CIS:3370 Intrusion to Investigation

Part I

Chavez | Turner

User Story

On May 14, 2021, our team was alerted to an intrusion within our system, we as the digital forensics team, and we as the intrusion detection team, were requested to study the case, documented in the GitHub is our findings (Digital Forensics) and our solutions to prevent this from happening in the future (Intrusion Detection). The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Due to the recent event we, as the IDS team, will be working with the digital forensics team, not only find the root of the problem but also come together and create a solution so that this will not happen again.

Summary of the Project

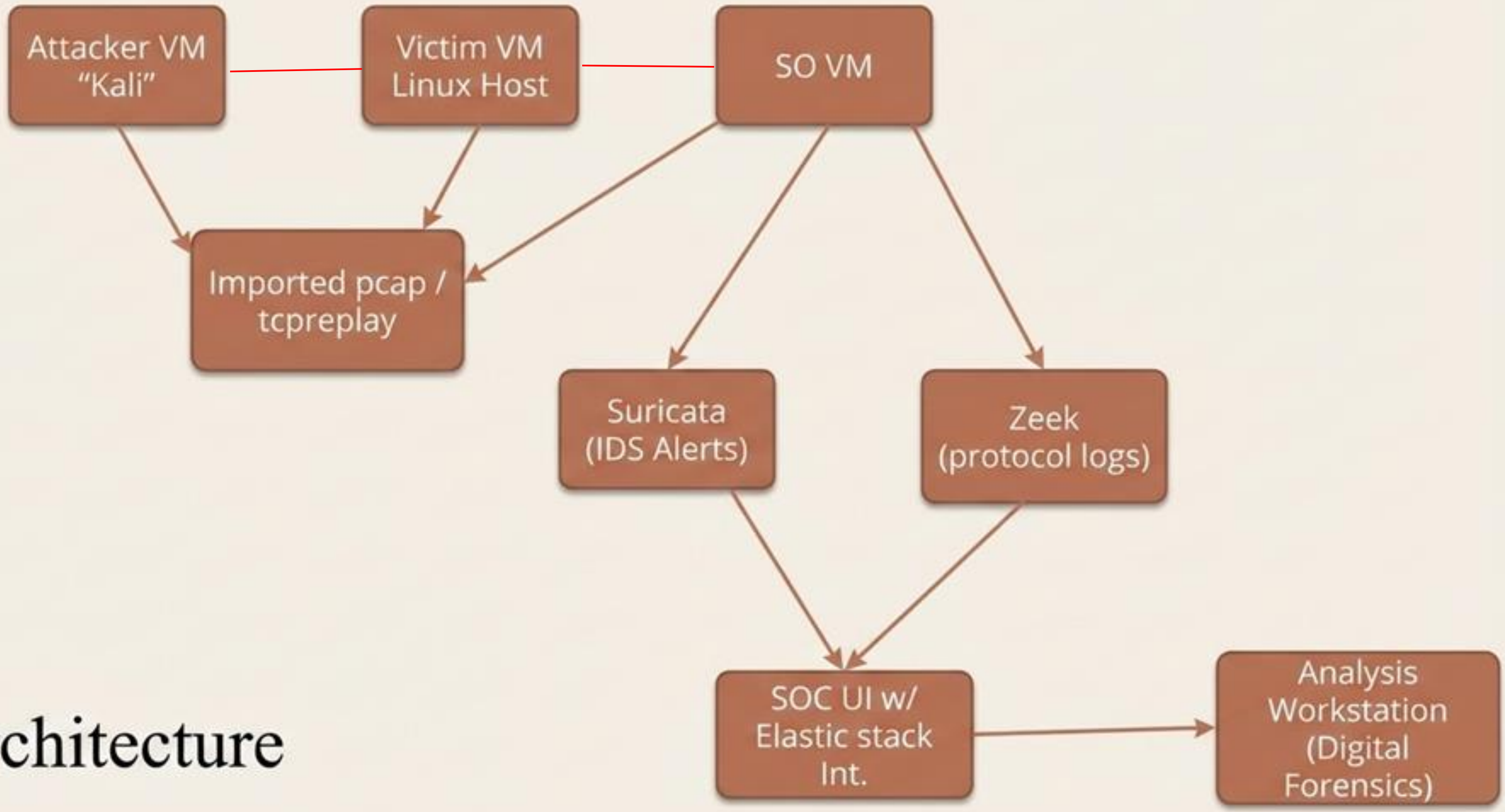
For this project, we will be implementing an intrusion detection system, utilizing suricata. For this we will be implementing our own clauses into suricata, and from there creating a system that we can gather more information for further projects.

Scope

This project designs, implements, and documents an end-to-end workflow that uses Security Onion (Suricata + Zeek) and Wireshark-based digital forensics to detect, reconstruct, and analyze a malware infection in captured network traffic, then produce actionable IOCs, a case report, and a short live demo that shows how detection and investigation work together.

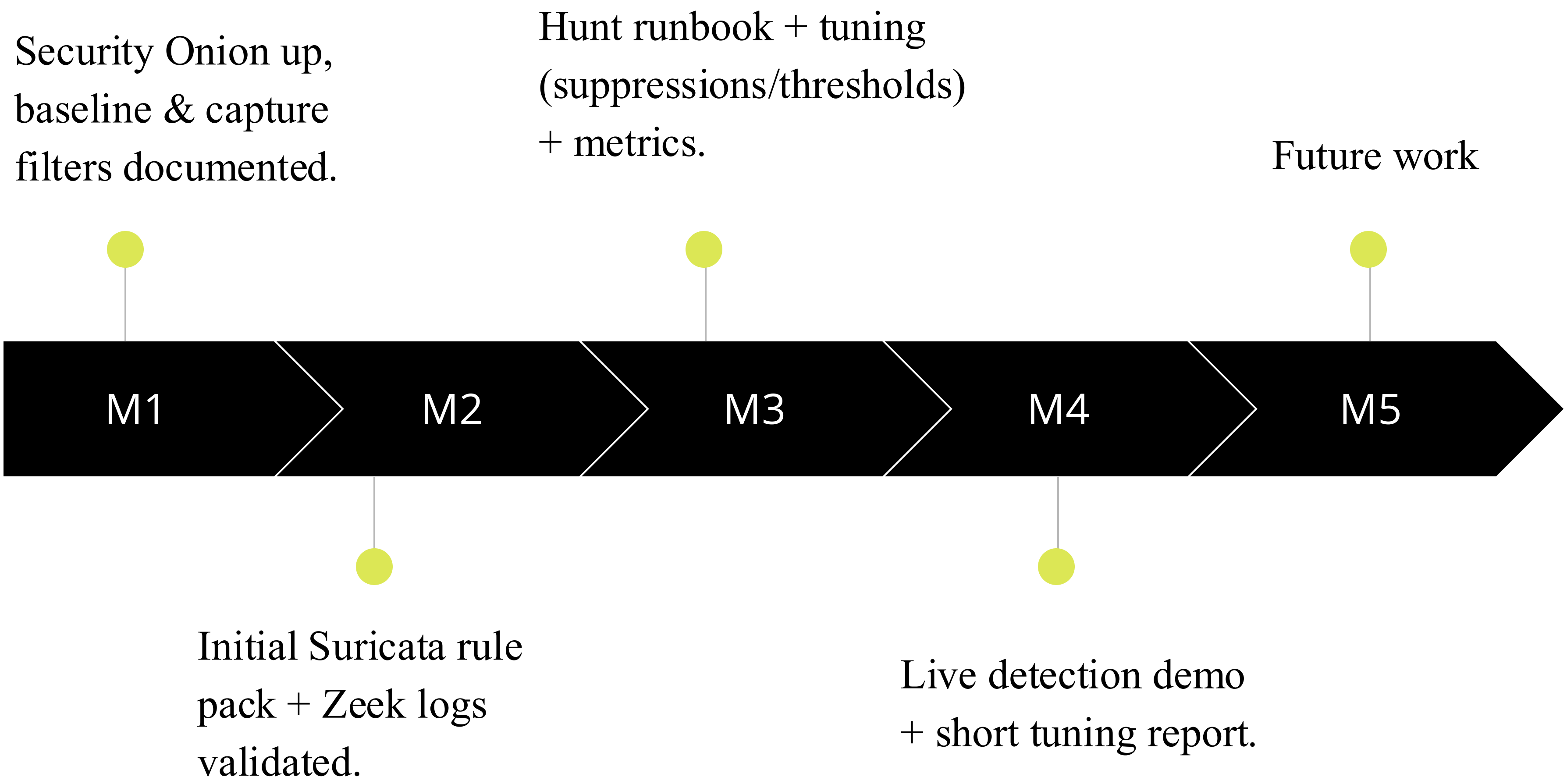
Materials

- A system with Wireshark
- VMware
- Security Onion
- Kali system run through the VM
- https://www.malware-traffic-analysis.net/index.html
- Private network, to be able to utilize security onion and its resources without anything blocking or interfering



Architecture

MILESTONES



M1: Security Onion up, baseline & capture filters documented.

