

# 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





## 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

\$ 100

DESTROY ALL INFORMATION

\$ 5000000

DOWNLOAD DATA AT ANY MOMENT

\$ 5000000

1-4 of 4



```
import sys
import subprocess
import schedule
import time
import re
import socket
from datetime import datetime
from datetime import date

#CONFIG PART
PATH_ANYCONNECT = "D:/CISCO_VPN_AUTO_CONNECT/python36/scripts/anyconnect.exe"
USER_ID = "..."
USER_PASS = "..."

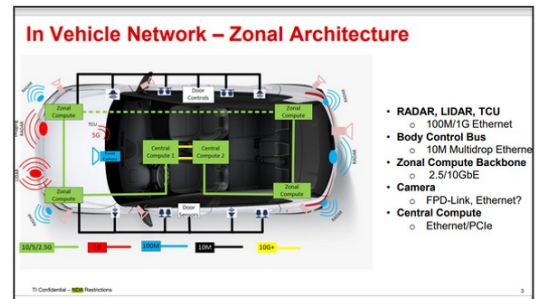
#CONST CONFIGS
UPDATE_IP_BAT_FILE_PATH = "D:/CISCO_VPN_AUTO_CONNECT/updateToIP.bat"

NUMBER_OF_CONNECTION_ATTEMPTS = 0
NUMBER_OF_CONNECTION_ATTEMPTS = 0

#CONNECTION STATUSES
STATE_CONNECTED = 0
STATE_UNKNOWN = 1
STATE_DISCONNECTED = 2

#GLOBAL FLAG TO IGNORE NEW CMD WINDOWS FOR NEW SUBPROCESSES REQUESTS
```

01_Configuration tool	8/6/2022 3:40 PM	File folder
02_ECU Firmware	8/6/2022 4:05 PM	File folder
03_Default Application	8/6/2022 7:44 PM	File folder
05_Button Designs	8/6/2022 4:17 PM	File folder
06_2D Vehicle Models	8/6/2022 4:29 PM	File folder
07_Configuration Tool Manual	8/6/2022 4:39 PM	File folder
08_Reduced 2D Models	8/6/2022 4:51 PM	File folder
NEW_CAMERA_ASM_TS_ReleaseV02_202...	8/6/2022 5:01 PM	File folder
01_ProViu 360 - Software Package_v1.07	3/4/2021 8:20 PM	Compressed (zipp...
01_Training ProViu360_EN_v1.07	7/1/2021 6:33 PM	Microsoft Edge P...
Camera_SVC211.stp	7/1/2021 6:33 PM	STP File
NEW_CAMERA_ASM_TS_ReleaseV02_202...	7/1/2021 6:33 PM	Compressed (zipp...
ProViu 2D Drawings	2/10/2022 10:57 PM	Compressed (zipp...
ProViu 360 - Scania v9	2/22/2021 7:42 PM	Compressed (zipp...
ProViuASL360_SW_Package_V4.5.28	4/21/2021 12:28 AM	Compressed (zipp...



more. Our Core Values Trust, Passion To Win, Freedom To Act and For One Another ...

**ALL AVAILABLE DATA PUBLISHED !**

UPLOADED: 02 NOV, 2022 15:45 UTC

UPDATED: 02 NOV, 2022 15:45 UTC

abgezogen hat, stellen die Cyberkriminellen jetzt für 50 Millionen US-Dollar zum Verkauf. Offenbar sind die Lösegeld-Verhandlungen weiterhin nicht erfolgreich gewesen.

# ...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.

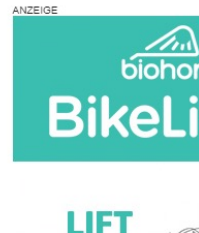


11. Januar 2023, 9:54 Uhr, Sebastian Grüner



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

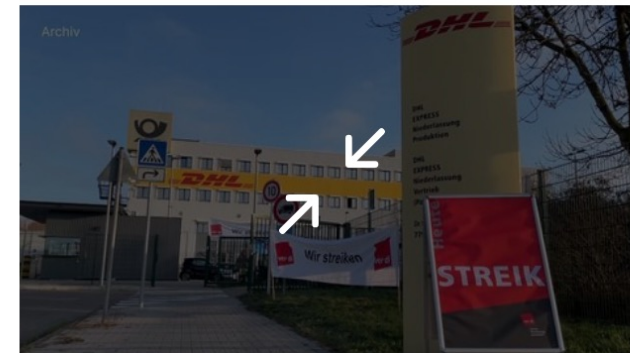
## Insolvenz von Traditionshersteller hat Konsequenzen für Lidl und Aldi-Kunden

