

**SOPHOS**



# **Sophos MDR** Managed Detection and Response

## **- Der Mehrwert erweiterter Telemetrie -**

Stefan Liß  
Senior Sales Engineer

Juni 2024



## TOP 3 URSACHEN FÜR BREACHES

### NICHT VERWALTETE GERÄTE

**80 %**

aller Ransomware-Verletzungen gehen von einem nicht verwalteten Gerät aus

### UNZUREICHEND GESCHÜTZTE GERÄTE

**74 %**

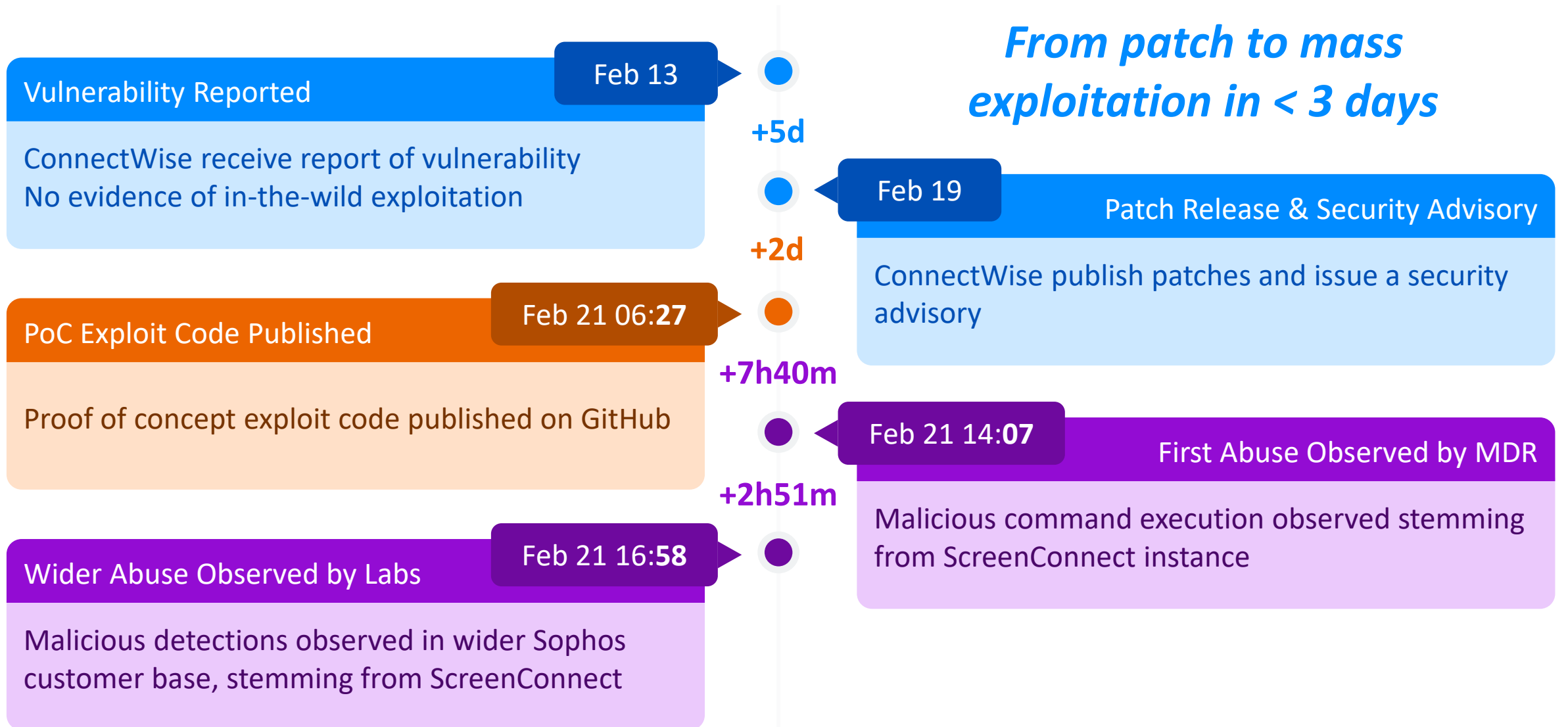
der Breaches sind auf den Menschen zurückzuführen, einschließlich Fehlkonfigurationen

