SOC (Security Operations Center)

Documentatie

Cybersecurity & Security Operation Center

Mathias Wouters 3CCS02

Academiejaar 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

INHOUDSTAFEL

INHOUDSTAFEL 3

1 INLEIDING 4

2 ATTACK 1/2 5

2.1 Install software with known CVE 5
2.2 Bruteforce via RDP or SSH 6
2.3 Tampering of important file (FIM) 7
2.4 Installation of rootkit 7
2.5 Download of malware 8

3 ATTACK 2/2: CALDERA 9

4 PRODUCTION SYSTEM 10

4.1 Ubuntu Server 22.04 10
4.2 pfSense 10

5 MEASURE / DETECTION: SURICATA 11

6 CORRELATE / ALERT: WAZUH 12

7 ENRICH WITH THREAT INTEL: VIRUSTOTAL 14

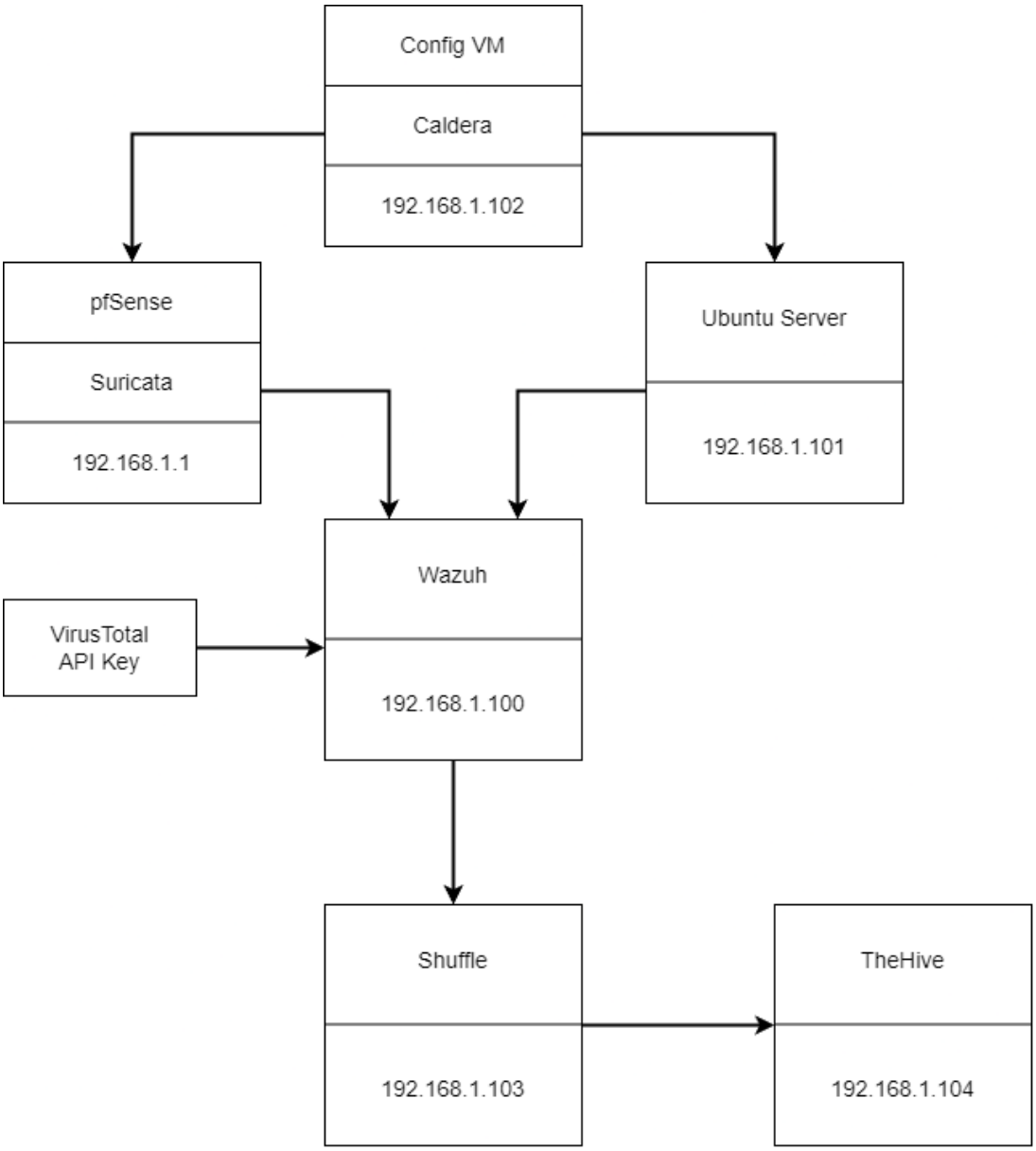
8 REMEDIATE / AUTOMATE: SHUFFLE I.O 15

9 THEHIVE 17

10 BESLUIT 18

1 INLEIDING

Voor het vak Cybersecurity & Security Operation Center kreeg ik de taak om een SOC (Security Operation Center) te maken. De SOC bestaat uit verschillende onderdelen, en voor elk onderdeel heb ik een bepaalde software moeten kiezen. Hieronder heb ik een schema toegevoegd dat een schematisch overzicht geeft van mijn SOC.



Ik heb ook nog een demo filmpje gemaakt, waarin ik mijn SOC toelicht en demonstreer:

YouTube link: https://youtu.be/N6xHx_H27Vk

2 ATTACK 1/2

2.1 Install software with known CVE

Een CVE is een Common Vulnerability and Exposure, dit is eigenlijk een vulnerability die in een applicatie of een operating system zit. Dit zijn publiek gekende vulnerabilities die door Wazuh worden gecheckt voor aanwezigheid op mijn systeem. Deze scans worden periodiek automatisch gedaan en als er iets gevonden is, wordt deze bekend gemaakt door een alert in Wazuh. Zulk een vulnerability kan je dan oplossen door die software uptedaten. Hieronder heb ik een screenshot toegevoegd van een voorbeeld alert in Wazuh.

