Managed Detection and Response

Christopher Erdmann

Sales Engineer

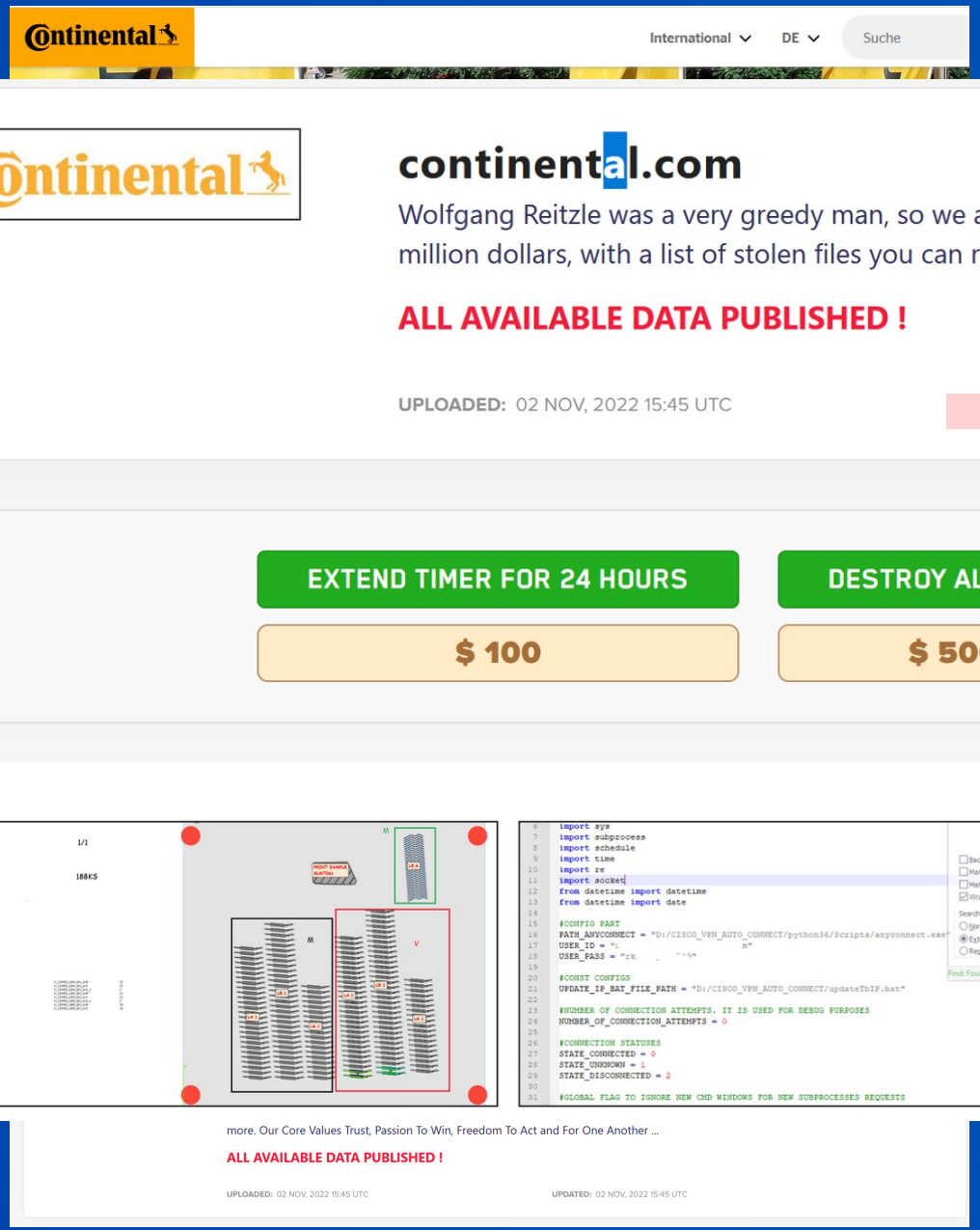
SOPHOS

Die Null muss stehen!

… oder was Sophos MDR mit Gegentoren zu tun hat.

15.000 : 0

SOPHOS



Continental-Einbruch: Lockbit-Cybergang

Continental

continental.com

Wolfgang Reitzle was a very greedy man, so we are ready to sell 40 terabytes of the company's private information in one hand for just 50 million dollars, with a list of stolen files you can read here.

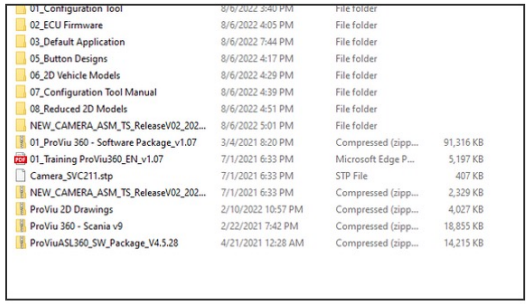
ALL AVAILABLE DATA PUBLISHED !

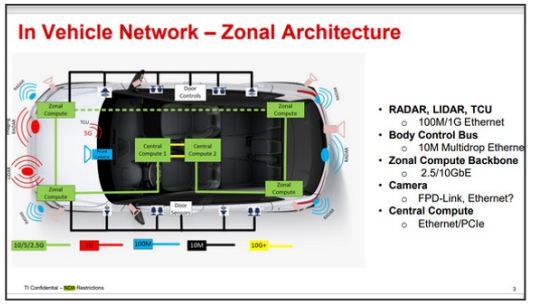
UPLOADED: 02 NOV, 2022 15:45 UTC

UPDATED: 10 NOV, 2022 15:09 UTC

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 100	$ 50000000	$ 50000000

1-4 of 4





Verkauf. Offenbar sind die Lösegeld-Verhandlungen weiterhin nicht erfolgreich gewesen.

https://www.heise.de/news/Continental-Einbruch-Lockbit-Cybergang-fordert-50-Millionen-US-Dollar-7336996.html

SOPHOS

…aus dem Leben: Konsequenzen für Unternehmen

PROPHETE

Hack wohl verantwortlich für Insolvenz von E-Bike-Hersteller

Die Insolvenz des Herstellers Prophete soll einen ungewöhnlichen Grund haben: Neben der Chipkrise sollen Hacker verantwortlich sein, die den Betrieb lahmgelegt haben.

in Pocket speichern | merken

11. Januar 2023, 9:54 Uhr, Sebastian Grüner

(Bild: Prophete)

Schlechtes Geschäft und ein Hacker-Angriff sollen die Insolvenz bei Prophete verursacht haben.