### UNTERBESETZTES TEAM

**90 %**

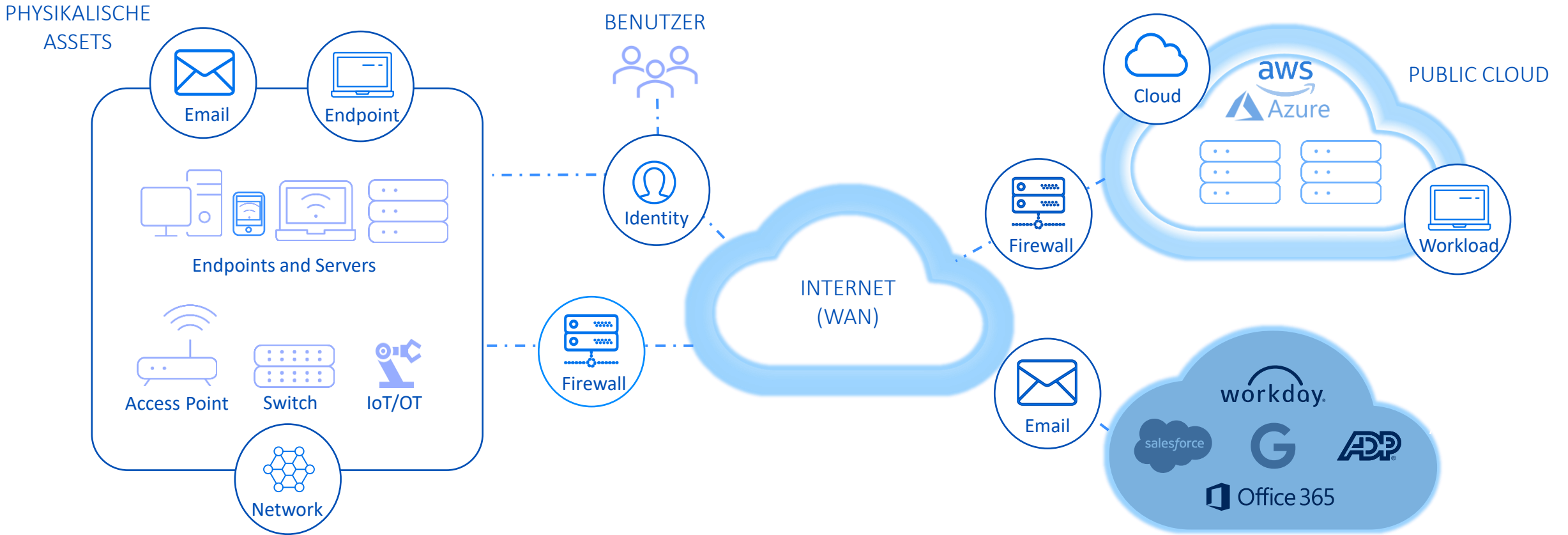
aller Ransomware-Angriffe beginnen außerhalb der normalen Geschäftszeiten

