Herausforderung Cyberversicherung – wie optimiere ich meine Security dafür?

Fabian Becker
Sales Engineer

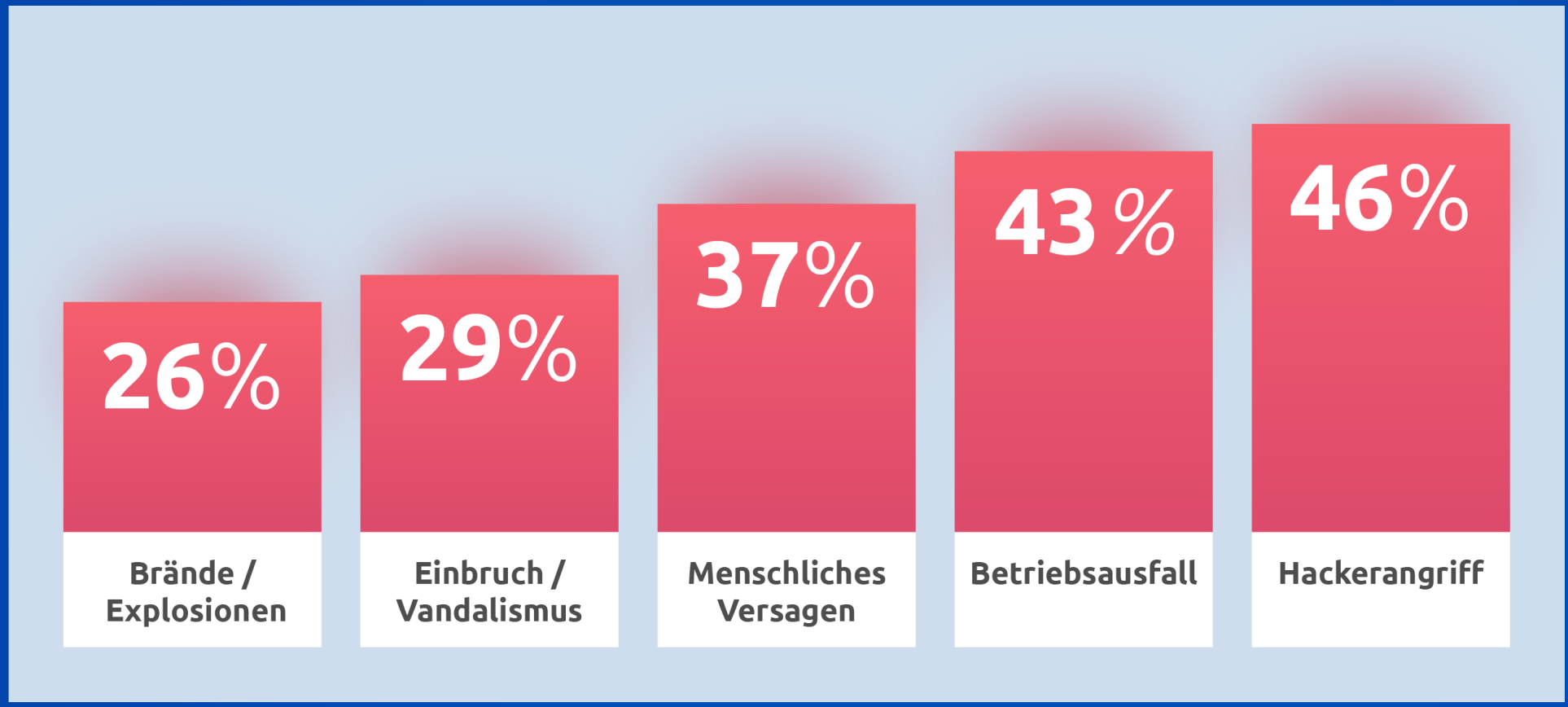
30.08.2022

SOPHOS

Cyberversicherung – wer, wie, was, warum?

SOPHOS

Die größten Risiken für Unternehmen



Auswertung einer Befragung von 1.005 Personen, die in ihrem Unternehmen für das Thema Versicherungen verantwortlich sind (Mehrfachnennung möglich).
Quelle: Gothaer KMU Studie 2021a

Quelle: https://www.fuer-gruender.de/wissen/unternehmen-gruenden/versicherung/cyber-versicherung

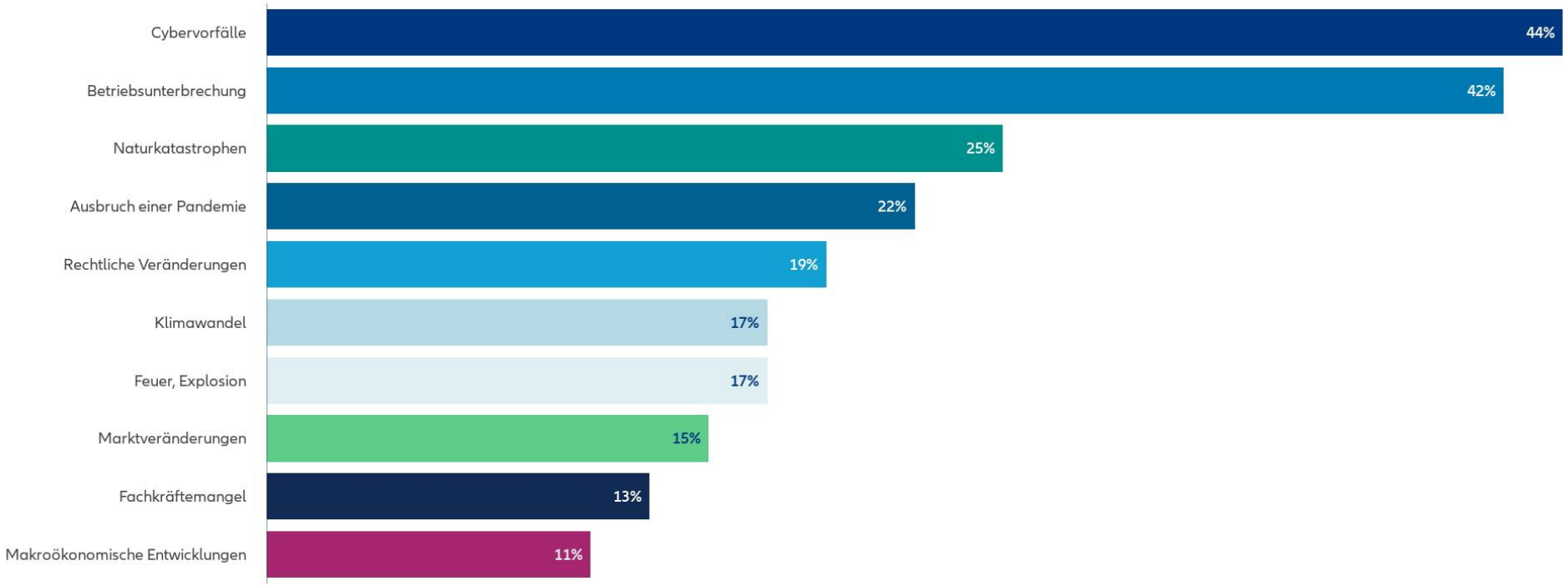
Ransomware und Datendiebstahl vs. Betriebsunterbrechnung

