

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**

	@timestamp ↓ 1	message	event.category	event.action
	13. Sep 2023 @ 03:34:08.098	—	—	—
	13. Sep 2023 @ 03:34:08.097	Process Create: RuleName: ...	process	process create (rule: proc...
	13. Sep 2023 @ 03:34:08.095	File created: RuleName: File...	file	file created (rule: filecreate)

Definition

Index patterns winlogbeat-* logs-endpoint.events.* logs-windows.* logs-system.*

Custom query process where event.type in ("start", "process_started") and process.name : "whoami.exe"

Rule type Event Correlation

Timeline template None

General

job_id	v2_windows_anomalous_user_name_ecs
job_type	anomaly_detector
job_version	7.17.5
create_time	2022-09-30 15:09:03
finished_time	2022-09-30 15:09:18
model_snapshot_id	1664543358
groups	endpoint, event-log, process, security, sysmon, windows, winlogbeat
description	This is a new refactored job which works on ECS compatible events across multiple indices. Security: Windows - Rare and unusual users that are not normally active may indicate unauthorized changes or activity by an unauthorized user which may be credentialed access or lateral movement.
model_snapshot_retention_days	10
daily_model_snapshot_retention_after_days	1
results_index_name	shared
allow_lazy_open	
state	closed

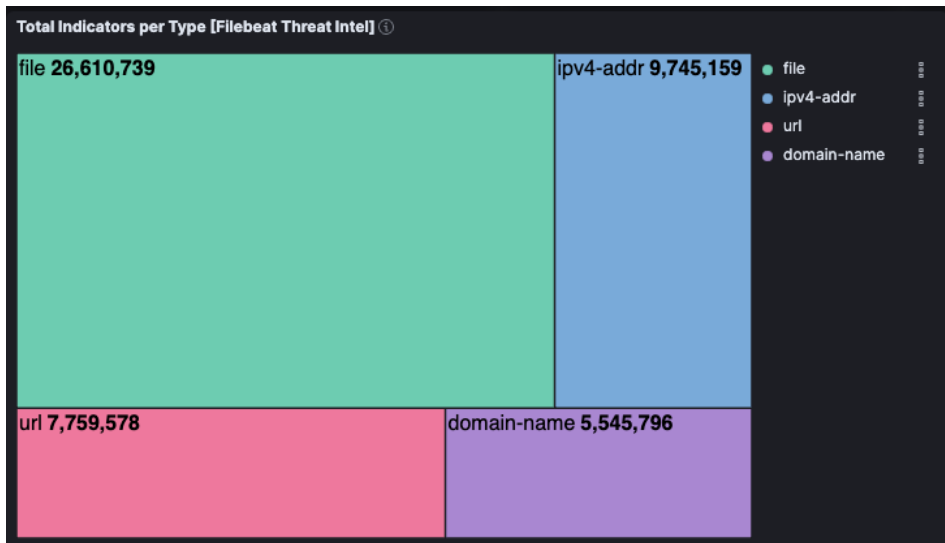
Erkennung und dadurch Abwehr von Bedrohungen in nahezu Echtzeit