# ConnectWise ScreenConnect : Timeline



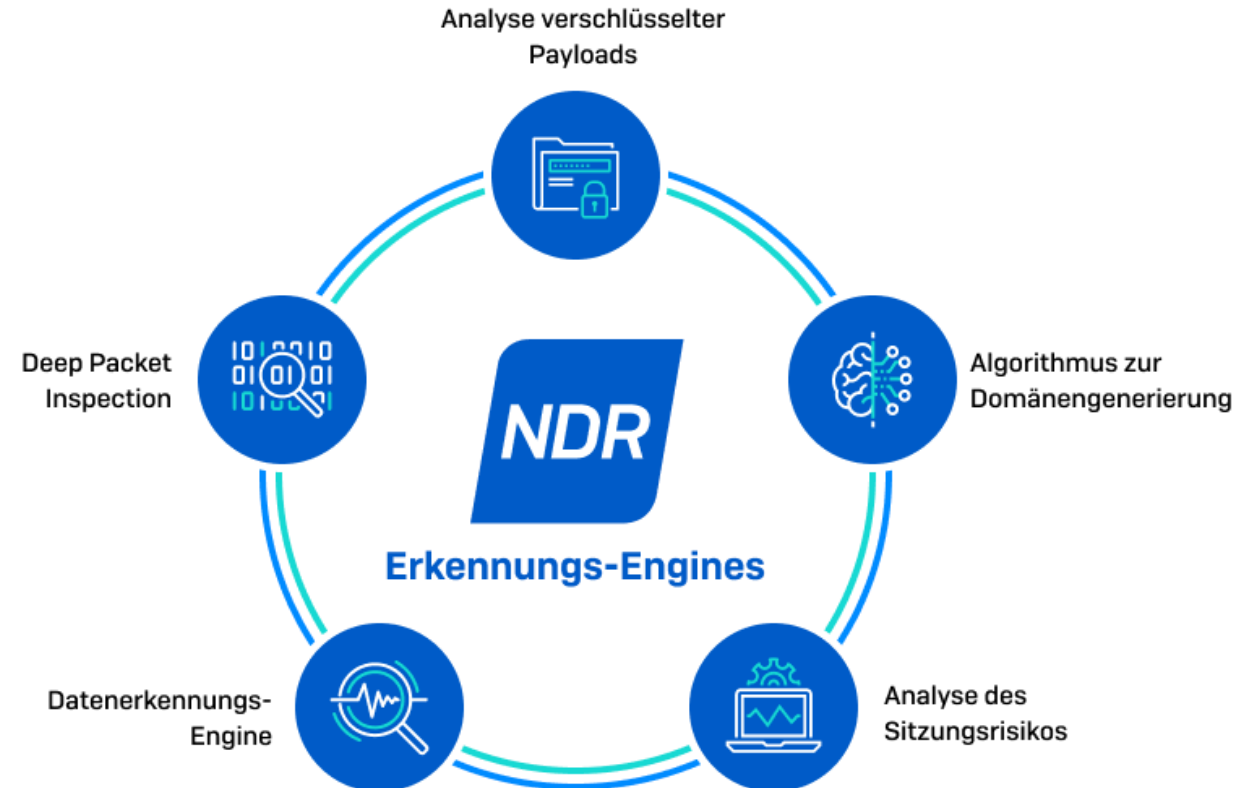
**Was kann ich tun?**

# „Sensoren“ verteilt in der gesamten Umgebung



# Network Detection and Response

-  Fremde und unbekannte Geräte
-  Angriffe auf IoT/OT
-  Lieferkettenangriffe
-  Insider-Bedrohungen
-  Versuchter Zugriff mit deaktivierten Accounts
-  Datenexfiltration via DNS oder Remote-Sitzungen



# Weitere Sensorik über 3<sup>rd</sup> Party Integrationen

**SOPHOS**  
✓ Integrations included

**Ep**  
Endpoint

**WP**  
Workload

**Mob**  
Mobile

**Cld**  
Cloud

**Fw**  
Firewall

**Em**  
Email

**ZT**  
ZTNA

**NDR**  
Network

**Endpoint**  
✓ Included

Microsoft **CROWDSTRIKE**

SentinelOne **TREND MICRO**

**Symantec** by Broadcom **BlackBerry** **CYLANCE**

+ Others with Sophos XDR Sensor agent

**Firewall**

**paloalto** NETWORKS **FORTINET**

**CHECK POINT** **CISCO Meraki**

**SONICWALL** **WatchGuard**

**Network**

**DARKTRACE**

**THINKST CANARY** **Securtec**

**Skyhigh** Security **CISCO Umbrella**

**Email**

Microsoft 365  
✓ Included

Google Workspace  
✓ Included

**mimecast**  
**proofpoint.**

**Productivity**  
✓ Included

Microsoft 365

Google Workspace

**Cloud**

**orca** security **aws**

**A** **Cloud**

**Identity**

Microsoft  
✓ Included

**okta** **auth0**

**CISCO DUO**

ManageEngine

**Backup and Recovery**

**veeam**

# Sophos X-Ops versorgt MDR mit führender Threat Intelligence

## Security Professionals

Die schnelle Einsatztruppe - Abfragen, Tools und Techniken vom CISO bis zur Frontline



## MDR SecOps Analysts

Erforschung neuer IOCs und Jagdmethoden, Wirkung in freier Wildbahn



**Sophos X-Ops**

500+ Experten

Bedrohungsinformationen, Analysen, Data Engineering, Data Science, Bedrohungsjagd, Verfolgung von Gegnern und Reaktion auf Vorfälle mit 6 globalen SOCs in jedem größeren Einsatzgebiet

## SophosLabs Researchers

Analysen von Dateien, E-Mails, Verhaltensweisen, URLs, IOCs und DPI



## Sophos AI Data Scientists

Entwicklung und Insights in fortschrittliche ML-Modelle, Automatisierung und Erkennung für MDR- und Sophos-Produkte



**Und wie sieht die Zusammenarbeit  
und die Reaktion aus?**

# Reaktion bei Bedrohungen

Autorisierte Kontakte

**Bedrohungsreaktion**

Kontoinformationen

## Bedrohungsreaktionsmodus

Legen Sie fest, wie wir auf aktive Bedrohungen reagieren sollen.

