Erkennung und Analyse von Cyberangriffen am Beispiel von Wazuh-XDR

Sebastian-Alexandru Pop

Motivation

- Wachsende Anzahl an komplexen und zielgerichteten Cyberangriffen
- Antivirus Systeme sind nicht ausreichend
- Komplexe IT-Infrastruktur erfordert Überwachung durch ausgereifte Technologien

Wazuh Komponenten

Endpoints

Log data generators

- Mit Agent
- Ohne Agent

Wazuh Server

Log data analizer

- Alert Generierung
- Regelwerk Personalisierung
- Alert & Log Speicherung

Presentation

Log data displayer

- Statistische Auswertung
- Personalisierte Filter

Lösung - XDR

eXtended Detection and Response Tools bieten eine einheitliche Plattform für die Erkennung und Analyse von Sicherheitsbedrohungen und unterstützen bei der Reaktion auf Vorfälle.

XDR-Tools bieten, über klassische Antivirus Lösungen hinaus, folgende Funktionen:

Überwachung der gesamten IT-Infrastruktur
Endpunkte – Netzwerkgeräte – Cloud-Instanzen

Korrelation von Daten aus mehreren Quellen
Logdateien – Telemetrie – Agent

Bereitstellung von Regelwerken zur Angriffserkennung
Standardregelwerk – Benutzerdefinierte Regeln – Skripte

Ermöglichung von Threat Hunting
Datenaufbereitung – Cyberangriffskette

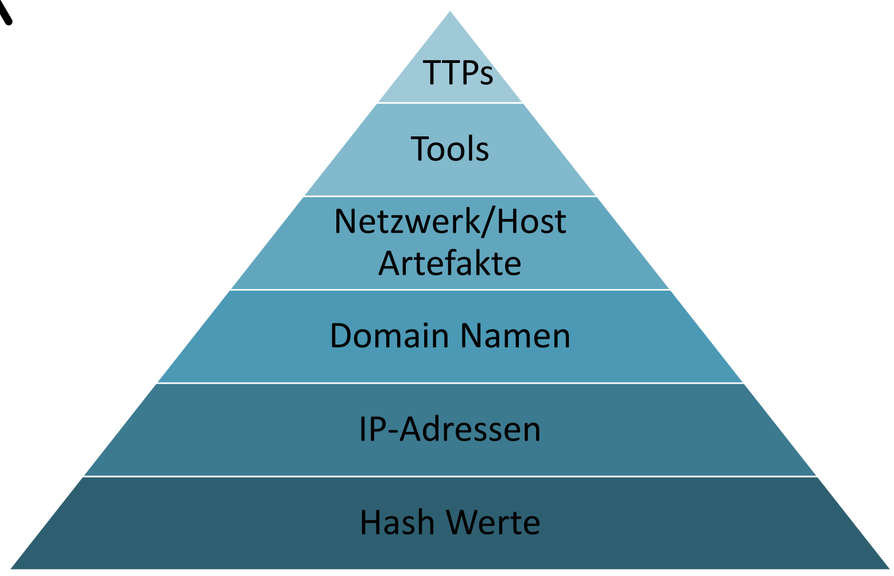
Ermöglichung von Integrity Monitoring
Systemänderungen – Dateiänderungen

Ermöglichung von Active Response
Automatisierte Interventionen – Quarantäne – Personalisierte Skripte

Tactics-Techniques-Procedures (TTPs) sind für Angreifer am schwierigsten zu umgehen und haben daher bei der Definition des Regelwerks oberste Priorität

Die **Pyramid of Pain** wird von Sicherheitsanalysten verwendet, um das Regelwerk von XDR-Systemen zu definieren

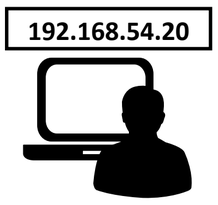
Die **Pyramid of Pain** ist eine aufsteigende Rangfolge von Kompromittierungsindikatoren