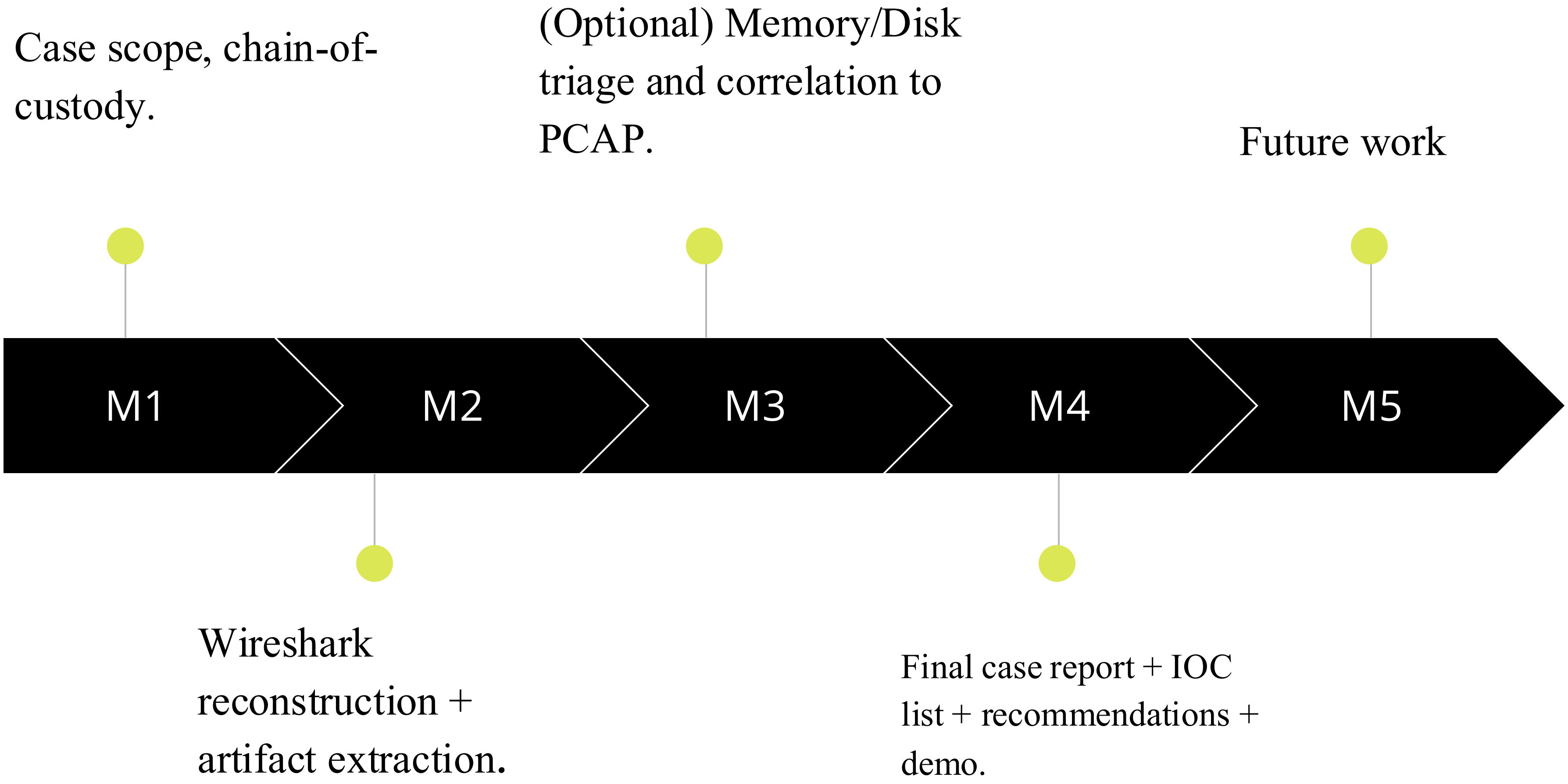
M2: Initial Suricata rule pack + Zeek logs validated.

M3: Hunt runbook + tuning (suppressions/thresholds) + metrics.

M4: Live detection demo + short tuning report.

M5: Future work

IDS



M1

Case scope, chain-of-custody.

M2

Wireshark reconstruction + artifact extraction.

M3

(Optional) Memory/Disk triage and correlation to PCAP.

M4

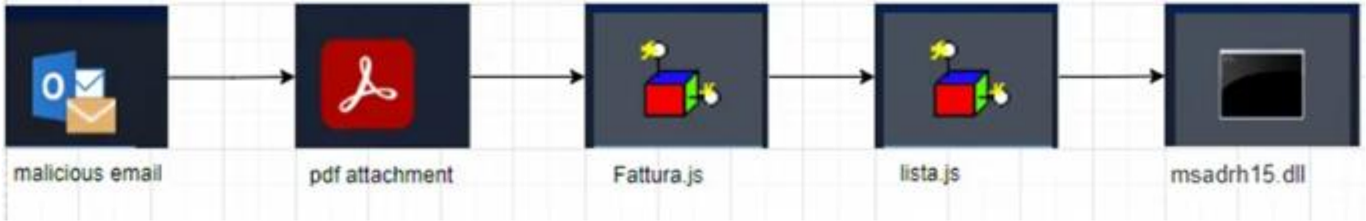
Final case report + IOC list + recommendations + demo.

M5

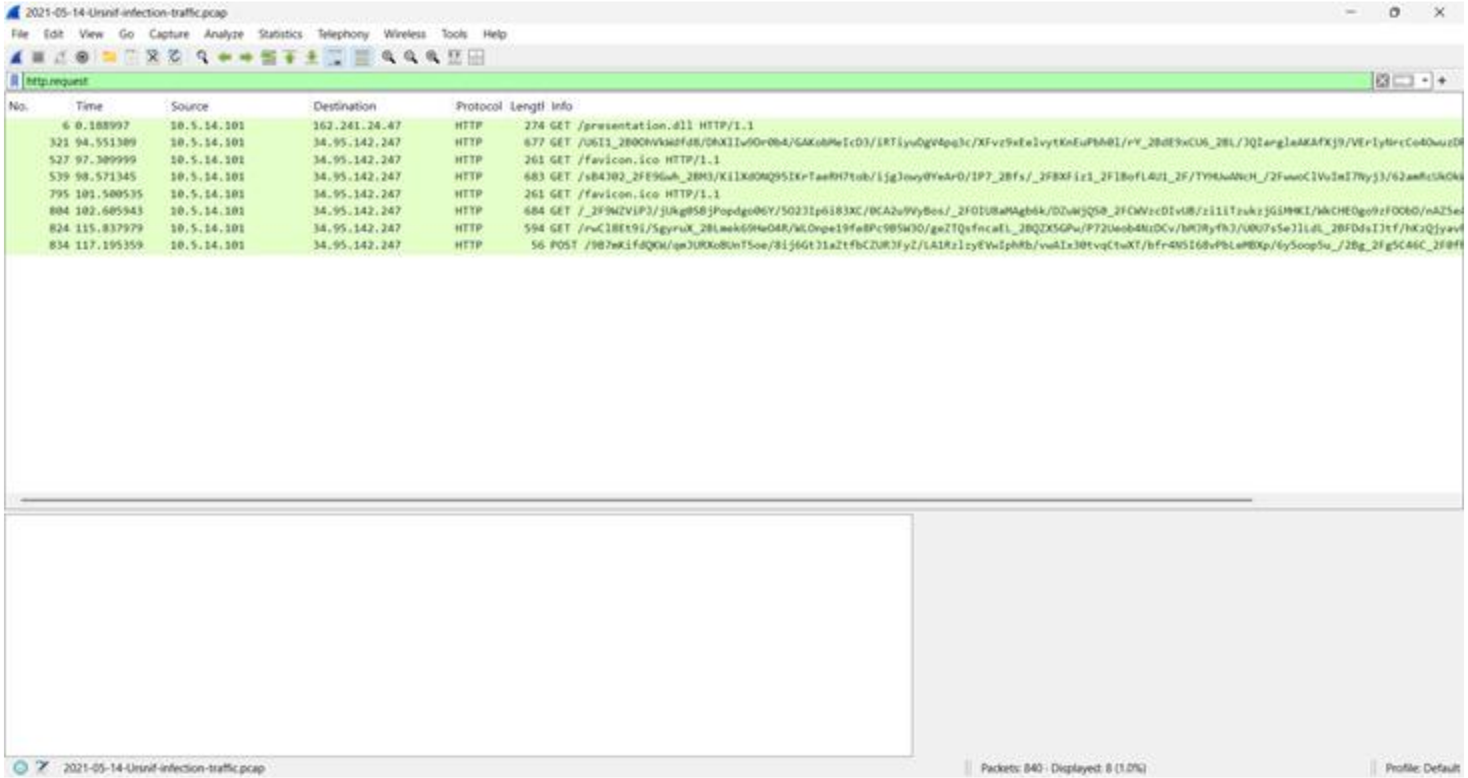
Future work

Initial Attack

The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Trojan Path is as follows:



Wireshark Analysis of Pcap file

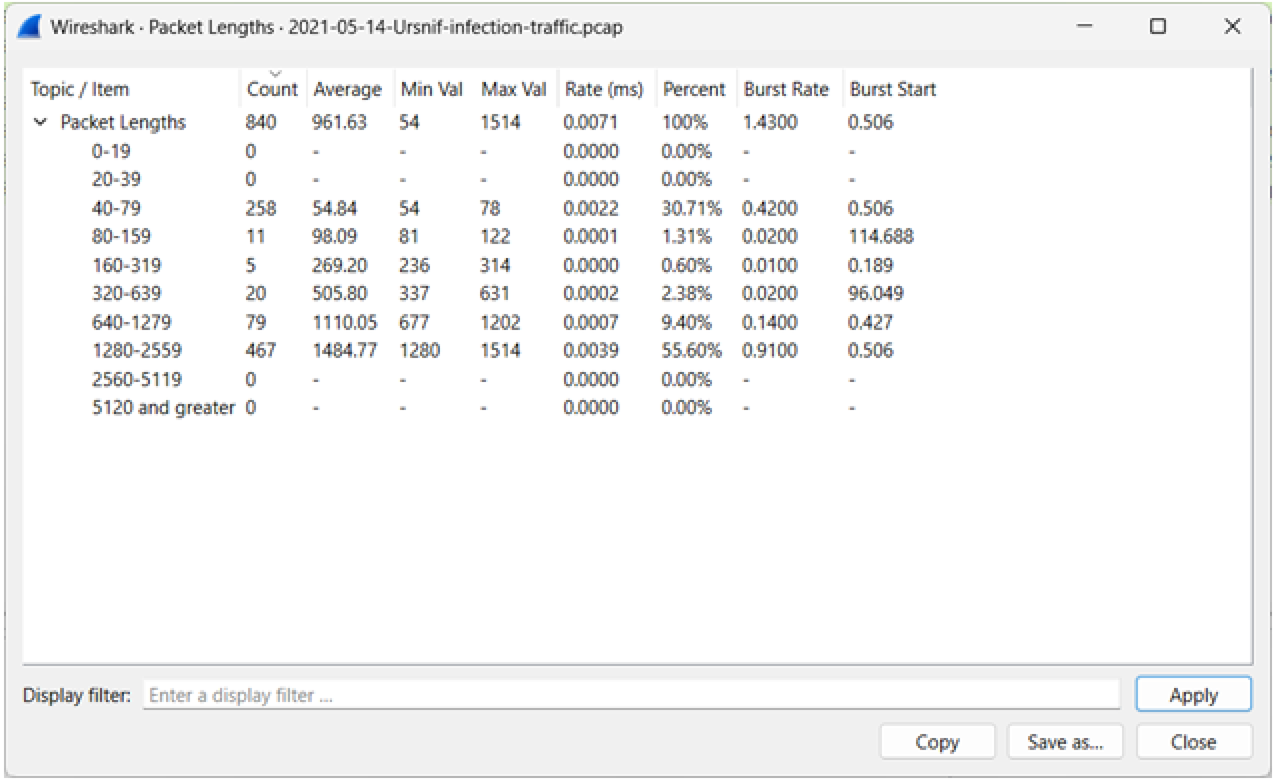


http.request

```
No.     Time          Source          Destination       Protocol Lengtl Info
      6 0.188997      10.5.14.101     162.241.24.47     HTTP      274 GET /presentation.dll HTTP/1.1
    321 94.551309     10.5.14.101     34.95.142.247     HTTP      677 GET /U6I1_2B0OhVkWdfd8/OhXIIw9Or0b4/GAKobMeIcD3/iRTiyuOgV4pq3c/XFvz9xEelvytKnEuPbhNl/rY_2BdE9xCU6_2BL/JQIangleAKAfKj9/VErlyNrcCo4OwuzD
    527 97.309999     10.5.14.101     34.95.142.247     HTTP      261 GET /favicon.ico HTTP/1.1
    539 98.571345     10.5.14.101     34.95.142.247     HTTP      683 GET /sB4J02_2FE9GwA_2BM3/KilKdONQ95IKrTaeRH7tob/ijgJowy0YeArO/1P7_2Bfs/_2FBXFiz1_2FlBofL4U1_2F/TYHJwANcH_/2FwwoClVuImI7Nyj3/62amRcSkOk
    795 101.500535    10.5.14.101     34.95.142.247     HTTP      261 GET /favicon.ico HTTP/1.1
    804 102.605943    10.5.14.101     34.95.142.247     HTTP      684 GET /_2F9WZViPJ/jUkg0S8jPopdgo06Y/5O2JIp6i83XC/0CA2u9VyBos/_2FOIUBaMAgb6k/DZuWjQS0_2FCWVzcDIvUB/zi1iTzukzjGiMHKI/WkCHEOgo9zFOObO/nAZSe
    824 115.837979    10.5.14.101     34.95.142.247     HTTP      594 GET /rwCl8Et9i/SgyruX_2BLmek69HeO4R/WLOnpe19fe8Pc9B5W3O/geZTQsfncaEL_2BQZX5GPw/P72Ueob4NzDCv/bMJRyfhJ/U0U7s5eJlLdL_2BFDdsIJtf/hKzQjyav
    834 117.195359    10.5.14.101     34.95.142.247     HTTP       56 POST /9B7mKifdQKW/qmJURKo8UnT5oe/8ij6GtJ1aZtfbCZURJFyZ/LA1RzlzyEVwIphRb/vwAIx30tvqCtwXf/bfr4NSI68vPbLeMBXp/6y5oop5u_/2Bg_2Fg5C46C_2F0f
```

2021-05-14-Ursnif-infection-traffic.pcap   Packets: 840 · Displayed: 8 (1.0%)   Profile: Default

Wireshark Analysis of Pcap File

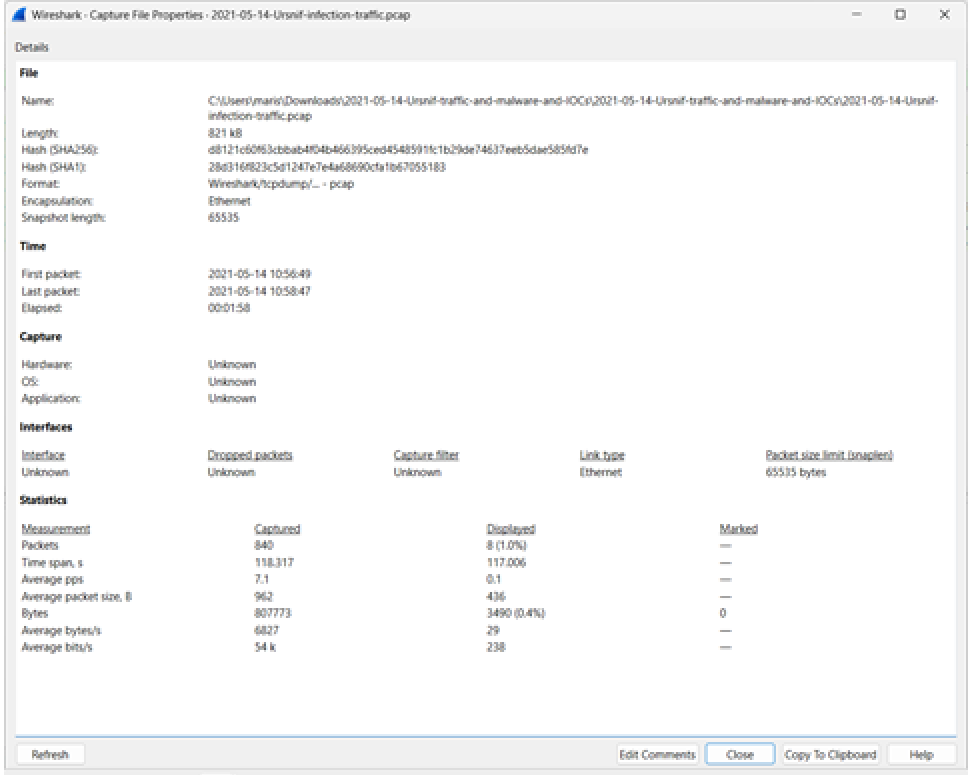


Wireshark · Packet Lengths · 2021-05-14-Ursnif-infection-traffic.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	840	961.63	54	1514	0.0071	100%	1.4300	0.506
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	258	54.84	54	78	0.0022	30.71%	0.4200	0.506
80-159	11	98.09	81	122	0.0001	1.31%	0.0200	114.688
160-319	5	269.20	236	314	0.0000	0.60%	0.0100	0.189
320-639	20	505.80	337	631	0.0002	2.38%	0.0200	96.049
640-1279	79	1110.05	677	1202	0.0007	9.40%	0.1400	0.427
1280-2559	467	1484.77	1280	1514	0.0039	55.60%	0.9100	0.506
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter: Enter a display filter ...

