THOMAS MORE

Security Operation Center

Thomas Deboel

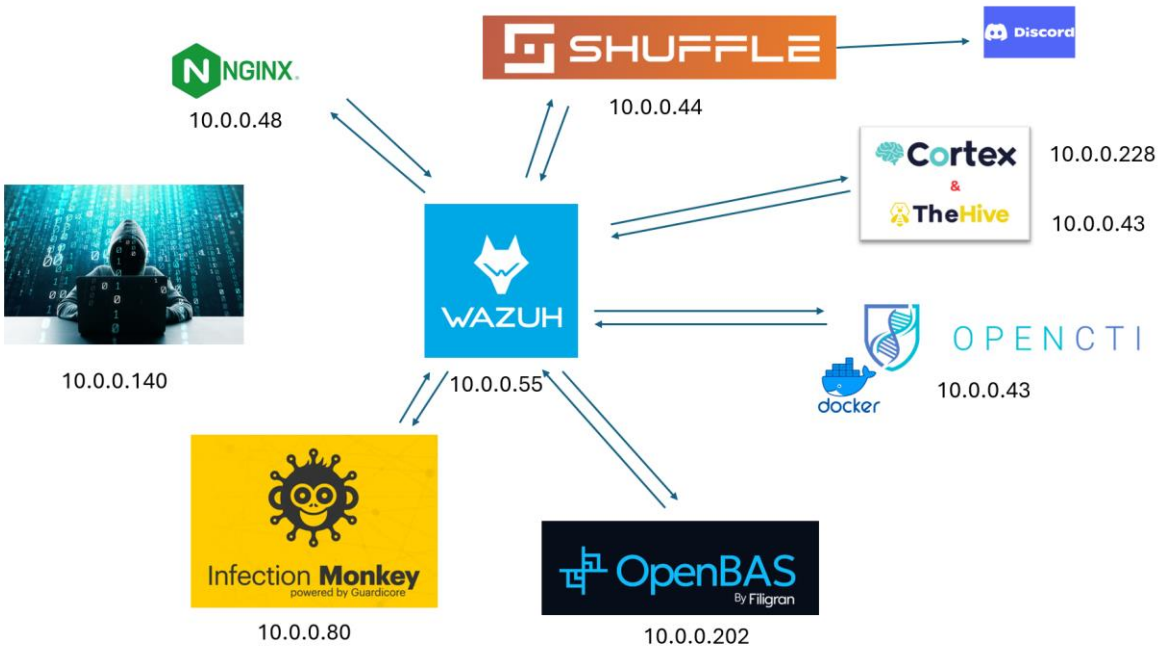
2024 - 2025

Inhoud

1. Overzicht

In dit deel van het document ga ik snel over wat er allemaal op mijn soc staat.