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<sup>1</sup>**

# 84

**Prozent der Unternehmen hatten  
Datendiebstahl, Ransomware, Sabotage<sup>1</sup>**

# 6,2

**Mrd.€ Investition in IT-Sicherheit 2021<sup>2</sup>**

<sup>1</sup> <https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022>

<sup>2</sup> <https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/>

# Bedrohungen nehmen zu in Menge, Komplexität, Schaden



**11 - 15 Tage**

Verweildauer im  
Unternehmen



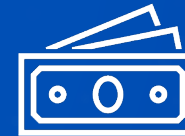
**4.3 Tage**

zwischen Datendiebstahl und  
Verschlüsselung



**90%**

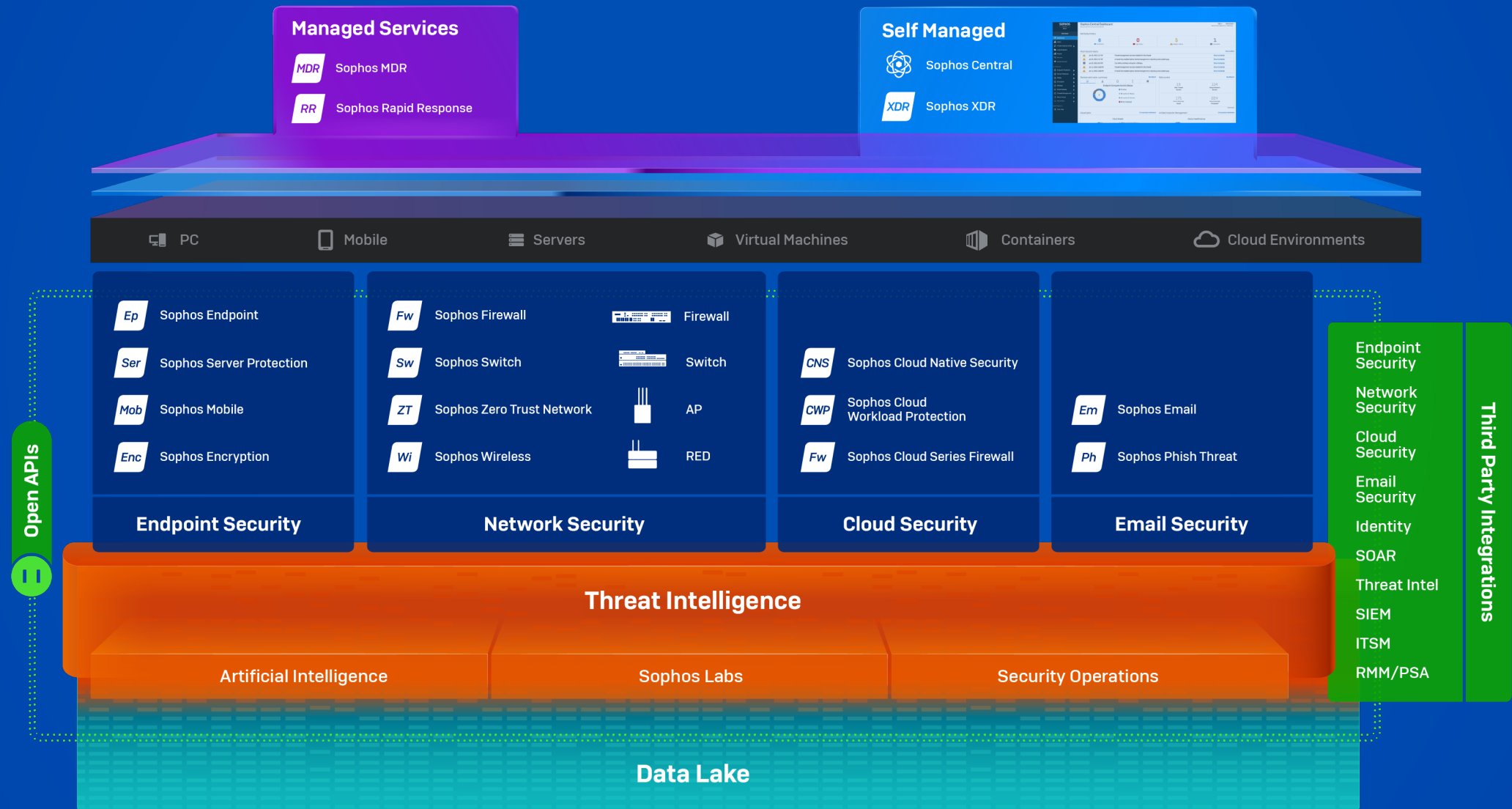
der Opfer hatten  
Einschränkungen der  
Produktion



