Die Rolle von SIEM-Systemen im Security Operations Center

NetEye User Group | 21.09.2023

1 | SIEM vs. SOC

SIEM ist die technologische Basis für Security Operations Center

2 | Security Analytics Tools

Security Analytics Tools unterstützen bei der Verarbeitung der Datenmengen

3 | Threat-Intelligence

Threat-Intelligence Daten unterstützen die Erkennung fortgeschrittener Bedrohungen

4 | Automatisierung

Durch Automatisierung mehr aus SIEM und SOC herausholen

5 | Sneak Peek

Sneak Peek in das agilimo SOC inkl. Fallbeispiele

6 | SOC as a Service

Etablierte SOC-Prozesse als Add-On für bestehende NetEye Umgebungen

1 | SIEM vs. SOC

SIEM ist die technologische Basis für Security Operations Center

SIEM

- Security Information and Event Management ist eine Technologie
- Zentrales Repository für Logs
- Normalisierung und Indizierung der Logs
- Zuordnung der Daten zu Felder
- Anreicherung der Daten durch andere Datenquellen

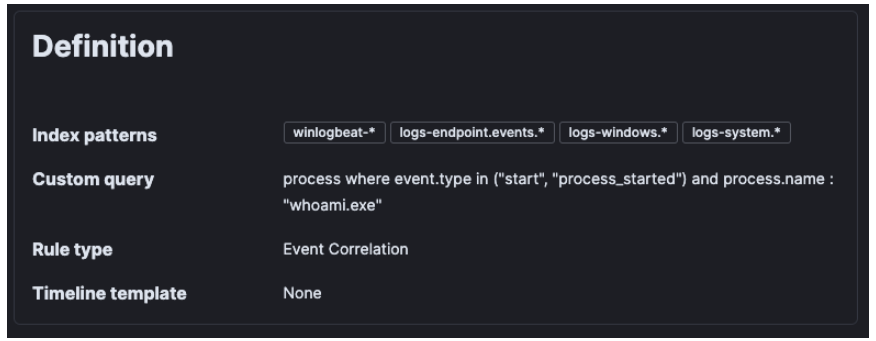
SOC

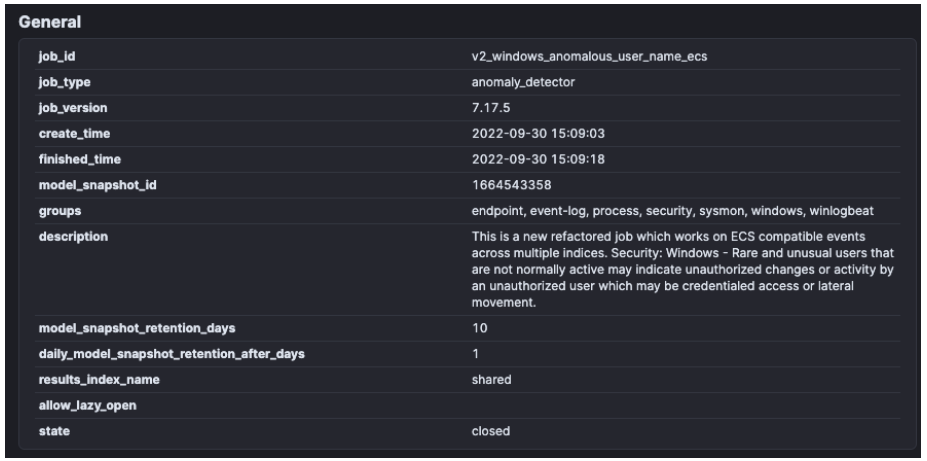
- Im SOC spielen Prozesse eine wichtige Rolle
- Playbooks zum Vorgehen bei Vorfällen
- Abläufe die regelmäßig trainiert werden
- Reaktion auf Ereignisse
- Menschen treffen letzte Entscheidung