>	Jan 5, 2024 @ 09:02:57.542	The CVE-2023-51767 that affected openssh-sftp-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.531	The CVE-2023-51767 that affected openssh-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.520	The CVE-2023-51767 that affected openssh-client was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.510	The CVE-2022-46908 that affected libsqlite3-0 was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.499	The CVE-2023-7104 that affected libsqlite3-0 was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.487	The CVE-2023-51385 that affected openssh-sftp-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.476	The CVE-2023-51385 that affected openssh-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.466	The CVE-2023-51385 that affected openssh-client was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.453	The CVE-2023-51384 that affected openssh-sftp-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.443	The CVE-2023-51384 that affected openssh-server was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:57.432	The CVE-2023-51384 that affected openssh-client was solved due to a package removal/update or a system upgrade	3	23502
>	Jan 5, 2024 @ 09:02:56.146	CVE-2023-51767 affects openssh-sftp-server	7	23504
>	Jan 5, 2024 @ 09:02:56.095	CVE-2023-51767 affects openssh-server	7	23504
>	Jan 5, 2024 @ 09:02:56.039	CVE-2023-51767 affects openssh-client	7	23504
>	Jan 5, 2024 @ 09:02:48.118	CVE-2023-7207 affects cpio	7	23504

2.2 Bruteforce via RDP or SSH

Tevens gebruik ik de Ubuntu server om elke SSH connectie die gemaakt wordt te monitoren. Ook als deze niet lukt monitor ik deze. Hierdoor kan ik makkelijk bruteforce attacks waarnemen die via SSH proberen binnen te komen. Ik voer de attack uit via de tool Hydra die gebruik maakt van een text bestandje met 10 voorbeeld wachtwoorden in. Hieronder een screenshots van de alerts die ik op Wazuh hiervan binnen krijg.

Jan 5, 2024 @ 11:23:36.507	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.504	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.502	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.498	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.495	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.493	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.491	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.487	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:36.487	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:34.592	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.592	PAM: Multiple failed logins in a small period of time.	10	5551
Jan 5, 2024 @ 11:23:34.592	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.592	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:34.547	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.547	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:34.546	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.546	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.546	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.527	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:34.527	PAM: User login failed.	5	5503
Jan 5, 2024 @ 11:23:34.527	sshd: brute force trying to get access to the system. Non existent user.	10	5712
Jan 5, 2024 @ 11:23:34.527	sshd: Attempt to login using a non-existent user	5	5710
Jan 5, 2024 @ 11:23:34.527	PAM: User login failed.	5	5503

2.3 Tampering of important file (FIM)

Ook heb ik ingesteld dat mijn Wazuh de /root en de /var/tmp directory moet monitoren. Als in een van deze directories een file wordt aangepast of verwijderd dan krijg ik daar meldingen van. Ik heb voor deze directories gekozen omdat er eigenlijk niets zomaar in de root directory mag geschreven worden zonder dat ik het bewust doe. En met de Caldera tool (die ik in punt 3 verder ga uitleggen) maak ik ook een bestand aan in de /var/tmp directory wat het ook makkelijk maakt om dat dan meteen te monitoren.

Ik had hier nog zeker veel meer directories en subdirectories kunnen toevoegen die ook belangrijk zijn om te monitoren, maar dat heb ik bewust niet gedaan omdat dit systeem toch op een intern netwerk zit waardoor het dus niet openstaat voor het internet. Ik ben dus normaal de enigste die hier aangeraakt en daarom heb ik dan gekozen om in die twee directories te werken. Hieronder een screenshot met de alerts die ik binnen krijg in Wazuh.

›	Jan 5, 2024 @ 12:13:22.224	File deleted.	7	553
›	Jan 5, 2024 @ 12:12:38.207	File added to the system.	5	⊕ ⊖ 554

2.4 Installation of rootkit

Rootkits zijn vaak moeilijk te vinden omdat deze zich verstoppen in software of zelfs in het operating system zelf. Hierdoor is het belangrijk om dit zo snel mogelijk te vinden mocht dit op uw systeem zitten. Ik heb mijn Wazuh ingesteld dat deze mijn systeem periodiek scant om te detecteren of er een rootkit aanwezig is. Ik kan dit simuleren door de binary van mijn Ubuntu server te veranderen naar een klein shell scriptje. Hieronder een screenshot van een rootkit alert in mijn Wazuh.

›	Jan 5, 2024 @ 11:47:17.796	Host-based anomaly detection event (rootcheck).	7	510
›	Jan 5, 2024 @ 11:47:17.759	Host-based anomaly detection event (rootcheck).	7	510

2.5 Download of malware

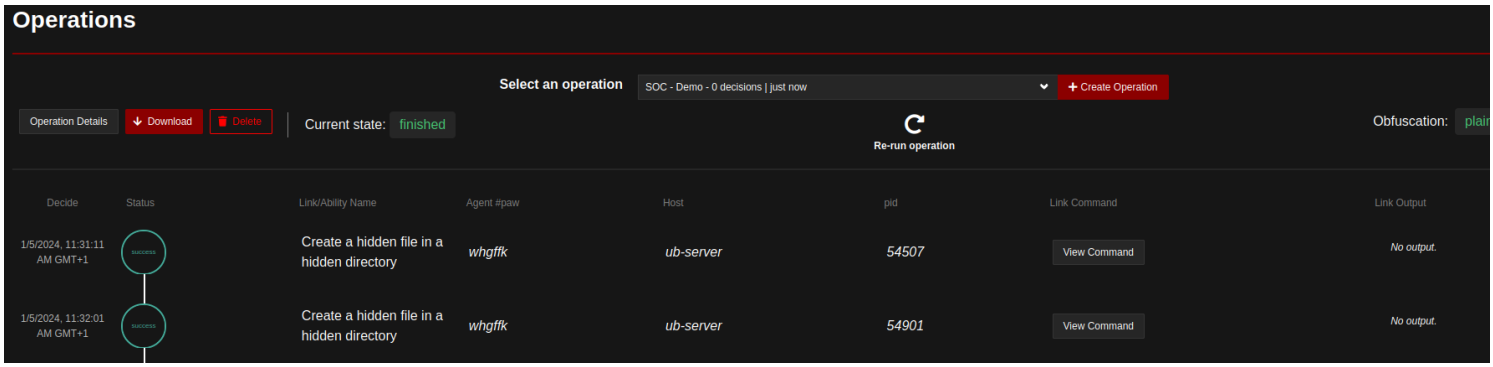
Malware op uw systemen hebben is een veel voorkomend probleem, daarom heb ik gekozen om dit ook na te kijken. Ik kijk dit momenteel alleen na in de root directory, maar natuurlijk kan je dit op je hele systeem nakijken. Als er een nieuw bestand in de root directory terecht komt, wordt dit gedetecteerd en nageken door mijn Wazuh. Deze wordt dan gescand door de VirusTotal API en als het bestand ook daadwerkelijk malware is wordt deze via een shell script verwijderd. Ik kan dit testen door de EICAR test file te downloaden en in mijn root directory te zetten, deze wordt dan automatisch verwijderd door de VirusTotal integratie. De EICAR test file wordt gebruikt als een malware test file omdat je anders echte malware moet downloaden om uw systemen op antivirussen en zo uit te testen. Deze EICAR test file kan geen schade toebrengen aan uw systeem terwijl echte malware dat wel kan doen. Hieronder een screenshot van de security alerts in Wazuh.

