Controlware Security Day 2022

Controlware SOC – ein Blick hinter die Kulissen

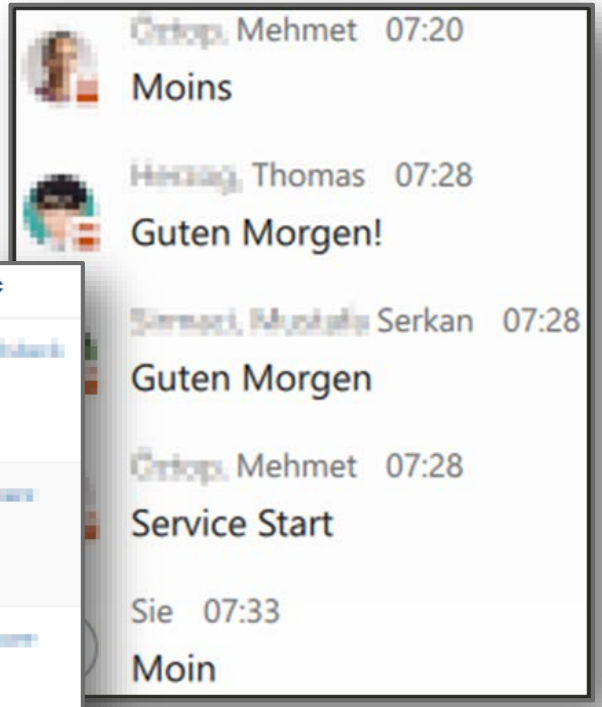
Andreas Bunten, Controlware GmbH, Controlware CSIRT

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau

Service Start: Montag 8 Uhr

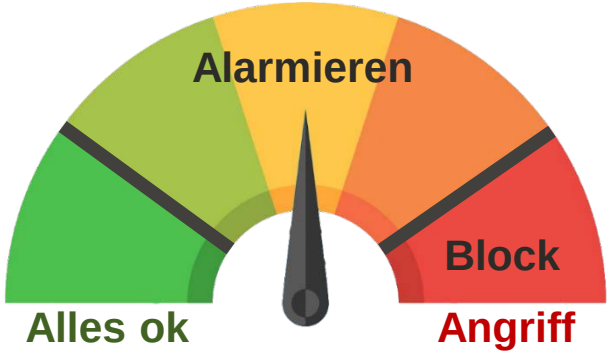
- Reguläre Servicezeit: Werktags 8h – 17h
- 8 Uhr? Informeller Start meistens früher
- Alarme kontrollieren in der Plattform

Severity	Read	Title	# Case	Type	Source
L	Unread	2 'Suspicious port scan' alerts detected by XDR Analytics on host 10.1.200.75	None	Cortex XDR Alert	
Cortex XDR					
M	Unread	PUA on 10.74.32.52	None	SentinelOne Alert	
SentinelOne					
M	Unread	PUA on 172.16.60.92	None	SentinelOne Alert	
SentinelOne					
M	Unread	Malware on 192.168.1.110	None	SentinelOne	



Woraus besteht der Managed SOC Service?

- Security Systeme bewerten auf einer Skala
- Trotz KI & Machine Learning kommt es zu Fehlern
- Schwellwerte bestimmen Anzahl der Fehler
  - **False Positives:** Legitime Aktion als Angriff erkannt
  - **False Negatives:** Echter Angriff wird *nicht erkannt*
- Unsere Lösung:
  - Automatisches blockieren bei hohem Schwellwert
  - Alarmierung und manuelle Analyse ab erstem Verdacht
- **Ziel:** sicher erkannte Angriffe verhindern & getarnte Angriffe zeitnah erkennen



Woraus besteht der Managed SOC Service? (III)

Woher kommen die Alarme?

Controlware Cyber Defense Services mit vier Komponenten

Vulnerability Managament (VMS) Erkennung & Management von Schwachstellen

Advanced Log Analytics (ALA) Log-Daten-Analyse / SIEM

Advanced Threat Detection (ATD) Sandboxing und Network Anomaly Detection

Endpoint Detection & Response (EDR) Angriffe am Endpunkte erkennen und stoppen

Woraus besteht der Managed SOC Service? (III)

Was ist EDR?

Endpoint Detection & Response

- Next-Generation AV
- Aktive Suche in Telemetriedaten
- Erstellung eigener Detection-Regeln
- Bereinigung (u.a. Rollback)
- Reaktion:
  - Prozesse stoppen
  - Systeme isolieren

Endpoint Protection / Anti-Virus

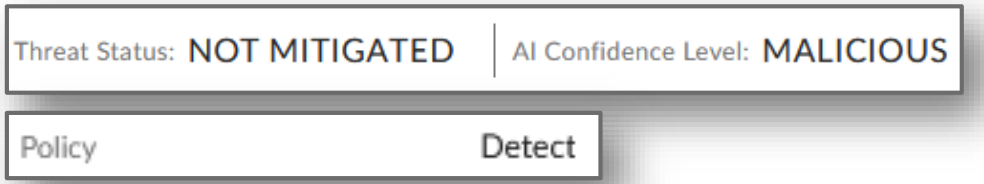
- Fokus auf Prävention
- Schutz vor bekannter Malware
- Erkennung überwiegend auf Basis von Signaturen