**\$1.4M**

Schaden pro Vorfall,  
vor allem durch  
Betriebsausfall

# SOPHOS Adaptive Cybersecurity Ecosystem



# Ursachenanalyse vs. XDR

**SOPHOS** Bedrohungsanalyse-Center - CryptoGuard

Übersicht / Bedrohungsanalyse-Center Dashboard / Entdeckte Bedrohungsfälle / CryptoGuard

Hilfe Christopher Erdmann  
Sophos SE - Admin with Live Response

Win10-ArthurD 172.17.150.186 → Hauptursache outlook.exe → Beacon ransomware.exe → Erkant 15. Juni 2021 16:44 → Bereinigt

**Zusammenfassung**

Name der Erkennung:	CryptoGuard
Grundursache:	outlook.exe
Mögliche involvierte Daten:	12 Geschäftsdateien
Wo:	Unter Win10-ArthurD Für Arthur Dent
Wann:	Erkannt am 15. Juni 2021 16:44

**Empfohlene nächste Schritte**

- Einen Status für den Bedrohungsfall setzen
- Dieses Gerät isolieren während Sie untersuchen
- Gerät scannen
- Live-Discover-Abfrage durchführen

Analysieren | Falldatensatz

Filter:  Prozesse  An...

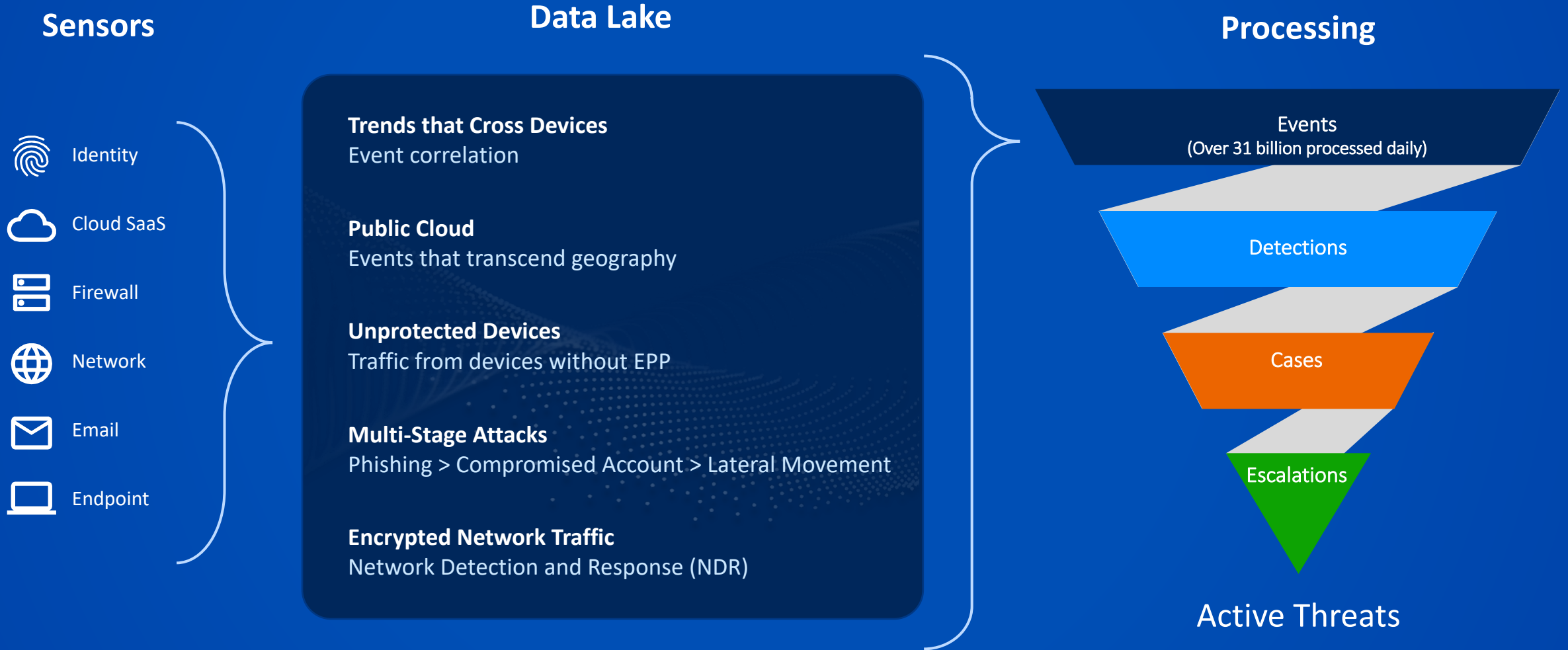