Wireshark Statistics (Filtered)



Wireshark · Capture File Properties · 2021-05-14-Ursnif-infection-traffic.pcap
Details

File

Name:	C:\Users\maris\Downloads\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-infection-traffic.pcap
Length:	821 kB
Hash (SHA256):	d8121c60f63cbbab4f04b466395ced4548591fc1b29de74637eeb5dae585fd7e
Hash (SHA1):	28d316f823c5d1247e7e4a68690cfa1b67055183
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2021-05-14 10:56:49
Last packet:	2021-05-14 10:58:47
Elapsed:	00:01:58

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

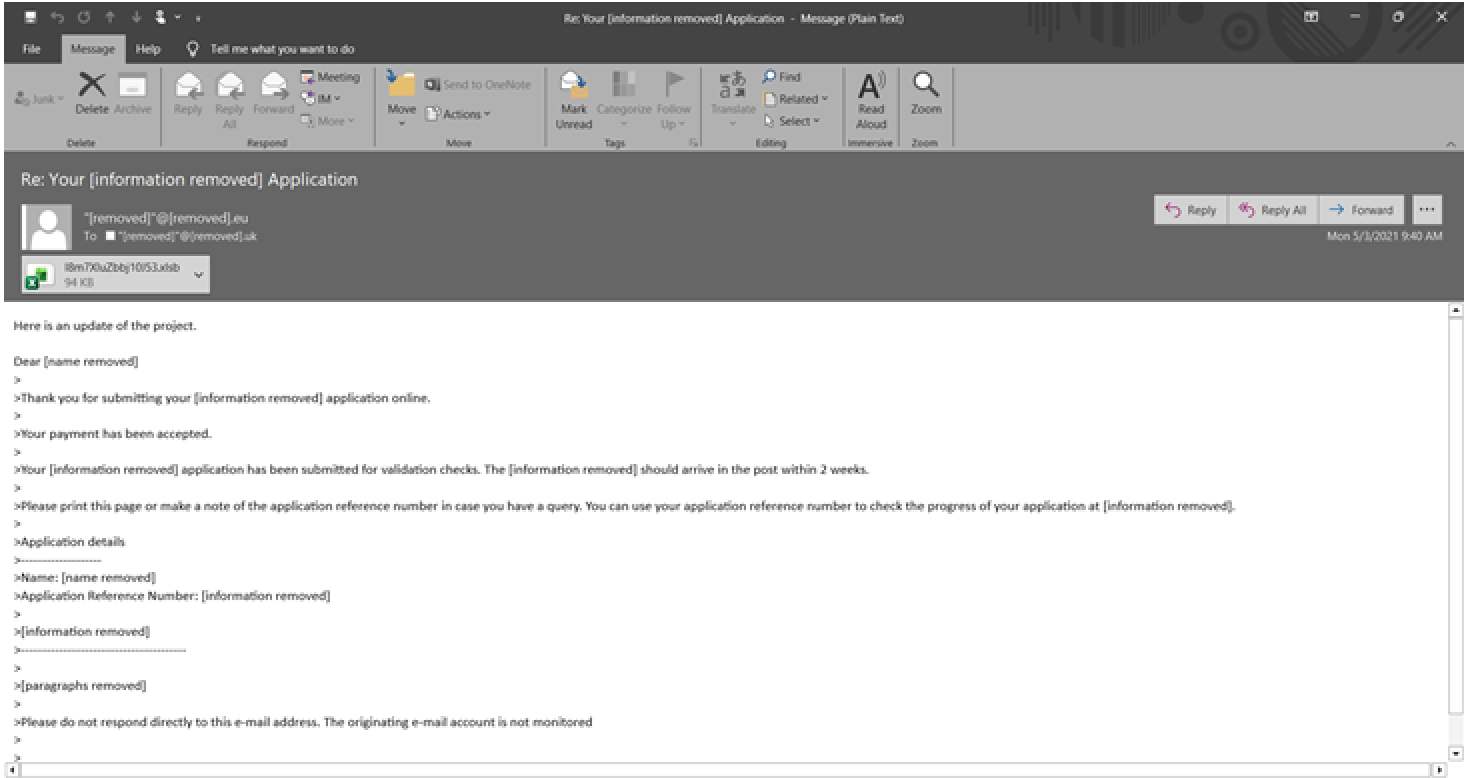
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	840	8 (1.0%)	—
Time span, s	118.317	117.006	—
Average pps	7.1	0.1	—
Average packet size, B	962	436	—
Bytes	807773	3490 (0.4%)	0
Average bytes/s	6827	29	—
Average bits/s	54 k	238	—

Original Phishing email



Re: Your [information removed] Application - Message (Plain Text)

Re: Your [information removed] Application

"[removed]"@[removed].eu

To "[removed]"@[removed].uk

Mon 5/3/2021 9:40 AM

i8m7X0uZbbj10/53.xlsb
94 KB

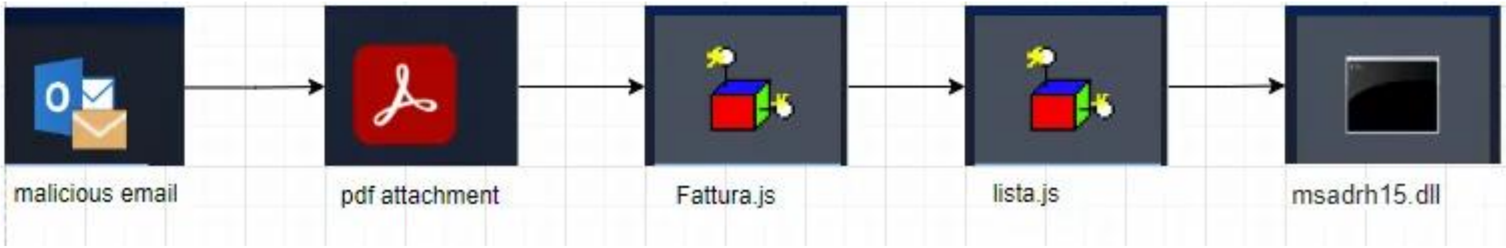
Here is an update of the project.

Dear [name removed]
>
>Thank you for submitting your [information removed] application online.
>
>Your payment has been accepted.
>
>Your [information removed] application has been submitted for validation checks. The [information removed] should arrive in the post within 2 weeks.
>
>Please print this page or make a note of the application reference number in case you have a query. You can use your application reference number to check the progress of your application at [information removed].
>
>Application details
>--------------------
>Name: [name removed]
>Application Reference Number: [information removed]
>
>[information removed]
>--
>
>[paragraphs removed]
>
>Please do not respond directly to this e-mail address. The originating e-mail account is not monitored
>
>

Ursnif, the banking trojan

Ursnif is a variant of the GOZI malware, usually disguises itself as a part of an invoice, was first seen in 2006, but had its script leaked in 2015, making it more accessible to other. So now it has a github:

- https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md



Milestone 1 - Security Onion, Baseline & capture

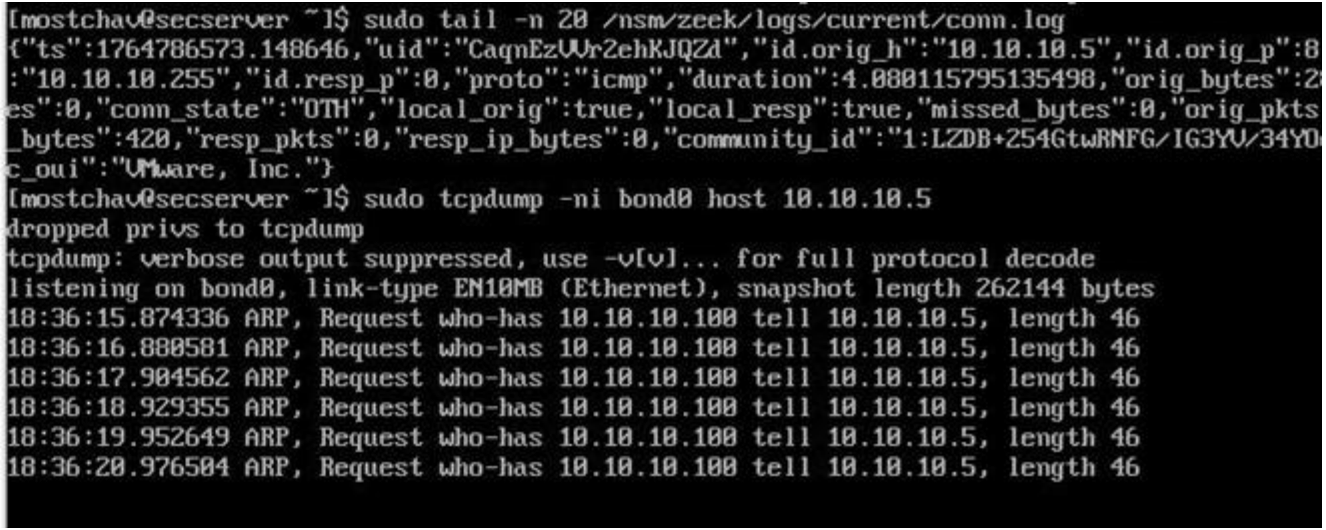
- Environment online
    - Security Onion
    - Kali
- Monitor using SO
- Gathering baseline traffic
- Capture Filters

M1 – Environment online and monitoring

- NIC/bridge configuration in Security Onion. See Figure 1.