Pyramid of Pain

Testfall: Brute Force Angriff


```
ncrack -v
-U /share/users.txt
-P /share/passwd.txt
192.168.54.20:22
```



Windows Security Log

```
Event_ID: 4625
Acc.Name: FakeUser
Acc.Domain: FakeDomain
```

Decoded Log

```
Agent_IP: 192.168.54.20
Agent_Name: Windows1
Full_Log: Event_ID:4625 …
```

Wazuh Rule

```
Rule_ID: 60122
Level: 3
Description:Logon failure
Trigger: ^529? | ^4625?
```

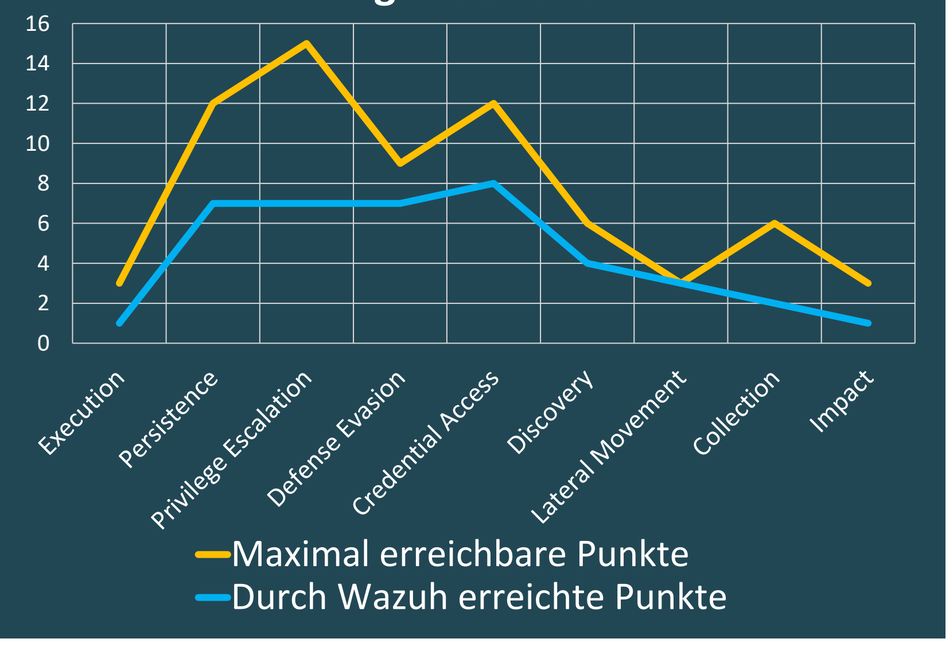
Alert

```
Level: 3
Agent_IP: 192.168.54.20
Agent_Name: Windows1
Win.SysMessage: sshd
```

New Alert

```
TIME | SOURCE
```

Punkteverteilung nach untersuchten Angriffstaktiken



Ergebnisse

Kategorie	Vorteile	Nachteile
Überwachung	▪ Geräte mit Agent ▪ Geräte ohne Agent	–
Regelwerk	▪ Personalisierte Regeln ▪ Personalisierte Skripte	▪ Keine differenzierte Standardabdeckung
Threat Hunting	▪ Gruppierte Ereignisinformationen ▪ Anzahl der Ereignisse als Diagramm	▪ Keine Erkennung/ Darstellung der Cyberangriffskette/ zusammenhängender Ereignisse
Active Response	▪ Eigene Response-Skripte auf dem Endpunkt starten	▪ Keine Werk-Responses ▪ Keine Quarantäne

Wazuh erfüllt die **Mindest-anforderungen** an ein XDR-Tool. Durch die Konfiguration eines differenzierten Regelwerks kann Wazuh mit seinen Mitbewerbern am Markt konkurrieren. In seiner derzeitigen Form kann Wazuh jedoch **nicht** als **vollwertiges XDR-Tool** betrachtet werden.

h_da hochschule darmstadt informatik
member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY
controlware

Praxisprojekt 2
Informatik Dual
2025

Gruppe A