**Ursachenanalyse**

**XDR**

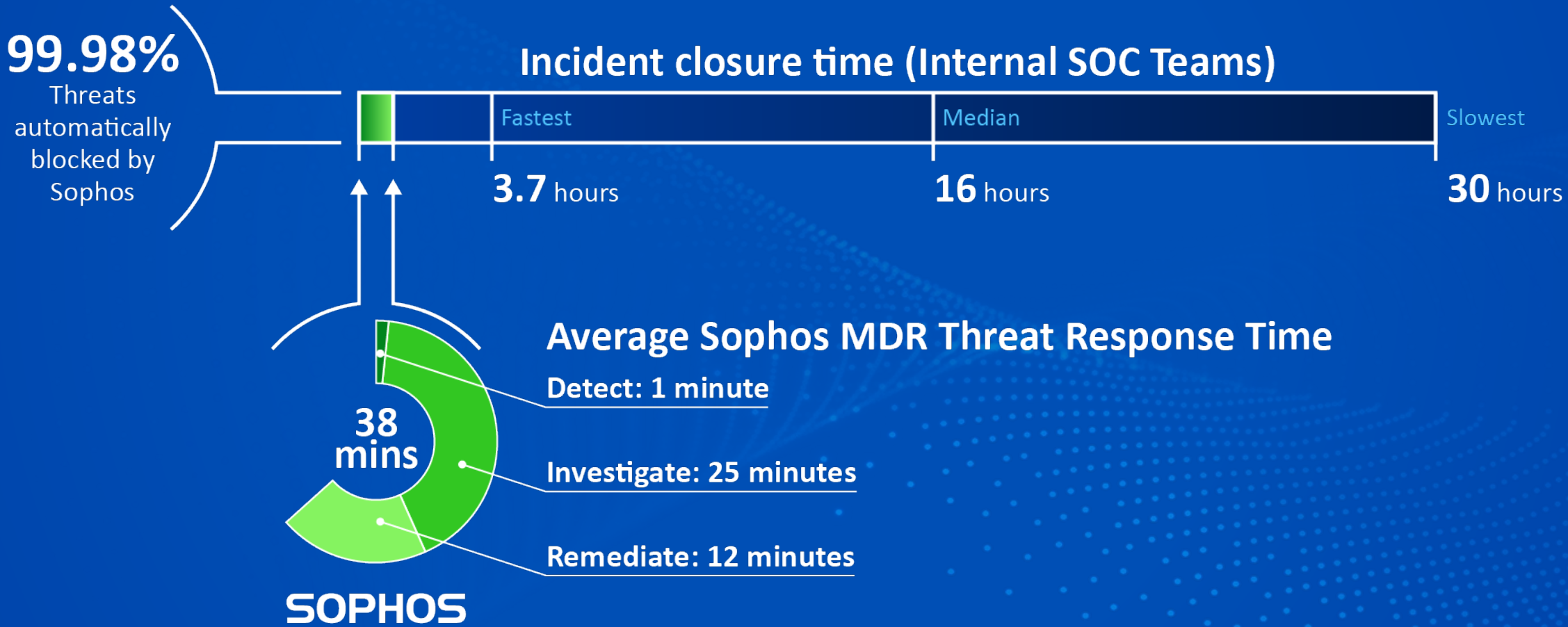
248 Zugriffe auf Registrierungs...  
URL-Zugriffe  
outlook.exe  
28 IP-Verbindungen  
45 Dateischiebvorgänge  
188 Dateilesevorgänge  
ho-securitymeasures.docm  
ho-securitymeasures.docm:zo...  
winword.exe  
19 Dateischiebvorgänge  
3 URL-Zugriffe  
14 IP-Verbindungen  
62 Zugriffe auf Registrierungsschlüssel  
winword.exe  
7 Zugriffe auf Registrierungsschlüssel  
winword.exe  
227 Dateischiebvorgänge  
111 Dateilesevorgänge  
powershell.exe  
2 IP-Verbindungen  
116 Dateilesevorgänge  
conhost.exe  
1 Zugriff auf Registrierungsschlüssel  
conhost.exe  
1 Zugriff auf Registrierungsschlüssel  
3 Zugriffe auf Registrierungsschlüssel  
conhost.exe  
1 Zugriff auf Registrierungsschlüssel  
ransomware.exe  
9 Dateilesevorgänge  
14 Dateischiebvorgänge  
18 Dateilesevorgänge  
ransomware.exe  
1 Zugriff auf Registrierungsschlüssel