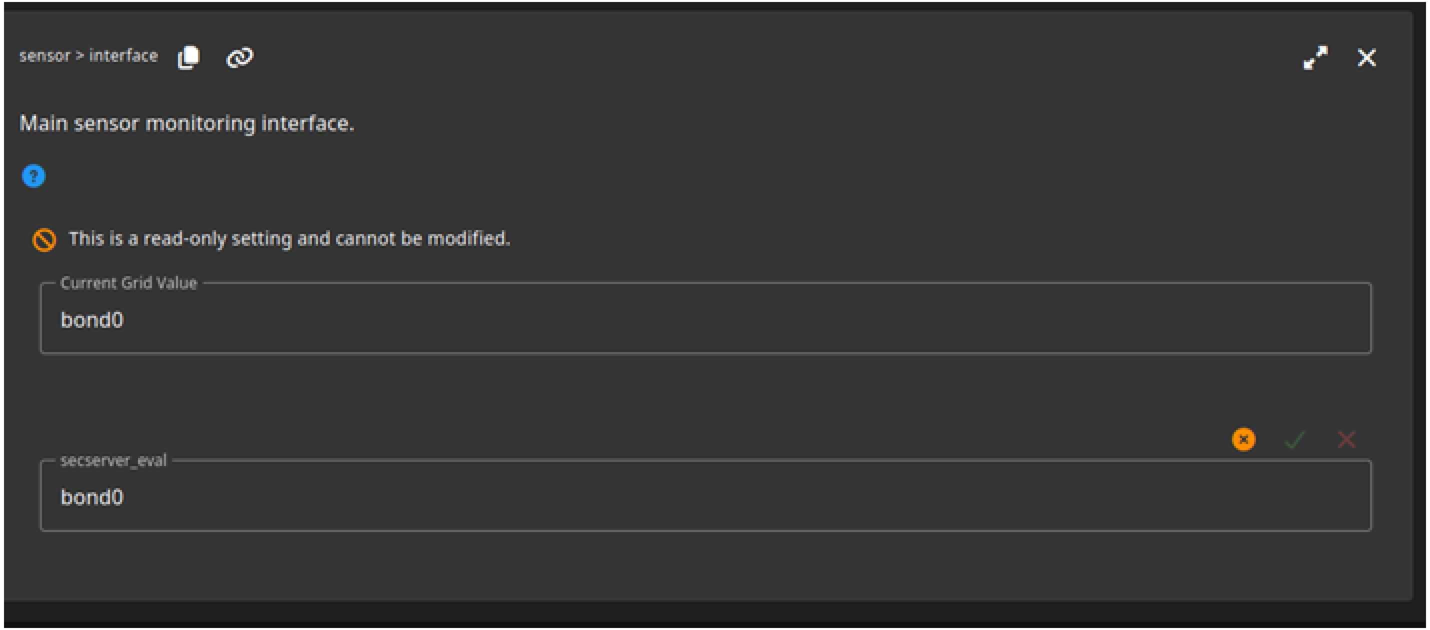
- Confirmed the sensor was actually seeing traffic from the lab network. See Figure 2.

M1-Figure 1



```
[mostchav@secserver ~]$ sudo tail -n 20 /nsm/zeek/logs/current/conn.log
{"ts":1764786573.148646,"uid":"CaqnEzVVr2ehKJQZd","id.orig_h":"10.10.10.5","id.orig_p":8
:"10.10.10.255","id.resp_p":0,"proto":"icmp","duration":4.080115795135498,"orig_bytes":2
es":0,"conn_state":"OTH","local_orig":true,"local_resp":true,"missed_bytes":0,"orig_pkts
_bytes":420,"resp_pkts":0,"resp_ip_bytes":0,"community_id":"1:LZDB+254GtwRNFG/IG3YV/34YO
c_oui":"VMware, Inc."}
[mostchav@secserver ~]$ sudo tcpdump -ni bond0 host 10.10.10.5
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on bond0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:36:15.874336 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
18:36:16.880581 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
18:36:17.904562 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
18:36:18.929355 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
18:36:19.952649 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
18:36:20.976504 ARP, Request who-has 10.10.10.100 tell 10.10.10.5, length 46
```

M1- Figure 2



sensor > interface

Main sensor monitoring interface.

This is a read-only setting and cannot be modified.

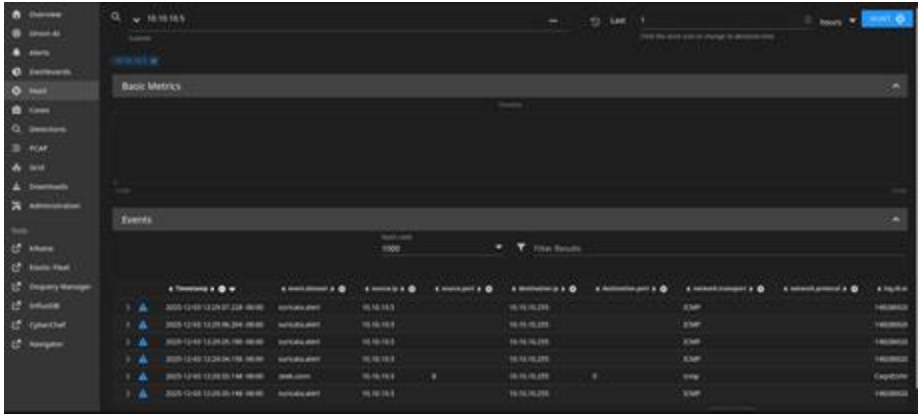
Current Grid Value: bond0

secserver_eval: bond0

M1 – Baseline traffic + capture filters

- Collected baseline traffic (normal browsing / no attacks).

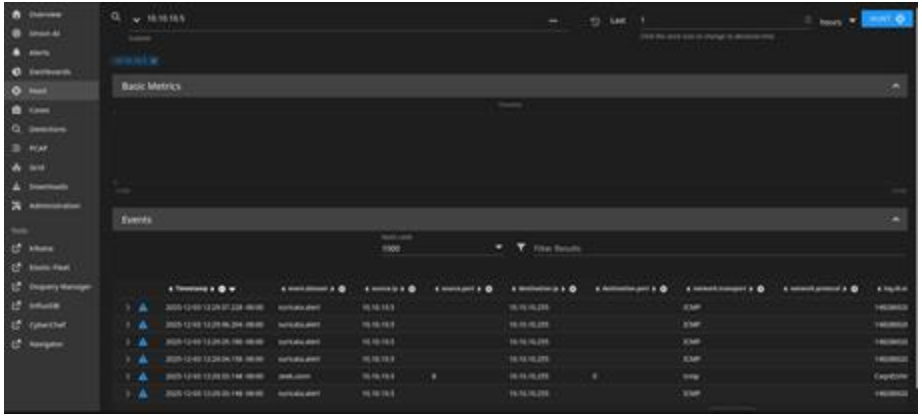
- Documented capture filter used (e.g. “only monitor relevant lab subnet and necessary ports”).



Milestone 2 - Rules + Zeek validation

- Configure Suricata
- Configure Zeek
- Rule Packs

Milestone 2 - Rules + Zeek validation



Timestamp	event.dataset	source.ip	source.port	destination.ip	destination.port	network.transport	network.protocol	log.id
[illegible]	suricata.alert	10.10.10.5		10.10.10.255		ICMP		[illegible]
[illegible]	suricata.alert	10.10.10.5		10.10.10.255		ICMP		[illegible]
[illegible]	suricata.alert	10.10.10.5		10.10.10.255		ICMP		[illegible]
[illegible]	suricata.alert	10.10.10.5		10.10.10.255		ICMP		[illegible]
[illegible]	zeek.conn	10.10.10.5	8	10.10.10.255	0	icmp		[illegible]
[illegible]	suricata.alert	10.10.10.5		10.10.10.255		ICMP		[illegible]

- Collected baseline traffic (normal browsing / no attacks).
- Documented capture filter used (e.g. “only monitor relevant lab subnet and necessary ports”).

