



Cybersecurity – aber Wo anfangen ?

Ronny Globisch
Senior Sales Engineer

SOPHOS

Fürchten Sie sich davor?



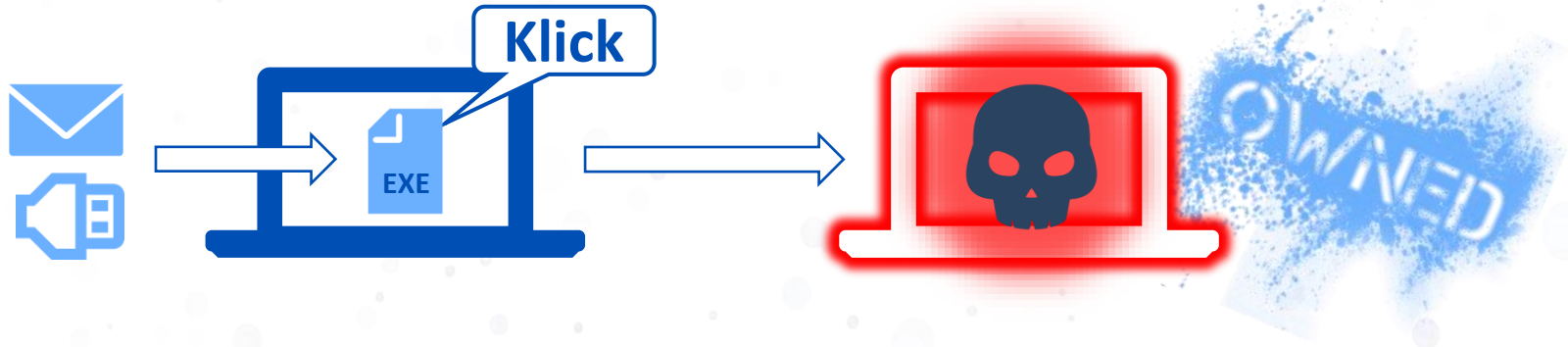
Hacker vor 5 Jahre



Hacker heute

Evolution der Bedrohungen

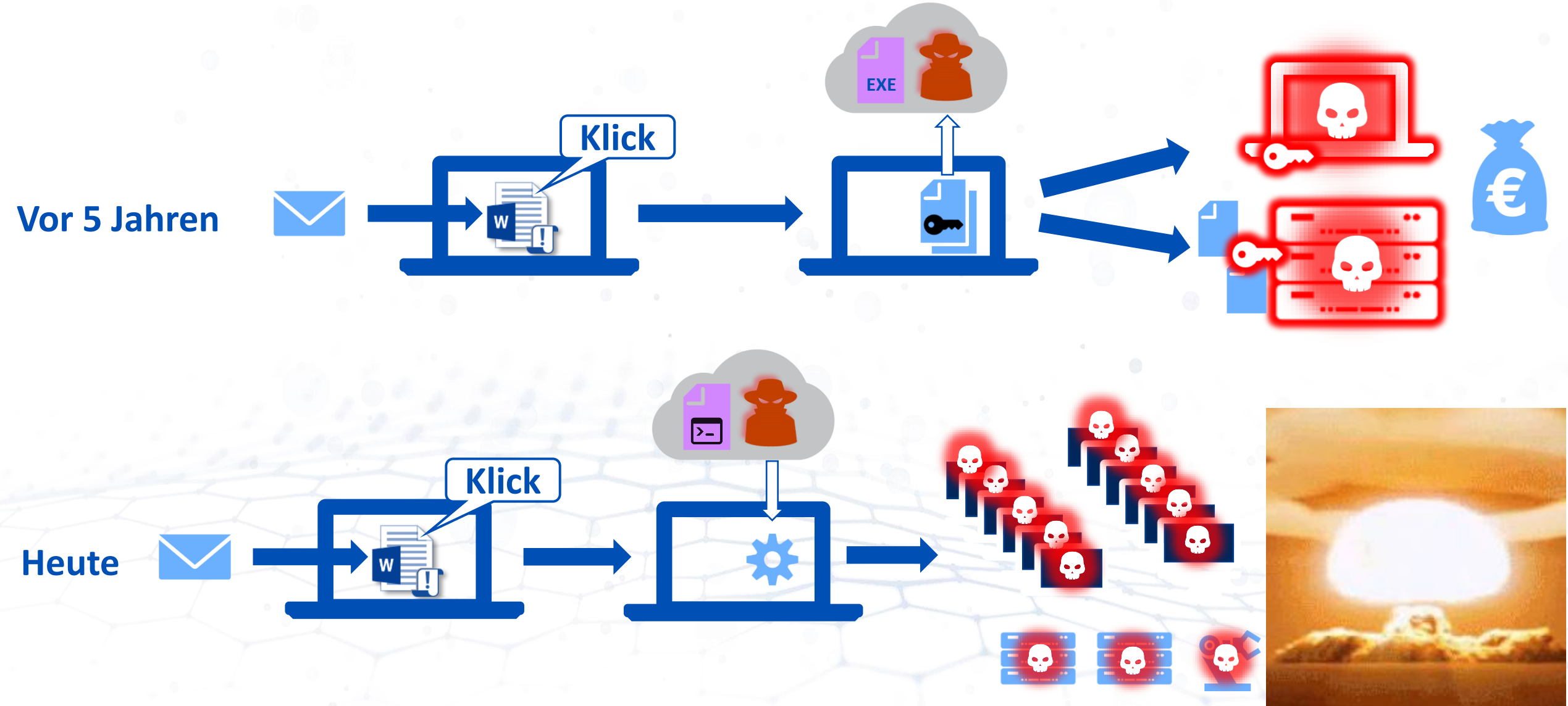
Vor 20 Jahren



Vor 10 Jahren



Evolution der Bedrohungen



Entwicklung

Anzahl der
Cyberattacken
nimmt zu.

Angriffe werden
raffinierter und
schneller.

61%

Mehr
Cyberangriffe als
im letzten Jahr

46%

Organisationen
mit Ransomware
angegriffen

54%

Angriffe zu
komplex für das
IT-Team

Todesfa

Ransomware Wie Erpres Corona-Ka

Auf der Corona-Deuts
Ludwigslust-Parchim
Wiederherstellung wi

17.11.2021, 10.31 Uhr

245

LESEN
SIE
AUCH



Autovermietung Hackera Kunden

Der Autovermiet
Details sind noc

02.05.2022, 17.05 UI

Nach Hackerangriff

Wie Sixt seine IT-Probleme schönredet

Sixt hat einen Cyberangriff frühzeitig eingedämmt – vor zwei Wochen. Folgenlos blieb die
Angriffe aber nicht, so sehr das Unternehmen auch versucht, diesen Eindruck zu erwecken.