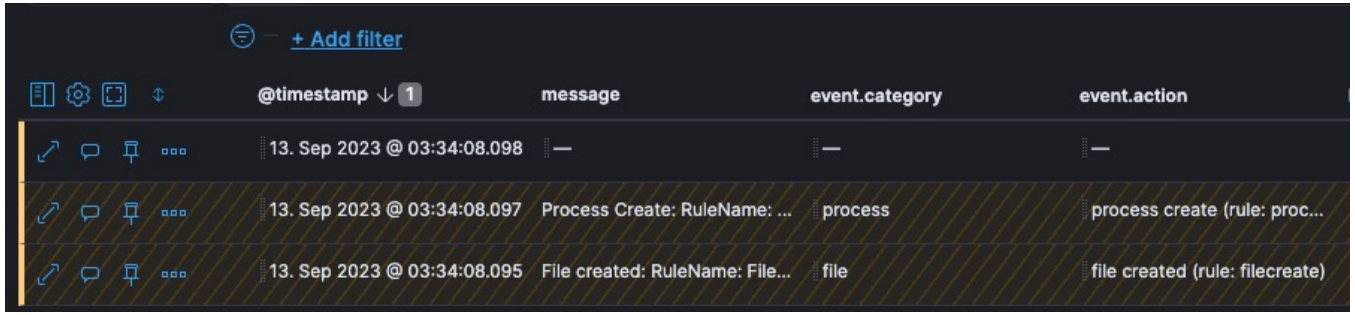
2 | Security Analytics Tools

Security Analytics Tools unterstützen bei der Verarbeitung der Datenmengen

- Detection Rules entdecken Auffälligkeiten in einzelnen Logs
- Machine Learning für Verhaltensanalyse
- Timelines setzen mehrere Ereignisse in Korrelation





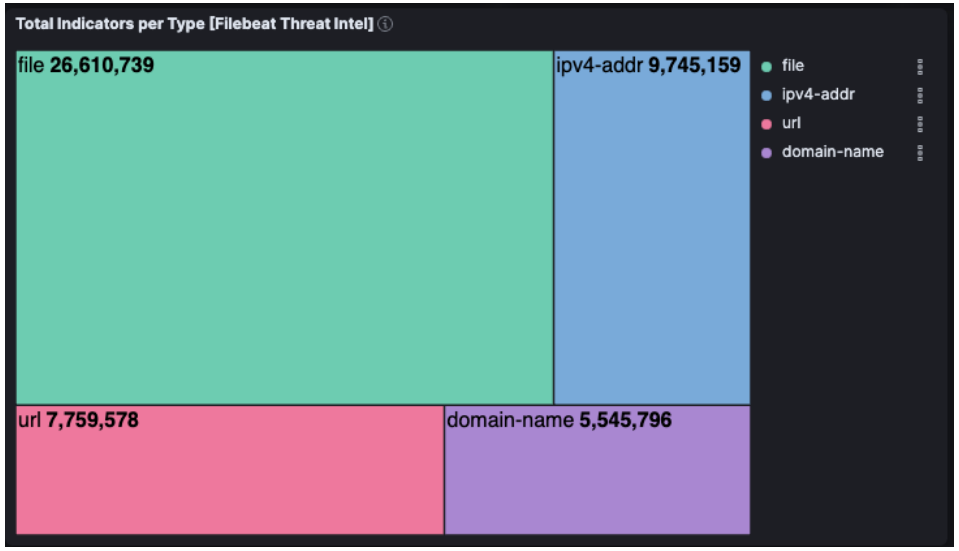


Erkennung und dadurch Abwehr von Bedrohungen in nahezu Echtzeit

3 | Threat-Intelligence

Threat-Intelligence Daten unterstützen die Erkennung fortschrittlicher Bedrohungen

- Beschreibungen von Tactics, Techniques and Procedures (TTPs)
- Ableitung von Indicators of Compromise (IOCs)
- Logs können mit diesen Daten verglichen werden
- Automatisiertes Abrufen neuer Threat-Intelligence Daten