# Breite und tiefgehende Telemetriedaten = Frühwarnsystem



# Leading Detection and Response Times



**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
<input type="checkbox"/>	> 10	1	<b>Threat</b> 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...
<input type="checkbox"/>	> 10	1	<b>Threat</b> 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...
<input type="checkbox"/>	> 10	2	<b>Threat</b> 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
<input type="checkbox"/>	> 10	7	<b>Threat</b> Some of the more advanced malware leverages scripts that are obfuscated or encryp...	4. Juni 2023 19:09:45		Webserver 1 mehr...		SOPHOS-DET-WINDOWS-A...	JUNE MSHTA
<input type="checkbox"/>	> 10	1	<b>Threat</b> 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...
<input type="checkbox"/>	> 10	1	<b>Threat</b> 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...
<input type="checkbox"/>	> 10	1	<b>Threat</b> Cryptoguard detected Ransomware	5. Juni 2023 16:03:32		Win10-1		SOPHOS-DET-WINDOWS-H...	2023-06-05-002
<input type="checkbox"/>	> 10	1	<b>Threat</b> 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
<input type="checkbox"/>	> 8	4	<b>Threat</b> 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...		EQL-WIN-EVA-PRC-MSHTA-...	JUNE MSHTA
<input type="checkbox"/>	> 8	2	<b>Threat</b>	5. Juni 2023	Defense Evasion	Win10-1		EQL-WIN-EVA-PRC-MSHTA-...	2023-06-05-002



## MDR

## ANALYSIEREN

Dashboard

Fälle

Berichtsverlauf

Benachrichtigungen

## KONFIGURIEREN

Einstellungen

Kontaktieren Sie uns



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:

Performance

Ausfall

[http://get.adobe.com/flashplayer/download/?installer=Flash\\_Player](http://get.adobe.com/flashplayer/download/?installer=Flash_Player)

<http://get.adobe.com/stats/AbfFcBebD/q=<base64-encoded data>>

Administrator: Command Prompt

```
C:\Users\sreekanth>ECHO %USERDOMAIN%
SREE
C:\Users\sreekanth>ECHO %USERNAME%
Sreekanth
C:\Users\sreekanth>ECHO %
Sreekanth\SREE
C:\Users\sreekanth>_
```

Registry Editor

Name	Type	Data
(Default)	REG_SZ	SYS:Microsoft\Windows NT\CurrentVersion\WOW\boot
ScreenSaverActive	REG_SZ	USR:Control Panel\Desktop
ScreenSaverSecure	REG_SZ	USR:Control Panel\Desktop
SCRNSAVE.EVE	REG_SZ	USR:Control Panel\Desktop
Shell	REG_SZ	SYS:Microsoft\Windows NT\CurrentVersion\Winlogon

Wana Decrypt0r 2.0

### Ooops, your files have been encrypted!

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left: 02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left: 06:23:57:37

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send \$300 worth of bitcoin to this address:  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment Decrypt