Der Fahrrad- und E-Bike-Hersteller Prophete aus Rheda-Wiedenbrück mit den weiteren Marken Kreidler, VSF Fahrradmanufaktur und E-Bikemanufaktur musste erst vor wenigen Wochen Insolvenz anmelden. Als Grund dafür nennt der vorläufige Insolvenzverwalter Manuel Sack der F.A.Z. einen Hacker-Angriff auf das Unternehmen, der über mehrere Wochen zu einem kompletten Betriebsausfall geführt haben soll. Ob es sich dabei um einen Ransomware-Angriff handelte, ist derzeit nicht klar, aber wahrscheinlich.

https://www.golem.de/news/prophete-hack-wohl-verantwortlich-fuer-insolvenz-von-e-bike-hersteller-2301-171104.html

echo24 › Leben › Verbraucher

Insolvenz von Traditionshersteller hat Konsequenzen für Lidl und Aldi-Kunden

Erstellt: 23.01.2023, 06:03 Uhr
Von: Juliane Reyle

Kommentare | Teilen

Mehrere Discounter-Riesen werden sogar ein Angebot aus ihren Geschäften verabschieden müssen. Prophete, ein deutscher Fahrradhersteller ist bankrott. Das Insolvenzverfahren läuft bereits.

Die Zukunft von Prophete, einem deutschen Traditionshersteller, ist derzeit ungewiss. Das Unternehmen meldete kurz vor Weihnachten die Insolvenz an. Ob der Betrieb des Fahrradherstellers zunächst weiterläuft oder direkt eingestellt werden muss, ist bislang noch nicht klar, wie „Chip“ schreibt. Einige Kunden von Aldi und Lidl werden die Folgen des Firmen-Bankrotts vermutlich sogar im Angebot der Discounter bemerken.

https://www.echo24.de/leben/verbraucher/lidl-aldi-insolvenz-tradition-hersteller-pleite-konsequenzen-kunden-fahrrad-prophete-angebot-zr-92010927.html

203 Mrd.€ Schaden für deutsche Unternehmen in 2021 durch Cyberangriffe[1]

84 Prozent der Unternehmen hatten Datendiebstahl, Ransomware, Sabotage[1]

6,2 Mrd.€ Investition in IT-Sicherheit 2021[2]

[1] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
[2] https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/