Endpoint Detection & Response

Endpoint Protecion / Anti-Virus

Alarm zu verdächtigem Attachment

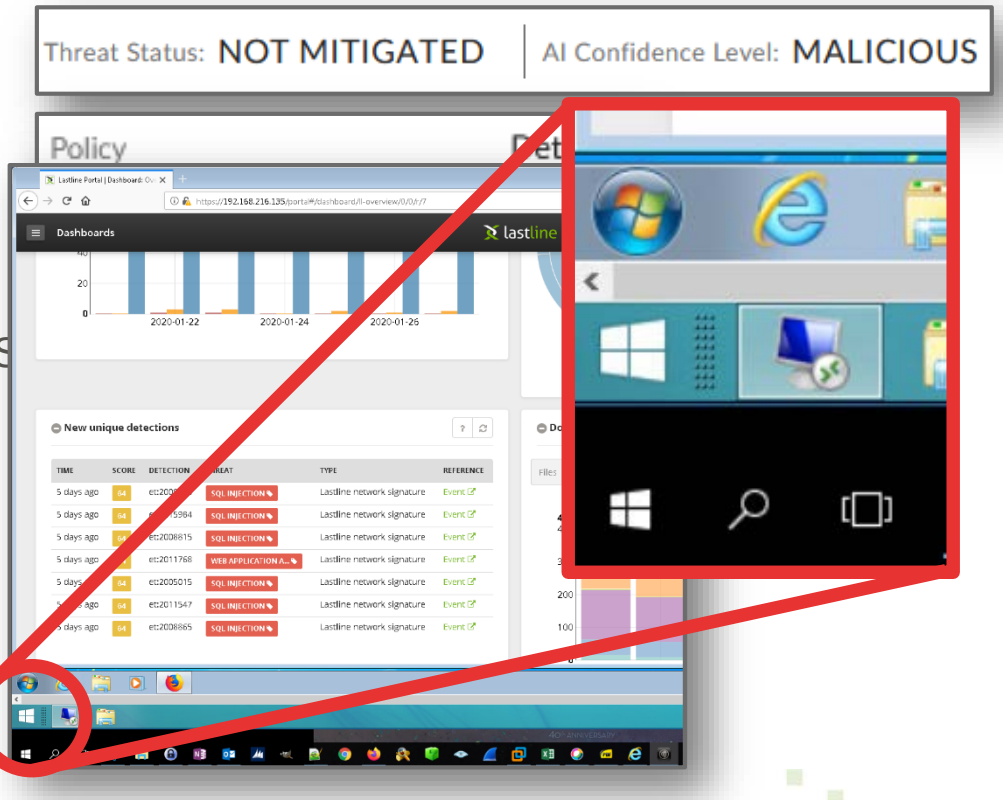
- Gefährliches Attachment erkannt
  ... aber nicht gestoppt
  - Ist es wirklich Malware?
  - Kam die Malware zum Start?



- Wenig Details bekannt:
  - Das Attachment besteht aus kleinem ISO Image ... ein schlechtes Omen
  - Auf VirusTotal aber unklar bewertet
- Transfer der Datei von VirusTotal in SOC Testumgebung

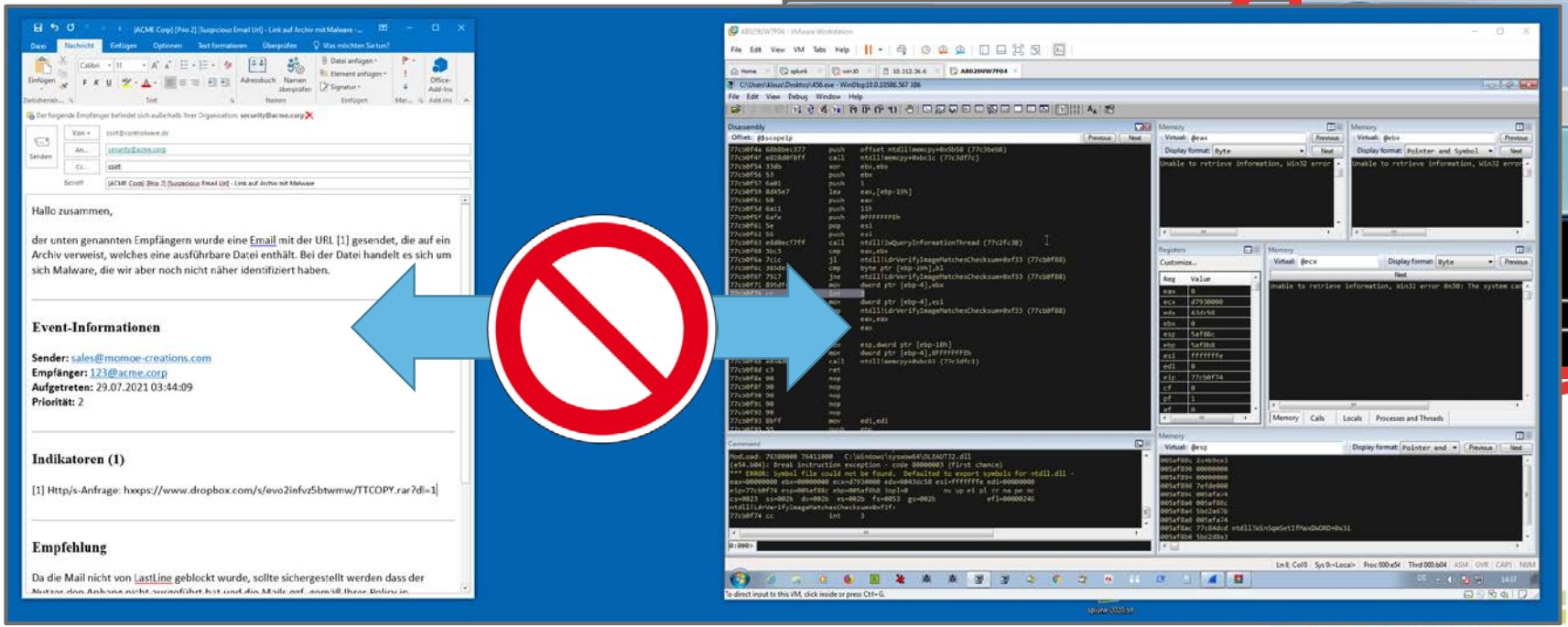
Alarm zu verdächtigem Attachment

- Gefährliches Attachment erkannt
  ... aber nicht gestoppt
  - Ist es wirklich Malware?
  - Kam die Malware zum Start?
- Wenig Details bekannt:
  - Das Attachment besteht aus kleinem IS
  - Auf VirusTotal aber unklar bewertet
- Transfer der Datei von VirusTotal in