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

SOPHOS

SOPHOS State of Ransomware 2022

5.600
IT-Entscheider

31
Länder

100 - 5.000
Mitarbeiter im Unternehmen

66 %
wurden Opfer eines Ransomware-Angriffs

65 %
der Angriffe führten zur Datenverschlüsselung

72 %
verzeichneten eine Zunahme bei der Zahl/ Komplexität/Schwere der Angriffe

46 %
zahlten das Lösegeld

4 %
derer, die das Lösegeld zahlten, erhielten ALLE Daten zurück

90 %
wurden durch den Angriff in ihrer Betriebsfähigkeit beeinträchtigt

86 %
verzeichneten Geschäftseinbußen/ Umsatzverluste

1,4 Mio. $
durchschnittliche Kosten für die Behebung der Angriffs-Folgen

1 Monat
durchschnittlich benötigte Zeit bis zur kompletten Wiederherstellung nach einem Angriff

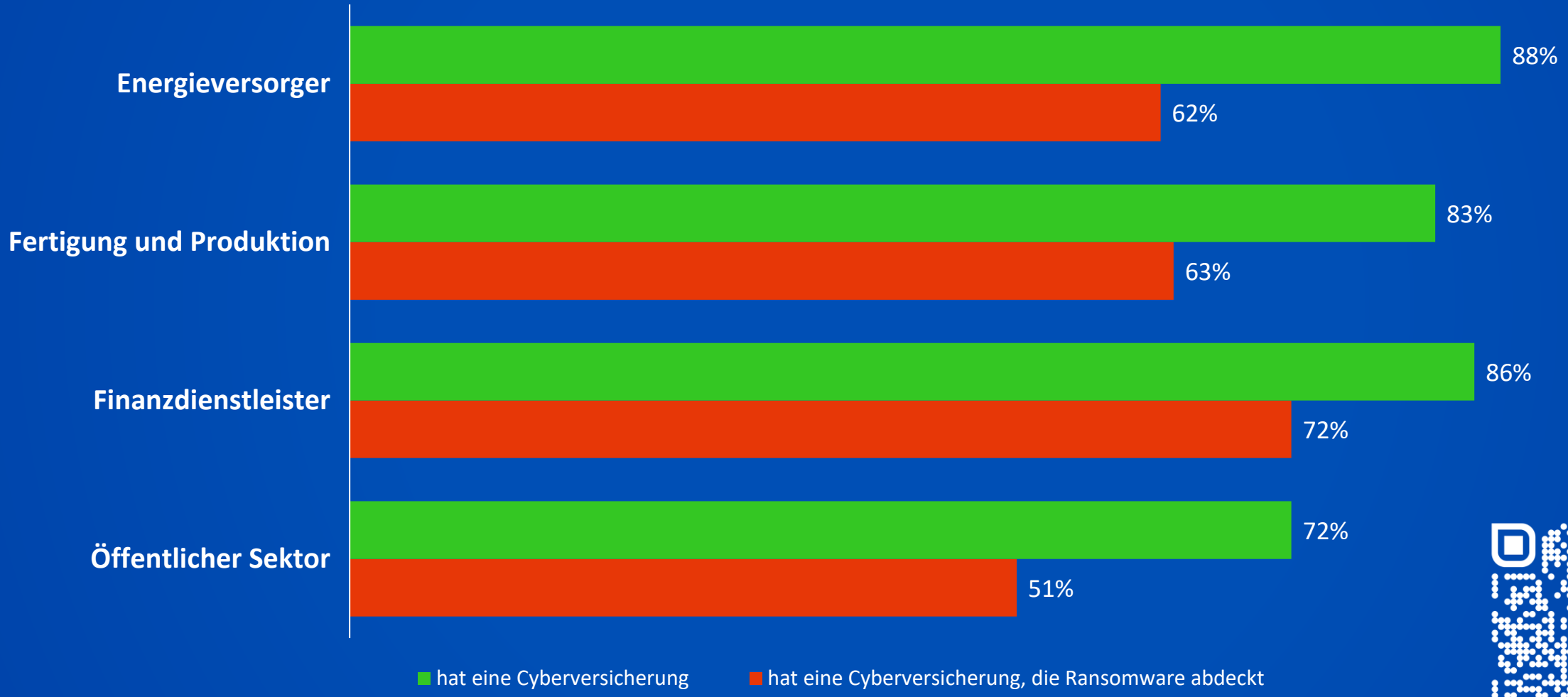
72 %
verlassen sich auf Methoden, die einen Angriff nicht verhindern

