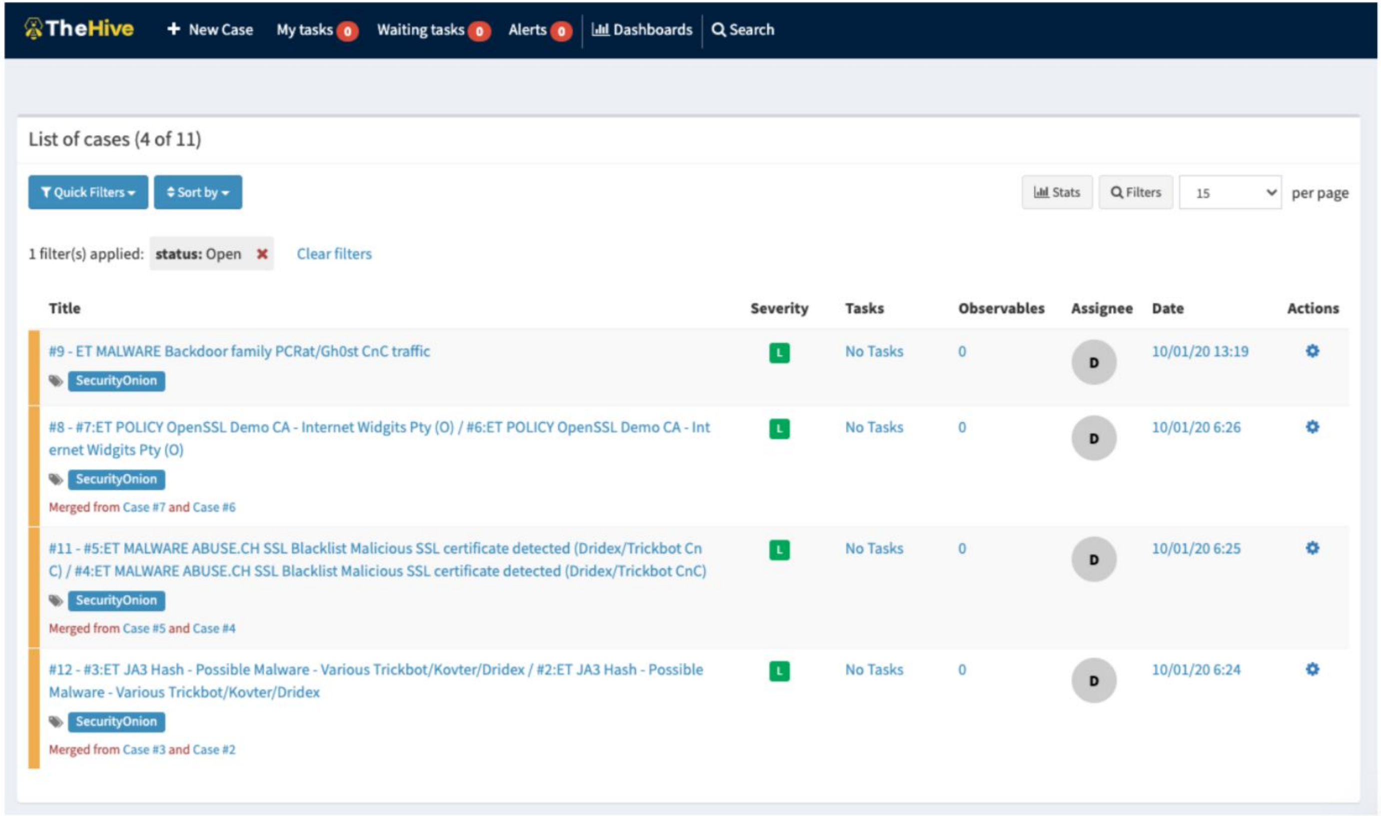
□	#	Status	Level	Playbook	Product	Title	Updated	
□	623	Draft	medium	community	windows	Harvesting of Wifi Credentials Using netsh.exe	05/13/2020 02:07 PM	···
□	622	Draft	medium	community	windows	Advanced IP Scanner	05/13/2020 02:07 PM	···
□	621	Draft	high	imported	windows	Whoami Execution	05/13/2020 02:05 PM	···
□	620	Draft	medium	imported	osquery	New Sensitive Shared Resource	05/13/2020 01:30 PM	···
□	618	Inactive	medium	community	windows	XSL Script Processing	05/03/2020 10:00 AM	···
□	617	Draft	high	community	windows	Wsreset UAC Bypass	05/01/2020 08:58 PM	···
□	616	Draft	high	community	windows	Microsoft Workflow Compiler	05/01/2020 08:57 PM	···
□	615	Draft	critical	community	windows	Wmiprvse Spawning Process	05/01/2020 08:57 PM	···
□	614	Draft	high	community	windows	WMI Spawning Windows PowerShell	05/01/2020 08:57 PM	···
□	613	Draft	high	community	windows	WMI Persistence - Script Event Consumer	05/01/2020 08:57 PM	···
□	612	Draft	critical	community	windows	WMI Backdoor Exchange Transport Agent	05/01/2020 08:57 PM	···
□	611	Draft	high	community	windows	Windows 10 Scheduled Task SandboxEscaper 0-day	05/01/2020 08:57 PM	···
□	610	Draft	high	community	windows	Run Whoami as SYSTEM	05/01/2020 08:57 PM	···
□	609	Draft	high	community	windows	Shells Spawned by Web Servers	05/01/2020 08:57 PM	···
□	608	Draft	high	community	windows	Webshell Detection With Command Line Keywords	05/01/2020 08:57 PM	···
□	607	Draft	medium	community	windows	Java Running with Remote Debugging	05/01/2020 08:57 PM	···
□	606	Draft	high	community	windows	Possible Privilege Escalation via Weak Service Permissions	05/01/2020 08:57 PM	···
□	605	Draft	high	community	windows	Bypass UAC via WSReset.exe	05/01/2020 08:57 PM	···
□	604	Draft	high	community	windows	Bypass UAC via Fodhelper.exe	05/01/2020 08:57 PM	···
□	603	Draft	high	community	windows	Bypass UAC via CMSTP	05/01/2020 08:57 PM	···
□	602	Draft	medium	community	windows	Domain Trust Discovery	05/01/2020 08:57 PM	···
□	601	Draft	high	community	windows	Terminal Service Process Spawn	05/01/2020 08:57 PM	···
□	600	Draft	high	community	windows	Tasks Folder Evasion	05/01/2020 08:57 PM	···
□	599	Draft	medium	community	windows	Tap Installer Execution	05/01/2020 08:57 PM	···
□	598	Draft	high	community	windows	System File Execution Location Anomaly	05/01/2020 08:57 PM	···