Alarm zu verdächtigem Attachment

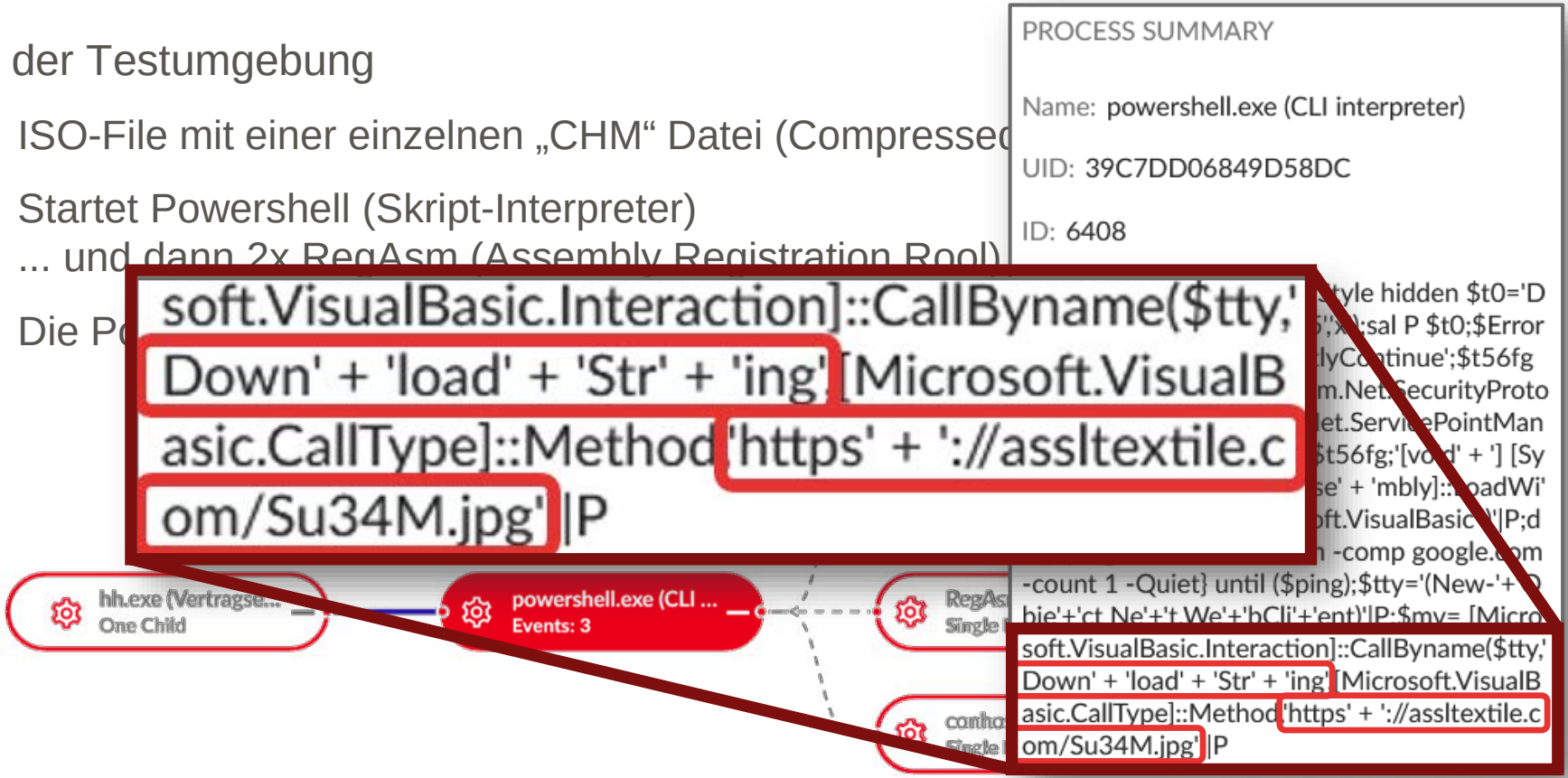
- Gefährliches Attachment erkannt
  ... aber nicht gestoppt
  - Ist es wirklich Malware?



Alarm zu verdächtigem Attachment (II)

In der Testumgebung

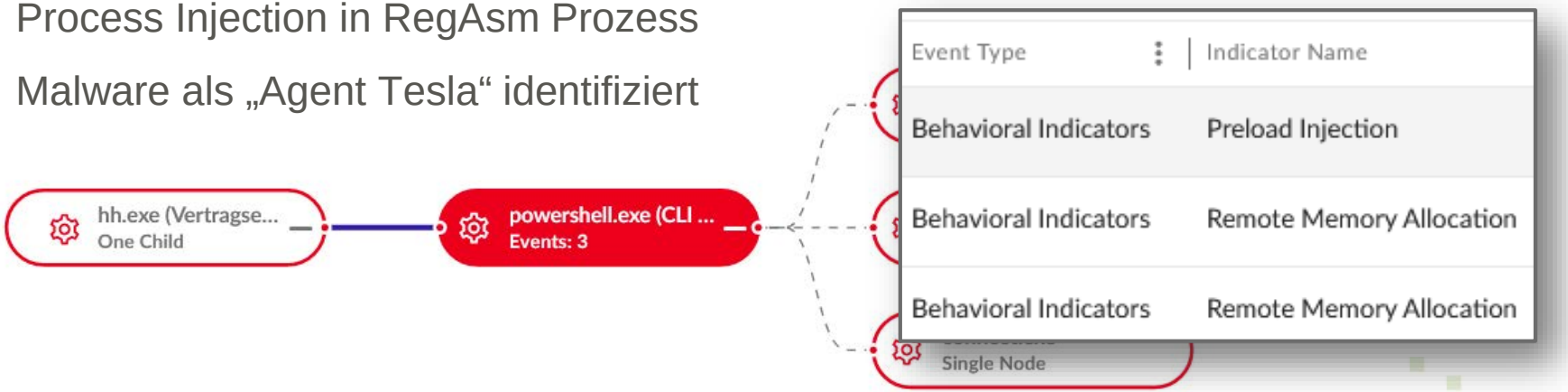
- ISO-File mit einer einzelnen „CHM“ Datei (Compressed
- Startet Powershell (Skript-Interpreter)
  ... und dann 2x RegAsm (Assembly Registration Tool)
- Die Po



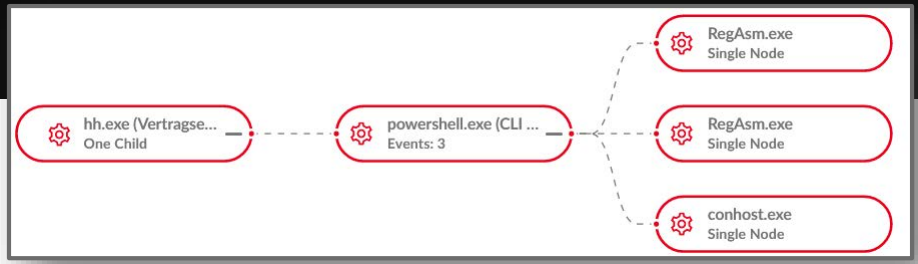
Alarm zu verdächtigem Attachment (II)

In der Testumgebung

- ISO-File mit einer einzelnen „CHM“ Datei (Compressed HTML Helpfile)
- Startet Powershell (Skript-Interpreter)
  ... und dann 2x RegAsm (Assembly Registration Rool)
- Die Powershell lädt ein „Bild“
- Process Injection in RegAsm Prozess
- Malware als „Agent Tesla“ identifiziert



Alarm zu verdächtigem Attachment (III)



Es ist Malware! Wurde sie gestartet?