Quelle: https://www.sophos.com/de-de/whitepaper/state-of-ransomware

Die Vorteile einer Cyberversicherung

- Finanzieller Schutz
  - Der Versicherer trägt aus Cybersecurity-Vorfällen entstehende Vermögensschäden
- Operative Unterstützung
  - Bei Vorfällen leisten externe Experten (IT-Forensik-Analysten, Anwälte für Datenschutzrecht und PR-Experten) Ihrem Unternehmen Soforthilfe
- Krisenvorsorge
  - Eine Cyber-Versicherung bestärkt das Vertrauen Ihrer Kunden, Partner, Zulieferer und Mitarbeiter in Ihr Unternehmen, da Sie auf Cybersecurity-Vorfälle vorbereitet und abgesichert sind

Cyberversicherungen im Branchenvergleich



Quelle: https://www.sophos.com/de-de/whitepaper/sophos-guide-to-cyber-insurance

Voraussetzungen für eine Cyberversicherung (Stand der Technik)

Voraussetzungen für eine Cyberversicherung

Alt:

- **Aktuelle Antivirus** Software für alle PCs
- Unternehmensnetzwerk muss mit einer **Firewall** abgesichert sein
- Regelmäßige offline bzw. Cloud **Backups**
- Sicheres **Zugriffs-** und **Berechtigungskonzept**

Neu:

- **EDR/XDR** System
- **MFA** (Multifaktor-Authentifizierung)

Stand der Technik + BSI Orientierungshilfe

- **Multifaktor-Authentifizierung**
- Verschlüsselung von Festplatten
- Verschlüsselung von E-Mails
- Einsatz von VPN
- Management mobiler Geräte
- Routersicherheit
- Netzwerküberwachung mittels IDS/IPS
- Schutz des Web-Datenverkehrs
- Schutz von Webanwendungen
- Serverhärtung
- **Endpoint Detection & Response Plattform**
- Sandboxing zur Schadcode-Analyse
- Cyber Threat Intelligence

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

Technische und organisatorische Maßnahmen

BSI veröffentlicht Community Draft der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Datum 13.06.2022

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Entwurf einer neuen Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (SzA) veröffentlicht. Der Community Draft liefert Anhaltspunkte für die Anforderungen an Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieanlagen und sorgungsnetzen und prüfende Stellen.

Bundesamt
für Sicherheit in der
Informationstechnik

Fazit:

Eine gute Cybersecurity im Unternehmen…

- …erleichtert den Abschluss von Cyber-Versicherungen
- …kann Prämien reduzieren
- …verringert die Wahrscheinlichkeit von Schadenfällen und somit höheren Beiträgen in der Zukunft
- …reduziert das Risiko, dass die Versicherung nicht zahlt
- …minimiert Schäden und Kosten durch Vorfälle

Herausforderung Cyberversicherung –

wie optimiere ich meine Security dafür?

SOPHOS

AV? EDR? XDR? MDR? SoC?

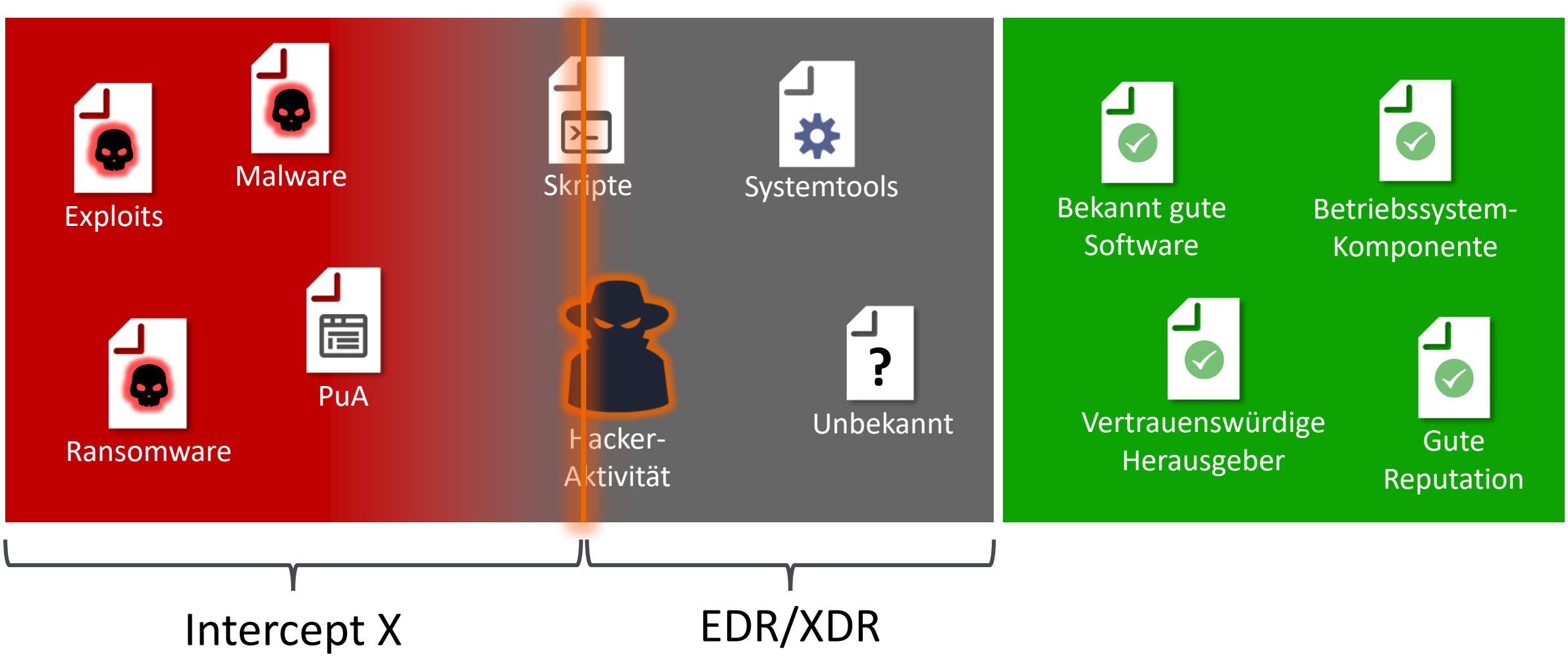
Anti-Virus macht schon alles?