›	Jan 5, 2024 @ 11:55:00.248	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
›	Jan 5, 2024 @ 11:54:59.170	File deleted.	7	553
›	Jan 5, 2024 @ 11:54:59.041	VirusTotal: Alert - /root/eicar.com - 61 engines detected this file	12	87105
›	Jan 5, 2024 @ 11:54:44.196	VirusTotal: Alert - No records in VirusTotal database	3	87103
›	Jan 5, 2024 @ 11:53:30.160	PAM: Login session closed.	3	5502
›	Jan 5, 2024 @ 11:53:28.248	File added to /root directory.	7	100201

3 ATTACK 2/2: CALDERA

Caldera is een adversary emulation platform, gemaakt om eenvoudig autonome inbreuk-en-aanval-simulatieoefeningen uit te voeren. Het kan ook worden gebruikt voor het uitvoeren van handmatige red-team-opdrachten of geautomatiseerde incidentrespons acties. Caldera is gemaakt op het MITRE ATT&CK framework. Dit is een samengestelde database en model voor het gedrag van cybervijanden, die de verschillende fasen van de aanvalslevenscyclus van een tegenstander weerspiegelen.

Ik gebruik Caldera om automatisch een attack uit te voeren op mijn productie systeem, in dit geval een Ubuntu server instantie. De aanval die ik uitvoer is het automatisch aanmaken van een hidden file in een hidden directory in de /var/tmp directory van mijn server. Deze wordt na het aanmaken ook terug automatisch verwijderd. Hieronder een screenshot van de aanval in Caldera.



Ik heb voor deze aanval gekozen omdat deze ook mooi samegaat met de Tampering of important file (FIM) attack bij puntje 2.3 . Dit wordt ook mooi in een alert in Wazuh weergegeven, die ik bij dat puntje al heb laten zien.

Er zijn zeker nog vele andere attacks binnen Caldera die gebruikt kunnen worden. Ik heb bijvoorbeeld nog wat discovery attacks uitgeprobeerdom te zien of deze door Wazuh herkend worden. De attacks die ik hiervoor gebruikt heb waren de volgende: kijken welke users er aanwezig zijn op het systeem, kijken welke rechten deze user hadden, en kijken wie de actieve user is. Deze werden niet door Wazuh herkend, dit gebeurde denk ik omdat dit niet echt attacks zijn waarbij er echt iets met het systeem gedaan wordt dus kan Wazuh dit ook niet waarnemen.

4 PRODUCTION SYSTEM

4.1 Ubuntu Server 22.04

Voor productie systeem heb ik gekozen voor een Ubuntu Server 22.04. Dit heb ik gedaan omdat er in de echte wereld toch meestal naar windows wordt gekeken omdat hier de meeste mensen ook het bekendst mee zijn en ook omdat hier toch wel het grootste deel van de aanvalllen tegen gedaan worden. Daarom koos ik om de wat minder bekeken kant uit te testen en ikzelf gebruik ook liever linux.

Om het voor Wazuh mogelijk te maken om de security events van dit systeem te kunnen loggen, heb ik hier een Wazuh agent op moeten installeren. Daarnaast heb ik ook verschillende aanpassingen moeten doen in de ossec.conf file om mijn verschillende attacks te kunnen loggen.