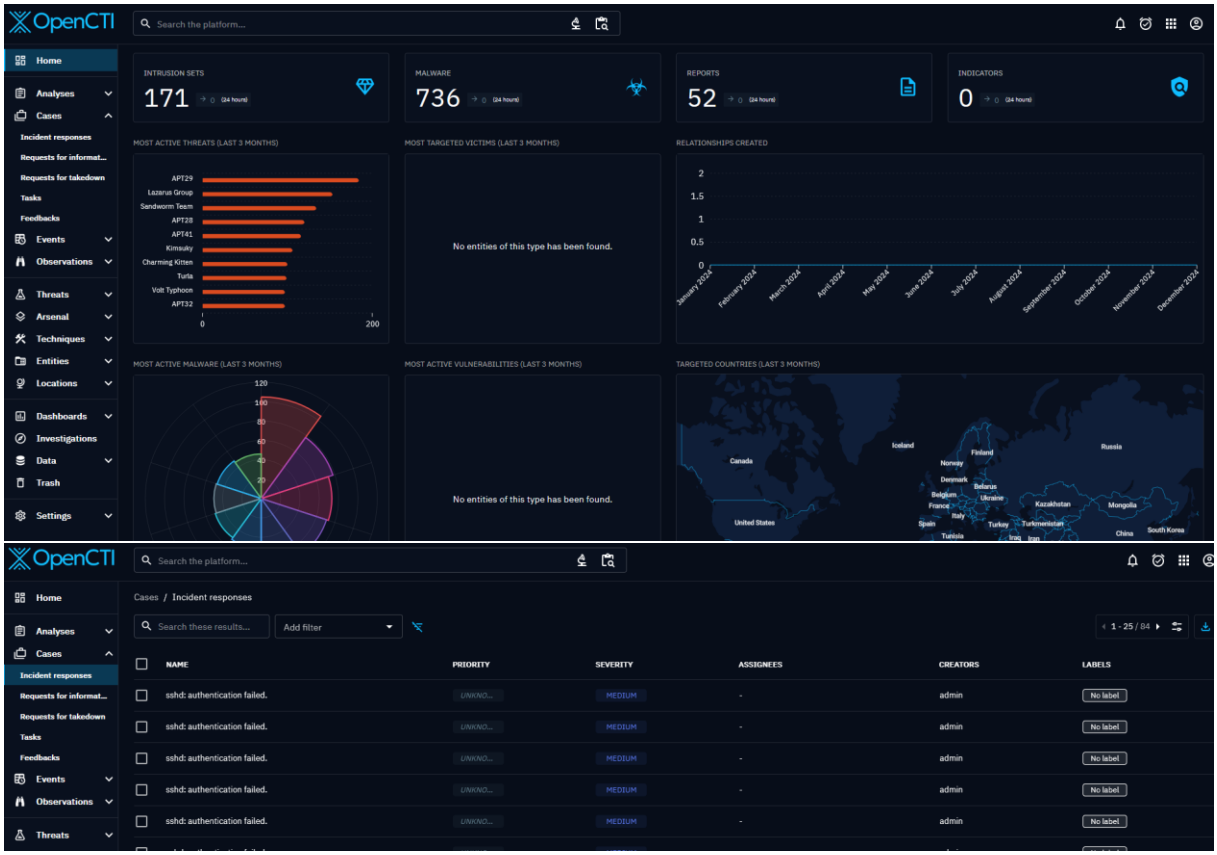
Naam	IP
Webserver	10.0.0.48
Wazuh	10.0.0.55
Opencti	10.0.0.172:8080
OpenBAS	10.0.0.202:8080
Shuffle	10.0.0.44:3443
Thehive	10.0.0.43:9000
Cortex	10.0.0.228:9001
Infection monkey	10.0.0.80:5000
Bad Actor:	10.0.0.140
~~**Misp**~~	~~10.0.0.195~~



2. Opencti

Waarom beginnen we met opencti omdat dit het meest appart is van al de rest. OpenCTI is een plek om mijn cyber threat intelligence kennis en observables te kunnen beheren. Het wordt vooral gebruikt voor

informatie op te doen van nieuwe threats maar het is ook geintegreerd met The Hive. De integratie met The Hive zorgt ervoor dat op het OpenCTI platform ikzelf nog eens kan zien welke cases dat ik heb binnen mijn eigen netwerk gebeurd is. De andere connectors die ik heb toegevoegd zijn “MITRE Datasets”, Sans RSS feed en TrendMicro RSS feed.