SOPHOS

Bedrohungen nehmen zu in Menge, Komplexität, Schaden

11 - 15 Tage

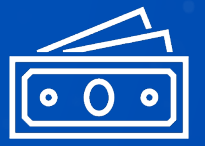
Verweildauer im Unternehmen

4.3 Tage

zwischen Datendiebstahl und Verschlüsselung

90%

der Opfer hatten Einschränkungen der Produktion



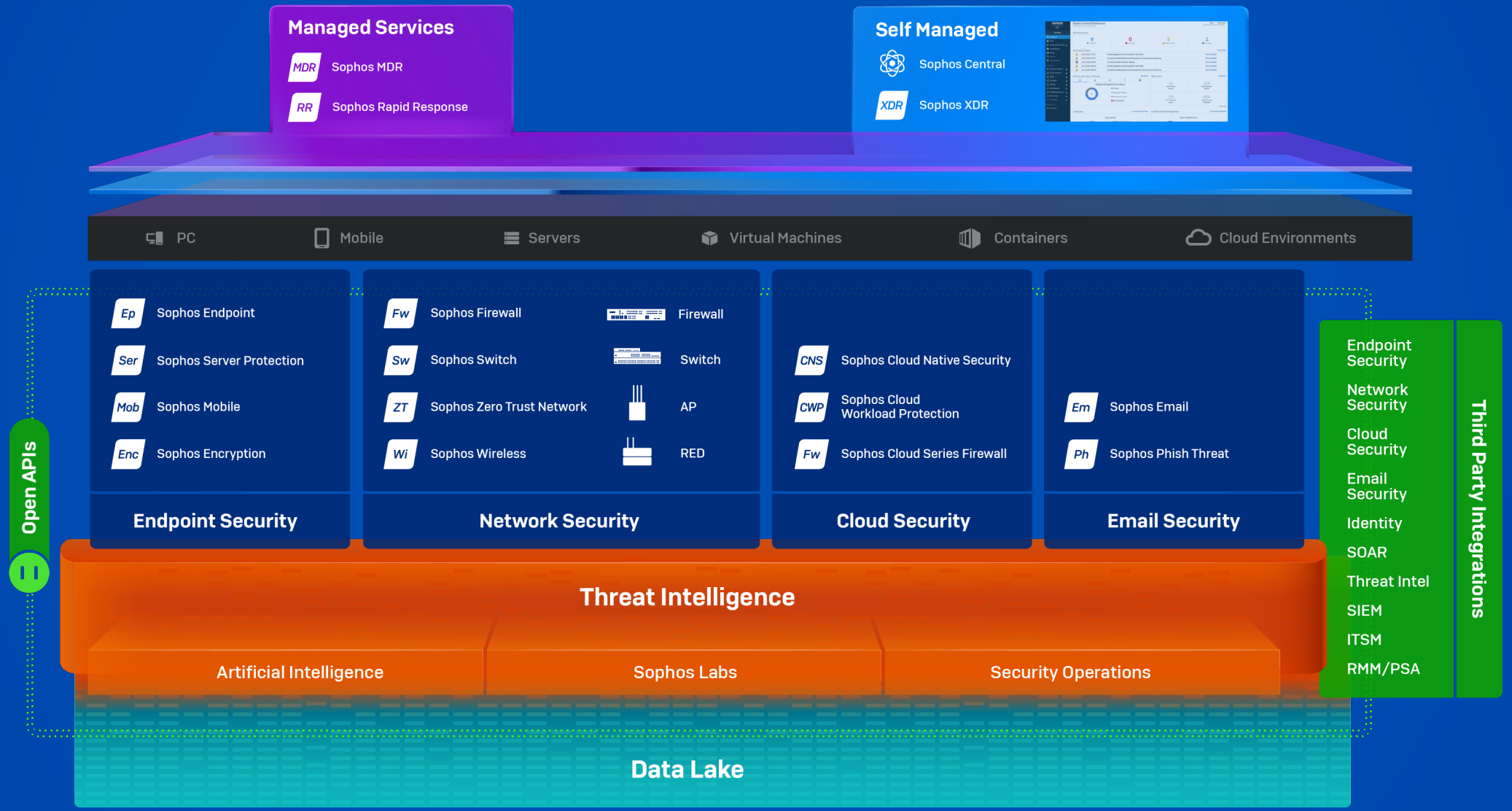
$1.4M

Schaden pro Vorfall, vor allem durch Betriebsausfall

Quelle: The State of Ransomware 2022, Sophos; The Active Adversary Playbook 2022, Sophos