Von **Markus Böhm**, **Jörg Breithut** und **Max Hoppenstedt**

16.05.2022, 12.45 Uhr

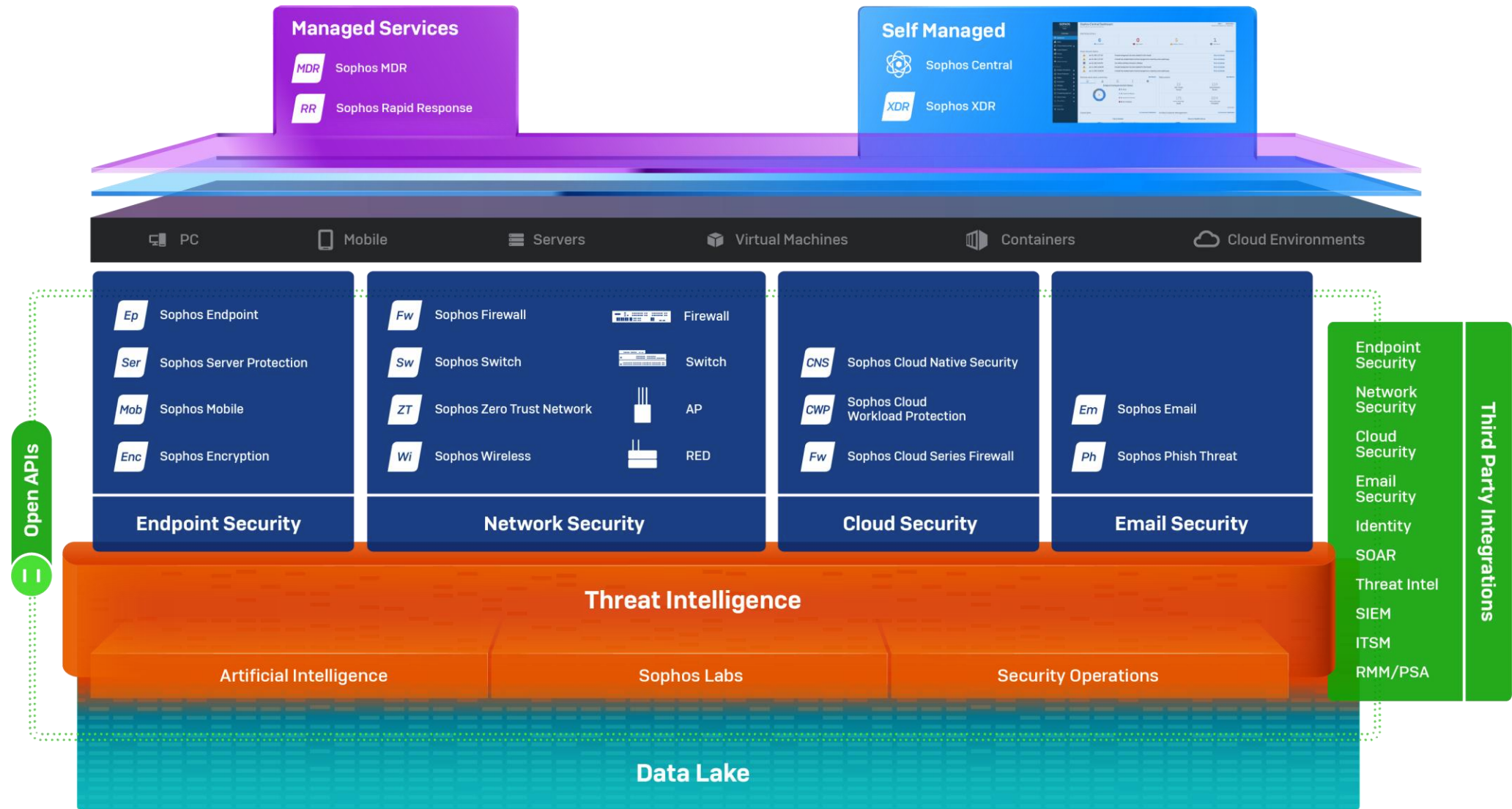


Corona-Karte des RKI: Für Ludwigslust-Parchim fehlen die Daten Foto: RKI

Cybersecurity – heute !

- komplex
- Reaktiv
- Unübersichtlich
- inkompatibel
- usw...

Adaptive Cybersecurity Ecosystem - ACE



Wer sagt, dass ich das wirklich brauche?

- Cyberrisikenversicherer
- DSGVO
- Regulierungsbehörden
- Während eines Vorfalls:
Jeder wünscht, es wäre schon da gewesen

Bundesverband IT-Sicherheit e.V.



IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

technischer und organisatorischer Maßnahmen

2021

3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

- Malware
- Exploitation
- Maliziöse Scripte
- Hacker-Aktivitäten
- Missbrauch von Administrativen Werkzeugen und Tools in schädlicher Absicht

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

EDR-Plattformen kombinieren wirksame Detektions- und Präventionstechniken, um die Kompromittierung von Clients und Servern, auch über Computer und Betriebssystemgrenzen hinweg, zu verhindern und sogar aktive Angreifer in Computernetzen zu enttarnen.