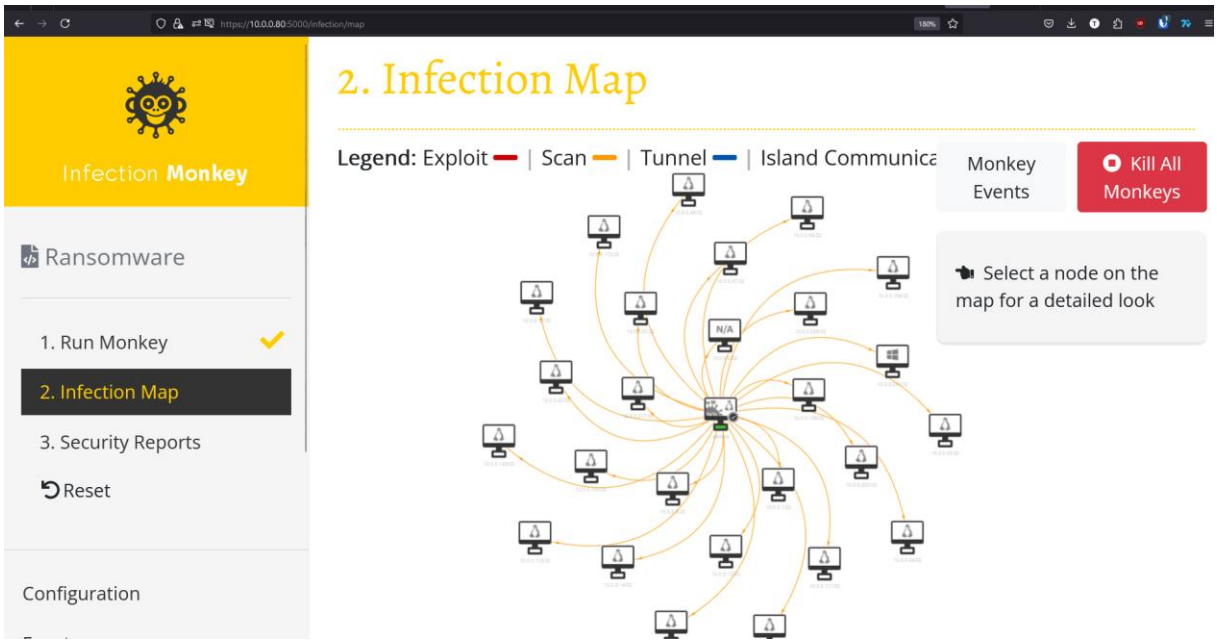


3. OpenBas, infection Monkey en Caldera

OpenBas, Infection Monkey en Caldera zijn allen Adversary Simulation Tools. Voor de Demo ga ik enkel gebruik maken van Infection monkey maar zowel OpenBas als Infection monkey zijn geinstalleerd. OpenBAS vond ik persoonlijk nog niet genoeg uitgewerkt om als enige Tool te laten zien en daarom heb ik uiteindelijk gekozen voor Infection monkey.
Voor infection Monkey heb ik gekozen voor Versie 2.0.0 doordat MongoDB V5+ niet geïnstalleerd kan worden op mijn hardware. Ik heb ook geprobeerd Caldera te installeren maar dit is spijtig genoeg niet gelukt maar dit is de reden waarom de server de naam Caldera heeft.

3.1. Infection Monkey

Infection monkey kan je verschillende aanvallen kiezen. Met de duidelijk een overzicht houden wat Infection monkey heeft gezien/gedaan. Het geeft ook een duidelijk overzicht wat er allemaal mis is met de omringende systemen met de infection map. Daarnaast maakt het ook een goed securityrapport dat onderverdeeld is in Ransomware Report en Security Report.



1. Breach

Ransomware attacks start after machines in the internal network get compromised. The initial compromise was simulated by running Infection Monkey Agents manually. Detecting ransomware at this stage will minimize the impact to the organization.

Learn techniques for early ransomware detection on Akamai's blog

Ransomware attack started from these machines on the network:

- **caldera** (10.0.0.80, 172.17.0.1 and 1 more) at **1/6/2025, 4:41:55 PM**

2. Lateral Movement

After the initial breach, the attacker will begin the Lateral Movement phase of the attack. They will employ various techniques in order to compromise other systems in your network.

See some real-world examples on Akamai's blog

Infection Monkey discovered 26 machines and successfully breached 0 of them.