4.2 pfSense

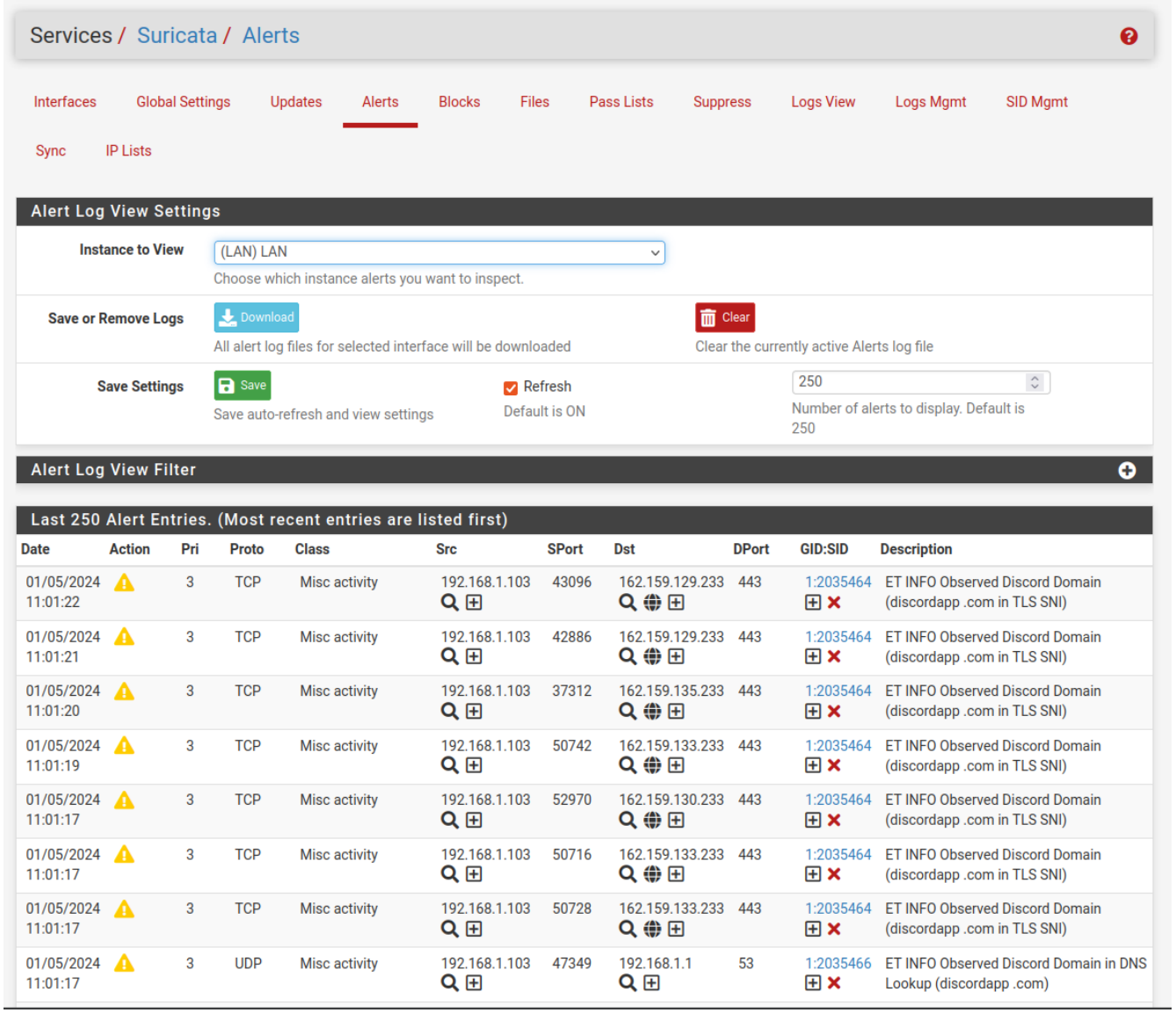
Ik draai ook een pfSense, omdat het mij zo makkelijk leek om een publiek gerichte VM te hebben die dan router speelt voor de rest van mijn VM's die in een intern netwerk zitten. Ik heb gewoon elke VM een statische IP gegeven die buiten mijn DHCP range viel. Hieronder een zicht op mijn IP tabel in pfSense.

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.1.104	08:00:27:62:8e:23	thehive		n/a	n/a	
192.168.1.103	08:00:27:77:14:c4	shuffle		n/a	n/a	
192.168.1.102	08:00:27:6b:7a:81	config-vm		n/a	n/a	
192.168.1.101	08:00:27:ba:25:2f	ub-server		n/a	n/a	
192.168.1.100	08:00:27:93:96:1a	wazuh-server		n/a	n/a	

Ik heb op deze pfSense instantie ook een Wazuh agent geinstalleerd, zodat ik mijn Suricata alerts naar mijn Wazuh kon doorsturen. Hierover zal ik meer vertellen in volgend puntje.

5 MEASURE / DETECTION: SURICATA

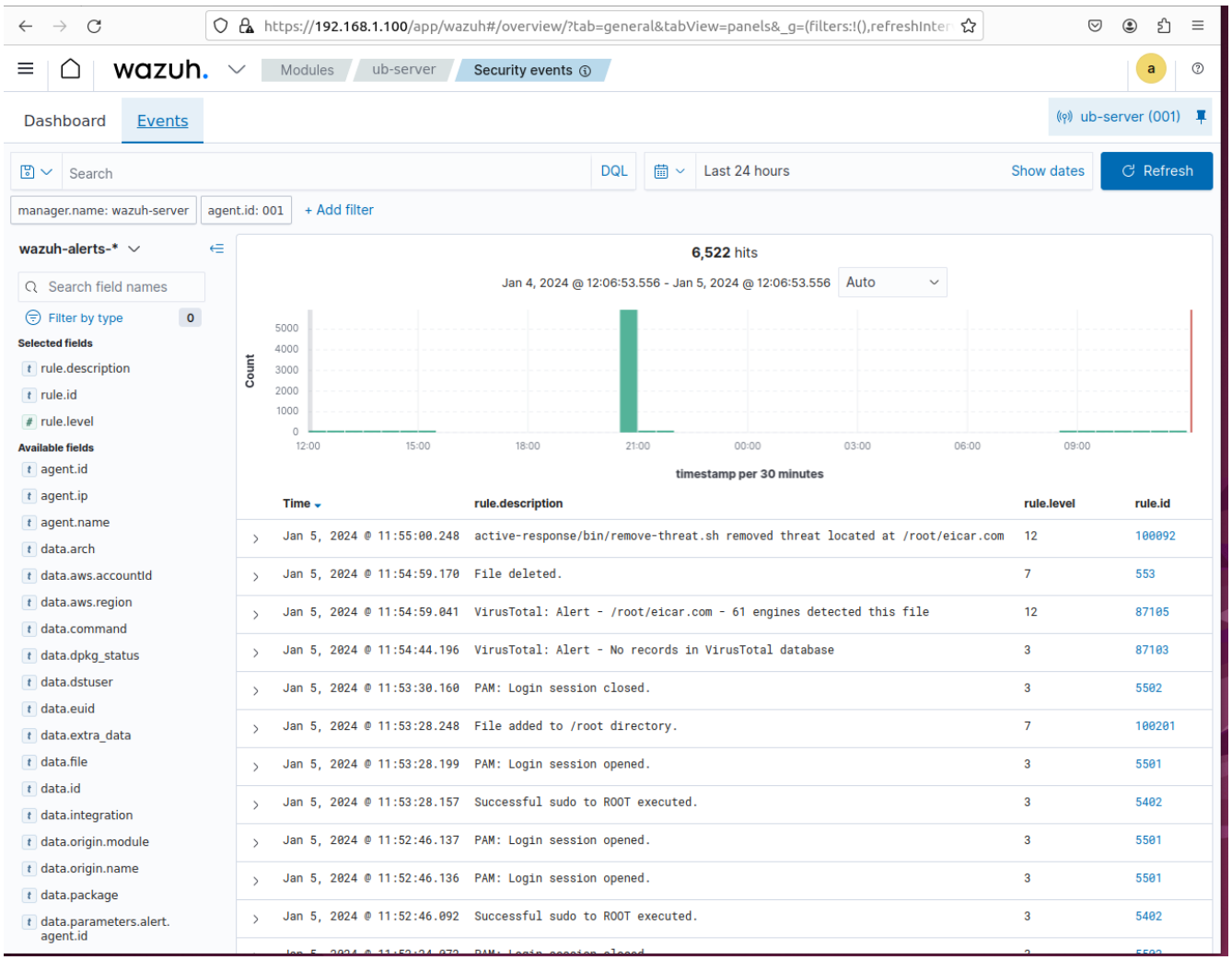
Suricata is een open-source inbraakdetectiesysteem (IDS) en inbraakpreventiesysteem (IPS) dat gebruikt kan worden om een breed scala aan netwerkbedreigingen te detecteren en te voorkomen. Dit heb ik dan ook rechtstreeks geinstalleerd op mijn pfSense, omdat ik dit wel logisch vond want Suricata scant mijn netwerk waardoor het best op de ethernet poort van mijn router komt te zitten omdat hier toch al mijn netwerk verkeer langskomt. Op mijn pfSense krijg ik dan security alerts binnen als er iets wordt gedetecteerd op mijn netwerk. Deze alerts stuur ik dan door naar mijn Wazuh om deze mooi te laten zien bij de rest van mijn alerts. Hieronder heb ik een overzicht gezet van de voorbeeld alerts die ik binnen krijg op mijn pfSense.