Zusammenarbeiten – Zusammenarbeit mit meinen Kontakten

Ich ermächtige das MDR-Team, Maßnahmen zu ergreifen, falls meine Kontakte nicht erreichbar sind und eine aktive Bedrohung besteht. (Für Details siehe die [Service-Beschreibung](#))

Autorisieren – Aktive Bedrohung beheben und meine Kontakte informieren (Hiermit wird das MDR-Team autorisiert, Maßnahmen zu ergreifen.)

# Threathunts



## Threat Hunt Report

Summary of threat hunts performed this month  
By Sophos MDR Adversarial Pursuit Team

Join us on the Sophos MDR ThreatCast - our monthly threat intelligence webinar

### Threat Hunt Outputs Last Month

17	5	4	6
MDR Detection Submitted	Labs Detection Submitted	Identified Activity Referred to MDR Operations	New Threat Hunt Idea

### MITRE ATT&CK Heatmap

Distribution of completed threat hunts across MITRE tactics.



There were **8** distinct ATT&CK Tactics observed across **30** threat hunts.

### Threat Hunts Completed Last Month

Hunt details with MITRE tactic and technique categorization.

#### Curl Sus Execution - Linux

ATT&CK Tactic	Execution
ATT&CK Technique	File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification (T1222.002)

This hunt focuses on identifying suspicious file download and execution activities on Linux systems, indicative of initial compromise stages or lateral movement by threat actors.

# MDR Beispielreport

## Timeline of Key Events (UTC)

The table below establishes the key events in the active incident timeline. Observed adverse to a MITRE Tactic highlighted in red, Sophos technology detections highlighted in blue, reported by the Sophos MDR team in green, and all other timeline notables highlighted in orange. For more information on the adversary behavior, refer to [MITRE ATT&CK Details](#) for the associated tactic.

Date (UTC)	Event	
2023-03-05 19:39	User 'USERNAME1' logged onto host 'HOSTNAME1' from an unmanaged device at IP <redacted> and saved the SAM hive to C:\temp\sam.save	
2023-03-05 19:40	User 'USERNAME1' observed initiating multiple recon/enumeration commands. User initiated 'net group "domain Admins" /domain'. Additionally observed: 'nltest /dclist:' and 'net view \\10.253'	
2023-03-05 19:43	User 'username1' accessed multiple files from C:\tmp\ via notepad.exe (example, TermServLicensing.bat, HOSTNAME5.txt, Print_Spooler.bat). Also observed file C:\Users\AUsername\Desktop\RegSrvr.xml accessed via notepad	<a href="#">Discovery</a>
2023-03-05 19:59	reg save HKLM\SYSTEM SystemBkup.hiv reg save HKLM\SYSTEM SamBkup.hiv	<a href="#">Credential Access</a>
2023-03-05 21:49	MDR escalated out of case <redacted> for credential dump activity on HOSTNAME5	Timeline Notable
2023-03-05 22:10	Partner responded to escalation from case <redacted> notifying MDR they were investigating	Timeline Notable
2023-03-06 08:21	Observed RDP from the remote IP '<redacted>' on the device 'HOSTNAME1' by the user 'username1'	<a href="#">Lateral Movement</a>
2023-03-06 14:31	Observed RDP from the remote IP '<redacted>' on the device 'HOSTNAME1' by the user 'username1'	<a href="#">Lateral Movement</a>
2023-03-06 14:40	User 'DOMAIN\username1'   C:\Program Files (x86)\AnyDesk\AnyDesk.exe installed by user 'USERNAME1' on host 'HOSTNAME3'	<a href="#">Command and Control</a>
2023-03-07 00:16	Partner responded to escalation from case <redacted> stating they were investigating	Timeline Notable