Breached Servers

Machine	IP Addresses	Exploits
No rows found		

3. Attack

After the attacker or malware has propagated through your network, your data is at risk on any machine the attacker can access. It can be encrypted and held for ransom, exfiltrated, or manipulated in whatever way the attacker chooses.

Learn about the financial impact of ransomware on Akamai's blog

Overview

✔ No critical security issues were detected.

⚠ To improve Infection Monkey's detection rates, try adding credentials under **Propagation - Credentials** and updating network settings under **Propagation - Network analysis**.

The first Infection Monkey Agent ran on 1/6/2025, 4:41:55 PM.

Infection Monkey started propagating from the following machines where it was manually installed:

- caldera

No credentials available for brute forcing.

Configured exploitation methods:

- Log4Shell Exploiter
- SMB Exploiter
- PowerShell Remoting Exploiter
- WMI Exploiter
- MSSQL Exploiter
- SSH Exploiter

Configured IPs to scan:

- 10.0.0.0/24

The Network from Infection Monkey's Eyes

Infection Monkey discovered 26 machines and successfully breached 0 of them.

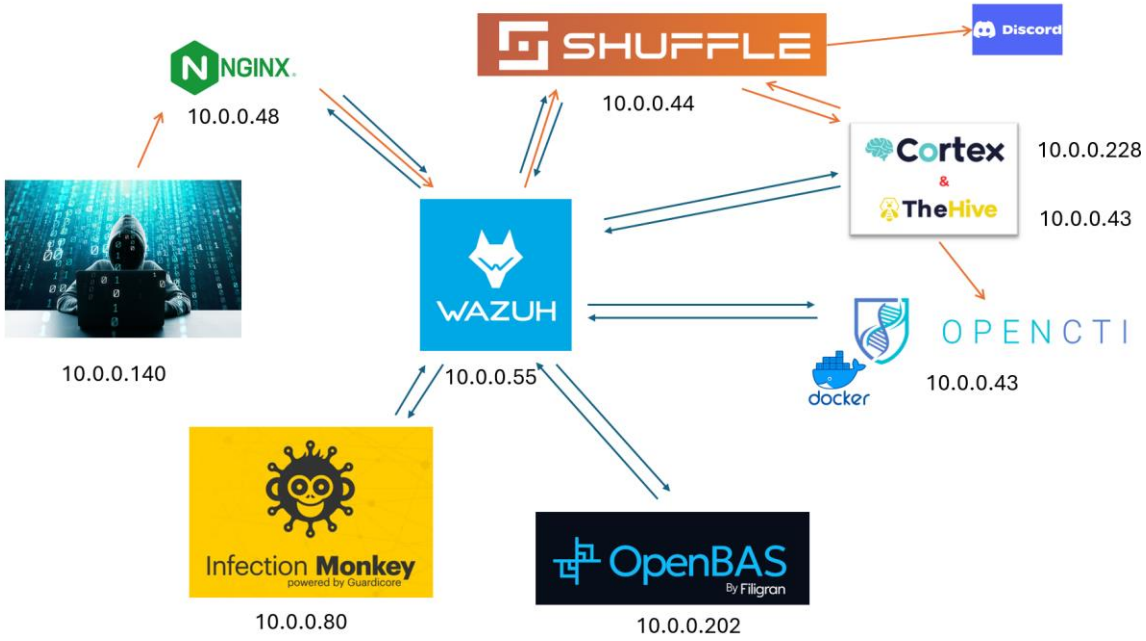
0% of scanned machines exploited

Infection Monkey discovered 0 open services on 26 machines:

Scanned Servers	
Machine	Services found
(10.0.0.1/32)	10.0.0.1:80 - unknown 10.0.0.1:443 - unknown
(10.0.0.3/32)	10.0.0.3:22 - unknown 10.0.0.3:80 - unknown 10.0.0.3:443 - unknown

4. De Attack

Hieronder vindt u de afbeelding van hoe dat de attack door mijn SOC gaat.