Schwellwert

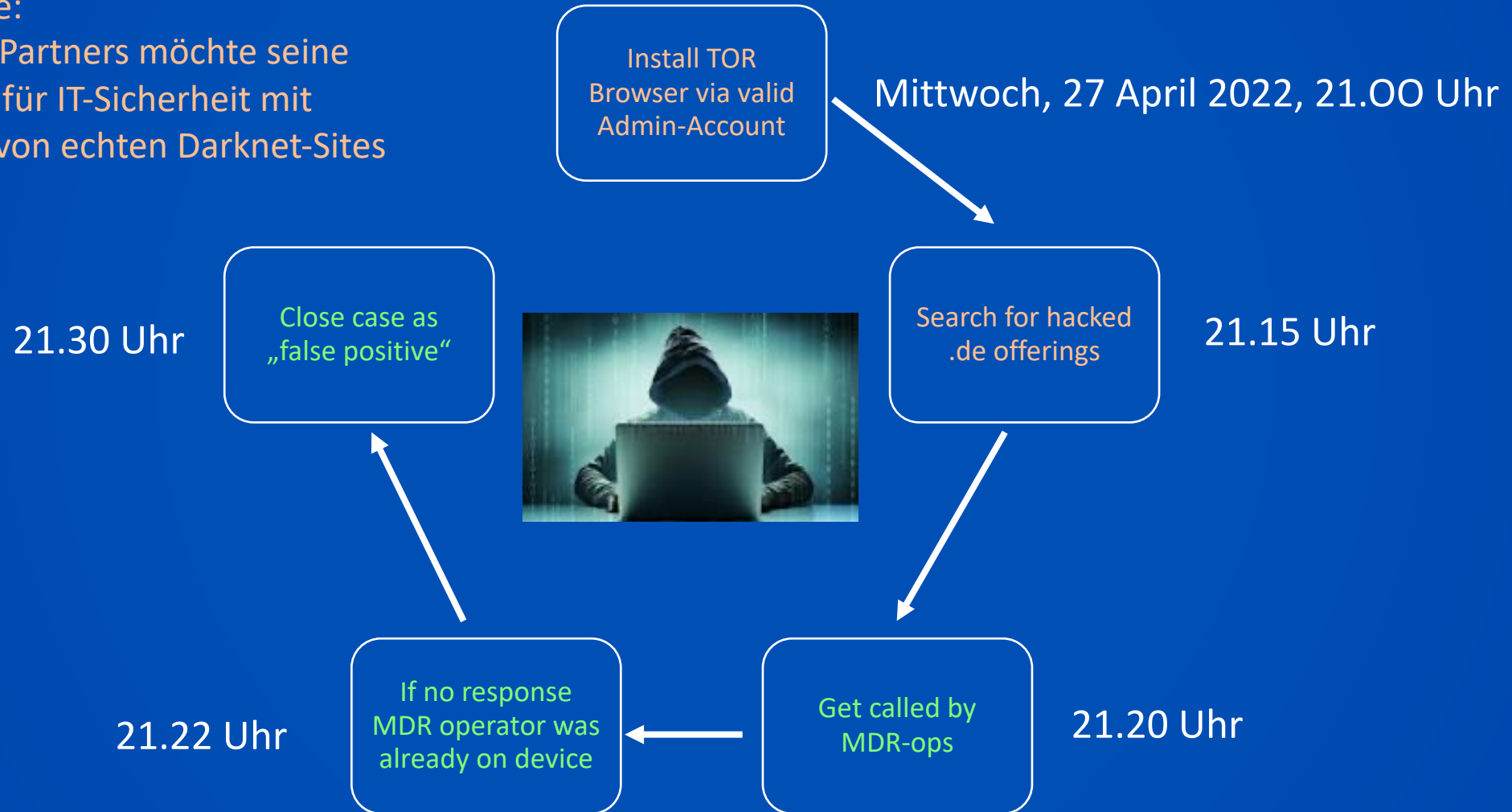
Ursache

t

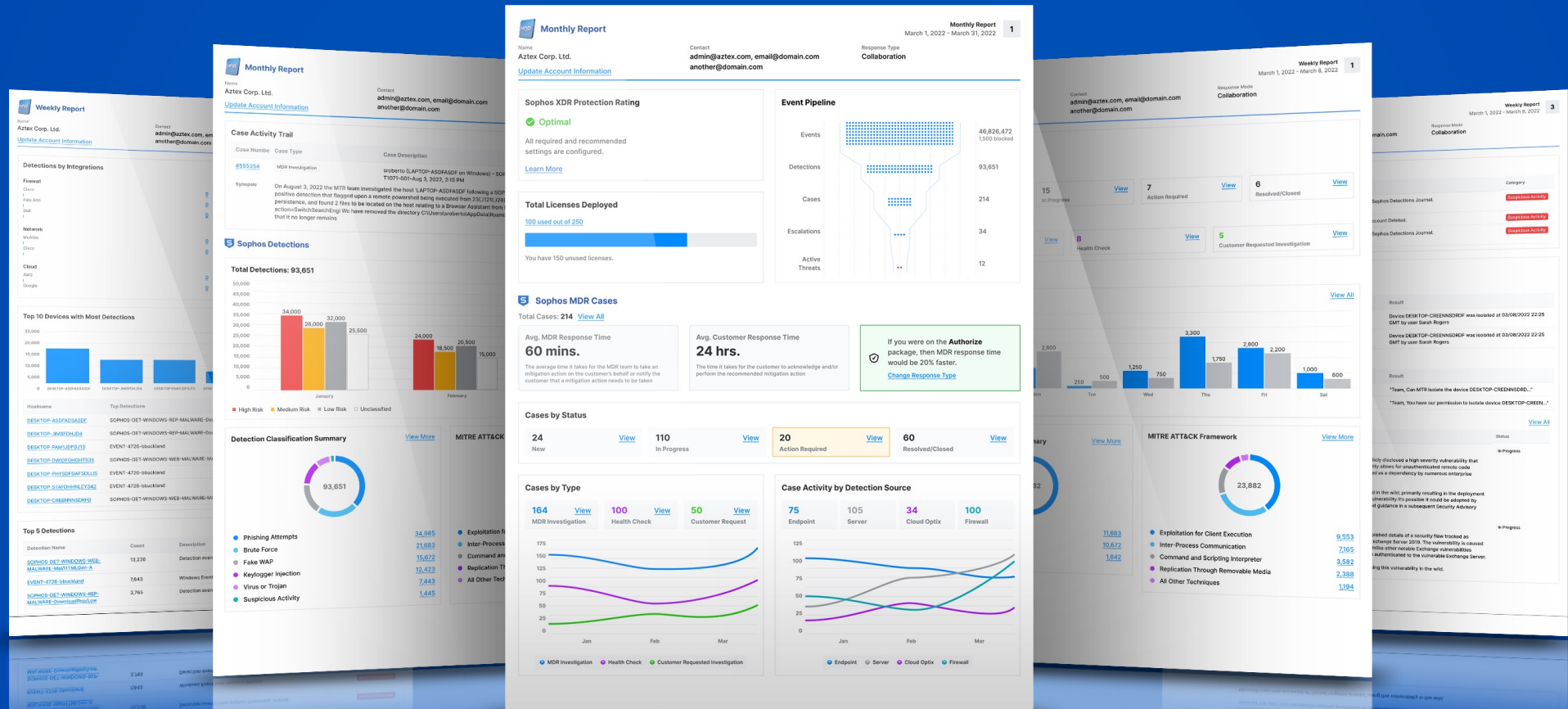
# Sophos Partner – nutzt selbst MDR

Business Case:

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



# Managementtaugliche Cybersecurity Reports



# SOPHOS MDR: Offen und flexibel



## 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



### Endpoint



### Firewall



### Cloud