- Malware Analyse liefert:
  - Code nachladen per HTTPS von *asstextile[dot]com/Su34M.jpg*
  - Übertragung gestohlene Daten per FTP an *ftp.akmokykla[dot]lt*
  - Ablauf: Benutzer klickt - hh.exe - Powershell - RegAsm.exe
- Indicators Of Compromise (IOC) – daran erkennbar, ob System betroffen ist
- EDR: der Analyst kontrolliert IOCs
  - Keine Wartezeit & kein Blockieren von IT-Mitarbeitern
  - Kontrolle von Netz-basierten *und lokalen* IOCs
  - Kontrolle auf allen Endpunkten, egal ob On Prem, Home Office oder in der Cloud
- Meldung an den Kunden mit IOC zur Kontrolle

Alarm zu verdächtigem Attachment (III)


```
DnsRequest Contains Anycase "akmokykla"

DstIP = "185.193.27.46" AND DstPort = "21"

SrcProcParentCmdLine ContainsCIS "explorer" AND
SrcProcName ContainsCIS "hh.exe" AND
TgtProcName ContainsCIS "powershell"
```

…om/Su34M.jpg
…mokykla[dot]lt
…gAsm.exe

…nnbar, ob System betroffen ist

SOURCE PROCESS PARENT DETAILS

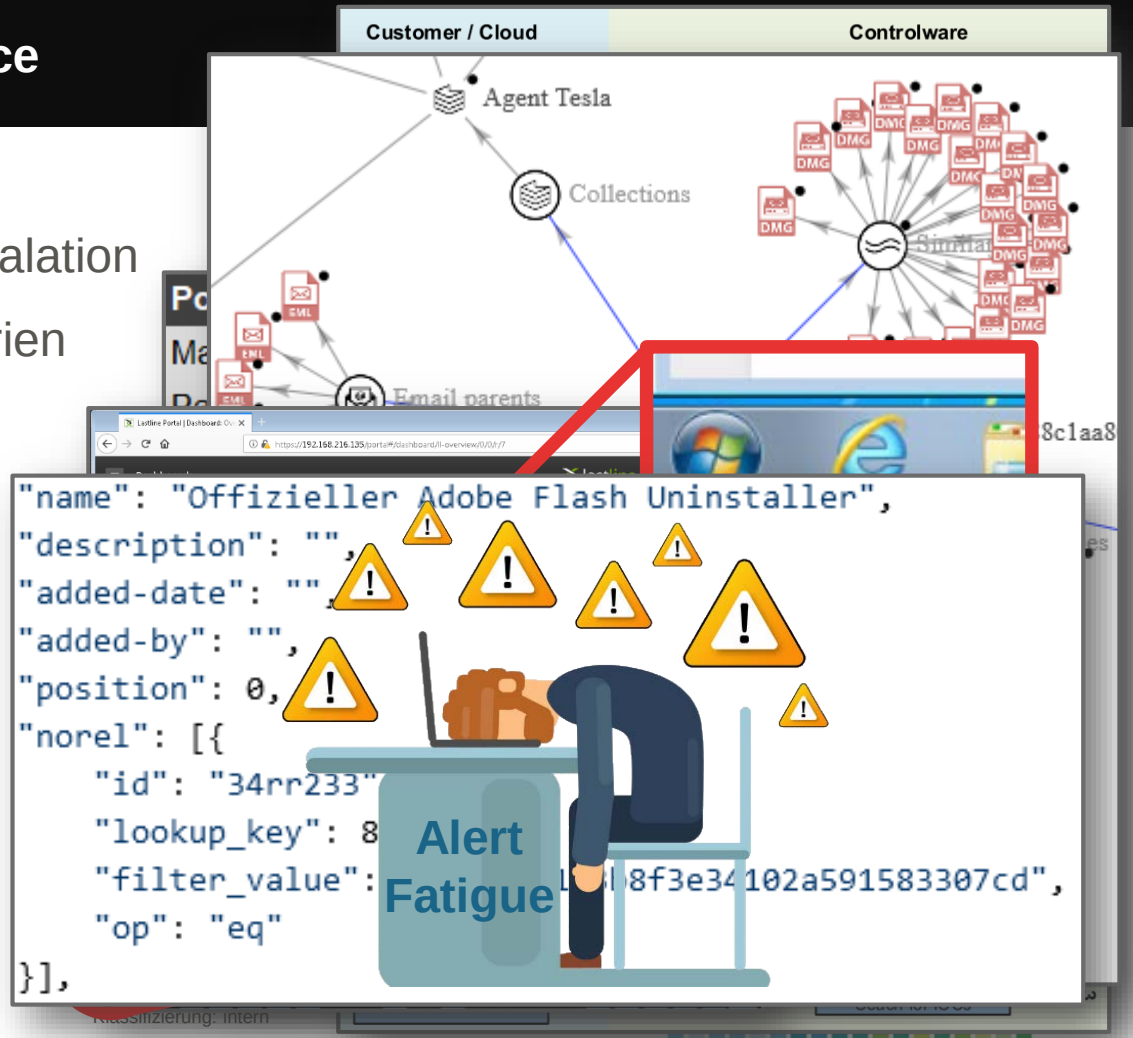
Name	explorer.exe
Storyline ID	C100F87F8ECCEEAC
Command Line	C:\Windows\Explorer.EXE
Start Time	Jul 29, 2022 07:25:11
Image Path	C:\Windows\explorer.exe
Unique ID	4796BA753C3A5D85
Image SHA1	45f9ee92250ee92a26172a4f1a546caec7da1bb1

SOURCE PROCESS DETAILS

Name	hh.exe
Storyline ID	B88C726839BF9DEB
Command Line	"C:\Windows\hh.exe" C:\Users\Elvis\Downloads\...
User	DESKTOP-5G9FACF\Elvis
Start Time	Sep 1, 2022 13:24:02
Image Path	C:\Windows\hh.exe
PID	4612

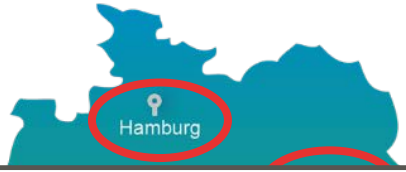
Zutaten für verlässlichen Service

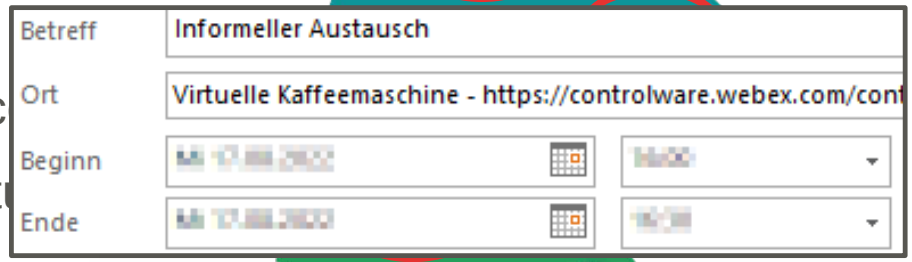
- Prozesse für Service und Eskalation
- Playbooks für Angriffs-Szenarien
- Pläne für Notfälle
- Threat Intelligence
- Sichere Testumgebung
- Wissensmanagement
- ... und erfahrene Analysten!