Sophos Realität

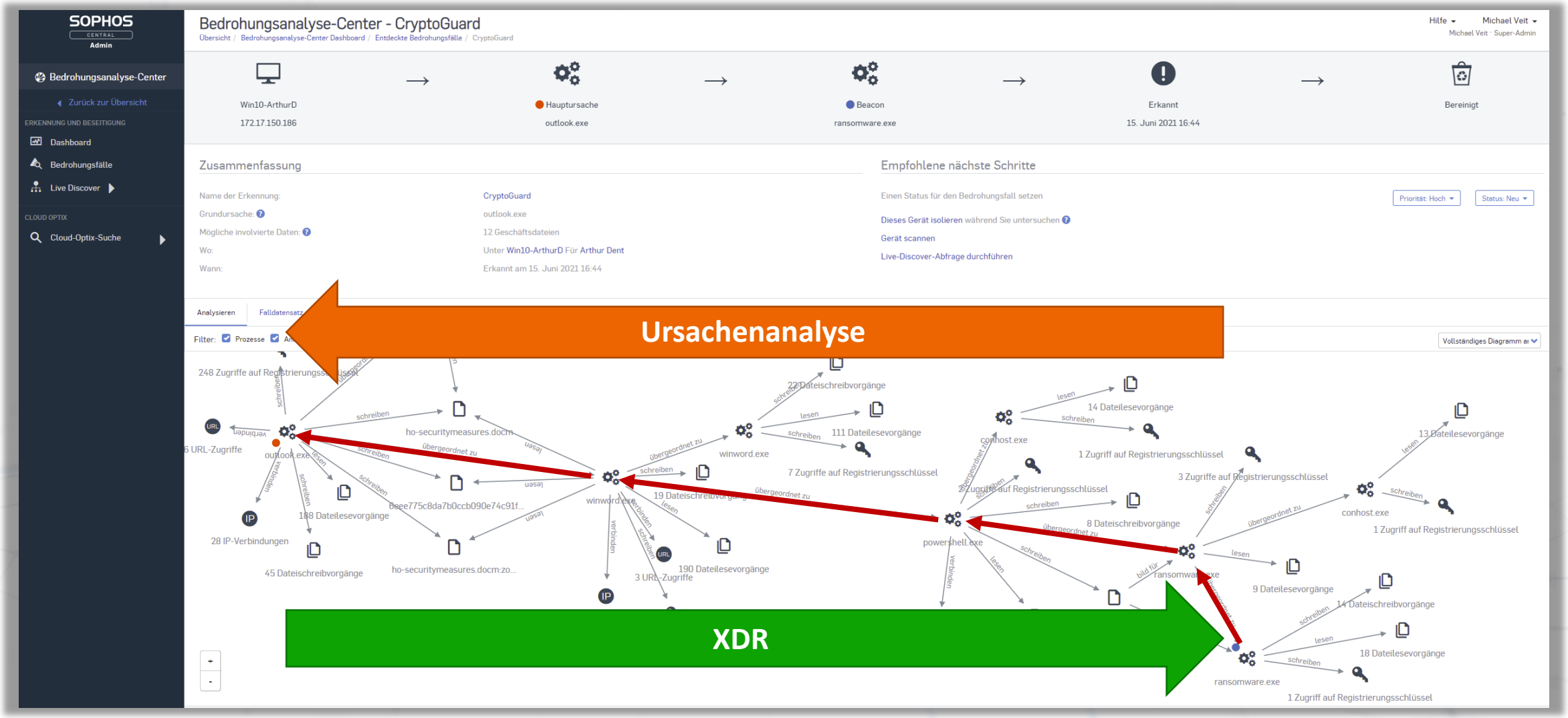
Wo setzt man die Grenze? -> Erkennung vs. False Positives!

Sophos Realität

Wo setzt man die Grenze? -> Erkennung vs. False Positives!



Ursachenanalyse vs. XDR



Was ist Endpoint Detection and Response?

Endpoint Detection and Response

Auf allen Unternehmens PCs..

…Ereignisse erfassen, analysieren und korrelieren und im Angriffsfall…

…per Remote-Zugriff gezielte Maßnahmen ergreifen.

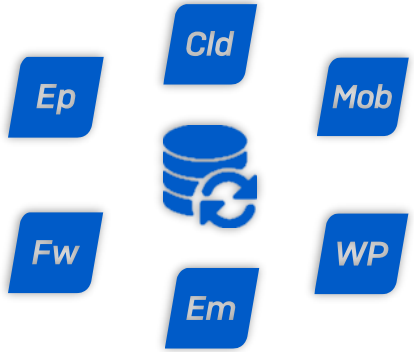
Unterschied EDR vs. XDR

EDR: Endpoint Detection and Response

Sammelt nur Daten und Ereignisse der **Endpoints**

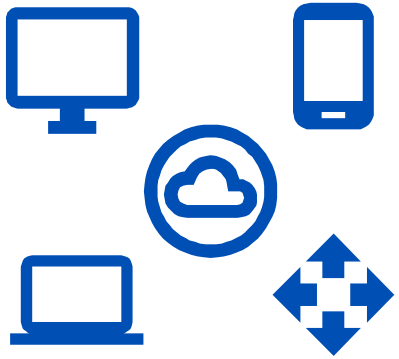
XDR: **Extended** Detection and Response

Sammelt Daten und Ereignisse aller **Endpoints, Cloud Umgebungen, mobiler Geräte, Firewalls, E-Mail Ereignisse, Server, Container, Drittanbieter, etc…**