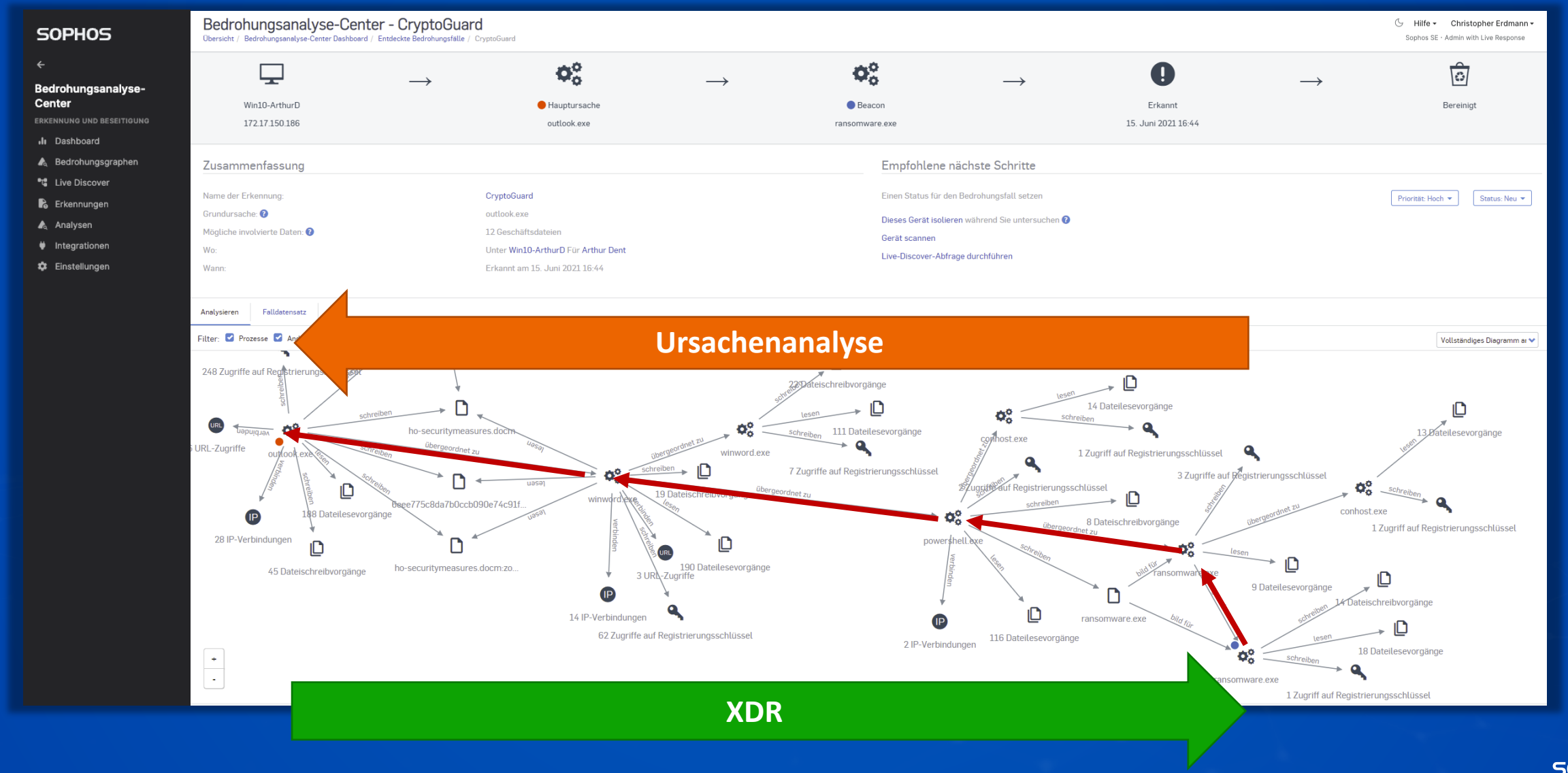
SOPHOS

SOPHOS Adaptive Cybersecurity Ecosystem



SOPHOS

Ursachenanalyse vs. XDR



Breite und tiefgehende Telemetriedaten = Frühwarnsystem

Sensors

- Identity
- Cloud SaaS
- Firewall
- Network
- Email
- Endpoint

Data Lake

Trends that Cross Devices
Event correlation

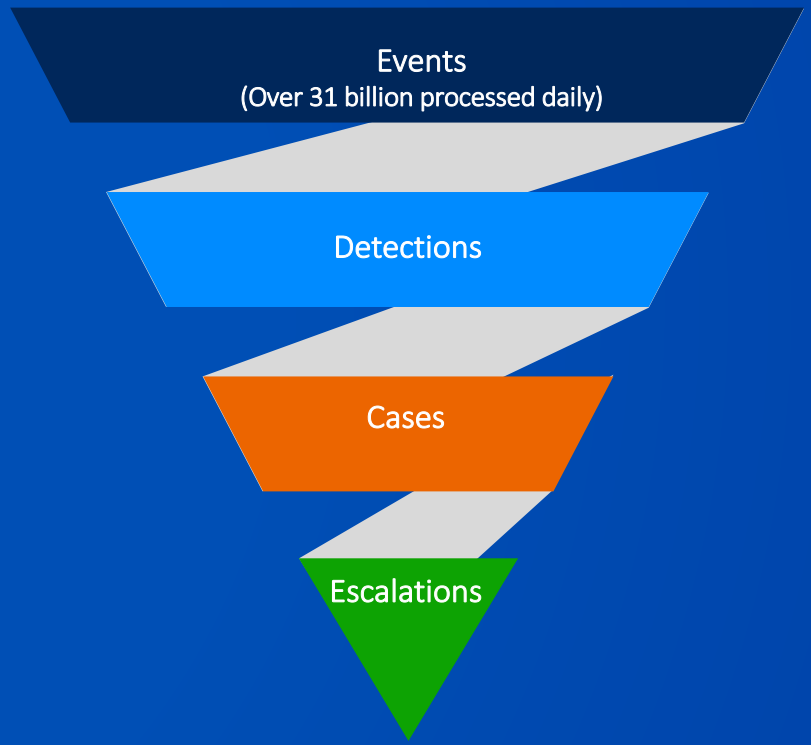
Public Cloud
Events that transcend geography

Unprotected Devices
Traffic from devices without EPP

Multi-Stage Attacks
Phishing > Compromised Account > Lateral Movement

Encrypted Network Traffic
Network Detection and Response (NDR)