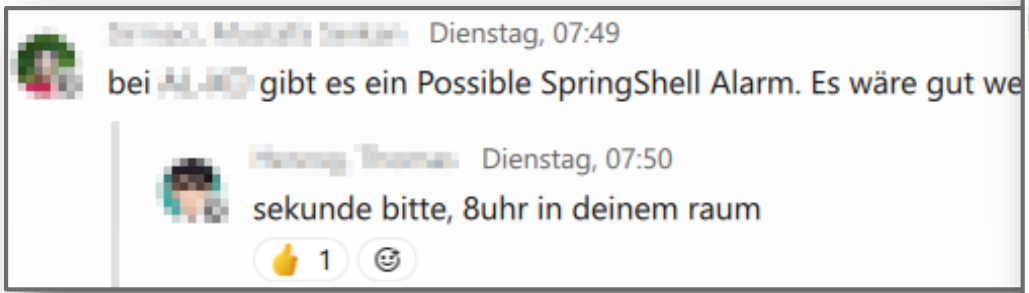


Und sonst so?

- Regelmäßige Service Meetings mit Kunden
- Nachschärfen Filter / Exclusions
- Weiterentwicklung Plattform und Servic
- Verbesserung Malware Analyse & Test
- Übungen – z.B. Live-Reaktion