Endpoint Detection & Response

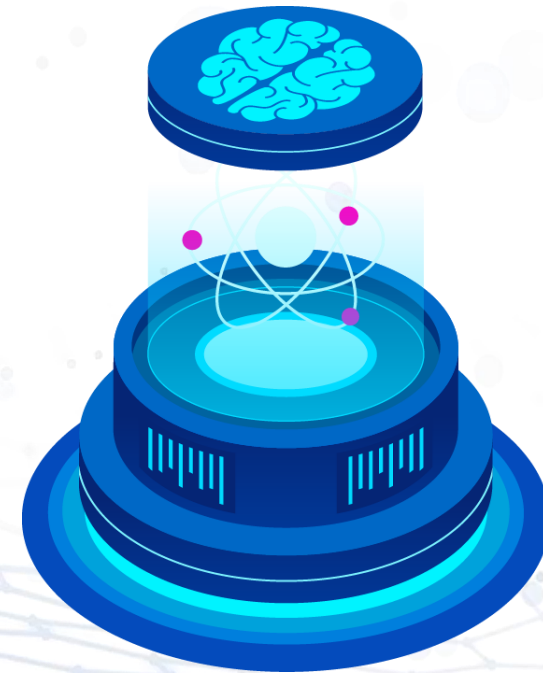


Prävention optimieren

Angriffsfläche reduzieren



Verhindern, dass Angriffe
ausgeführt werden



eXtended Detection & Response



Stoppen Sie mehr Bedrohungen schneller



**PRÄVENTION
OPTIMIEREN**



**MINIMIEREN SIE DIE
ZEIT ZUM ERKENNEN
UND REAGIEREN**

Sensoren in jedem Bereich





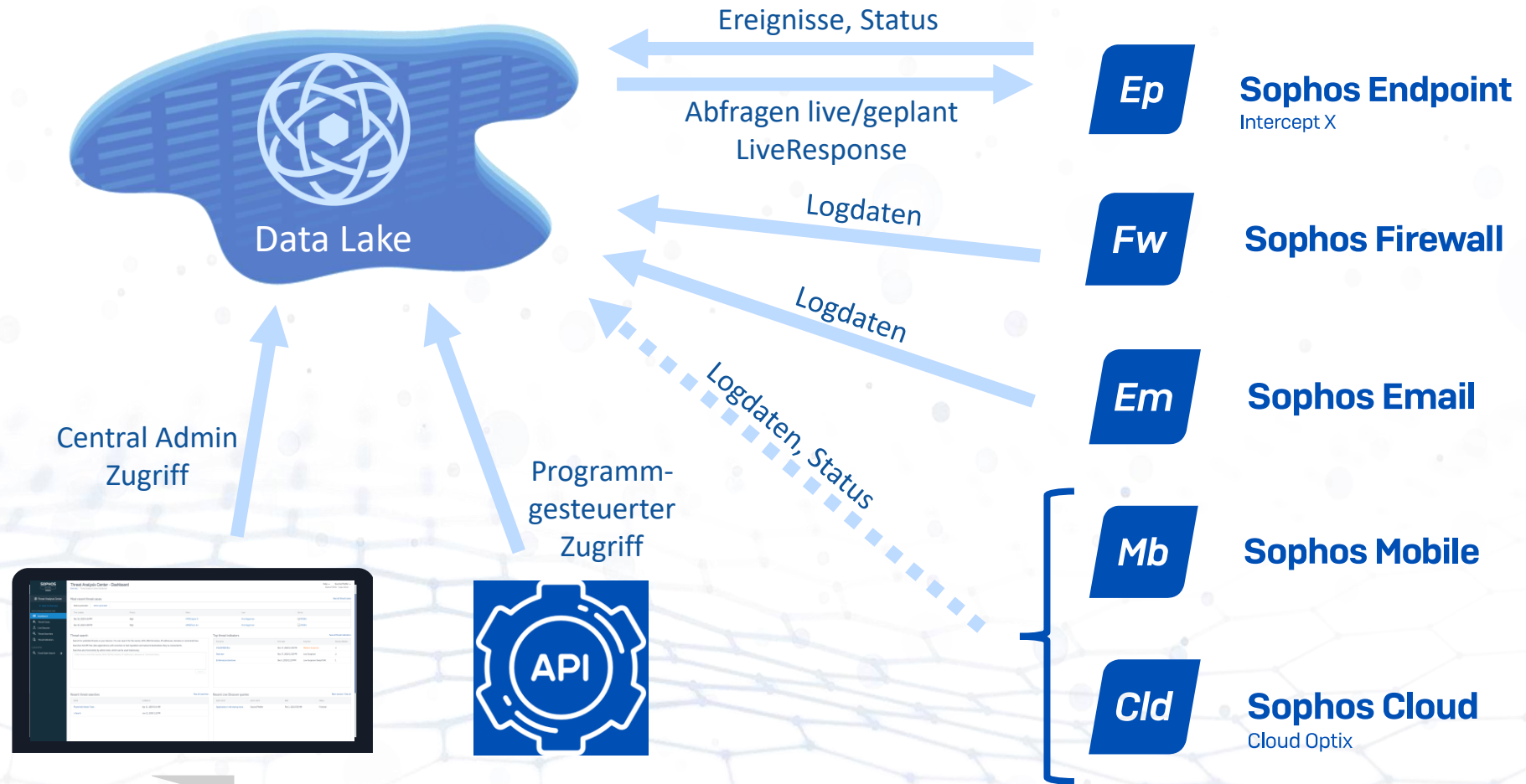
Endpoint Detection and Response (EDR)