Was ist Sophos XDR?

eXtended Detection and Response



Auf allen Unternehmensgeräten bis zu 90 Tage …

…Ereignisse erfassen, analysieren und korrelieren und im Angriffsfall…

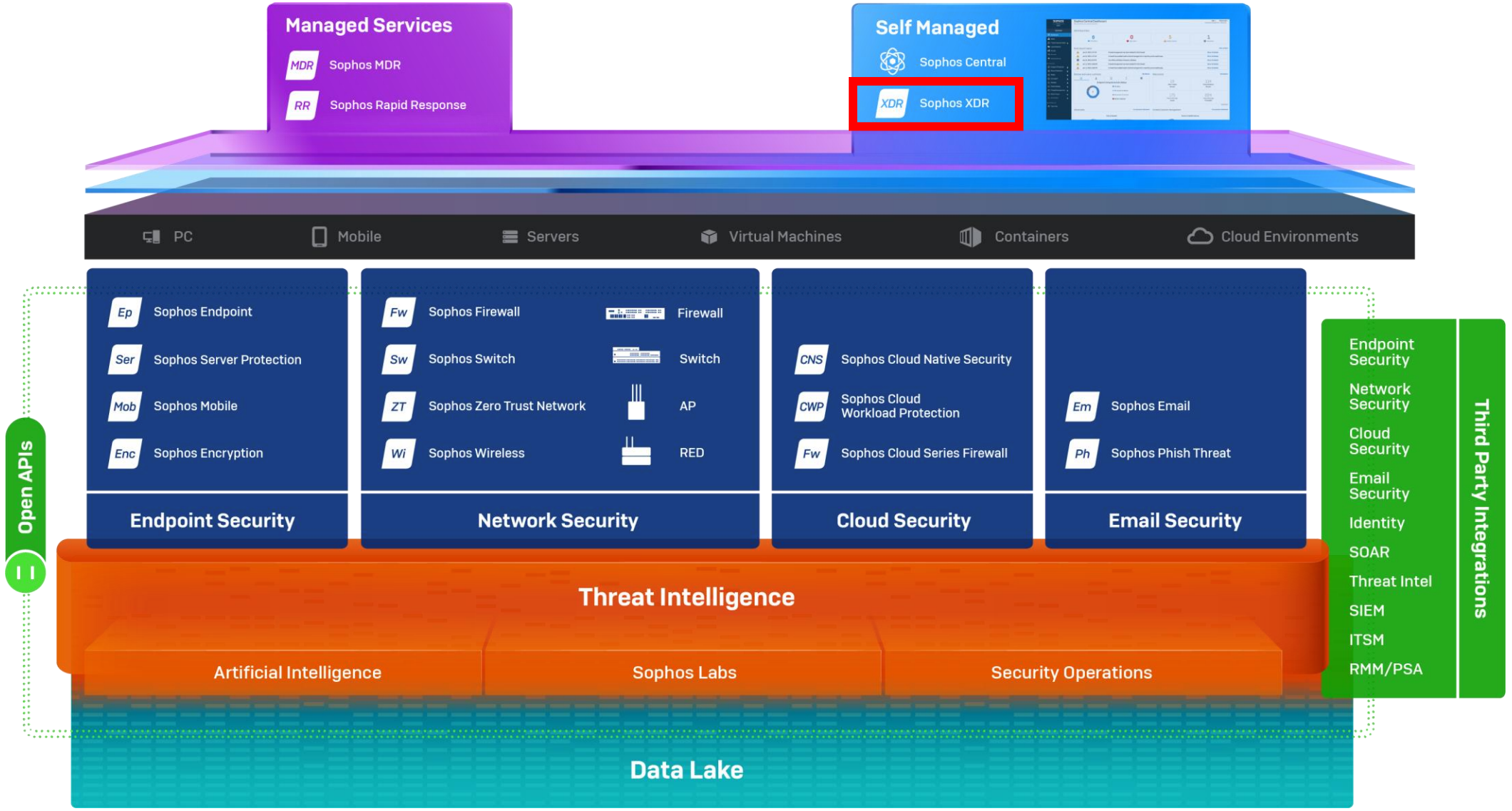
…per Remote-Zugriff gezielte Maßnahmen ergreifen.

Warum brauche ich XDR?

- Technologie mit der man grundlegende Aussagen zu folgenden Fragen treffen kann
  - Bin ich gerade mitten in einem Cyberangriff?
  - Hatte ich einen Datenabfluss?
  - Muss ich einen Complianceverstoß melden?
  - Wie ist der Zustand meiner IT?