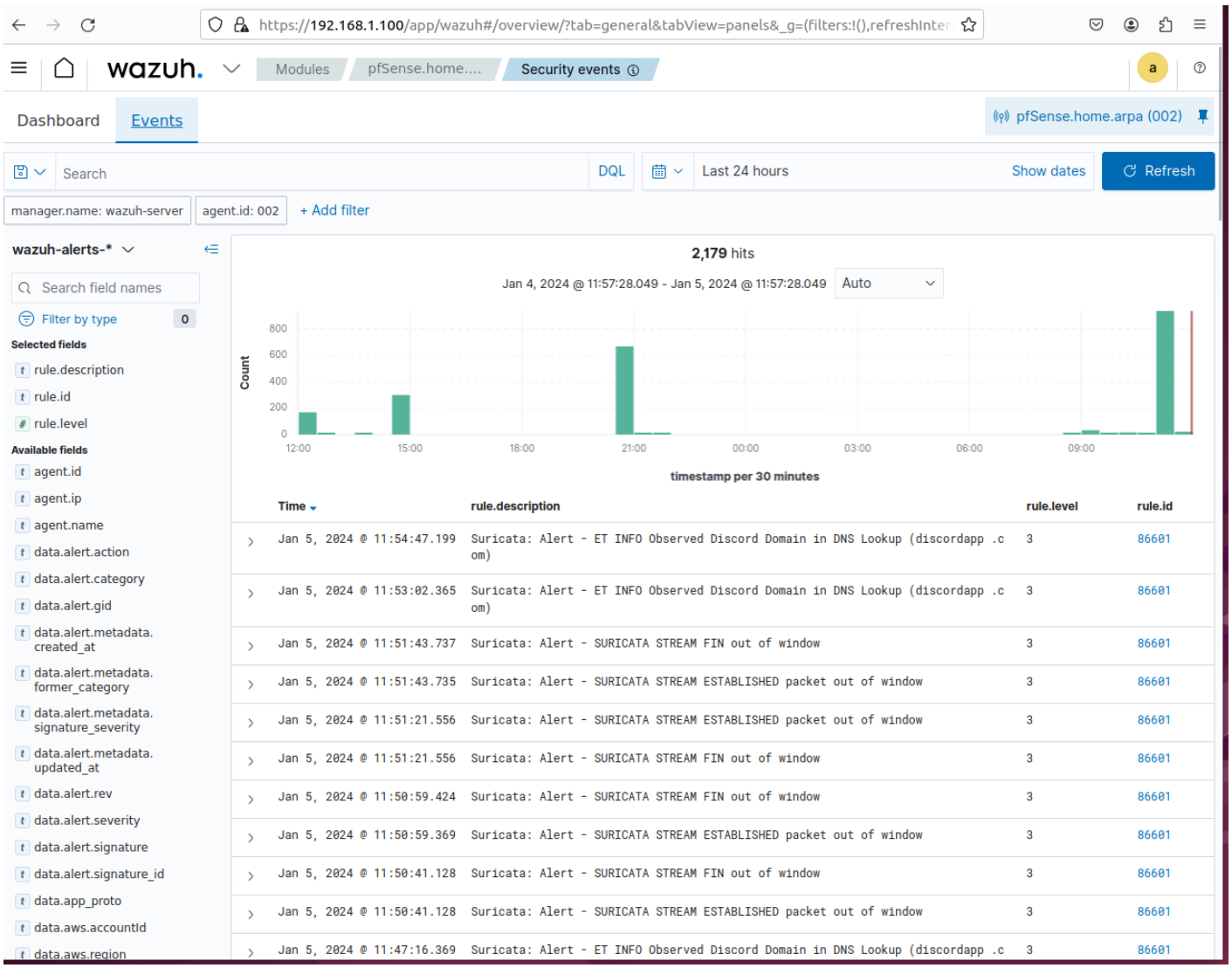


Zoals u kunt zien zijn de alerts die er nu staan iets van discord. Dit is mijn shuffle integratie met discord waarover ik het zometeen nog ga hebben. Omdat mijn discord niet geauthoriseerd is, worden hiervoor alerts gegeven denk ik.