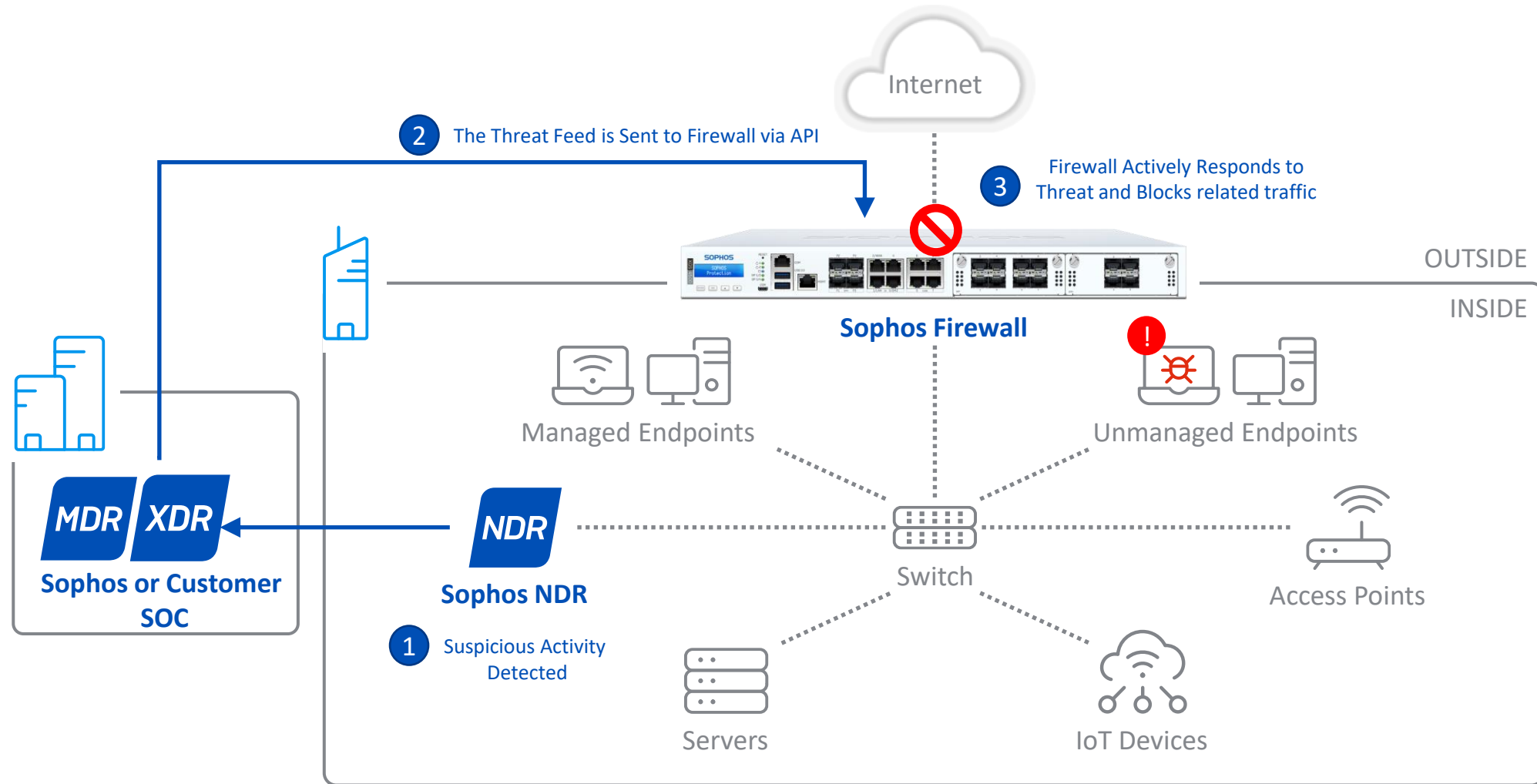
2023-03-07 10:15	Observed RDP from the remote IP '<redacted>' on the device 'HOSTNAME3' by the user 'username1'	<a href="#">Lateral Movement</a>
2023-03-07 10:25	Observed ntds dump on host "C:\Windows\system32\ntdsutil.exe" "ac in ntds" "ifm" "cr fu c:\programdata\abc" q q. with parent as C:\ProgramData\ntds.bat executed from AnyDesk.exe	<a href="#">Credential Access</a>
2023-03-07 10:26	Observed commands used to Dump Domain Password Hashes on host "HOSTNAME3" "C:\Windows\system32\ntdsutil.exe" "ac in ntds" "ifm" "cr fu c:\programdata\abc" q q	<a href="#">Credential Access</a>
2023-03-07 12:15	ping request initiated by user username1 to servers. ping HOSTNAME6 -n 1 ping domain.local -n 1	<a href="#">Discovery</a>
2023-03-07 20:24	'C:\Users\username1\Desktop\sys64.bat.bat' was created by user username1 with the following contents included in the file. 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f' 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f' 'reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" attrib -s -h %userprofile%\documents\Default.rdp del %userprofile%\documents\Default.rdp del /f /s /q /a %AppData%\Microsoft\Windows\Recent\AutomaticDestinations'	<a href="#">Execution</a>