Sophos XDR

Sophos ACE

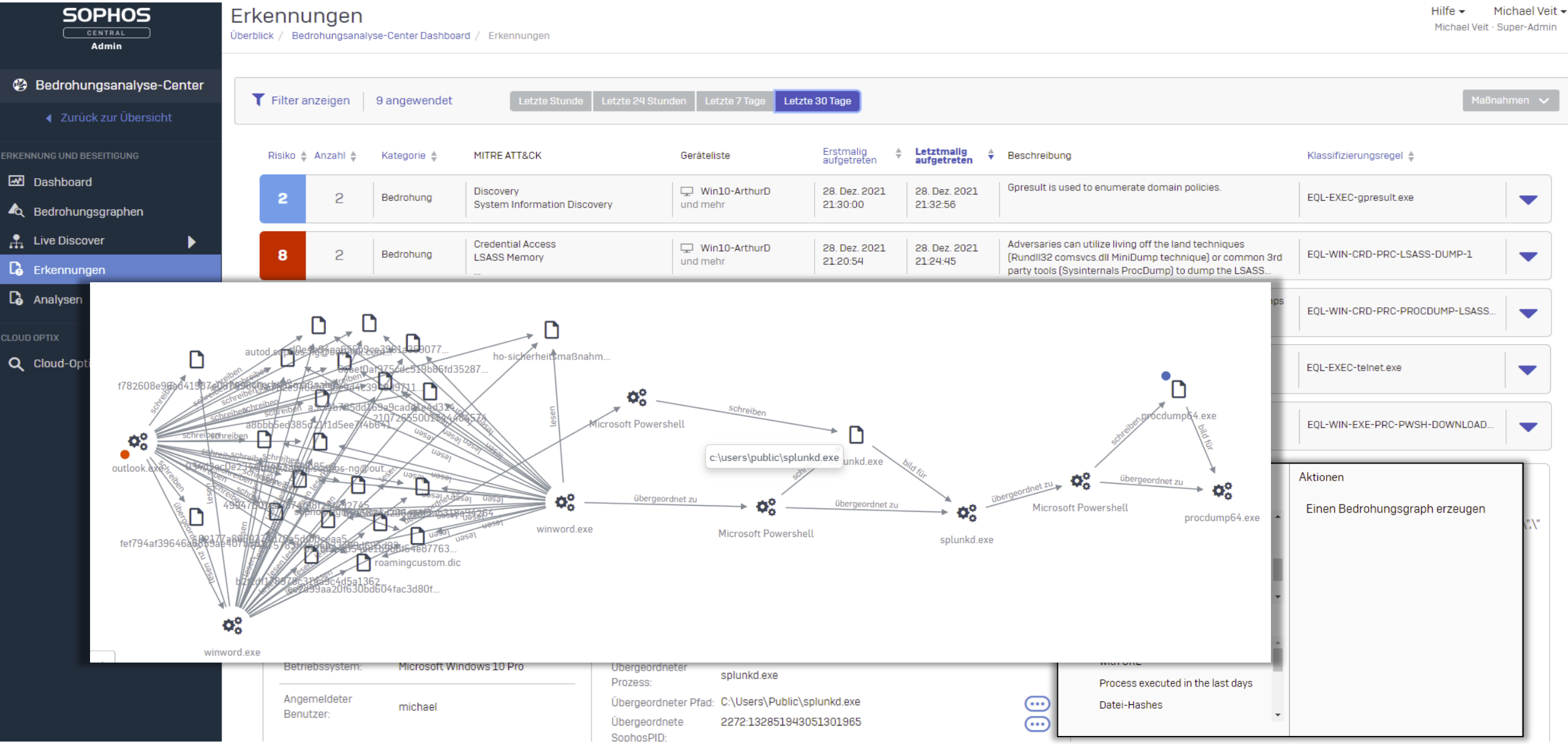


SOPHOS

Sophos XDR in der Praxis

SOPHOS

XDR Erkennungen: KI sortiert verdächtige Ereignisse vor



Threat Analysis Center - Live Discover

Designer Mode
Lets you create or edit queries

Query : Select One - 0 Categories, 0 Queries

All Queries | Endpoint Queries | Data Lake Queries

Queries that get data from devices or from the Data Lake

Endpoint queries get data from devices that are currently connected. Data Lake queries get data from the Data Lake that your devices upload their data to.

Search

Run Query

Sophos XDR in der Praxis

SOPHOS

SOPHOS

Sophos Central

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports
- People
- Devices
- Global Settings
- Third-party Connectors
- Protect Devices
- Account Health Check

MY PRODUCTS

- Endpoint Protection
- Server Protection
- Mobile
- Encryption
- Wireless
- Email Security
- Firewall Management
- Phish Threat
- Cloud Native Security
- ZTNA
- Switches

Sophos Central Dashboard

See a snapshot of your security protection

18	9	2	7
Total Alerts	High Alerts	Medium Alerts	Low Alerts

Most Recent Alerts

View all Alerts

	Jul 30, 2022 9:55 AM	Firewall has not checked in with Sophos Central for the past 1209 minu...			Show full details
	Jul 29, 2022 1:59 PM	Firewall has not checked in with Sophos Central for the past 5 minutes			Show full details
	Jul 29, 2022 10:18 AM	Manual PUA cleanup required: 'Generic ML PUA' at 'C:\Users\sophos\A...	ztnauser	win10	Show full details
	Jul 29, 2022 9:56 AM	Firewall connection to Sophos Central has been restored			Show full details
	Jul 29, 2022 9:14 AM	Firewall connection to Sophos Central has been restored			Show full details

Devices and users: summary

See Report

Endpoint Computer Activity Status

- 1 Active
- 1 Inactive 2+ Weeks
- 0 Inactive 2+ Months
- 0 Not Protected

Web control

See Reports

0	0
Web Threats Blocked	Policy Violations Blocked
1	1

Was benötige ich, um XDR effektiv zu nutzen?

Effektive Werkzeuge für Erkennung, Analyse und Reaktion -> Intercept X with XDR

Geschultes Personal: Analysten, Threat Hunter, Forensiker, Incident/Responder
im 24/7 Betrieb mit unverzüglicher Reaktion -> eigenes SOC

Aktuelle Informationen über Bedrohungen -> externe Threat Feeds

Noch effektiver wird XDR mit weiteren Sensoren im Netzwerk, in der Cloud, in Email etc.

Wer bedient mein XDR?

- XDR ist ein reiner Cybersecurity „Werkzeugkasten“
- XDR muss aktiv und kontinuierlich (!) bedient werden
- Bei fehlendem Personal / Expertise: ~~XDR~~ -> MDR

Sophos Managed Detection and Response

Sophos MDR - 24/7 Erkennung und Reaktion auf Vorfälle

Superior outcomes

(less risk, greater efficiency, lower costs)

SOPHOS

Sophos MDR in der Praxis

Erkennungen

Bedrohungsanalyse-Center
Zurück zur Übersicht

ERKENNUNG UND BESEITIGUNG
Dashboard
Bedrohungsgraphen
Live Discover
Erkennungen
Analysen
Einstellungen

Filter anzeigen | 5 angewendet | Letzte Stunde | Letzte 24 Stunden | Letzte 7 Tage | Letzte 30 Tage | Aktionen

Diese Erkennungen dienen Ihnen als MTR-Kunde nur zur Informationen für alle Geräte mit MTR-Lizenz. Unserer MTR-Team wird Sie kontaktieren, falls Sie Maßnahmen ergreifen müssen.