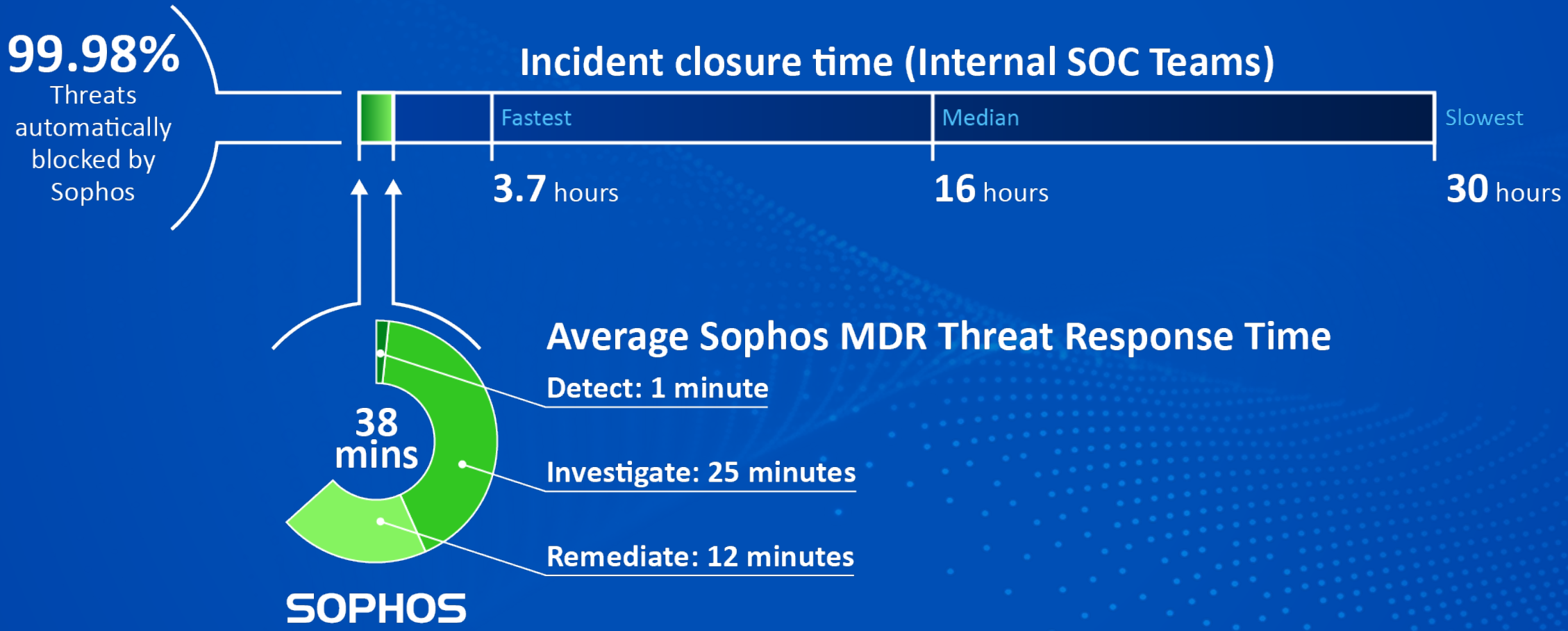
Processing

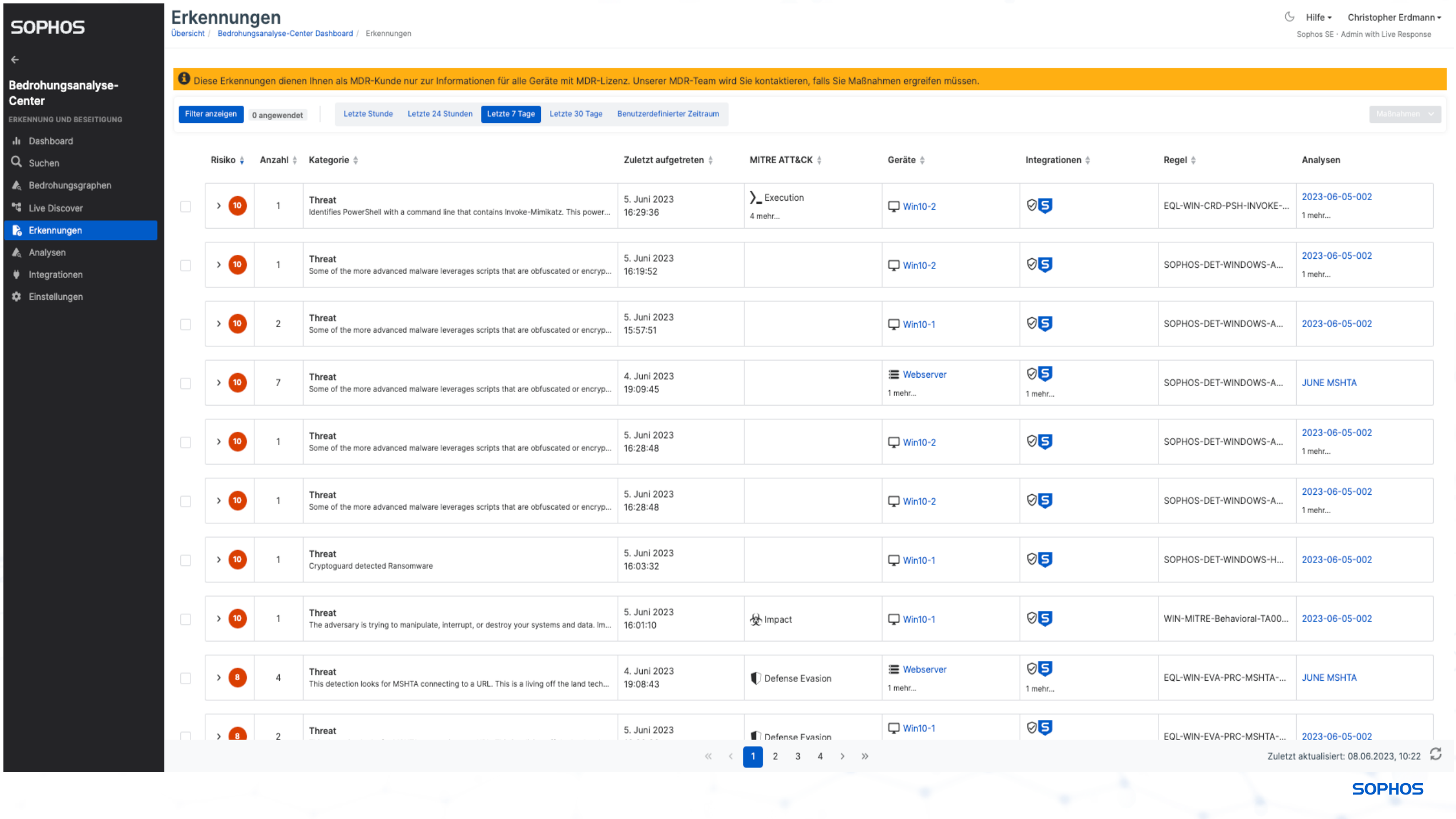


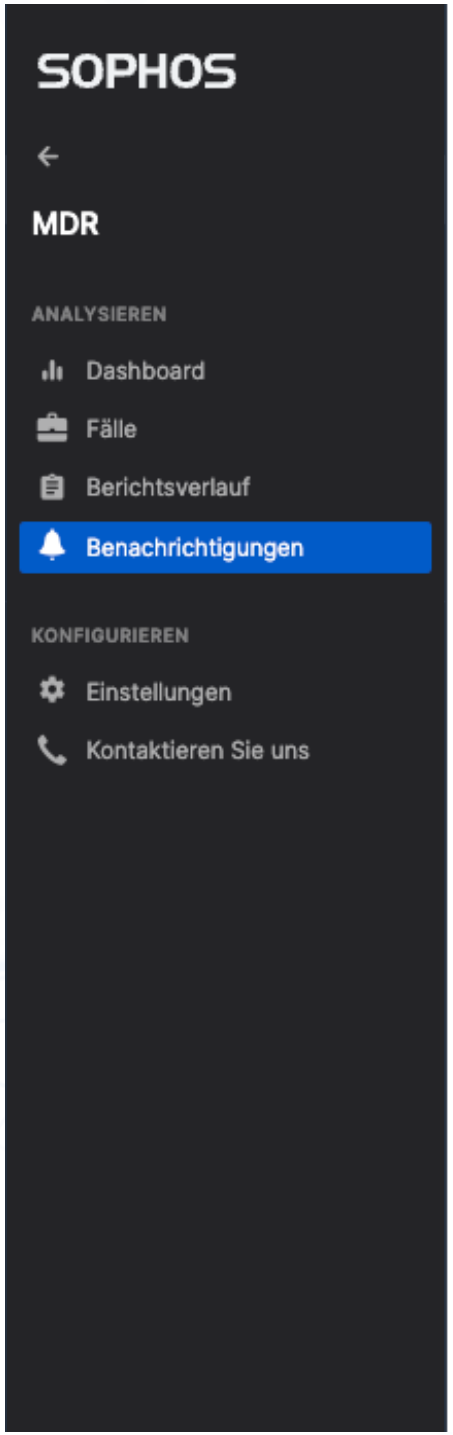
Active Threats

SOPHOS

Leading Detection and Response Times




SOPHOS
Bedrohungsanalyse-Center
ERKENNUNG UND BESEITIGUNG
Dashboard
Suchen
Bedrohungsgraphen
Live Discover
Erkennungen
Analysen
Integrationen
Einstellungen
Erkennungen
Übersicht / Bedrohungsanalyse-Center Dashboard / Erkennungen
Hilfe
Christopher Erdmann
Sophos SE · Admin with Live Response
Diese Erkennungen dienen Ihnen als MDR-Kunde nur zur Informationen für alle Geräte mit MDR-Lizenz. Unserer MDR-Team wird Sie kontaktieren, falls Sie Maßnahmen ergreifen müssen.
Filter anzeigen
0 angewendet
Letzte Stunde
Letzte 24 Stunden
Letzte 7 Tage
Letzte 30 Tage
Benutzerdefinierter Zeitraum
Maßnahmen
Risiko
Anzahl
Kategorie
Zuletzt aufgetreten
MITRE ATT&CK
Geräte
Integrationen
Regel
Analysen
10 1 Threat Identifies PowerShell with a command line that contains Invoke-Mimikatz. This power... 5. Juni 2023 16:29:36 Execution 4 mehr... Win10-2 EQL-WIN-CRD-PSH-INVOKE-... 2023-06-05-002 1 mehr...
10 1 Threat Some of the more advanced malware leverages scripts that are obfuscated or encryp... 5. Juni 2023 16:19:52 Win10-2 SOPHOS-DET-WINDOWS-A... 2023-06-05-002 1 mehr...
10 2 Threat Some of the more advanced malware leverages scripts that are obfuscated or encryp... 5. Juni 2023 15:57:51 Win10-1 SOPHOS-DET-WINDOWS-A... 2023-06-05-002
10 7 Threat Some of the more advanced malware leverages scripts that are obfuscated or encryp... 4. Juni 2023 19:09:45 Webserver 1 mehr... 1 mehr... SOPHOS-DET-WINDOWS-A... JUNE MSHTA