4.1. Hydra

Voor mijn attack ga ik gebruik maken van een random ubuntu machine die op het netwerk zit met hydra geinstalleerd. Met hydra ga ik een SSH brute force proberen naar mijn webserver.

```
thomas@thomas-virtual-machine:~$ hydra -l thomas -P best1050.txt 10.0.0.48 ssh 22
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpos
es (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-04 23:48:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting
, ./hydra.restore
```

4.2. Wazuh

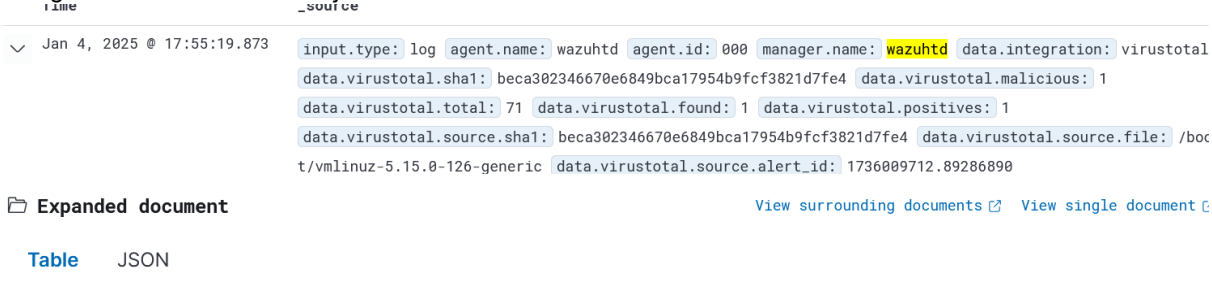
4.2.1. Attack

Voor de attack gaat Wazuh doormiddel van een custom rule doorgeven wanneer dat er een Brute force attack wordt gedaan op een van de servers. Met Deze custom Rule gaat wazuh dan een api request sturen naar Shuffle met alle data van de rule. Daarnaast gaat Wazuh ook automatisch het ip blockeren voor 180 seconde.

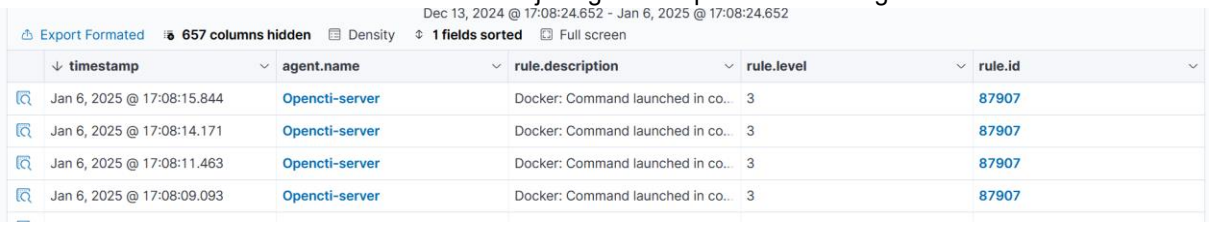
```
thomas@thomas-virtual-machine:~$ ping 10.0.0.48
PING 10.0.0.48 (10.0.0.48) 56(84) bytes of data.
^C
--- 10.0.0.48 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms

thomas@thomas-virtual-machine:~$ ssh thomas@10.0.0.48
^C
thomas@thomas-virtual-machine:~$ curl 10.0.0.48
^C
thomas@thomas-virtual-machine:~$
```