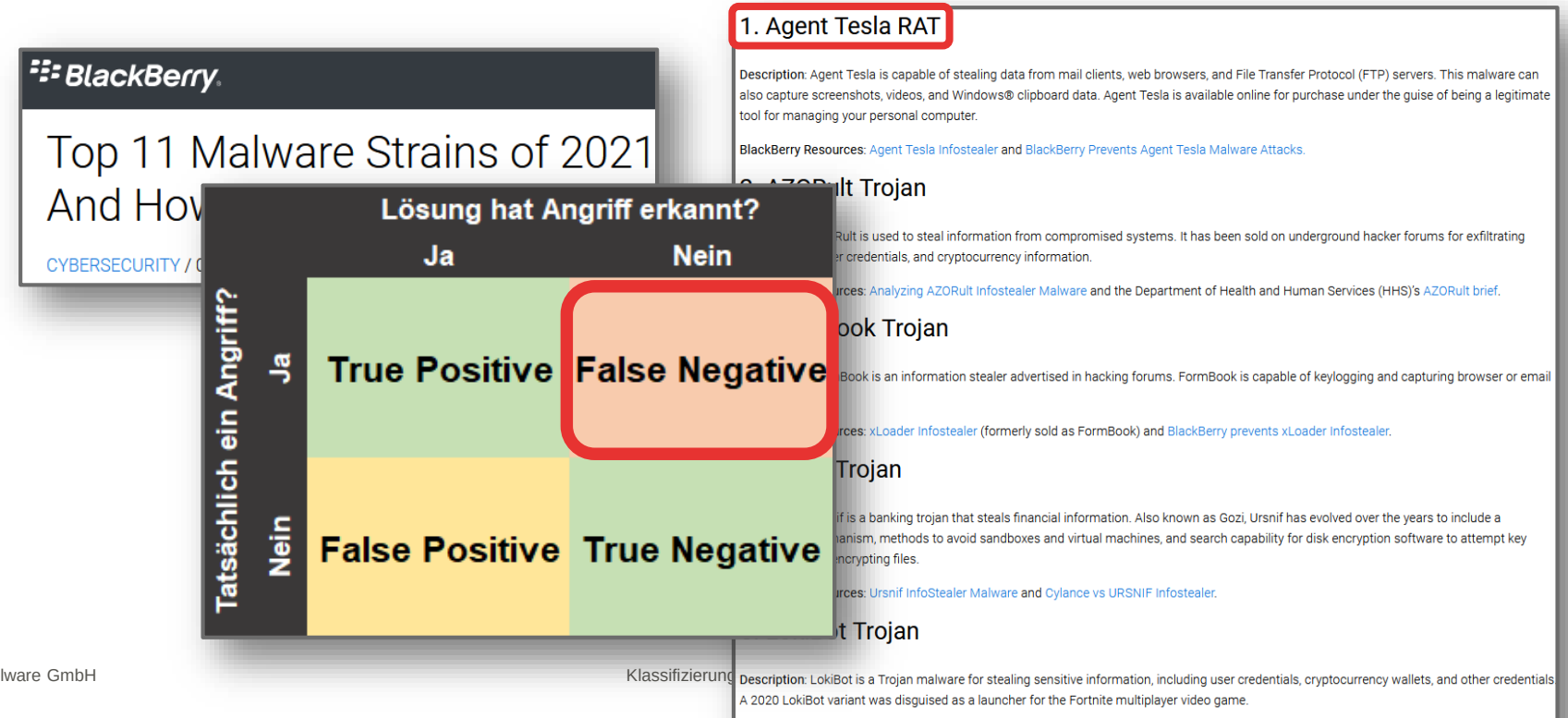






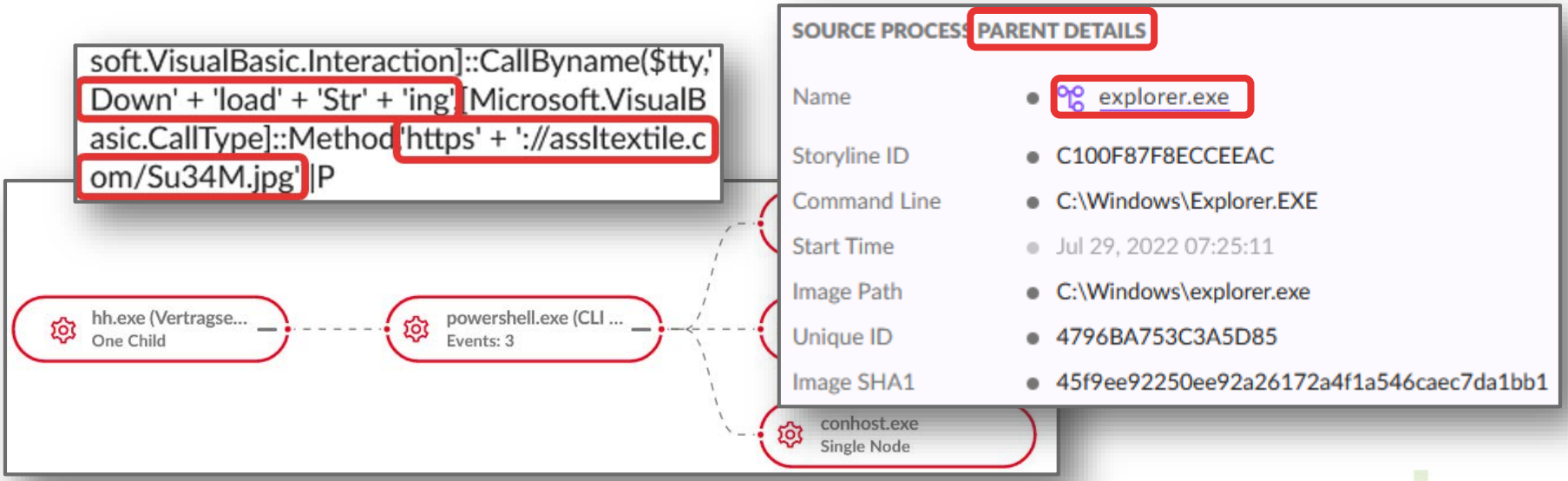
Anfragen übersetzen

- Agent Tesla begegnet uns aktuell oft



Anfragen übersetzen

- Agent Tesla begegnet uns aktuell oft
- Verhalten aus eigener Analyse und Threat Reports bekannt



Anfragen übersetzen

```
config case_sensitive = false |
preset = network_story |
filter agent_os_type = ENUM.AGENT_OS_WINDOWS and
causality_actor_process_image_name contains "hh.exe" and actor_process_image_name contains "powershell"
and action_remote_ip !~= "^10\.|^(172\.1[6-9]|172\.2\d|172.3[0-1]{1})|^(192.168.)|^127."
```

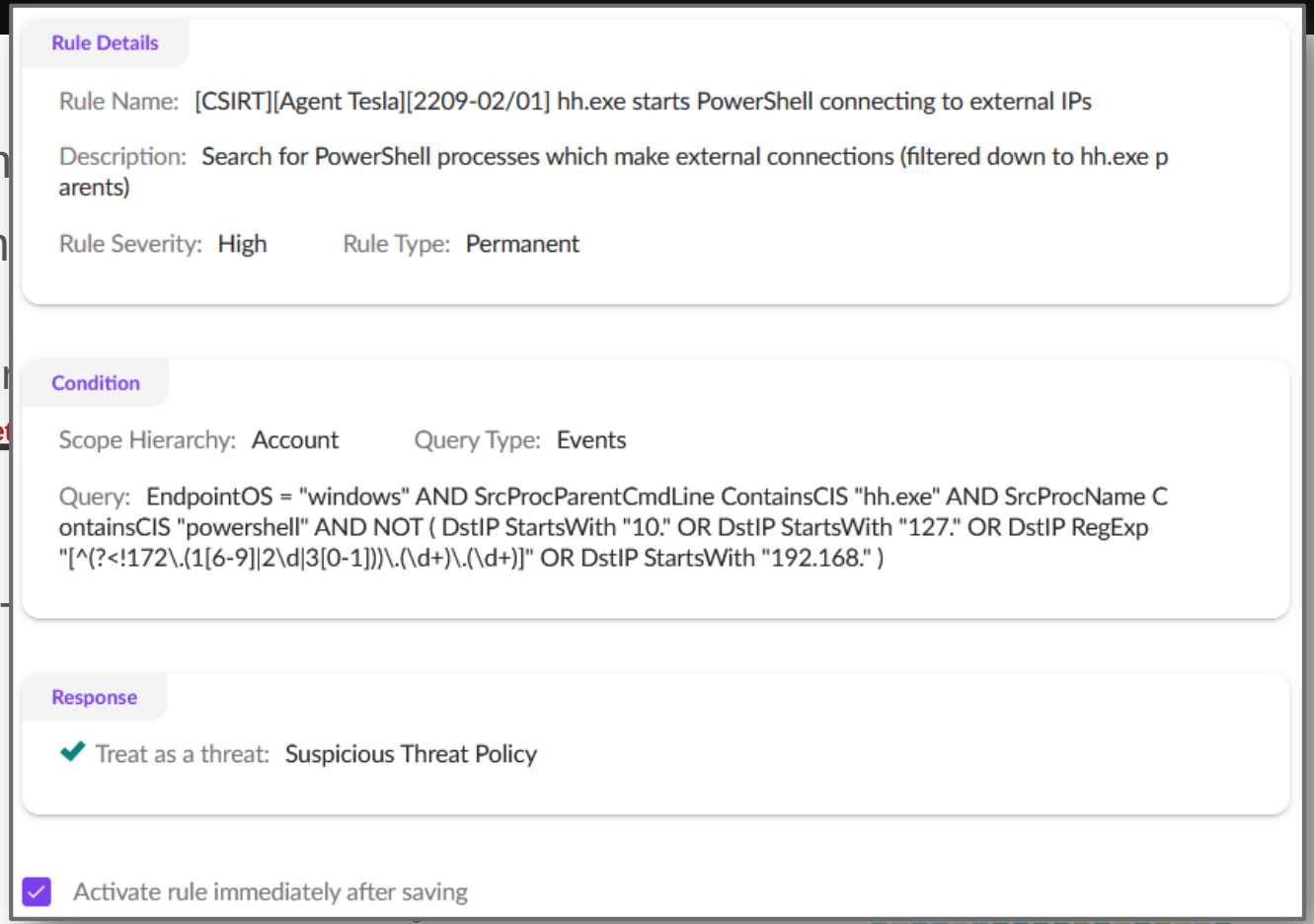
- powershell

```
DeviceProcessEvents
| where InitiatingProcessFileName has "hh.exe"
| where FileName has "powershell.exe"
| join (DeviceNetworkEvents
      | where ipv4_is_private(RemoteIP) == false and not( RemoteIP startswith "127" ))
 on $left.FileName == $right.InitiatingProcessFileName
```

```
EndpointOS = "wi
SrcProcParentCmd
SrcProcName Contains("powershell") AND NOT
  (DstIP StartsWith "10." OR DstIP StartsWith "127." OR
   DstIP RegExp "[^(?<!172\.(1[6-9]|2\d|3[0-1]))\.(\d+)\.(\d+)]" OR DstIP StartsWith "192.168." )
```