10 1 Threat Some of the more advanced malware leverages scripts that are obfuscated or encryp... 5. Juni 2023 16:28:48 Win10-2 SOPHOS-DET-WINDOWS-A... 2023-06-05-002 1 mehr...
10 1 Threat Some of the more advanced malware leverages scripts that are obfuscated or encryp... 5. Juni 2023 16:28:48 Win10-2 SOPHOS-DET-WINDOWS-A... 2023-06-05-002 1 mehr...
10 1 Threat Cryptoguard detected Ransomware 5. Juni 2023 16:03:32 Win10-1 SOPHOS-DET-WINDOWS-H... 2023-06-05-002
10 1 Threat The adversary is trying to manipulate, interrupt, or destroy your systems and data. Im... 5. Juni 2023 16:01:10 Impact Win10-1 WIN-MITRE-Behavioral-TA00... 2023-06-05-002
8 4 Threat This detection looks for MSHTA connecting to a URL. This is a living off the land tech... 4. Juni 2023 19:08:43 Defense Evasion Webserver 1 mehr... 1 mehr... EQL-WIN-EVA-PRC-MSHTA-... JUNE MSHTA
8 2 Threat 5. Juni 2023 Defense Evasion Win10-1 EQL-WIN-EVA-PRC-MSHTA-... 2023-06-05-002
1 2 3 4
Zuletzt aktualisiert: 08.06.2023, 10:22
SOPHOS



suchibrato.mahato@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

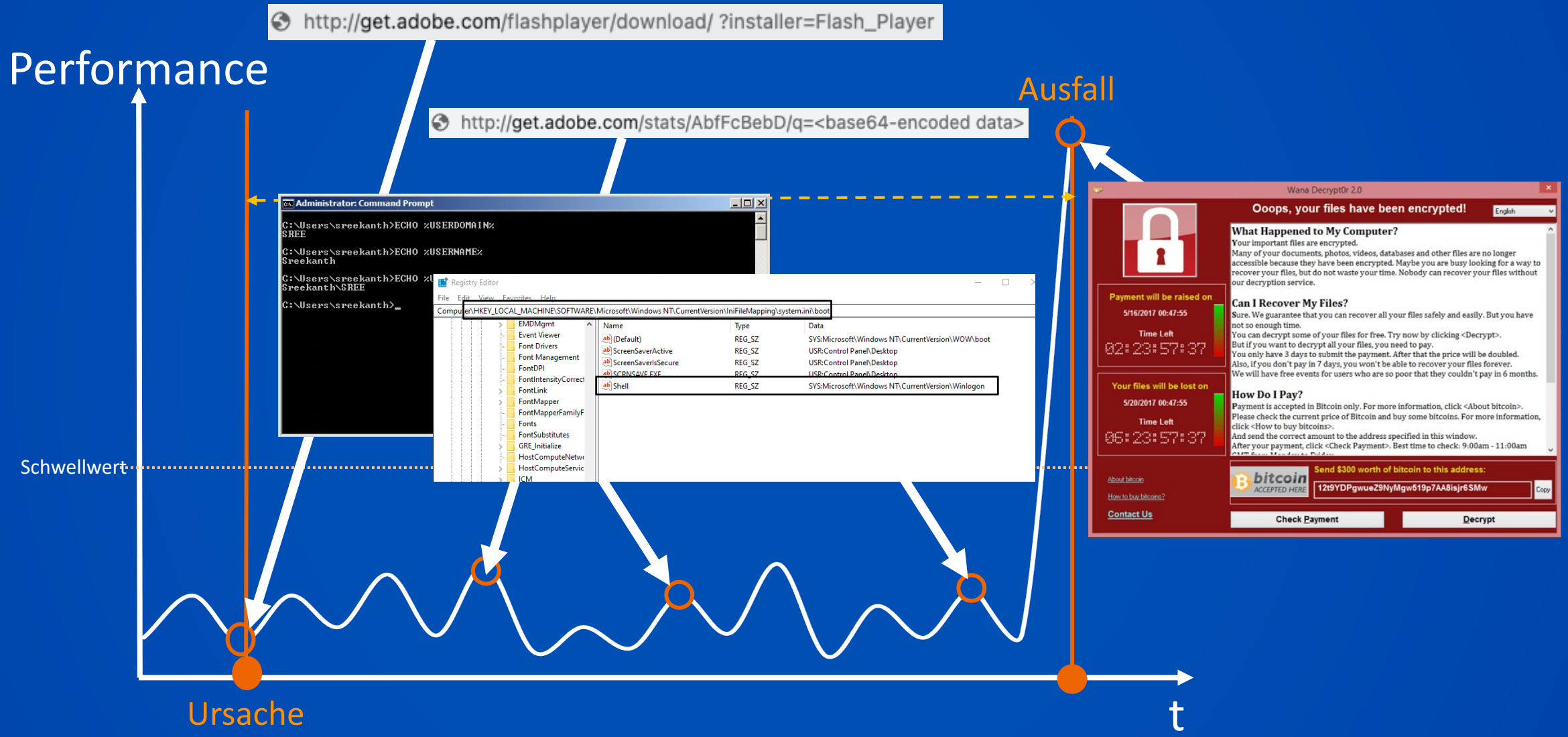
Additionally looking into IIS logs, we observed some inbound reconnaissance attempts on the host "EC2AMAZ". We have not observed any outbound connections and investigating surrounding activities did not reveal any signs of active exploitation.
We have also performed a proactive threat hunt for exploitation 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