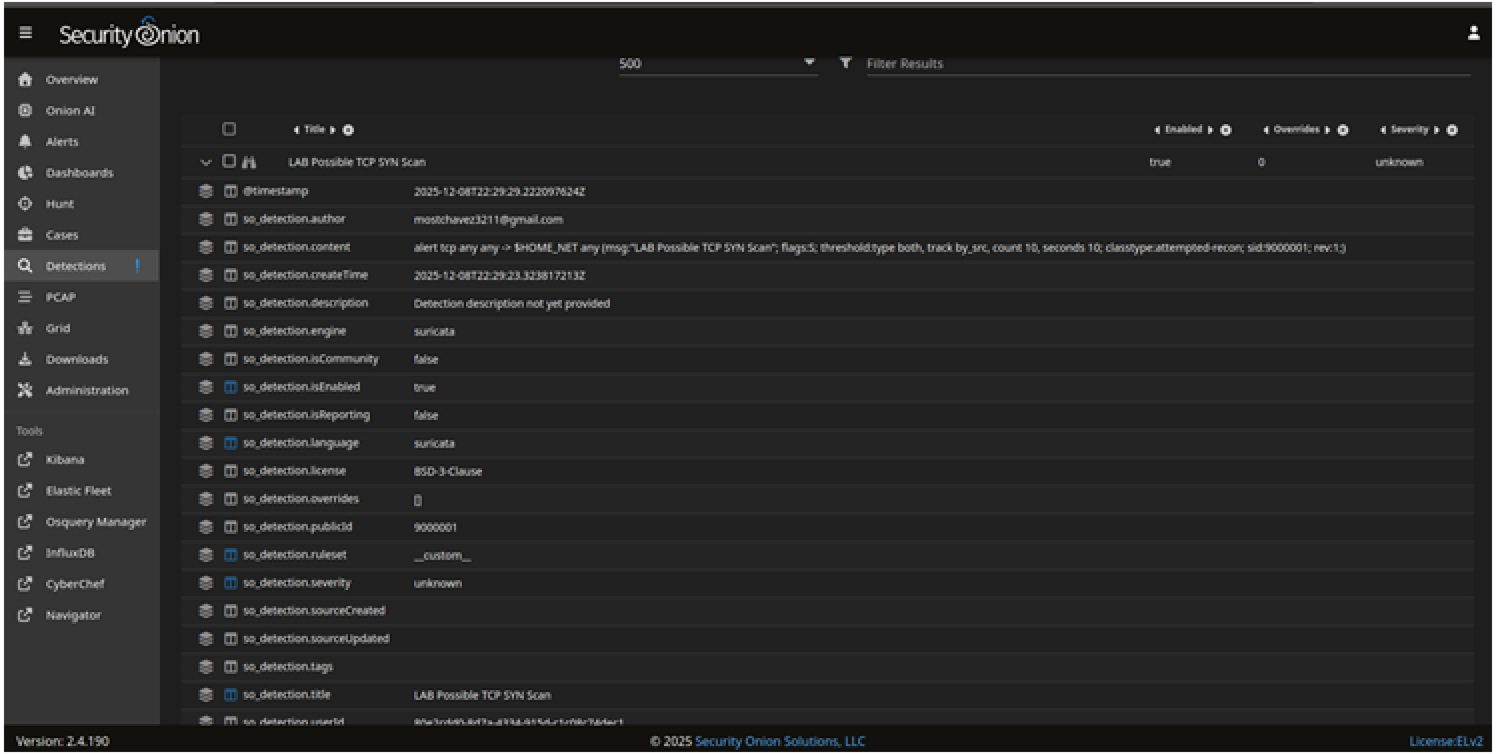
M2 – Suricata rule pack + Zeek validation

Wrote a small custom rule pack for three attacks:

- Port scanning
- HTTP attack pattern
- SSH brute-force

Enabled and tested them in Security Onion.

M2 - Port scan detection (Suricata + Zeek)



□ Title	Enabled	Overrides	Severity
LAB Possible TCP SYN Scan	true	0	unknown

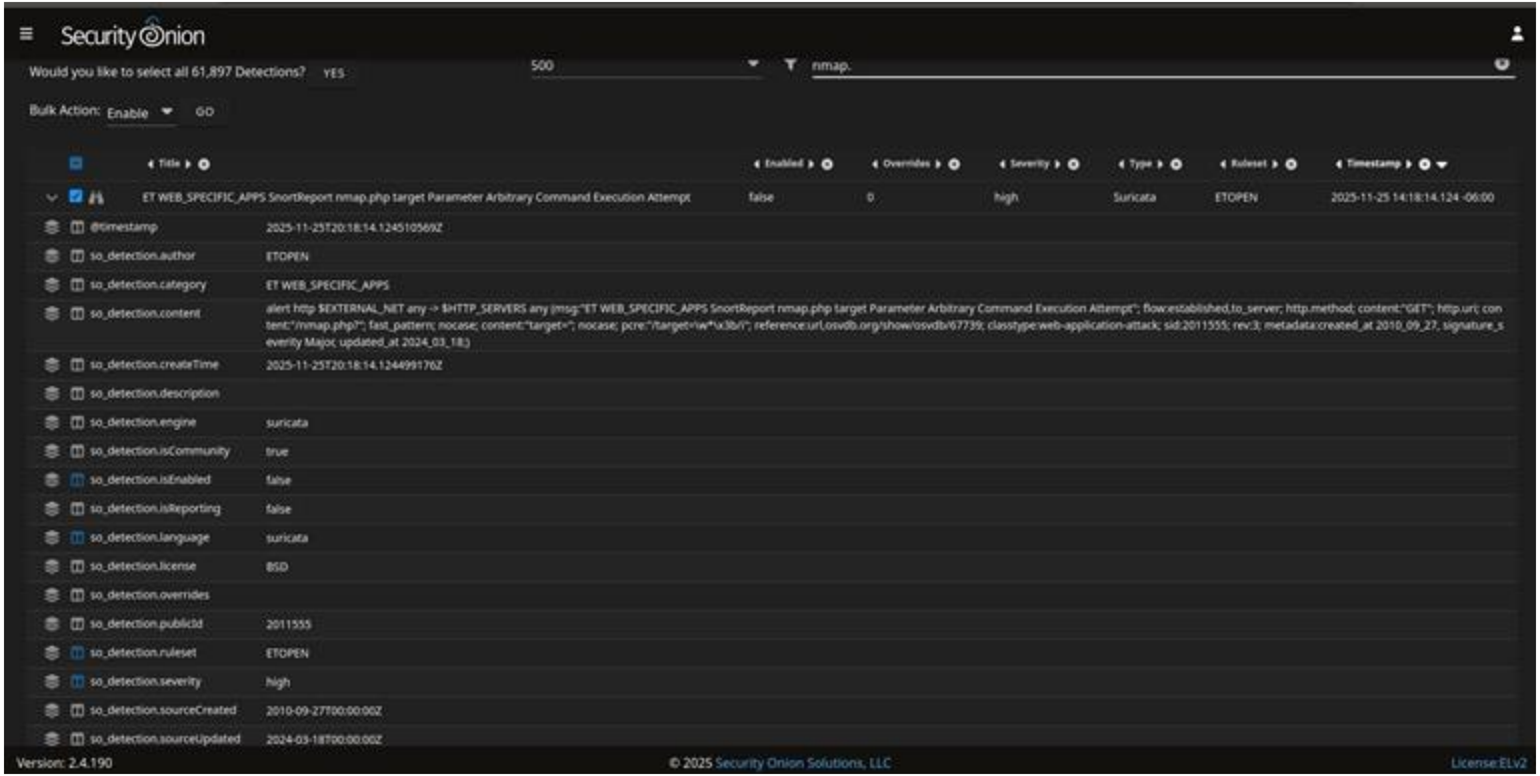
@timestamp	2025-12-08T22:29:29.222097624Z
so_detection.author	mostchavez3211@gmail.com
so_detection.content	alert tcp any any -> $HOME_NET any (msg:"LAB Possible TCP SYN Scan"; flags:S; threshold:type both, track by_src, count 10, seconds 10; classtype:attempted-recon; sid:9000001; rev:1;)
so_detection.createTime	2025-12-08T22:29:23.323817213Z
so_detection.description	Detection description not yet provided
so_detection.engine	suricata
so_detection.isCommunity	false
so_detection.isEnabled	true
so_detection.isReporting	false
so_detection.language	suricata
so_detection.license	BSD-3-Clause
so_detection.overrides	[]
so_detection.publicId	9000001
so_detection.ruleset	__custom__
so_detection.severity	unknown
so_detection.sourceCreated	
so_detection.sourceUpdated	
so_detection.tags	
so_detection.title	LAB Possible TCP SYN Scan
so_detection.userId	80e3cd4f0-8d7a-4334-815d-c1c09c7dd4ec1

Version: 2.4.190

© 2025 Security Onion Solutions, LLC

License:ELv2

M2 - HTTP attack detection



Would you like to select all 61,897 Detections? YES

500 ▾ | nmap.