# MDR Beispielreport

2023-03-10 02:32	Partner updates Customer Name's response mode from 'Collaborate' to 'Authorize' allowing the MDR team to perform response actions	Timeline Notable
2023-03-10 02:36	MDR adds hashes for 'AnyDesk.exe' to blocked items in Sophos Central	Response Action
2023-03-10 04:27	MDR adds hashes for 'sys.exe' to blocked items in Sophos Central	Response Action
2023-03-10 05:09	MDR adds hashes for 'ISL Light.exe' to blocked items in Sophos Central	Response Action
2023-03-10 05:12	MDR adds hashes for 'AdFind.exe' to blocked items in Sophos Central	Response Action
2023-03-10 05:15	MDR adds hashes for 'PSTools.zip' to blocked items in Sophos Central	Response Action
2023-03-10 05:26	MDR adds hashes for 'ProcessHacker.exe' to blocked items in Sophos Central	Response Action

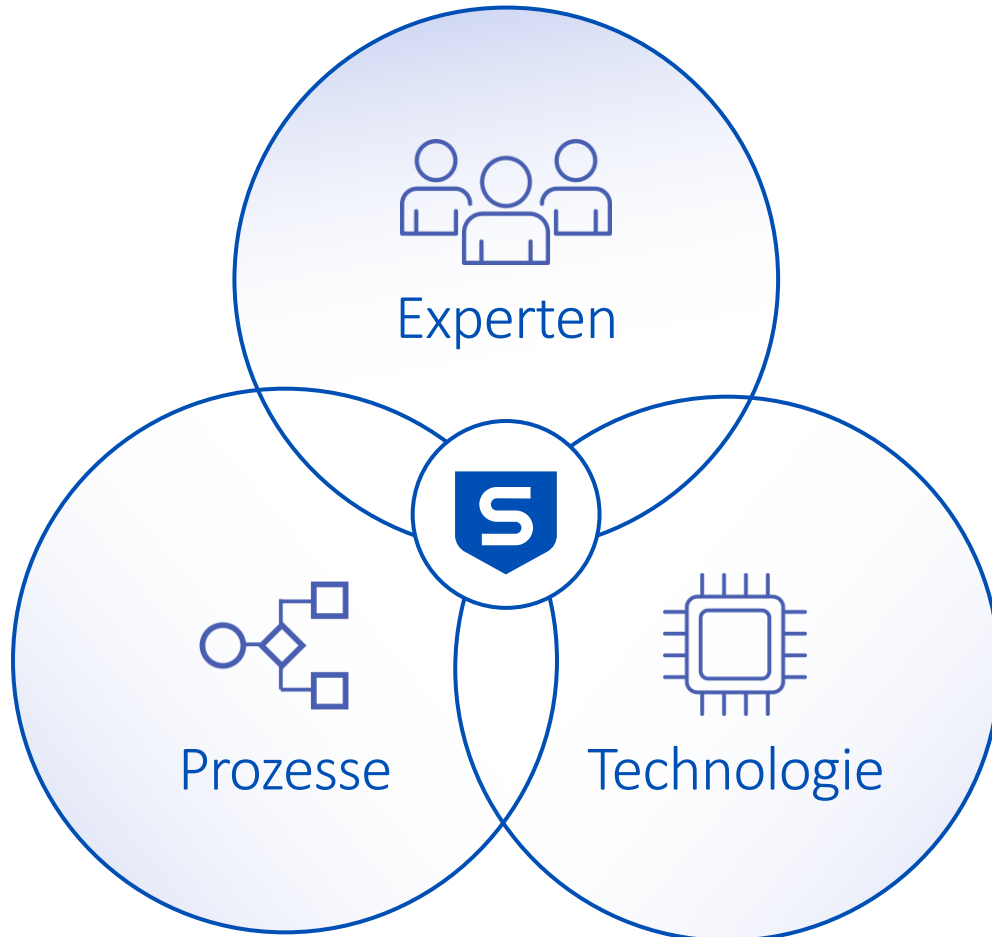
2023-03-10 05:46	Folder and Files were removed from host 'HOSTNAME1': C:\New folder\2.xml C:\New folder\netscan.exe C:\New folder\netscan.lic C:\New folder\netscan.xml C:\New folder\oui.txt	Response Action
2023-03-10 08:00	'AnyDesk' and 'ISL Online' processes killed. Files and services were removed on host 'HOSTNAME3'	Response Action
2023-03-10 08:05	'AnyDesk' and 'ISL Online' related files removed on host 'HOSTNAME2'	Response Action
2023-03-10 08:08	'AnyDesk' and 'ISL Online' related files removed on host 'HOSTNAME7'	Response Action
2023-03-10 08:35	'C:\README.TXT' was removed throughout the estate per Partner's request	Response Action
2023-03-10 08:39	'C:\Users\username1\Desktop\README.TXT' and 'C:\Users\Public\Desktop\README.TXT' were removed throughout the estate per Partner's request	Response Action
2023-03-10 09:15	MDR adds hashes for 'netscan.exe' to blocked items in Sophos Central	Response Action
2023-03-10 16:32	'C:\Users\username1\Desktop\sys64.bat.bat' was removed from host 'HOSTNAME3'	Response Action
2023-03-10 16:52	'C:\Users\username1\AppData\Local\Temp\85\Isass.DMP' was removed from host 'HOSTNAME2'	Response Action
2023-03-10 17:05	'C:\Program Files (x86)\ISL Online\ISL AlwaysOn\ISLAlwaysOnService.exe' process was terminated via PID: 3188 on host 'HOSTNAME1'	Response Action
2023-03-10 17:08	'C:\Program Files (x86)\ISL Online\ISL AlwaysOn\ISLAlwaysOnService.exe' was removed from host 'HOSTNAME1'. File was still present on the host queried as of March 11 <sup>th</sup> 2023	Response Action
2023-03-10 19:27	'C:\Users\username1\AppData\Local\Microsoft\Windows\WinX' was deleted from host 'HOSTNAME2'	Response Action
2023-03-10 19:31	File 'C:\programdata\ISL Light.exe' was removed from host 'HOSTNAME2'	Response Action
2023-03-10 19:32	Folder 'C:\programdata\anydesk\' was deleted from host 'HOSTNAME2'	Response Action
2023-03-10 19:33	Session: disconnected session (ID 85) for user 'USERNAME1' was terminated on host 'HOSTNAME2'	Response Action