Proaktive Sicherheit:



SOPHOS

Sophos Partner – nutzt selbst MDR

Business Case:
Admin eines Partners möchte seine Präsentation für IT-Sicherheit mit Screenshots von echten Darknet-Sites anreichern

Install TOR Browser via valid Admin-Account

Mittwoch, 27 April 2022, 21.OO Uhr

Search for hacked .de offerings

21.15 Uhr

Get called by MDR-ops

21.20 Uhr

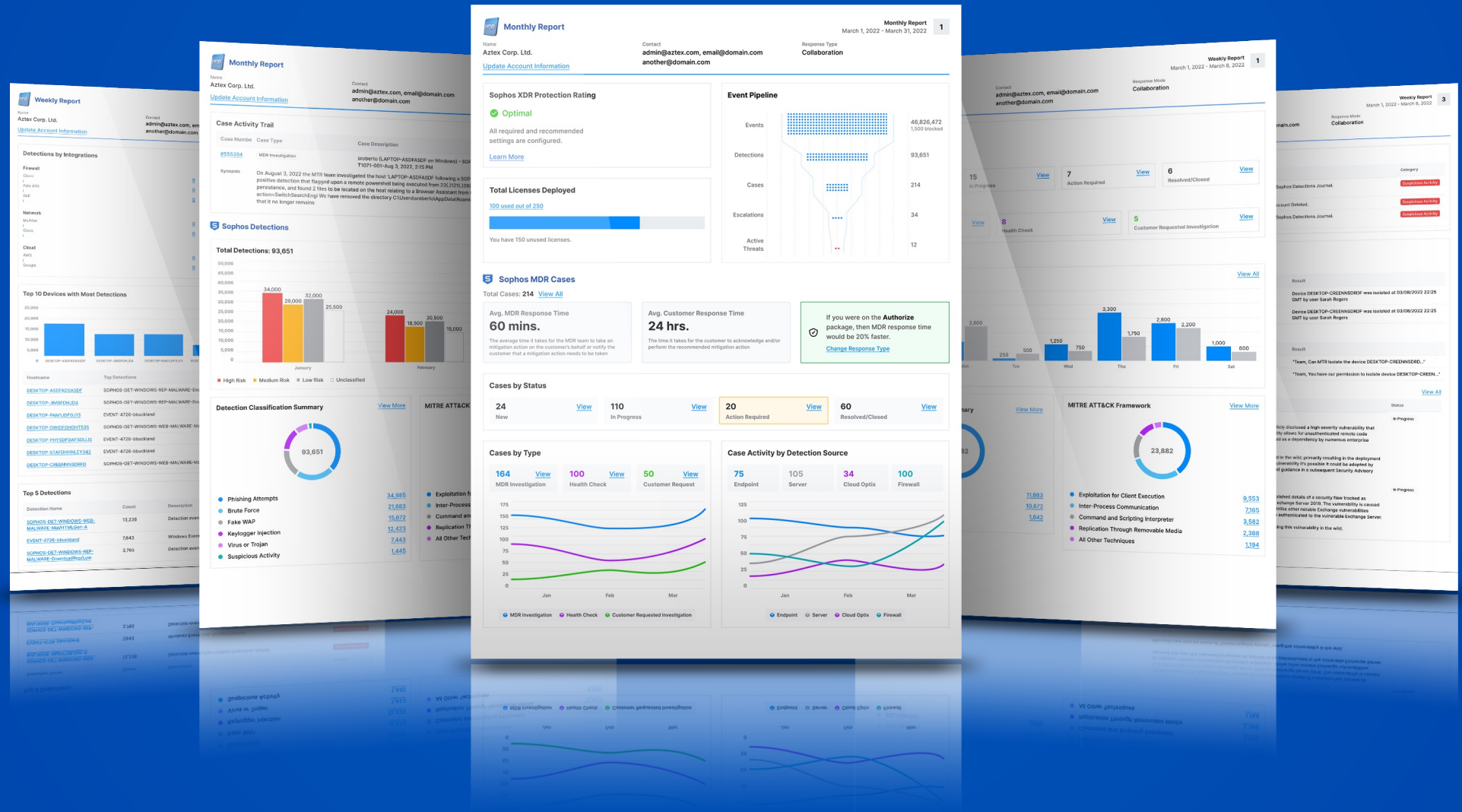
If no response MDR operator was already on device

21.22 Uhr

Close case as „false positive“

21.30 Uhr

Managementtaugliche Cybersecurity Reports



SOPHOS

SOPHOS MDR: Offen und flexibel

MDR **Sophos MDR**

Kompatibel mit Ihrer Umgebung
Wir nutzen Sophos Werkzeuge, die Werkzeuge anderer Anbieter – oder eine Kombination aus beiden

Kompatibel mit Ihren Anforderungen
Wir bieten komplettes Incident Response - oder Unterstützung für Ihr Team

Kompatibel mit Ihrem Unternehmen
Unser Team hat umfangreiche Erfahrung mit Angriffen auf Unternehmen aller Branchen

SOPHOS

XDR Sophos XDR
Fw Sophos Firewall
Cld Sophos Cloud
NDR Sophos NDR
Em Sophos Email
Ep Sophos Endpoint

Endpoint

Microsoft
CROWDSTRIKE
McAfee
SentinelOne
CHECK POINT
TREND MICRO
Malwarebytes
BlackBerry CYLANCE

Firewall

paloalto NETWORKS
FORTINET
CHECK POINT
CISCO
SONICWALL

Cloud SaaS

aws
Azure
Google Cloud
orca security

Email

Microsoft 365
mimecast
proofpoint

Identity

Microsoft [Azure IDP, ATA]
okta
DUO

Network

DARKTRACE
Forcepoint

SOPHOS

… 13 Jahre in Folge!