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**

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Direct Compromise	Cloud Infrastructure Command	Account Manipulation	Abuse Discretion	Abuse Discretion	Adversary in the Media	Account Discovery	Exploitation of Remote Services	Adversary in the Media	Adversary in the Media	Adversary in the Media	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Exploit Public-Facing Application	Command and Control	MITRE Jobs	Access Token Manipulation	Access Token Manipulation	Abuse Discretion	Internal Application	Internal Spearphishing	Address Collected Data	Local Process	Substitution Through Remote Media	Data
Gather Victim Identity Information	Compromise Accounts	Internal Remote Services	Commander Administration Command	Build or Logon Automated Execution	Build or Logon Automated Execution	Build or Logon Automated Execution	Build or Logon Automated Execution	Cloud Infrastructure	Control Host Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Ingress
Gather Victim Network Information	Infrastructure	Hardware	Deploy Container	Build or Logon Initialization Scripts	Build or Logon Initialization Scripts	Build or Logon Initialization Scripts	Build or Logon Initialization Scripts	Cloud Service	Remote Service	Advanced	Data	Exfiltration	Data
Gather Victim Org Information	Develop Capabilities	Phishing	Cloud Infrastructure	Remote Extensions	Create or Modify System Process	Debugger Evasion	Debugger Evasion	Cloud Service	Session Hijacking	Reverse Session Hijacking	System	Exfiltration Over Other Network Medium	Manipulation
Phishing for Information	Establish Capabilities	Implication Through Remote Media	Malware Process	Compromise Cloud Software Binary	Domain Policy Modification	Domain Policy Modification	Domain Policy Modification	Cloud Service	Replication Through Remote Media	Clipboard	Encrypted	Exfiltration Over Physical Medium	Data Wipe
Search Closed Sources	Obtain Capabilities	Stolen Credentials	Communication	Cache Account	Cache to Host	Cache to Host	Cache to Host	Cloud Storage	Remote Deployment Tools	Remote	Clipboard	Exfiltration Over Other Web Service	Exploit Denial of Service
Search Open Sources	Days Capabilities	Stolen Credentials	Scheduled Task	Event Triggered Execution	Event Triggered Execution	Event Triggered Execution	Event Triggered Execution	Container and Process	Task Scheduling	Data Post-Configuration	Registry	Scheduled Transfer	Firmware
Search Victim-Owned Resources		Stolen Credentials	Malware	Share Remote Services	Task Scheduler	Task Scheduler	Task Scheduler	Discovery	Discovery	Discovery	Discovery	Transfer to Cloud Account	Conceal Host System
			Deployment Tools	Malware Execution Flow	Malware Execution Flow	Malware Execution Flow	Malware Execution Flow	Discovery	Discovery	Discovery	Discovery	Discovery	Recovery
			System Services	Inject Internal Scripts	Scheduled Task	Scheduled Task	Scheduled Task	Discovery	Discovery	Discovery	Discovery	Discovery	Network Denial of Service
			User Execution	Malware	Malware	Malware	Malware	Discovery	Discovery	Discovery	Discovery	Discovery	Host System
			Windows Management	Office Application	Office Application	Office Application	Office Application	Discovery	Discovery	Discovery	Discovery	Discovery	Service Stop
								Discovery	Discovery	Discovery	Discovery	Discovery	Shutdown/Reboot

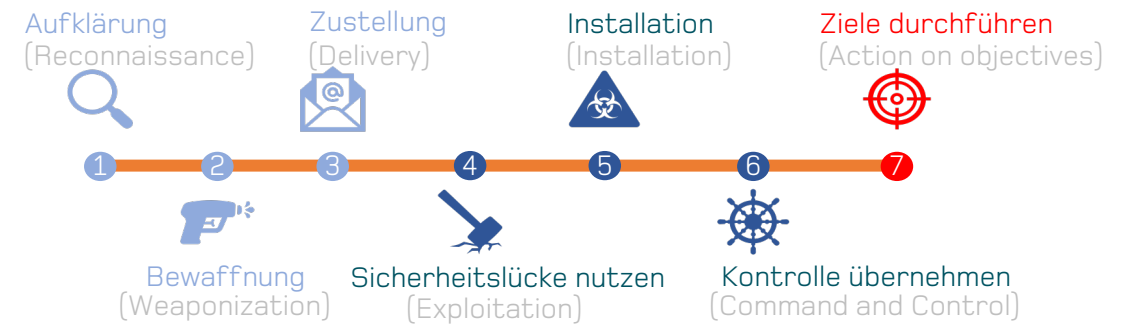
- ✓ Zeitgewinn
- ✓ Aus reaktiv (Detection and Response) wird proaktiv mittels Threat-Hunting

5 | Sneak Peek



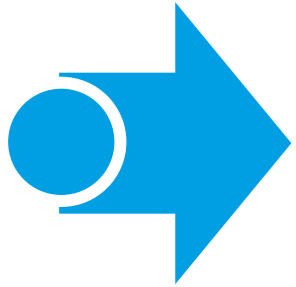
Sneak Peek in das agilimo SOC

- 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 Phoenix **SATAYO** zur **Identifizierung** des **External Exposure**