4.2.2. Extra

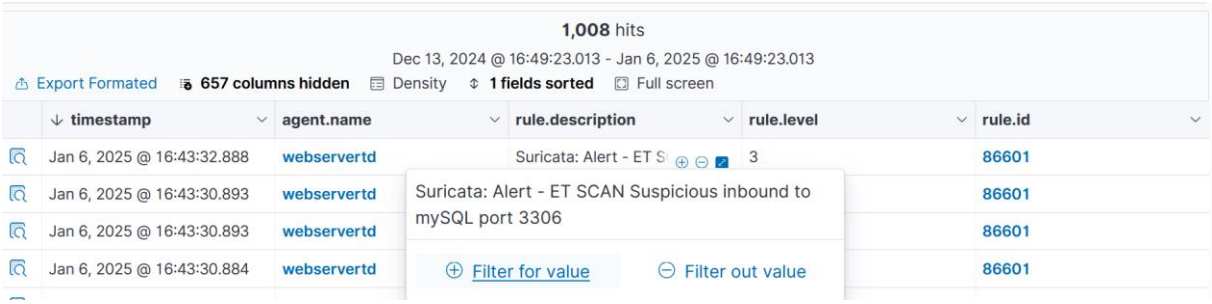
Daarbuiten is Wazuh ook geintegreerd met Virustotal die automatisch onbekende files scanned en doorgeeft of deze malicieus zijn of niet.



Wazuh is verbonden met elke Virtual machine die in mijn SOC steekt door middel van de wazuh agent. Bij de Wazuh Agent van de server van OpenCTI heb ik ook geconfigureerd dat deze ook meldingen van Docker Doorstuurd waardoor ik kan zien wat er juist gebeurt op de docker images.

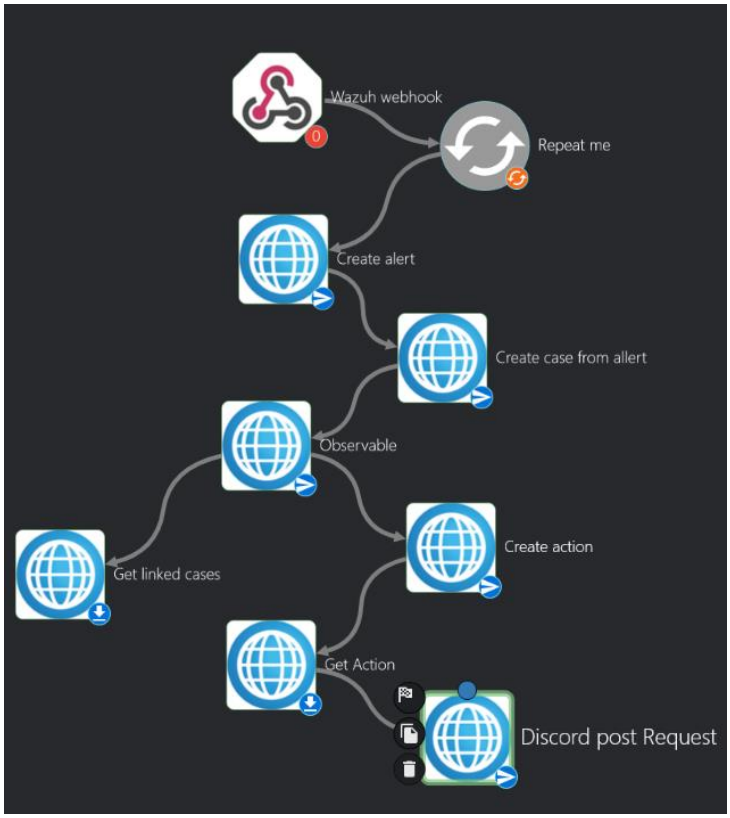


Daarbuiten heeft Wazuh ook een integratie met suricata die op de webserver staat om vreemde internet traffic door te geven zoals de scans van Infection Monkey.