Extended Detection and Response (XDR)

XDR – Endpoints/Server + Firewall + Email +..

Intercept X with EDR
Data Lake 7 Tage frei

Central XDR
+30 Tage Daten im Data Lake
+ Zugriff auf Central Firewall Reporting Daten und weitere Produkte



Ursachenanalyse vs. XDR

SOPHOS
CENTRAL
Admin

Bedrohungsanalyse-Center - CryptoGuard
Übersicht / Bedrohungsanalyse-Center Dashboard / Entdeckte Bedrohungsfälle / CryptoGuard

Hilfe Michael Veit
Michael Veit - Super-Admin

Win10-ArthurD
172.17.150.186

Hauptursache
outlook.exe

Beacon
ransomware.exe

Erkannt
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 Andere Dateien Geschäftsdateien Netzwerkverbindungen

Ursachenanalyse

XDR

Threat Hunting: Firewall meldet ATP-Kommunikation..

Firewall AT

src_ip

172.17.150.189

172.17.150.189

172.17.150.186

URL-Aktivität

epName

Win10Pro-Michael

Win10Pro-Michael

Win10Pro-Michael

Win10Pro-Michael

Win10Pro-Michael

Win10Pro-Michael

Win10Pro-Michael

Analysieren | Falldatensatz

Filter: Prozesse Andere Dateien Geschäftsdateien Netzwerkverbindungen Registrierungsschlüssel

Direkten Pfad anzeigen

Hauptursache Beacon Unsichere Reputation

Suchen

Name	Typ	Reputation	Protokollierte Uhrzeit:	Interaktionen:
unknown.exe	Prozess	Unsichere Reputation	26. Mai 2021 10:02	51

te Geräte

username

SYSTEM

SYSTEM

SYSTEM

michael

michael

michael

michael

michael

michael

michael

Name	Typ	Reputation	Protokollierte Uhrzeit:	Interaktionen:
Win10Pro-Michael	Prozess	Unsichere Reputation	26. Mai 2021 08:02:24	51
Win10Pro-Michael	Prozess	Unsichere Reputation	26. Mai 2021 08:02:24	51

Sophos XDR: Anwendungsbeispiele



Schatten-IT

-> welche Geräte in meinem Netzwerk sind nicht verwaltet oder ungeschützt?

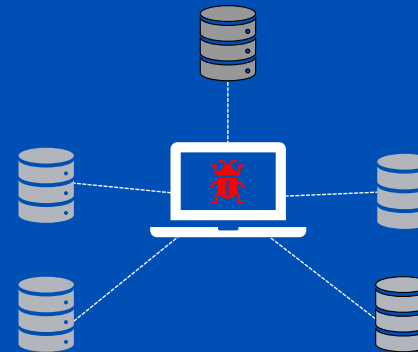


ATP-Erkennung auf Firewall Ebene

-> was ist davor auf dem Endpoint/Server passiert?



Sind unsichere Versionen von Software installiert – und wurde das bereits ausgenutzt?