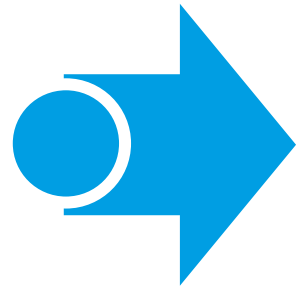




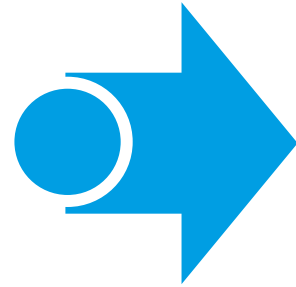
Fallbeispiel 1: Verdächtige Anmeldung via VPN



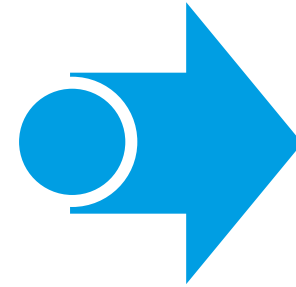
Machine Learning
Job entdeckt Login
zu ungewöhnlicher
Tageszeit



Alert und Case
in Elastic



Jira Ticket

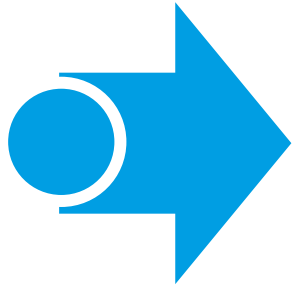


Playbook
„Account
Compromise“

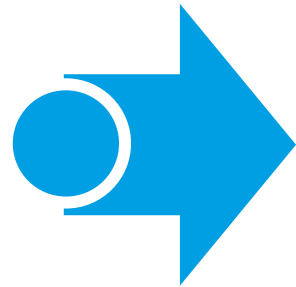
- Prüfen der Source IP
- Sperren des Accounts
- Prüfen ob weitere Accounts betroffen sind
- Report für den Kunden erstellen



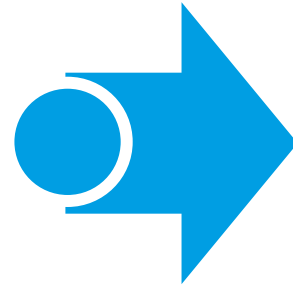
Fallbeispiel 2: Malware auf Server entdeckt



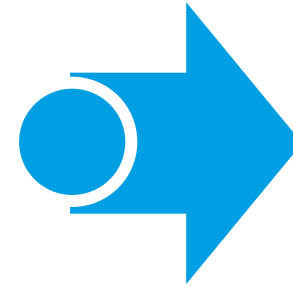
AURORA meldet
Malware auf einem
Server
Severity HIGH



Case in ASGARD
Analysis Cockpit



Jira Ticket

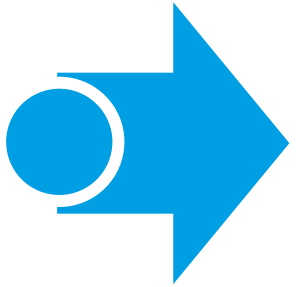


Playbook
„Malware“

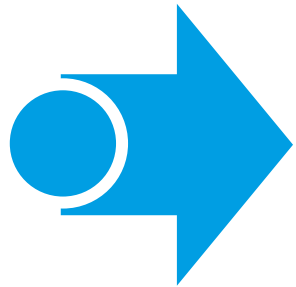
- Prüfen des Systems
- Logs in NetEye SIEM analysieren
- Entfernen der Malware
- Erneute Prüfung des Systems
- Report für den Kunden erstellen



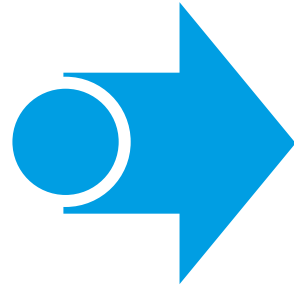
Fallbeispiel 3: Kompromittierung durch Advanced Persistent Threat (APT)



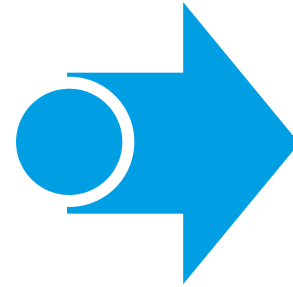
AURORA meldet
Erkennung eines
Cobalt Strike
Beacons
Severity CRITICAL



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



- 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



- Hardware
- Device Handling



- 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