6 CORRELATE / ALERT: WAZUH

Als SIEM oplossing heb ik gekozen voor Wazuh. Omdat dit toch de meest bekende open-source SIEM oplossing is dat er bestaat. Daarnaast ken ik het door de TryHackMe rooms en in de cursus hebben we het er ook al over gehad. Hierdoor ben ik toen al wat in de documentatie gaan rondneuzen en was ik positief verrast over de goede en duidelijke documentatie die Wazuh had. Wazuh detecteert gevaren op de gemonitorde systemen, waardoor deze ook voorkomen kunnen worden wat dan weer zorgt voor een veiligere infrastructuur. Wazuh maakt gebruik van agents, wat betekent dat je de Wazuh agent moet installeren op de systemen die dat je wilt monitoren. Naast de Wazuh agent heb je ook nog de Wazuh indexer, server en het dashboard. De indexer is een component die security alerts indexeert en bewaart binnenin Wazuh. Hiernaast heb je ook de Wazuh server die de gecollecteerde gegevens die worden ontvangen vanuit de gemonitorde endpoints analyseert. En ten slotte hebben we het Wazuh dashboard, dit is wel de meest bekende component omdat we hier het meeste mee in aanraking komen. Het dashboard is een interface die de gecollecteerde data en alerts mooi visualiseert in tabellen en grafieken. Via het dashboard is het ook mogelijk om de configuratie bestanden van Wazuh te veranderen zodat je niet steeds in de commandline van Wazuh moet werken. Hieronder zal ik nog 2 afbeeldingen toegevoegd, de eerste is het dashboard van mijn Ubuntu endpoint en de tweede is van mijn pfSense endpoint.




https://192.168.1.100/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInter
wazuh.
Modules
pfSense.home....
Security events
Dashboard
Events
pfSense.home.arpa (002)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
agent.id: 002
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.alert.action
data.alert.category
data.alert.gid
data.alert.metadata.created_at
data.alert.metadata.former_category
data.alert.metadata.signature_severity
data.alert.metadata.updated_at
data.alert.rev
data.alert.severity
data.alert.signature
data.alert.signature_id
data.app_proto
data.aws.accountId
data.aws.region
2,179 hits
Jan 4, 2024 @ 11:57:28.049 - Jan 5, 2024 @ 11:57:28.049
Auto
Count
800
600
400
200
0
12:00
15:00
18:00
21:00
00:00
03:00
06:00
09:00
timestamp per 30 minutes
Time
rule.description
rule.level
rule.id
Jan 5, 2024 @ 11:54:47.199 Suricata: Alert - ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) 3 86601
Jan 5, 2024 @ 11:53:02.365 Suricata: Alert - ET INFO Observed Discord Domain in DNS Lookup (discordapp .com) 3 86601
Jan 5, 2024 @ 11:51:43.737 Suricata: Alert - SURICATA STREAM FIN out of window 3 86601
Jan 5, 2024 @ 11:51:43.735 Suricata: Alert - SURICATA STREAM ESTABLISHED packet out of window 3 86601
Jan 5, 2024 @ 11:51:21.556 Suricata: Alert - SURICATA STREAM ESTABLISHED packet out of window 3 86601
Jan 5, 2024 @ 11:51:21.556 Suricata: Alert - SURICATA STREAM FIN out of window 3 86601
Jan 5, 2024 @ 11:50:59.424 Suricata: Alert - SURICATA STREAM FIN out of window 3 86601
Jan 5, 2024 @ 11:50:59.369 Suricata: Alert - SURICATA STREAM ESTABLISHED packet out of window 3 86601
Jan 5, 2024 @ 11:50:41.128 Suricata: Alert - SURICATA STREAM FIN out of window 3 86601
Jan 5, 2024 @ 11:50:41.128 Suricata: Alert - SURICATA STREAM ESTABLISHED packet out of window 3 86601
Jan 5, 2024 @ 11:47:16.369 Suricata: Alert - ET INFO Observed Discord Domain in DNS Lookup (discordapp .c 3 86601

7 ENRICH WITH THREAT INTEL: VIRUSTOTAL

Ik heb een integratie met VirusTotal toegepast in mijn Wazuh configuratie. Dit heb ik gedaan om automatisch malware te kunnen verwijderen van mijn systeem. Als er een nieuw bestand op mijn systeem kotm, wordt er nagekeken bij VirusTotal of dit malware is, en zo ja wordt er een shell script uitgevoerd dat dit bestand automatisch verwijdert. Hiervoor maak ik gebruik van de API van VirusTotal.

VirusTotal is een online dienst die wordt gebruikt om bestanden en URL's te scannen op mogelijke malware en virussen. De dienst werkt door bestanden of URL's die je wilt controleren te uploaden naar de VirusTotal-website. Het systeem voert vervolgens een scan uit met meer dan 70 verschillende antivirusprogramma's en andere malware-detectietechnieken, waaronder handtekeninggebaseerde detectie, gedragsanalyse en heuristische analyses. VirusTotal bied hun API aan, waardoor het mogelijk is om de scans te automatiseren.