Anfragen übersetzen

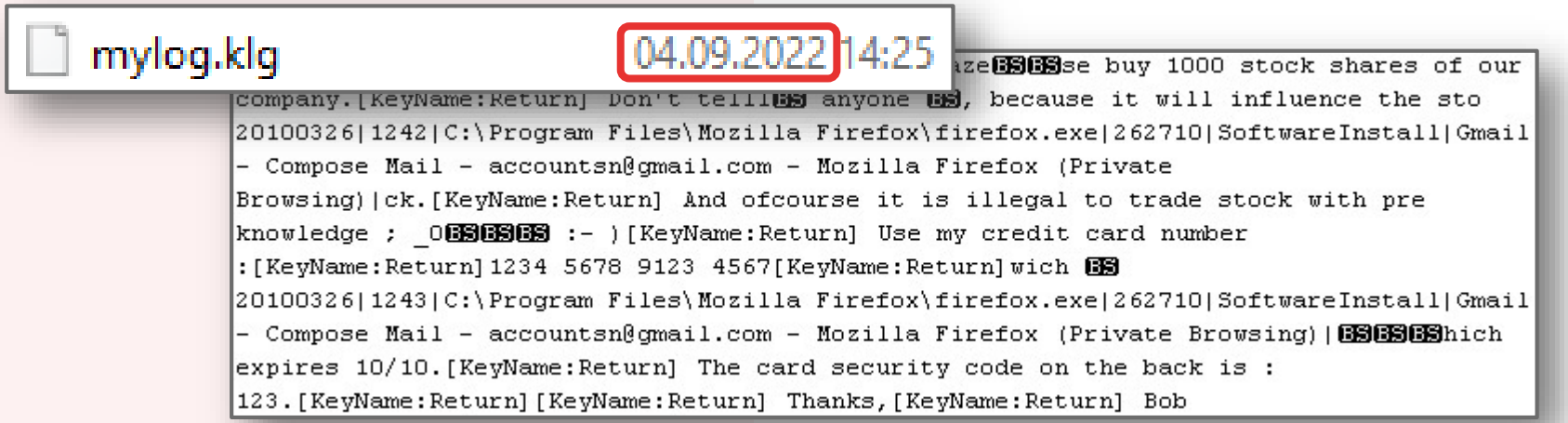
- Agent Tesla begegn
- Verhalten aus eigen
  - explorer.exe startet
  - hh.exe startet power
  - powershell.exe startet
- Übersetzen, testen,
- Feste Alarmierungs-



Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie ≠ Realität
  Dateien ohne Zugriff gibt es nicht



Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie ≠ Realität
  Dateien ohne Zugriff gibt es nicht

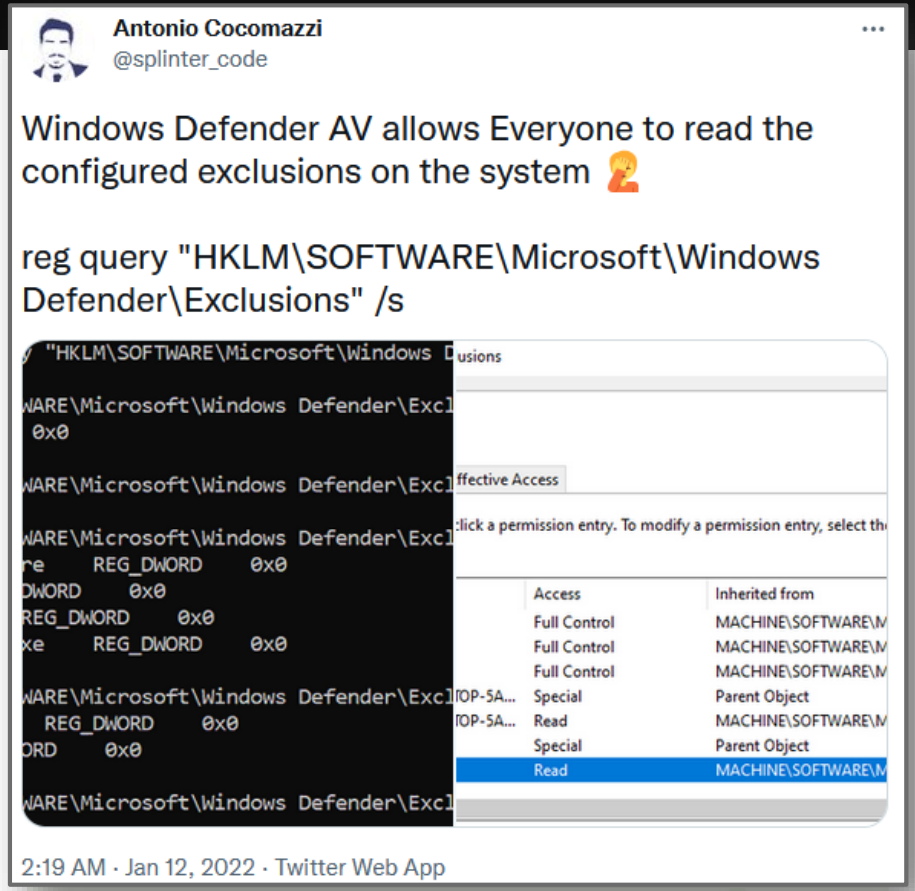
Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall

Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie ≠ Realität
  Dateien ohne Zugriff gibt es nicht
- Schwachstellen
  - Deaktivieren des Agenten
  - Manipulation der Freigabe-Liste



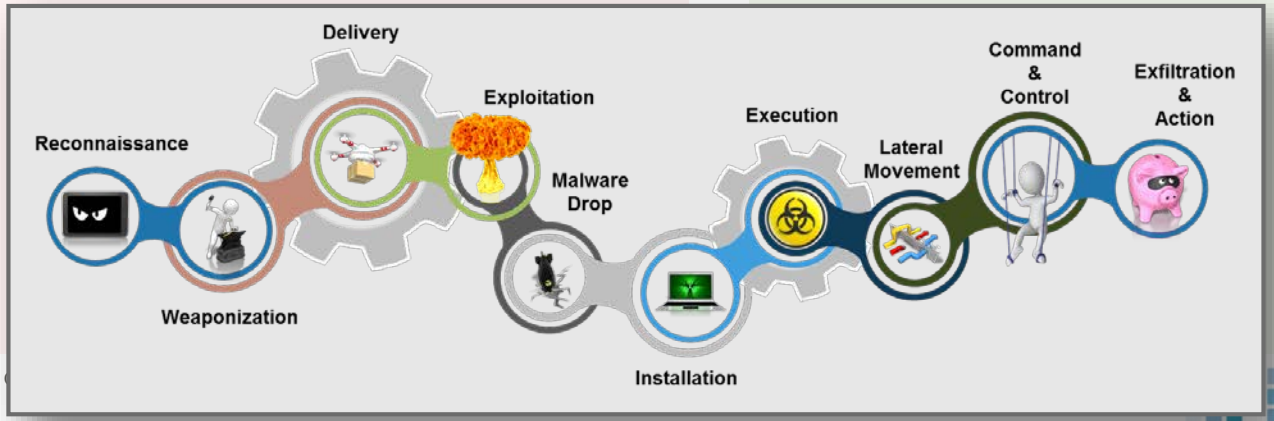
Anfragen übersetzen (II)