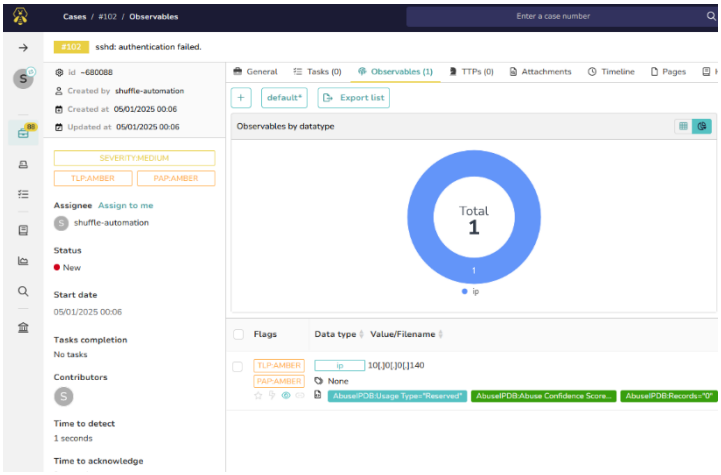
4.3. Shuffle

Doormiddle van een webhook van shuffle komt de data van wazuh binnen. Deze data wordt dan een alert in The Hive doormiddel van een api Post request (Create alert). Dan wordt er onmiddelijk een case van gemaakt en deze cases worden ook in OpenCTI getooont. Daarna wordt er een observable bij gevoegd en op deze observable gaan we dan een actie uitvoeren. Na dat de actie gedaan (10s) is gaat er een Discord bericht worden verstuurd met alle informatie.



4.4. The hive + Cortex

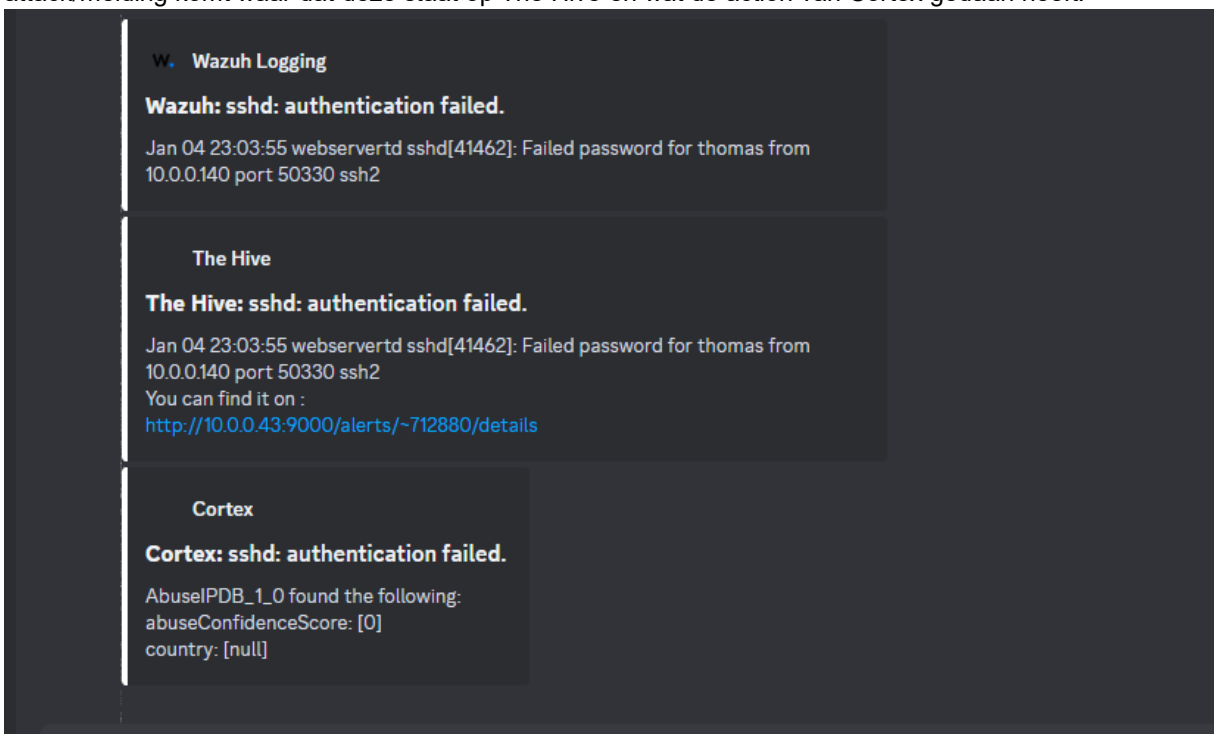
Daarnet spraken we van een alert, case en actie deze worden gemaakt in The hive en de actie wordt uitgevoerd in Cortex.
De alert wordt momenteel direct omgezet in een case maar als ik het in productie zou doen zou ik er eerst voor zorgen dat er minstens 3-4 alerts waren voor dat ik er een case van maakte en dan zou ik met de node “Get linked Cases” in shuffle deze samen linken.
Bij de gemaakte case voegen we een Observable uit, de ip waarvan de attack komt. Deze gaan we met cortex en AbuseIPDB gaan checken of deze slecht is.