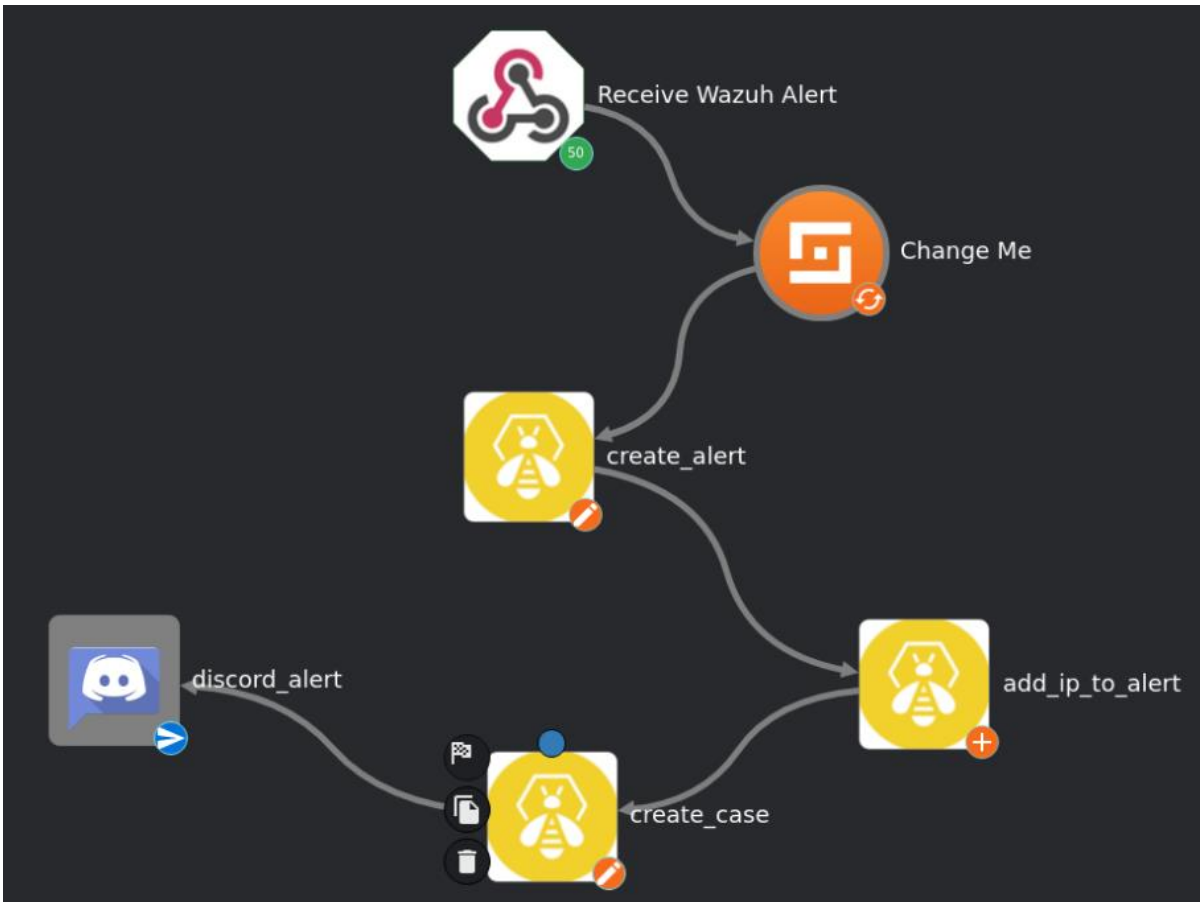
8 REMEDIATE / AUTOMATE: SHUFFLE IO

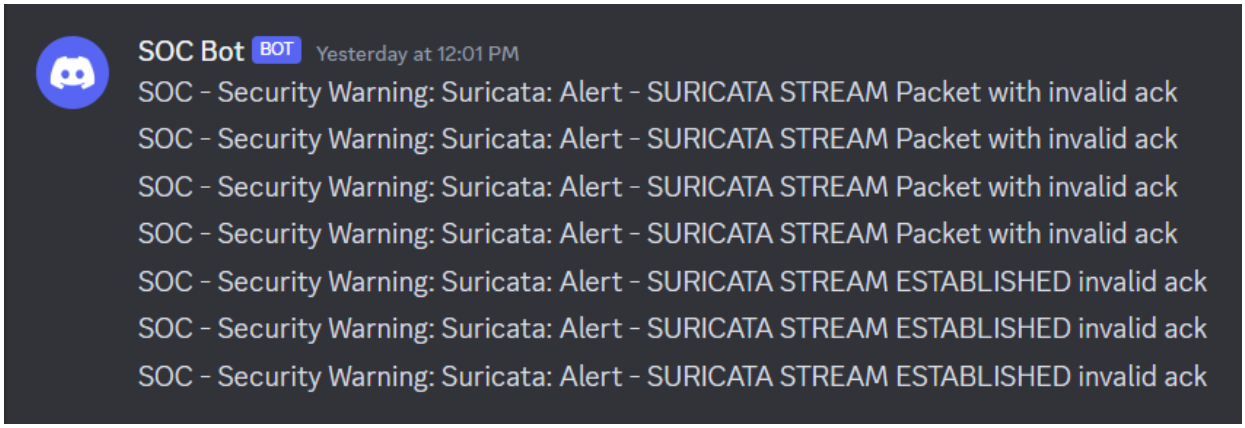
Shuffle IO is een open-source SOAR solution. Security Orchestration, Automation and Response, or SOAR, is een stack van compatibele softwareprogramma's waarmee een organisatie gegevens over beveiligingsbedreigingen kan verzamelen en kan reageren op beveiligingsgebeurtenissen met weinig of geen menselijke hulp.

Een SOAR heeft 3 verschillende componenten. De eerste is security orchestration, dit zorgt voor een verbonden en geintegreerde security solution bestaande uit verschillende security applicaties. De tweede component is security automation, dit is een toepassing die zorgt voor zo min mogelijk handmatige acties in de security workflow. Het automatiseert het hele security proces. En de laatste component is security response, dit biedt analisten één overzicht van de planning, het beheer, de monitoring en de rapportage van acties die worden uitgevoerd nadat een bedreiging is gedetecteerd.

De shuffle workflow die ik heb toegepast bestaat uit het binnenhalen van mijn security alerts van Wazuh om deze dan aan te bieden in TheHive, dit ga ik in volgend puntje beter uitleggen. Het volgende dat ik doe is als er een IP adres bekend is in de alert, voeg ik deze toe als een observable binnen in TheHive. Mijn volgende stap was om automatisch een case aan te maken in TheHive van mijn security alerts, maar omdat ik hier problemen had met de case templates is dit niet gelukt. Als laatste heb ik nog de discord integratie toegevoegd die mij automatisch al mijn security alerts ook toont in mijn SOC discord channel. Dit kun je ook doen via mail of slack, maar ik vond discord het makkelijkst en daarenboven gebruik ik discord veel.

Een mogelijke uitbreiding die ik nog graag wou doen was voor elke soort security alert een workflow te maken waardoor dit overzichterlijker wordt en ik ook meer specifieke uitbreidingen kon toepassen per soort van security alert. Hoe ik het nu heb opgezet is dat ik alle alerts vanaf een bepaald level, in mijn geval level 3, doorstuur naar shuffle. Hieronder heb ik een afbeelding toegevoegd van mijn shuffle workflow en ook een weergave van mijn discord meldingen.


Receive Wazuh Alert
50
Change Me
create_alert
add_ip_to_alert
discord_alert
create_case


SOC Bot BOT Yesterday at 12:01 PM
SOC - Security Warning: Suricata: Alert - SURICATA STREAM Packet with invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM Packet with invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM Packet with invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM Packet with invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM ESTABLISHED invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM ESTABLISHED invalid ack
SOC - Security Warning: Suricata: Alert - SURICATA STREAM ESTABLISHED invalid ack

9 THEHIVE

De laatste applicatie die ik heb toegevoegd aan mijn SOC was TheHive. Dit is een open-source security incident response platform dat wordt gebruikt in SOC-omgevingen voor het beheren van beveiligingsincidenten.