Date (UTC)	IOC
2023-09-18 20:40	87.251.67.46:80
2023-09-18 20:40	185.123.53.150:80
2023-09-18 20:40	103.208.86.81:80
2023-09-18 18:50	14.19.144.23:8443
2023-09-18 18:50	38.180.74.55:445
2023-09-18 18:49	94.237.58.198:5985
2023-09-18 18:49	16.171.237.4:443
2023-09-18 18:49	202.162.108.120:443
2023-09-18 18:49	47.245.42.208:443
2023-09-18 18:49	192.144.211.13:443
2023-09-18 18:49	175.27.146.212:443
2023-09-18 18:47	194.68.26.216:8080
2023-09-18 18:47	194.68.26.216:8000
2023-09-18 18:47	188.127.242.204:8443
2023-09-18 18:15	http://christopherantonio.top/e9c3...
2023-09-18 15:54	ptzbubble.shop
2023-09-18 15:54	trpihgram.space
2023-09-18 15:54	209.127.19.241:10284
2023-09-18 15:54	https://uploads.dachhost.top
2023-09-18 15:54	46.4.98.104:443

4 | Automatisierung

Durch Automatisierung mehr aus SIEM und SOC herausholen

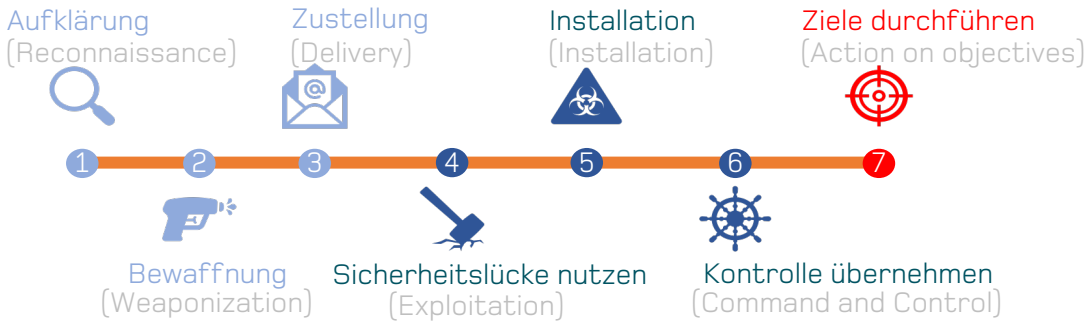
- Vorher definierte Abläufe beim Auftreten von Ereignissen
- Kombination mehrerer Tools
- Security Orchestration and Response (SOAR)
- Mapping von MITRE ATT&CK TTPs und testen der Detection Rules

✓ Zeitgewinn
✓ Aus reaktiv (Detection and Response) wird proaktiv mittels Threat-Hunting

5 | Sneak Peek

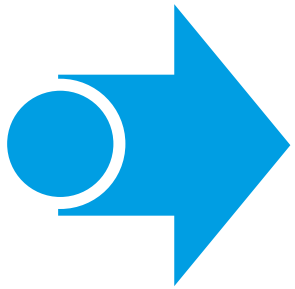
Sneak Peek in das agilimo SOC

- Basis ist die Cyber Kill Chain
- MITRE ATT&CK Framework zur Identifizierung relevanter TTPs
- NetEye SIEM als NDR
- NEXTRON AURORA als EDR
- NEXTRON THOR für forensische Untersuchungen
- Würth Phönix SATAYO zur Identifizierung des External Exposure

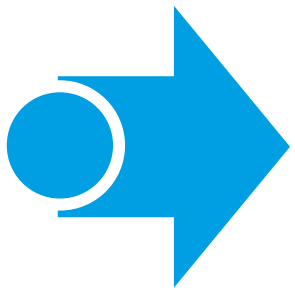


Fallbeispiel 1: Verdächtige Anmeldung via VPN

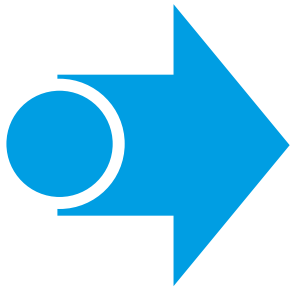
Machine Learning Job entdeckt Login zu ungewöhnlicher Tageszeit



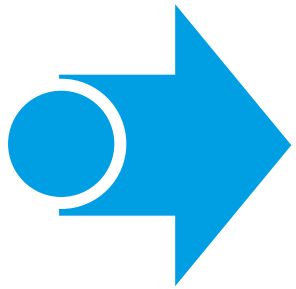
Alert und Case in Elastic



Jira Ticket



Playbook „Account Compromise“



- Prüfen der Source IP
- Sperren des Accounts
- Prüfen ob weitere Accounts betroffen sind
- Report für den Kunden erstellen