SaaS



### Email



### Identity



### Network





... **13 Jahre in Folge!**

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

#sophos #sophosMDR #csaas

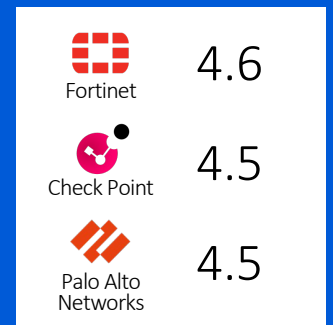
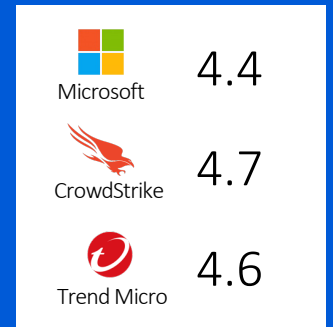
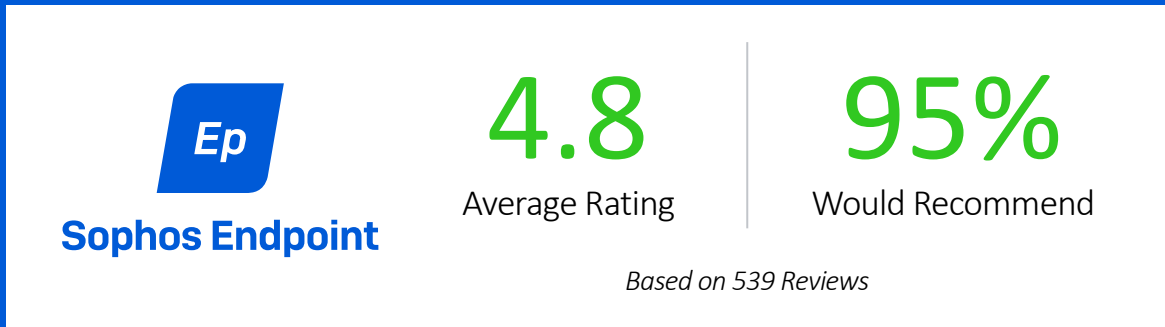
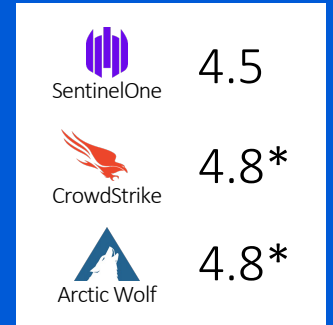
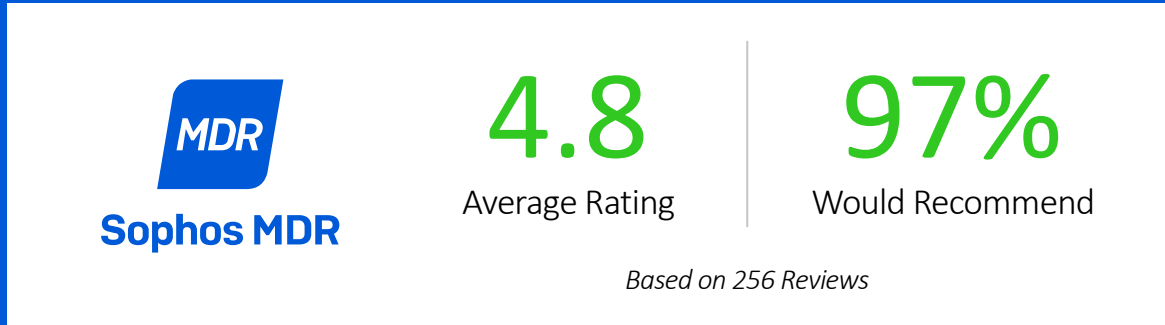
**Sophos ist ein  
Leader im**