De reden dat we dit allemaal in The hive steken is om de beveiligingsincidenten te beheren en onderzoeken, als ik met een team zou zijn zou ik automatisch een persoon aan de case kunnen linken zodat die persoon aan die case zou kunnen werken en dat er gemakkelijk een timeline kan worden getoond van wanneer is het gebeurd en van wanneer is het opgelost.
Daarnaast hebben we eerder vermeld dat de cases ook naar openCTI gaan zodat iedereen met toegang tot de eigen gehoste website kan bekijken.

4.5. Discord

Op discord doormiddel van een Webhook kunnen we dus gemakkelijk en overzichtelijk zien vanwaar een attack/melding komt waar dat deze staat op The Hive en wat de action van Cortex gedaan heeft.



5. Extra?

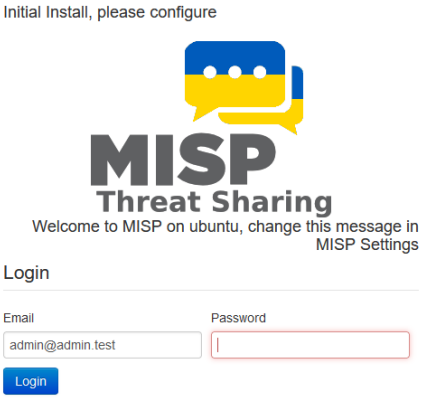
Wat heb ik nog geprobeerd te installeren:

5.1. OpenCTI en OpenBAS

Doordat openBAS zo nieuw is zijn er nog niet veel integraties met anderen waardoor ik moeite heb gehad om OpenBAS in werking te krijgen. Dat is de reden dat ik terug ben overgestapt naar Infection monkey. Doordat het zo nieuw is is er geen gemakkelijke integratie tussen OpenBAS en OpenCTI (wat ze wel vermelden) maar dat betekent niet dat ik niet heb geprobeerd als dit gelukt was zou ik het veel fijner hebben gevonden.

5.2. Misp

Door het slecht inplannen van mijn tijd heb ik geen tijd gehad om Misp te configureren, het staat wel op maar ik heb geen interacties tussen Misp en andere platformen.



5.3. Graylog

Voor het installeren van graylog heb ik heel veel tijd verdoen, het wilt niet installeren doordat MongoDB V5+ niet op de hardware die ik gebruik kan draaien het zou ervoor hebben gezorgd dat ik terug moest gaan van de huidige versie 6.1.x naar versie 4.2.x.

Maar dit heb ik wel gedaan voor infection monkey want ik vond dat OpenBAS niet goed genoeg was.

6. Links

Attack: https://youtu.be/t3PgGzgTVy8
Infection monkey: https://youtu.be/gChPRK7SM6Y

CONTACT

Thomas Deboel | Student
r0841840@studentthomasmore.be

THOMAS MORE