Fallbeispiel 2: Malware auf Server entdeckt

AURORA meldet Malware auf einem Server
Severity HIGH

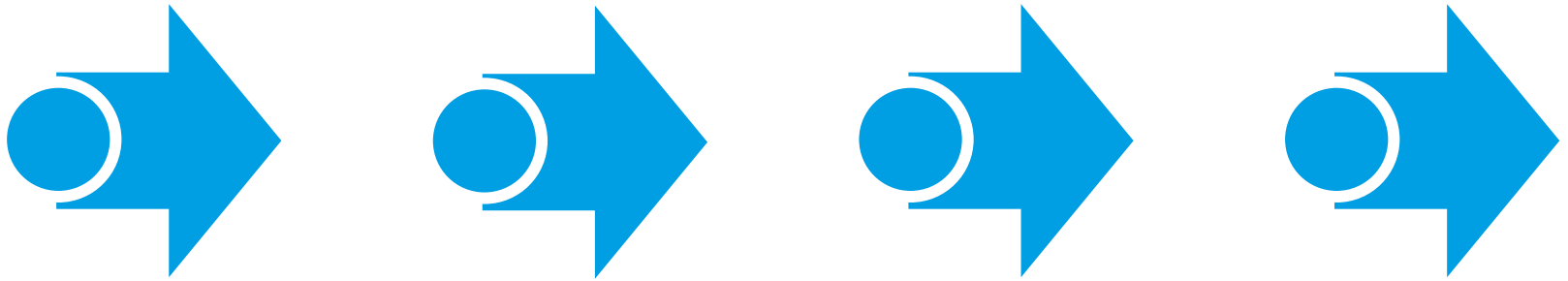
Case in ASGARD Analysis Cockpit

Jira Ticket

Playbook „Malware“

- Prüfen des Systems
- Logs in NetEye SIEM analysieren
- Entfernen der Malware
- Erneute Prüfung des Systems
- Report für den Kunden erstellen

Fallbeispiel 3: Kompromittierung durch Advanced Persistant Threat (APT)



AURORA meldet Erkennung eines Cobalt Strike Beacons Severity CRITICAL

Case in ASGARD Analysis Cockpit

Jira Ticket

Playbook „Critical“

- Automatisierter intensive THOR-Scan
- Incident Response Team wird aktiviert
- Einrichtung eines „War-Rooms“
- Vor-Ort Analyse der Infrastruktur
- Ggf. isolieren betroffener Systeme oder kappen von Verbindungen
- Report für den Kunden erstellen

6 | SOC as a Service

Etablierte SOC-Prozesse als Add-On für bestehende NetEye Umgebungen

SIEM

- Security Information and Event Management ist eine Technologie
- Zentrales Repository für Logs
- Normalisierung und Indizierung der Logs
- Zuordnung der Daten zu Felder
- Anreicherung der Daten durch andere Datenquellen

SOC

GRAVITATE

- Im SOC spielen Prozesse eine wichtige Rolle
- Playbooks zum Vorgehen bei Vorfällen
- Abläufe die regelmäßig trainiert werden
- Reaktion auf Ereignisse
- Menschen treffen letzte Entscheidung

Die agilimo Group auf einen Blick

- 4 Standorte
- 75 Mitarbeiter
- 105 Mio. Euro Umsatz in 2021
- ISO 27001 zertifiziert
- 2 eigene Rechenzentren / RIPE Mitgliedschaft
- Mehr als 400 erfolgreiche Projekte im Bereich IT Sicherheit

agilimo group

HiFiextra®

- Hardware
- Device Handling

agilimo consulting

- IT-Beratung
- MSSP / SOC

Ihre Ansprechpartner

Marcus Heinrich
Geschäftsführer

marcus.heinrich@agilimo.de
Tel +49 6022 65193-10

Thomas Edelmann
Geschäftsführer

thomas.edelmann@agilimo.de
Tel +49 6022 65193-20

Michael Fornoff
Strategic Account Manager

michael.fornoff@agilimo.de
Tel +49 6022 65193-15