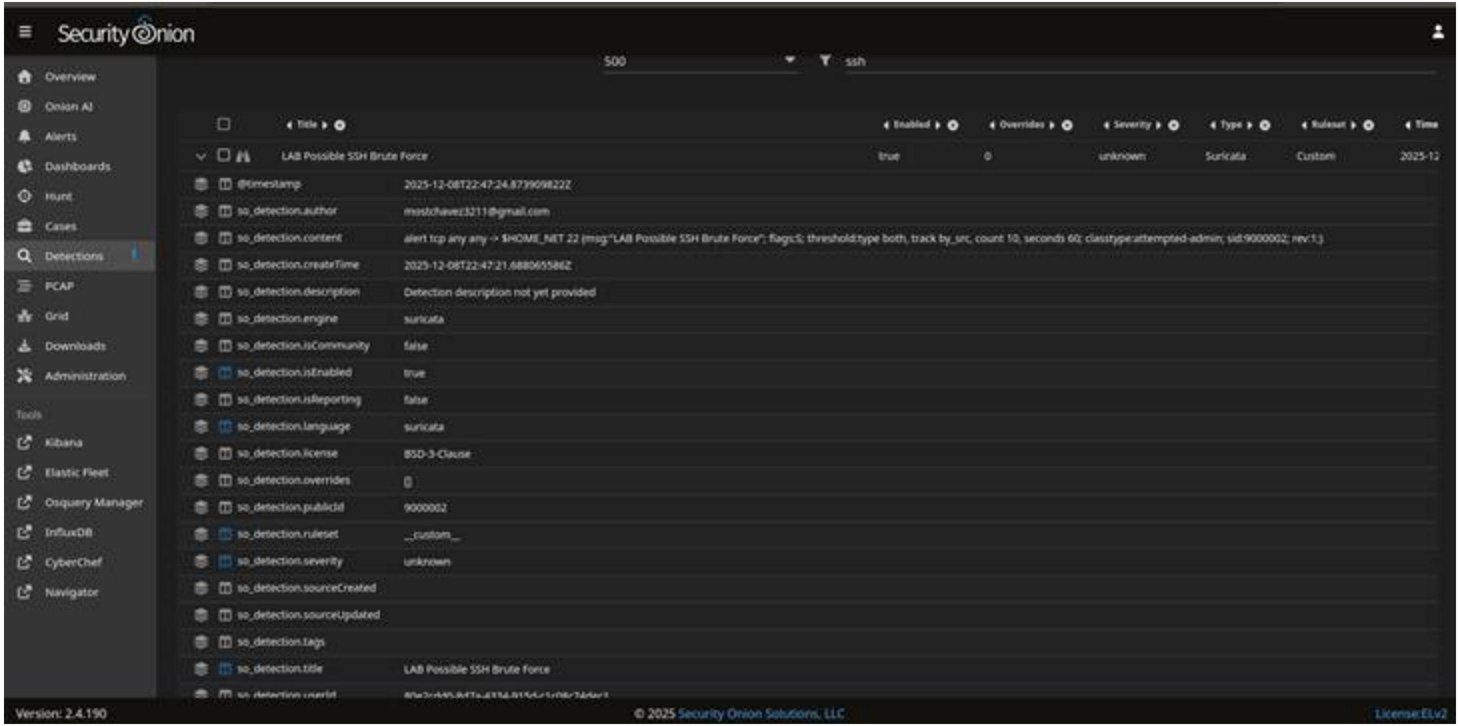
Bulk Action: Enable ▾ GO

	Title	Enabled	Overrides	Severity	Type	Ruleset	Timestamp
☑	ET WEB_SPECIFIC_APPS SnortReport nmap.php target Parameter Arbitrary Command Execution Attempt	false	0	high	Suricata	ETOPEN	2025-11-25 14:18:14.124 -06:00

@timestamp	2025-11-25T20:18:14.124510569Z
so_detection.author	ETOPEN
so_detection.category	ET WEB_SPECIFIC_APPS
so_detection.content	alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SPECIFIC_APPS SnortReport nmap.php target Parameter Arbitrary Command Execution Attempt"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"/nmap.php?"; fast_pattern; nocase; content:"target="; nocase; pcre:"/target=\w*\x3b/i"; reference:url,osvdb.org/show/osvdb/67739; classtype:web-application-attack; sid:2011555; rev:3; metadata:created_at 2010_09_27, signature_severity Major, updated_at 2024_03_18;)
so_detection.createTime	2025-11-25T20:18:14.124499176Z
so_detection.description	
so_detection.engine	suricata
so_detection.isCommunity	true
so_detection.isEnabled	false
so_detection.isReporting	false
so_detection.language	suricata
so_detection.license	BSD
so_detection.overrides	
so_detection.publicId	2011555
so_detection.ruleset	ETOPEN
so_detection.severity	high
so_detection.sourceCreated	2010-09-27T00:00:00Z
so_detection.sourceUpdated	2024-03-18T00:00:00Z

Version: 2.4.190 © 2025 Security Onion Solutions, LLC License:ELv2

M2 - SSH brute-force detection



500 ▾ ssh

□	Title	Enabled	Overrides	Severity	Type	Ruleset	Time
□	LAB Possible SSH Brute Force	true	0	unknown	Suricata	Custom	2025-12

@timestamp	2025-12-08T22:47:24.873909822Z
so_detection.author	mostchavez3211@gmail.com
so_detection.content	alert tcp any any -> $HOME_NET 22 (msg:"LAB Possible SSH Brute Force"; flags:S; threshold:type both, track by_src, count 10, seconds 60; classtype:attempted-admin; sid:9000002; rev:1;)
so_detection.createTime	2025-12-08T22:47:21.688065586Z
so_detection.description	Detection description not yet provided
so_detection.engine	suricata
so_detection.isCommunity	false
so_detection.isEnabled	true
so_detection.isReporting	false
so_detection.language	suricata
so_detection.license	BSD-3-Clause
so_detection.overrides	[]
so_detection.publicId	9000002
so_detection.ruleset	__custom__
so_detection.severity	unknown
so_detection.sourceCreated	
so_detection.sourceUpdated	
so_detection.tags	
so_detection.title	LAB Possible SSH Brute Force
so_detection.userId	80e2cd45-8d7a-4334-915d-c1c08c74dec1

Version: 2.4.190

© 2025 Security Onion Solutions, LLC

License:ELv2

Milestone 3 – Hunt runbook, tuning, metrics

- Create a Hunt runbook
- Test and tune it
- Gather metrics

M3 – Hunt runbook: from alert → decision

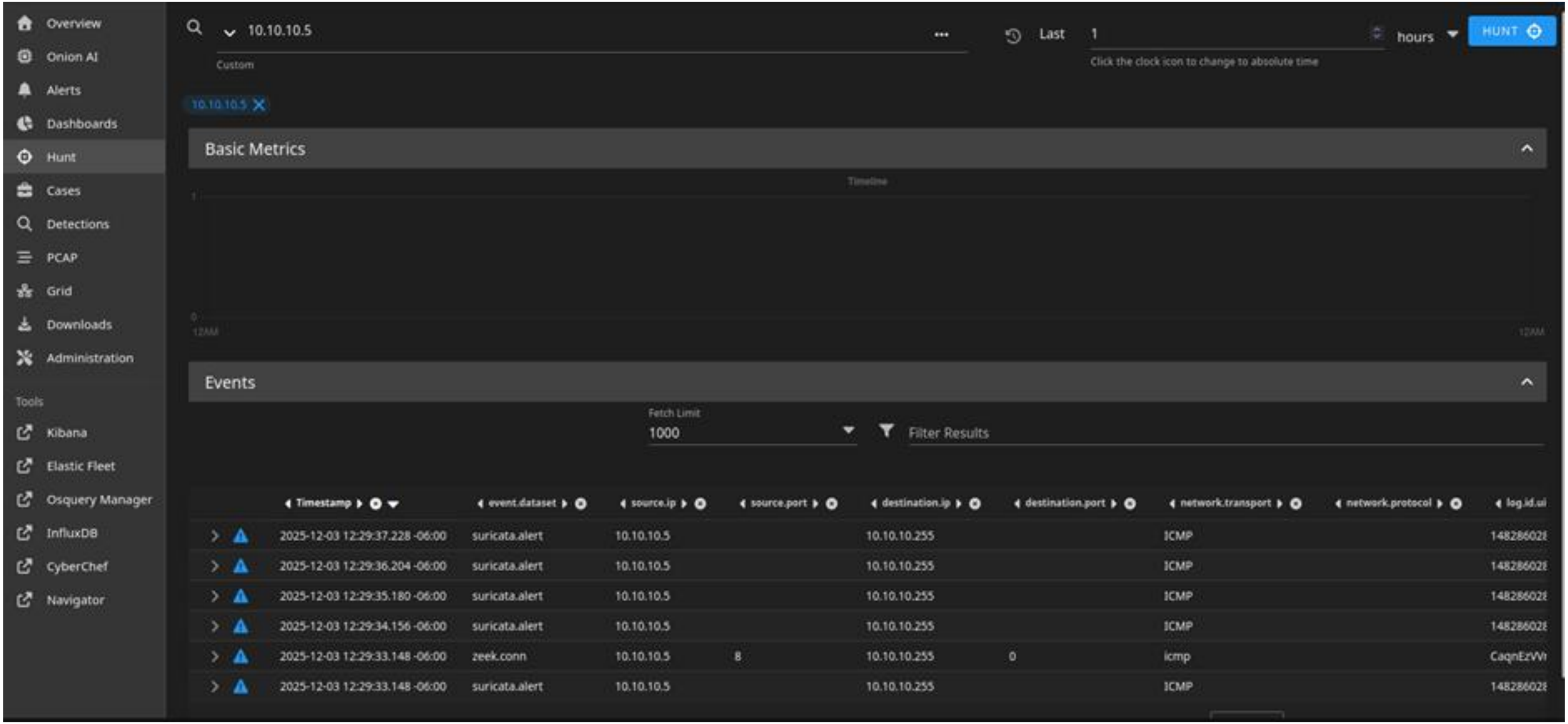
Start with a **hypothesis or alert** (e.g., “suspicious DNS,” “port scan”).