Sophos wurde von Gartner als Leader im Magic Quadrant für Endpoint Protection Platforms (EPP) ausgezeichnet.

#sophos #sophosMDR #csaas

Gartner
Peer Insights™

Der am **besten bewertete** und am **häufigsten getestete** MDR-Service bei Gartner Peer Insights

Sophos MDR

4.8
Average Rating

97%
Would Recommend

Based on 256 Reviews

SentinelOne	4.5
CrowdStrike	4.8*
Arctic Wolf	4.8*

Sophos Endpoint

4.8
Average Rating

95%
Would Recommend

Based on 539 Reviews

Microsoft	4.4
CrowdStrike	4.7
Trend Micro	4.6

Sophos Firewall

4.8
Average Rating

95%
Would Recommend

Based on 362 Reviews

Fortinet	4.6
Check Point	4.5
Palo Alto Networks	4.5

Reviews from last 12 months as of August 1, 2022
*Vendors with fewer than 50 customer reviews

SOPHOS

The Sophos Breach Protection Warranty covers up to $1 million in response expenses

Included with new **Sophos MDR Complete annual** (term) subscriptions – at no additional cost

Built-in automatically with **1-, 2- and 3-year licenses**, both new customers and renewals

Comprehensive coverage: endpoints, servers, Windows, macOS, no geographic limits

Underwritten by Sophos, demonstrating our confidence in our protection

For full terms and conditions of the warranty see www.sophos.com/legal.

SOPHOS

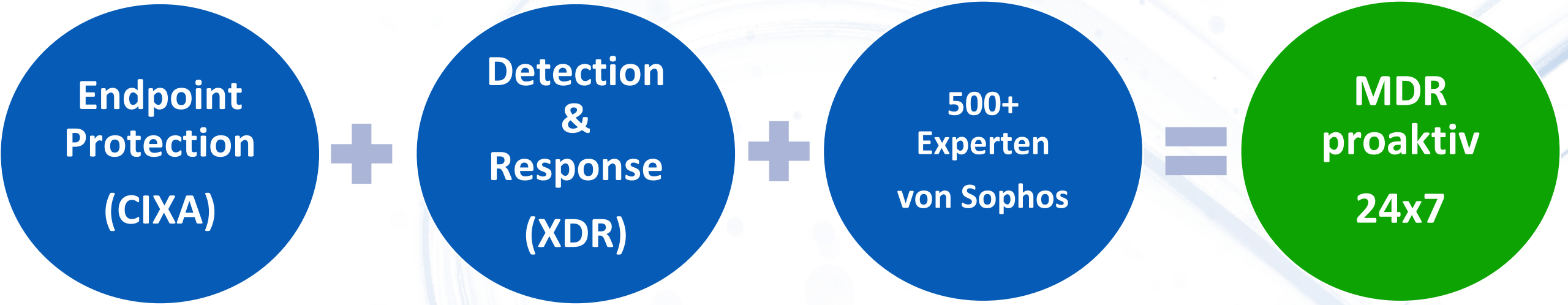
Sophos Security Services

“Wurde bei mir eingebrochen?”	“Bei mir wurde eingebrochen. Was mache ich jetzt?”	“Ich möchte keinen Einbruch (mehr). Wie kann ich das verhindern?”
Sophos Compromise Assessment	**Sophos Rapid Response**	**Sophos MDR**

Make or Buy ?

Intercept X Advanced + XDR oder MDR?

Intercept X Advanced + XDR oder MDR?



Butter bei die Fische!

…lassen Sie uns über Geld sprechen

Build vs. Buy – selber machen oder Managed Service ?

Beispiel: 100 Endpoints und 10 Server	Selber machen	SOPHOS
Tools	**€ 40.945**	
Endpoint /Server Protection + XDR	€10.945 *	*Listpreis
Workflow/SIEM/SOAR	€10,000	Alle Tools, die zum proaktiven Erkennen, Untersuchen und Reagieren (Schützen) auf Sicherheitsereignisse verwendet werden, sind in MDR enthalten und werden von unserem MDR-Team verwendet.
Threat Intelligence (z.B. Intel feeds/honeypots)	€13.000	
Connectors: Network & Public Cloud	€ 7.000	
Mitarbeiter	**€ 752.000**	
1 SOC Manager	€120,000	Fachkräftemangel ist nicht ihr Problem. Sophos rekrutiert seine Talente weltweit nach anspruchsvollen Kriterien.
2 Engineers	€200.000 (€100.000 x 2)	
6 Analysts (6 - 8 erforderlich für 24/7 Dienst)	€432.000 (€72.000 x 6)	
Prozess		
Incident investigation/verification	€50.000	Zeit 24/7, Ressourcen und Infrastruktur, die für die Ausführung aufgewendet werden. Wir leiten Maßnahmen ein, um Bedrohungen zu unterbrechen, einzudämmen und zu neutralisieren, damit Sie sich auf die Verwaltung anderer Aspekte Ihres Unternehmens konzentrieren können. Dies ist in unserem MDR-Service enthalten.
Hunting methodology		
Event/alert triage (playbooks)		
Alert management/notification		
Tool management/tuning		
Annual Total (Euro)	€ 842.945	€ 38.572*

Durchschnitts-gehälter von Glassdoor

*Listpreise Sophos, 12 Monate

SOPHOS

… sprechen wir über Geld

Bereich	Verhältnis
Selber machen	
MDR Complete + NDR, 12 Monate	ca. 4,6 % zu Selber machen
MDR Complete-Kosten/Tag	für 24/7 instant response + leadless Threathunting
MDR-Kosten/Tag & Lizenz (Endpoints &	für 24/7 instant response + leadless Threathunting

SOPHOS

Cybersecurity delivered.