# Weitere Response-Aktion: Active Threat Response



**NDR + MDR/XDR + Firewall = Immediate Response - No Firewall Rule Configuration Required**

# SOPHOS MDR – Ihr Boxenteam für schnelle Entscheidungen



- ✓ Proaktive Bedrohungssuche
- ✓ 24/7 Erkennung und Reaktion durch Analysten
- ✓ Vollständige Ursachenanalyse + Incident Response
- ✓ Mehr als 22.000 MDR Kunden
- ✓ Telemetrie von mehr als 600.000 Unternehmenskunden
- ✓ All-inclusive Service – keine versteckten Kosten
- ✓ Bestmögliches Ergebnis für Ihre IT-Sicherheit

# Jetzt informieren



## Sophos MDR

24/7 Schutz vor Cyberangriffen – mit Ihrem persönlichen MDR-Service:  
Weitere Informationen zu unserer Lösung Sophos MDR erhalten Sie auf unserer Produktseite.

[sophos.de/mdr](https://sophos.de/mdr)



## Sophos NDR

NDR ermöglicht es Sophos XDR sowie MDR-Kunden von zusätzlicher Telemetrie zu profitieren, um noch frühzeitiger auf Angriffe zu reagieren zu können.

[Zur Community](#)



## Herstellerübergreifende Telemetrie-Analyse

Erfahren Sie, wie durch die Integration von Daten und Telemetrie aus Sicherheitslösungen von Drittanbietern Sophos MDR Bedrohungen besser und schneller erkennen und beseitigen kann.

[Zum Sophos Blog](#)



## Sophos Retainer

Der Sophos Incident Response Retainer ermöglicht bei Bedarf den Zugriff auf Sophos Incident Response Experten, um aktive Angriffe zu stoppen und den normalen Betrieb wiederherzustellen.

[sophos.com/retainer](https://sophos.com/retainer)



**SOPHOS**  
Defeat Cyberattacks