Risiko	Anzahl	Kategorie	MITRE ATT&CK	Geräteliste	Erstmalig aufgetreten	Letztmalig aufgetreten	Beschreibung	Klassifizierungsregel	Analysen
10	2	Classifier	Impact Data Encrypted for Impact	Win10-1	7. März 2022 01:31:59	7. März 2022 15:31:34	The adversary is trying to manipulate, interrupt, or destroy your systems and...	WIN-MITRE-Behavioral-TA0040-T1486	2022-03-07-0... und mehr
8	2	Classifier	Defense Evasion Process Hollowing	Win10-1	7. März 2022 01:31:59	7. März 2022 15:26:25	The adversary is trying to avoid being detected. Defense Evasion consists...	WIN-MITRE-Behavioral-TA0005-T105...	2022-03-07-0... und mehr
8	3	Bedrohung	Defense Evasion Mshta	Win10-1 und mehr	7. März 2022 01:11:05	7. März 2022 15:24:11	This detection looks for MSHTA connecting to a URL. This is a living off the...	EQL-WIN-EVA-PRC-MSHTA-HTTP	2022-03-07-0... und mehr
7	1	Bedrohung	Execution Windows Management Instrumentation ...	Win10-4	-	7. März 2022 01:40:38	Ransomware has leveraged Windows Management...	EQL-WIN-IMP-PRC-SHADOWCOPY-SE...	2022-03-07-0...
7	1	Bedrohung	Impact Inhibit System Recovery	Win10-4	-	7. März 2022 01:40:38	Adversaries may delete or remove built-in operating system data and turn off...	EQL-WIN-IMP-PRC-VSSADMIN-DELET...	2022-03-07-0...
8	2	Bedrohung	Discovery Domain Trust Discovery	Win10-4	7. März 2022 01:40:20	7. März 2022 01:40:20	The legitimate tool ADFind has been observed being used by ransomware cre...	EQL-WIN-DIS-PRC-ADFIND-1	2022-03-07-0...
6	1	Bedrohung	Defense Evasion Windows File and Directory Permissions M	Win10-4	-	7. März 2022 01:40:20	Identifies the use of `icacls.exe` to grant full access to everyone on a...	EQL-WIN-EVA-PRC-ICACLS-GRANT-E...	2022-03-07-0...
8	1	Bedrohung	Defense Evasion Regsvr32	Win10-4	-	7. März 2022 01:14:06	Uses regsvr32 to load unauthorized script objects.	EQL-WIN-EVA-PRC-REGSVR32-SCRO...	2022-03-07-0...
6	1	Bedrohung	Command and Control Ingress Tool Transfer ...	Win10-4	-	7. März 2022 01:10:57	HTML Help is a built in Windows executable that can be used to download...	EQL-WIN-EVA-PRC-HTML-HELP-1	2022-03-07-0...
6	1	Bedrohung	Defense Evasion InstallUtil	Win10-4	-	7. März 2022 01:10:57	Code can be executed through InstallUtil which can be used to bypass...	EQL-WIN-EVA-PRC-INSTALLUTIL-PRO...	2022-03-07-0...

Zuletzt aktualisiert: 11.03.2022, 15:03

Fälle

Aktualisieren Letzte 7 Tage

Gesamtzahl der Fälle	Aktive Fälle	Behobene Fälle	Aktion erforderlich
3	2	1	2
Von 0 in Vorperiode	Von 0 in Vorperiode	Von 0 in Vorperiode	Von 0 in Vorperiode

Fälle durchsuchen

Kennung	Status	Fallerstellung	Schweregrad	Beschreibung	Zusammenfassung
106087	Aktion erforderlich	Feb. 5, 2022 at 12:10 PM	Wert 2	Threat Hunt - Proxyshell	Sophos MTR team conducted a Proxyshell threat hunt on the estate. We have observed the creation of web shells on EC2AMAZ . We noticed the Exchange server host is not patched against the Proxyshell vulnerability and is vulnerable to exploitation. SAV has removed the malicious web shells but due to persistence still remaining on the host (in the form of config file entries, exchange certificate and mailbox export requests), the shells are keeping on replicating. Escalated to customer to remove persistence and patch the server.
106066	Aktion erforderlich	Feb. 5, 2022 at 9:30 AM	Wert 3	Threat Hunt - Log4j VMWare Horizon	The MTR team conducted an investigation across the estate for indications of vulnerable Log4J instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified instances of log4j which require patching. Escalated to customer with recommendations
105049	Behoben	Feb. 1, 2022 at 11:27 AM	Wert 3	Threat Hunt - Malicious persistence	The MTR Team has performed a leadless hunt across the estate and observed persistence of IsErik adware on the host Win10-3-LR. During our review, we observed a malicious domain and directory related to IsErik and persistence through a scheduled task. MTR has removed the scheduled task and persistent folder since the response mode was Authorize.