Ein Client mit einer Ransomware-Erkennung wird automatisch im Netzwerk isoliert

KI identifiziert verdächtige Ereignisse

SOPHOS

CENTRAL

Admin

Bedrohungsanalyse-Center

Zurück zur Übersicht

ERKENNUNG UND BESEITIGUNG

Dashboard

Bedrohungsgraphen

Live Discover

Erkennungen

CLOUD OPTIX

Cloud-Optix-Suche

Erkennungen

Bedrohungsanalyse-Center Dashboard

Hilfe Michael Veit

Michael Veit · Super-Admin

Filter anzeigen

9 angewendet

Letzte Stunde

Letzte 24 Stunden

Letzte 7 Tage

Letzte 30 Tage

Risiko	Anzahl	Kategorie	MITRE ATT&CK	Geräteleiste	Erstmals aufgetreten	Letztmalig aufgetreten	Beschreibung	Klassifizierungsregel
5	2	Threat	Execution PowerShell	Win10Pro-Michael	30. Nov. 2021 10:17:49	30. Nov. 2021 10:26:33	The PowerShell cmdlet Start-BitsTransfer can be used to start a Background Intelligent Transfer Service (BITS) job. This can be utilized...	EQL-WIN-EXE-PRC-POWERSHELL-...
2	1	Threat	Discovery System Information Discovery	Win10Pro-Michael	-	30. Nov. 2021 10:21:52	Gpresult is used to enumerate domain policies.	EQL-EXEC-gpresult.exe
8	5	Threat	Execution PowerShell	Win10Pro-Michael	30. Nov. 2021 09:41:22	30. Nov. 2021 10:17:49	PowerShell is downloading unknown data which can be executed.	EQL-COMMAND-b9b3df2c6627e9b...

Erkennungszeitpunkt: 30. Nov. 2021 10:17:49

Gerät: Win10Pro-Michael

Typ: computer

IPv4-Adresse: 172.17.150.189

Standort: Zornheim, Rheinland-Pfalz, Germany

Betriebssystem: Microsoft Windows 10 Pro

Angemeldeter Benutzer: michael

Prozess: procdump64.exe

Pfad: C:\Users\Public\temp\procdump64.exe

Prozessbesitzer: michael

Signatur-Info:

SophosPID: 7032:132827371804127956

SHA256: 1a107c3ece1880cbbdc0a6c0817624b0dd033b02ebaf7fa366306aaca22c103d

Sophos-Machine-Learning-Wert: Nicht bewertet [-1]

SophosLabs-Intelix-Bedrohungswert: Vertrauenswürdige Anwendung [78]

Übergeordneter Prozess: powershell.exe

Übergeordneter Pfad: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Übergeordnete SophosPID: 424:132827371789154957

Befehlszeile: "C:\Users\Public\temp\procdump64.exe" -accepteula -ma lsass.exe

Sophos Lösungen und Services

Schutz

+

Detection & Response



Do it yourself?



Werkzeug



EDR (Endpoint Detection and Response) ist ein ganzheitlicher Ansatz der Endpoint/Server Sicherheit

XDR (eXtended Detection and Response) ermöglicht produktübergreifende Korrelation von Ereignissen

Denken Sie, was ich denke?

- Wow, das ist echt ein mächtiges Werkzeug
- Ich wusste gar nicht, was alles möglich ist
-

Wer, Wie und Wann ???

Managed Detection & Response



Sophos Lösungen und Services

Schutz

+

Detection & Response



Do it yourself?



Werkzeug



EDR (Endpoint Detection and Response) ist ein ganzheitlicher Ansatz der Endpoint/Server Sicherheit

Outsourcing?