« Previous 1 2 3 … 13 Next » (1-25/310) Per page: 25, 75, 150

Also available in: Atom | CSV | PDF

HIVE

TheHive is the case management interface. As you are working in *Alerts*, *Hunt*, or *Kibana*, you may find alerts or logs that are interesting enough to send to *TheHive* and create a case. Other analysts can collaborate with you as you work to close that case.

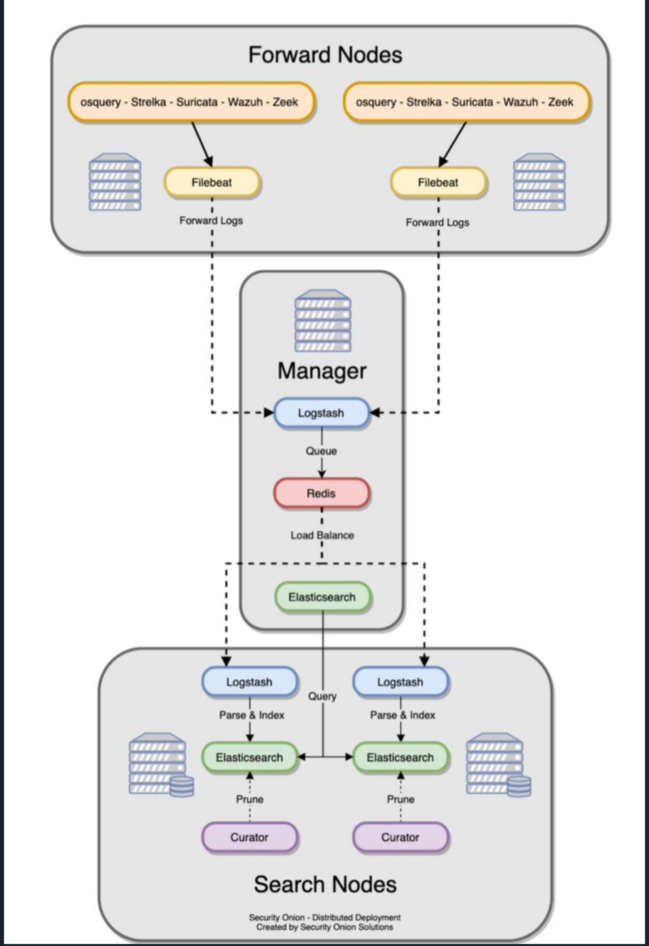


List of cases (4 of 11)

1 filter(s) applied: **status:** Open ✖

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#9 - ET MALWARE Backdoor family PCRat/Gh0st CnC traffic SecurityOnion	L	No Tasks	0	D	10/01/20 13:19	⚙
#8 - #7:ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) / #6:ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O) SecurityOnion Merged from Case #7 and Case #6	L	No Tasks	0	D	10/01/20 6:26	⚙
#11 - #5:ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) / #4:ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) SecurityOnion Merged from Case #5 and Case #4	L	No Tasks	0	D	10/01/20 6:25	⚙
#12 - #3:ET JA3 Hash - Possible Malware - Various Trickbot/Kovter/Dridex / #2:ET JA3 Hash - Possible Malware - Various Trickbot/Kovter/Dridex SecurityOnion Merged from Case #3 and Case #2	L	No Tasks	0	D	10/01/20 6:24	⚙

ARCHITECTURE DESIGN AND SUPPORT HIGH LOAD OF LOG


Forward Nodes
osquery - Strelka - Suricata - Wazuh - Zeek
osquery - Strelka - Suricata - Wazuh - Zeek
Filebeat
Filebeat
Forward Logs
Forward Logs
Manager
Logstash
Queue
Redis
Load Balance
Elasticsearch
Logstash
Logstash
Query
Parse & Index
Parse & Index
Elasticsearch
Elasticsearch
Prune
Prune
Curator
Curator
Search Nodes
Security Onion - Distributed Deployment
Created by Security Onion Solutions