« ‹ 1 › » 10

[redacted]@sophos.com

Gesendet Sa. Feb. 5, 2022 at 9:47 AM

Team,
Case ID: 2-106066
Date: 2022-02-05 09:30:16 UTC

// Analysis:
We have conducted an investigation across your environment for indications of vulnerable Log4J instances. After investigation, the MTR team did not identify malicious activity associated with the critical vulnerability in Apache Log4j. However, we identified the following instances of log4j which require your attention as some of them are End of Life and some are vulnerable to CVE-2021-44228:
Format Below: Hostname -Path -Log4j Version

- Win10-1 - C:\Xilinx\xic\tps\win64\jre\bin\java.exe - log4j-1.2.15.jar
- Win10-2 - C:\Users\armando.taveras\Downloads\arduino-1.8.16-windows\arduino-1.8.16\java\bin\javaw.exe- log4j-api-2.12.0.jar
- Win10-4 - D:\USERDATA\miguel.garabito\AppData\Roaming\.minecraft\runtime\jre-legacy\windows\jre-legacy\bin\javaw.exe - log4j-api-2.8.1.jar

Additionally looking into IIS logs, we observed some inbound reconnaissance attempts on the host "EC2AMAZ". We have not observed any outbound connections and investigating surrounding activities did not reveal any signs of active exploitation.
We have also performed a proactive threat hunt for exploitation of the Log4Shell vulnerability CVE-2021-44228 occurring on VMware Horizon Server and the MTR team did not identify malicious activity.
We will continue to monitor your environment and alert you to any malicious activity detected.
At this time, we recommend performing the below-referenced remediation steps as soon as possible. If you have any questions regarding this escalation, please reply to this email.

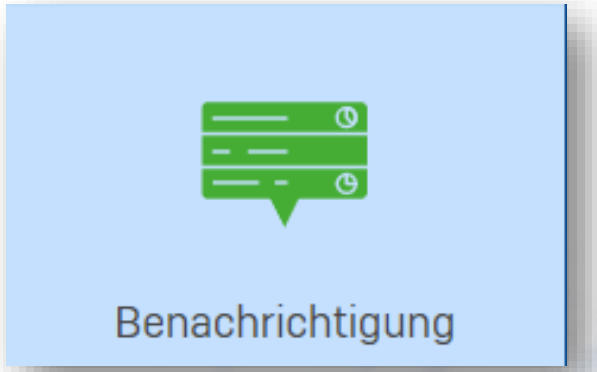
// Recommendations:

- If you are using Java 8 (or later) then you should upgrade Log4j to release 2.17.1 and Java 7 users should upgrade to release 2.12.4. Otherwise, in any release other than 2.16.0, you may remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
  - Refer: https://logging.apache.org/log4j/2.x/security.html
- In circumstances where it's not possible to update from an affected version, the following mitigations can be considered:
  - Restrict or isolate these systems from the Internet until patching is possible.
  - Implement outbound network filtering to restrict LDAP, LDAPS, and RMI traffic originating from servers to the Internet.
  - Ensure WAF and IPS rules are on the latest content versions to help with prevention monitoring and response.
- If the patching activity is not planned in the near future then please consider blocking the IPs mentioned, if there are no business dependencies associated, as they have been observed to be scanning for the Log4j vulnerability in your environment.
  - 45[.]155[.]205[.]233
  - 195[.]251[.]41[.]139
  - 45[.]130[.]229[.]168
  - 191[.]232[.]38[.]25
  - 5[.]157[.]38[.]50
  - 138[.]197[.]72[.]76
  - 45[.]83[.]64[.]1
  - 195[.]54[.]160[.]149
  - 45[.]146[.]164[.]160
  - 162[.]55[.]90[.]26
  - 31[.]131[.]16[.]127
  - 167[.]71[.]175[.]10
- Please notify the MTR team about your Findings and Actions.

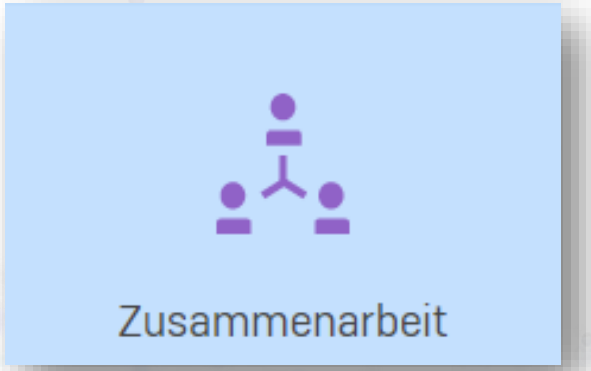
// References:

- https://logging.apache.org/log4j/2.x/security.html
- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
- https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce
- https://news.sophos.com/en-us/2021/12/17/log4shell-response-and-mitigation-recommendations

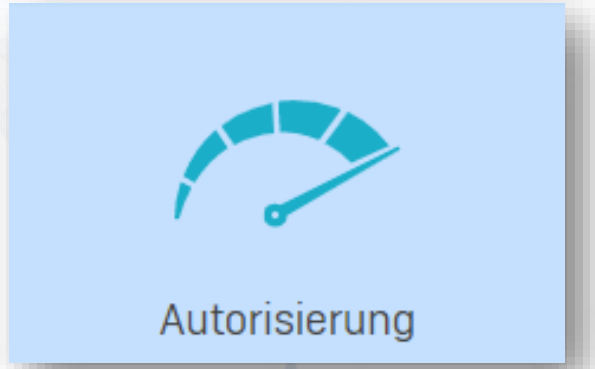
Zusammenarbeit mit dem MDR Team



Sophos: *„Auf diesen 10 Rechnern haben wir einen Angriff mit folgenden Aktivitäten festgestellt.“*
Kunde: *„Danke, wir übernehmen."*



Sophos: *„Sollen wir in diesem Fall den Angriff stoppen?“*
Kunde: *„Ja bitte, aber während der Geschäftszeiten immer nachfragen, dafür nachts und am Wochenende bitte sofort loslegen!"*



Kunde: *„Sophos, bitte stoppt jeden eindeutigen Angriff!“*
Sophos: *„Wird gemacht."*

Fazit

- Intercept X = bester proaktiver Grundschutz

- Sophos **XDR = Werkzeuge** für Schutz, Erkennung, Analyse und Reaktion
  - XDR-Werkzeuge **müssen** 24/7 aktiv bedient werden
  - Bedienung kann durch die eigene IT bzw. das Systemhaus stattfinden

- **Sophos MDR** = Komplette Bedienung von XDR durch Sophos

Q&A

SOPHOS

SOPHOS

Cybersecurity delivered.