Triage in Security Onion: look at alert details, source/dest, rule message.

Pivot in Zeek logs: dns.log → conn.log → http.log, etc.

Enrichment: hostnames, GeoIP/IP reputation (even if just discussed, mention it).

Decision & documentation: benign vs malicious, note IOCs, note next actions.



10.10.10.5

Custom

Last 1 hours

Click the clock icon to change to absolute time

10.10.10.5 ✕

Fetch Limit
1000

	Timestamp	event.dataset	source.ip	source.port	destination.ip	destination.port	network.transport	network.protocol	log.id.ui
> ⚠	2025-12-03 12:29:37.228 -06:00	suricata.alert	10.10.10.5		10.10.10.255		ICMP		148286028
> ⚠	2025-12-03 12:29:36.204 -06:00	suricata.alert	10.10.10.5		10.10.10.255		ICMP		148286028
> ⚠	2025-12-03 12:29:35.180 -06:00	suricata.alert	10.10.10.5		10.10.10.255		ICMP		148286028
> ⚠	2025-12-03 12:29:34.156 -06:00	suricata.alert	10.10.10.5		10.10.10.255		ICMP		148286028
> ⚠	2025-12-03 12:29:33.148 -06:00	zeek.conn	10.10.10.5	8	10.10.10.255	0	icmp		CaqnEzVVi
> ⚠	2025-12-03 12:29:33.148 -06:00	suricata.alert	10.10.10.5		10.10.10.255		ICMP		148286028

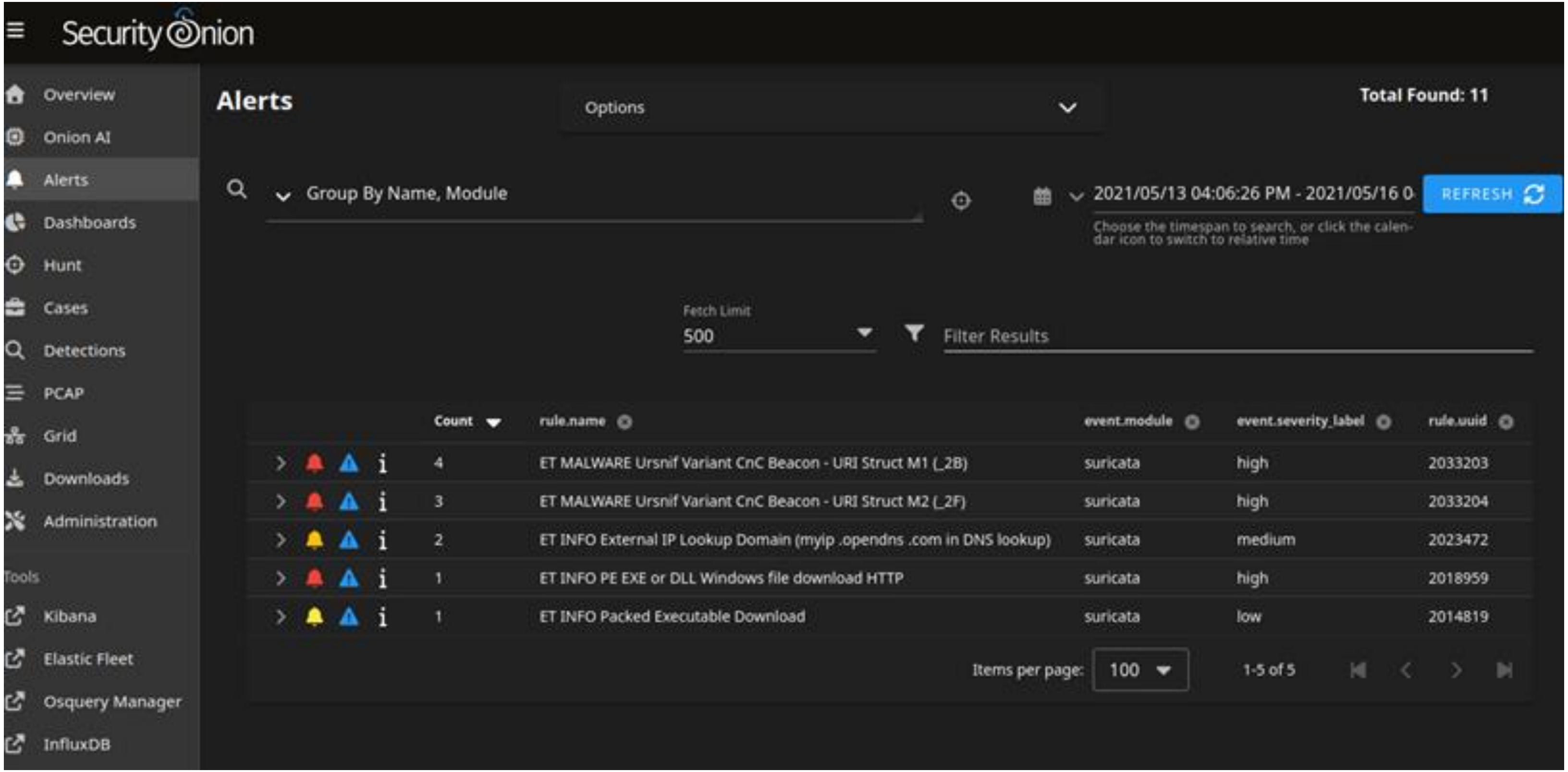
M3 – Tuning noisy rules + metrics

- Suppressions
- Thresholds

Milestone 4 – Malicious PCAP demo + takeaways

- Malicious PCAP
- IOCs
- Takeaway

M4 – Malicious PCAP analysis and IOCs



Alerts

Total Found: 11

Group By Name, Module

2021/05/13 04:06:26 PM - 2021/05/16 0

Choose the timespan to search, or click the calendar icon to switch to relative time

Fetch Limit
500

Count	rule.name	event.module	event.severity_label	rule.uuid
4	ET MALWARE Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	suricata	high	2033203
3	ET MALWARE Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	suricata	high	2033204
2	ET INFO External IP Lookup Domain (myip .opendns .com in DNS lookup)	suricata	medium	2023472
1	ET INFO PE EXE or DLL Windows file download HTTP	suricata	high	2018959
1	ET INFO Packed Executable Download	suricata	low	2014819

Items per page: 100

1-5 of 5

Key Takeaways

- Raw packets → baseline → rules → alerts → hunts → tuning
- Biggest Technical Challenge:
  - Networking/Visibility Issue
  - Rule Mismatches
  - Noisy Alerts

GITHUB

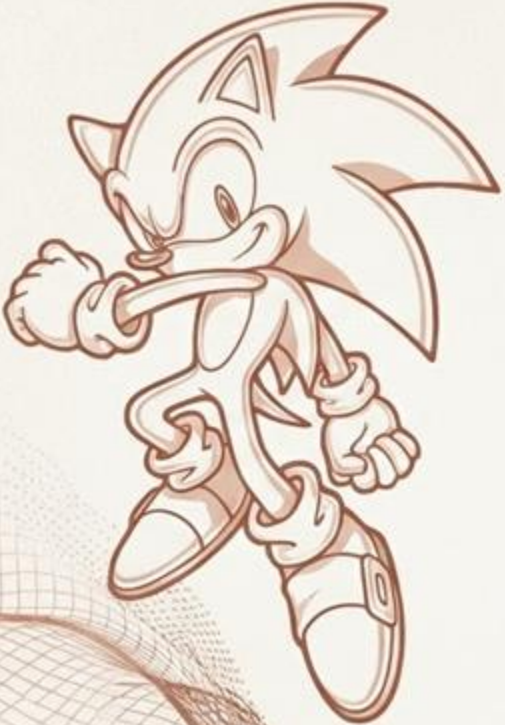
https://github.com/mwchavez/IDS_DF_F2025_Project_MC_MT_DP

Future Status of the project

- Expand rule set
- Automation (Training)

Resources used in gathering information

- https://www.malware-traffic-analysis.net/2021/05/14/index.html
- https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md
- https://www.acronis.com/en/tru/posts/ursnif-the-banking-trojan/
- https://attack.mitre.org/software/S0386/



Thank You!!