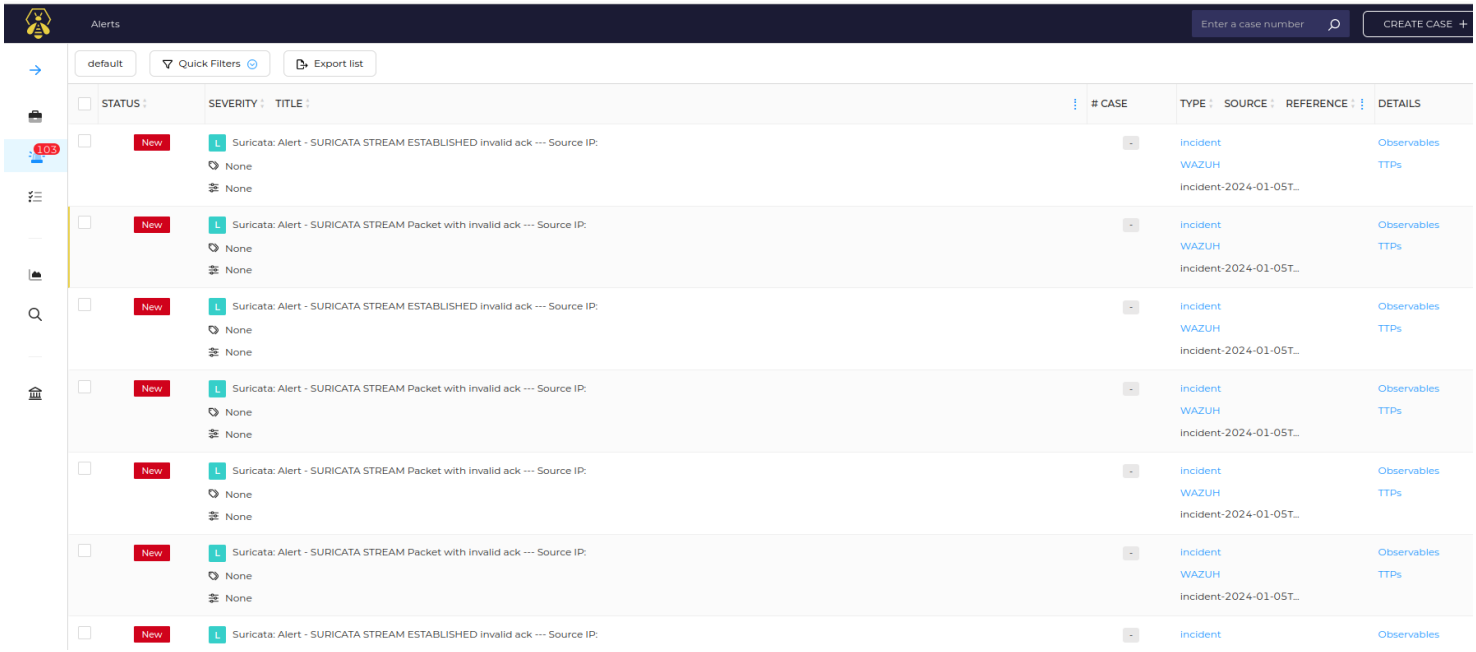
Het heeft verschillende functies die het nuttig maken in een SOC omgeving:

- Incidentbeheer: TheHive biedt een centrale plaats voor het registreren, classificeren en volgen van beveiligingsincidenten. Het stelt teams in staat om incidenten te organiseren op basis van ernst, type en andere parameters.

- Samenwerkingstools: Het platform ondersteunt samenwerking tussen teamleden door middel van opmerkingen, toewijzingen en het delen van informatie. Dit vergemakkelijkt effectieve communicatie en gezamenlijke acties bij het aanpakken van incidenten.

- Rapportage en Analyse: TheHive verzamelt gegevens tijdens het incidentresponsproces. Na afloop kunnen teams deze gegevens analyseren en rapporten genereren om lessen te trekken uit incidenten en om processen te verbeteren voor toekomstige incidenten.

Hieronder heb ik nog een afbeelding toegevoegd met mijn alerts op het TheHive platform.



10 BESLUIT

Het ontwikkelen van dit Security Operations Center (SOC) bood een unieke kans om verschillende aanvalsscenario's te simuleren en een breed scala aan beveiligingsmaatregelen te implementeren. Met behulp van geavanceerde tools zoals Wazuh, Suricata en Caldera, heb ik een solide infrastructuur kunnen opzetten die actief bedreigingen detecteert, waarschuwingen genereert en zelfs geautomatiseerde responsmogelijkheden biedt.

Dit SOC-project richtte zich niet alleen op het detecteren van aanvallen, maar legde ook de nadruk op het formuleren en implementeren van doeltreffende responsstrategieën. Daarom integreerde ik tools als TheHive en Shuffle IO om een gestroomlijnde incidentrespons te waarborgen.

Gedurende dit proces heb ik geleerd hoe belangrijk het is om proactief te zijn bij het identificeren en aanpakken van potentiële kwetsbaarheden. Het integreren van Threat Intelligence via VirusTotal heeft mijn vermogen vergroot om snel te reageren op mogelijke bedreigingen door verdachte bestanden te analyseren en te verwijderen.

Bovendien heb ik het belang erkend van voortdurende evaluatie en verbetering. Het is van essentieel belang om deze SOC-infrastructuur continu te monitoren, de strategie te herzien en nieuwe bedreigingen te onderzoeken om de beveiliging te waarborgen.

Dit SOC-project heeft niet alleen mijn technische vaardigheden op het gebied van cybersecurity versterkt, maar heeft ook mijn begrip verdiept van het belang van proactieve, geïntegreerde en geautomatiseerde beveiligingsmaatregelen.

Het heeft me voorbereid op de uitdagingen van een dynamisch en snel evoluerend beveiligingslandschap. Ik ben ervan overtuigd dat de ervaring die ik heb opgedaan van onschatbare waarde zal zijn in toekomstige cybersecurity-initiatieven.