Tücken im Detail

- Telemetrie ≠ Realität
  Dateien ohne Zugriff gibt es nicht
- Schwachstellen
  - Deaktivieren des Agenten
  - Manipulation der Freigabe-Liste

Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall
- Kontrolle der Agenten
- Abdecken des gasamten Angriffs (*Cyber Kill Chain*)

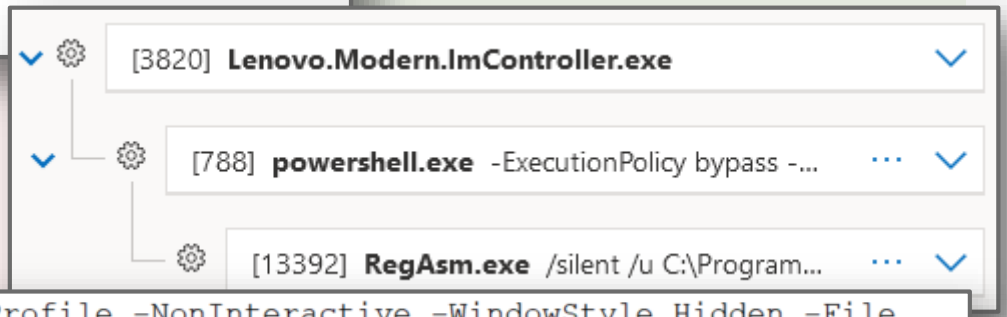


Anfragen übersetzen (II)

```
DeviceProcessEvents
| where InitiatingProcessFileName has "powershell.exe"
| where FileName has "regasm.exe"
```

Dateien ohne Zugriff gibt es nicht

- Schwachstellen
  - Deaktivieren des Agenten




```
powershell.exe -ExecutionPolicy bypass -NoProfile -NonInteractive -WindowStyle Hidden -File
  C:\ProgramData\Lenovo\iMController\Plugins\LenovoBatteryGaugePackage\x64\UnInstall.PS1

"RegAsm.exe" /silent /u
  C:\ProgramData\Lenovo\ImController\Plugins\LenovoBatteryGaugePackage\x64\PluginsContract.dll
```

- Threat Hunt *(False Positives)*
- Passende Arbeitsabläufe

```
DeviceProcessEvents
| where InitiatingProcessFileName has "powershell.exe"
| where FileName has "regasm.exe"
| where not (InitiatingProcessParentFileName has "Lenovo.Modern.ImController.exe")
```

Anfragen übersetzen (II)

Tücken im Detail

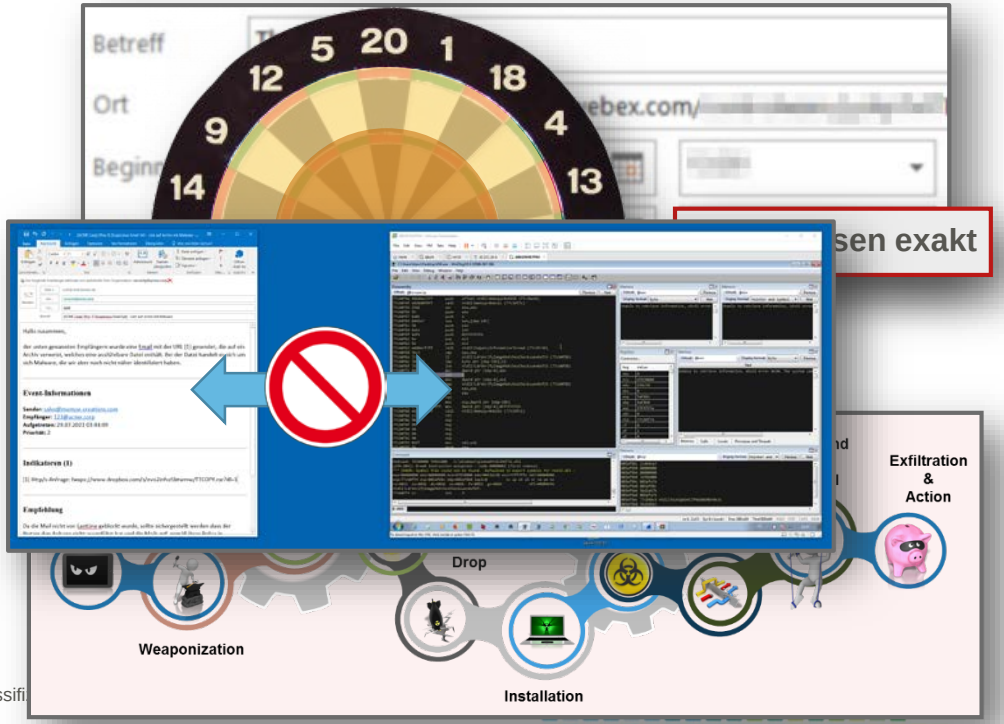
- Telemetrie ≠ Realität
  Dateien ohne Zugriff gibt es nicht
- Schwachstellen
  - Deaktivieren des Agenten
  - Manipulation der Freigabe-Liste
- EDR findet viel bei Scans
- Viele falsche Treffer bei der Threat Hunt (*False Positives*)

Abhilfe

- Queries vorsichtig aufbauen
- Full Scans im Verdachtsfall
- Kontrolle der Agenten
- Abdecken des gasamten Angriffs (*Cyber Kill Chain*)
- Wissensmanagement (Freigaben)
- Passende Arbeitsabläufe
- Gute Analysten mit viel Geduld

Voraussetzungen für Threat Hunting

- Statt zu reagieren sucht das SOC aktiv nach Angriffen
- Feste Abläufe
  - Threats auswählen
  - Wechselnde Teams bearbeiten Hunts
- Gute aufgebaute Queries
  - Robuste Anfragen
  - Hochwertige IOCs
  - Vollständige Abdeckung des Angriffs
- Ausführliche Tests



Zum Mitnehmen

- EDR/XDR ist aus gutem Grund aktuell sehr beliebt
  - Weniger Abhängigkeit von Signaturen
  - Sichtbarkeit: Man muss nicht alles glauben, sondern schaut nach
  - Reaktion: Angreifer effektiv stoppen können
- Auch EDR/XDR ist keine Wunderwaffe
  - Es muss zeitnah auf Alarme reagiert werden
  - Informationen sind manchmal unvollständig
  - Aktive Reaktion auf Angriffe muss man testen und üben
- Hinter einem verlässlichen SOC Service steckt eine Menge Arbeit
  - Automatisierung & Filter, Wissensmanagement, Training, ...
  - Viele weitere Teams im Controlware Service Center sind beteiligt

controlware

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!
Dankon pro via antento!