**Gartner® Magic Quadrant™  
für Endpoint Protection  
Platforms.**

**SOPHOS**

# Gartner Peer Insights™

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



Reviews from last 12 months as of August 1, 2022

\*Vendors with fewer than 50 customer reviews

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

# 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

# Sophos Security Services

“Wurde bei mir eingebrochen?”



**Sophos Compromise Assessment**

“Bei mir wurde eingebrochen.  
Was mache ich jetzt?”



**Sophos Rapid Response**


“Ich möchte keinen Einbruch (mehr).  
Wie kann ich das verhindern?”



**Sophos MDR**

**Bei Ihnen findet gerade ein Cyberangriff statt?**

Unsere Incident-Response-Experten helfen Ihnen 24/7.  
Service sowohl für Sophos-Kunden als auch Nichtkunden verfügbar.

 **+49 611 711 867 66**

 **RapidResponse@sophos.com**

**Sofort-Hilfe erhalten**



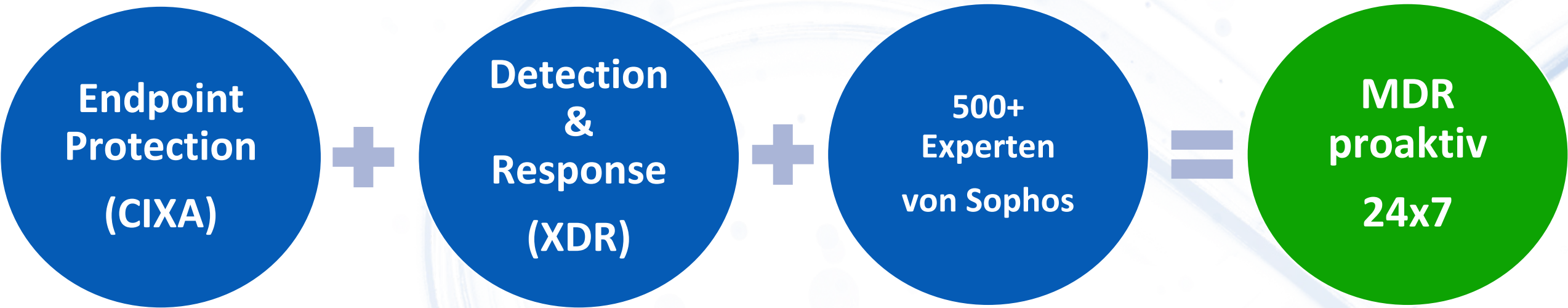
**SOPHOS**

# 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
<b>Tools</b>	<b>€ 40.945</b>	
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	
<b>Mitarbeiter</b>	<b>€ 752.000</b>	
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)	
<b>Prozess</b>		
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)	<b>€ 842.945</b>	<b>€ 38.572*</b>

Durchschnitts-  
gehälter von  
Glassdoor

\* Listpreise  
Sophos, 12 Monate

# ... sprechen wir über Geld

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



**SOPHOS**  
Cybersecurity delivered.