+ Service

Managed
Detection &
Response



Managed Detection & Response

Modernste Schutztechnologien

Workstations und Servern

24/7 Angriffserkennung

24/7 Stoppen und Bereinigung von Bedrohungen

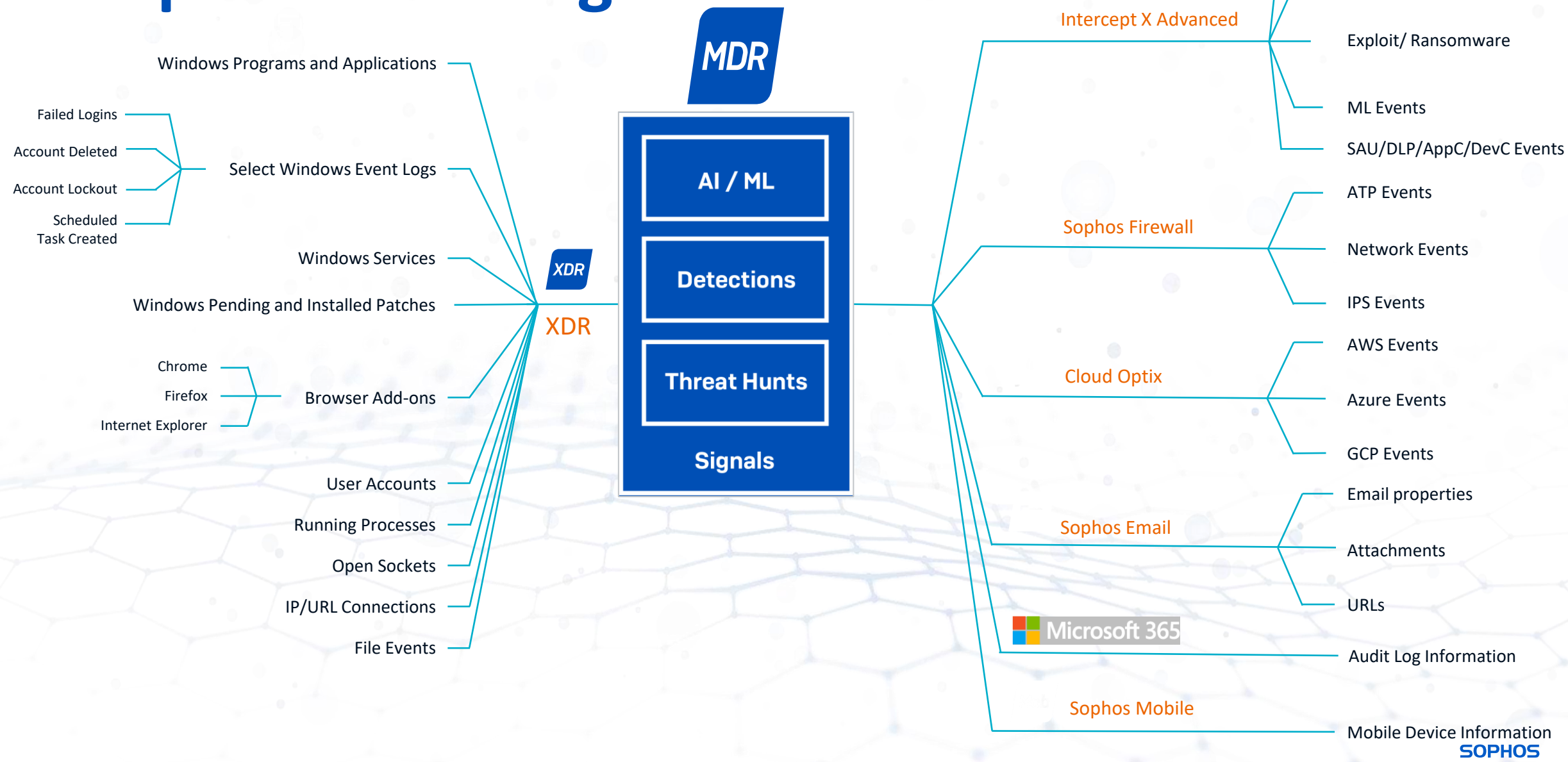
24/7 Threat Hunting

Proaktive Verbesserung der Sicherheit



Rundum-sorglos-
Service zur Abwehr
vor Cyber-Kriminellen

Datenquellen und Signale für MTR



24/7 Erkennung und Reaktion auf Vorfälle



Schutz

99.98% der Gefahren werden blockiert¹



Erkennung

Durchschnittliche Erkennungszeit < 1 Minute



Untersuchung

Durchschnittliche Untersuchungsdauer 25 Minuten



Reaktion

Durchschnittliche Bereinigungsdauer 12 Minuten

- Bestmöglicher Schutz
- Reduziertes Risiko
- Kosteneffizienz
- Ruhiger Schlaf

Zusammenarbeit mit dem - Team



Benachrichtigung

Sophos: „Auf diesen 10 Rechnern haben wir einen Angriff mit folgenden Aktivitäten festgestellt.“

Kunde: „Danke, wir übernehmen.“



Zusammenarbeit

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!“



Autorisierung

Kunde: „Sophos, bitte stoppt jeden eindeutigen Angriff!“

Sophos: „Wird gemacht.“

MDR Reports & Benachrichtigungen

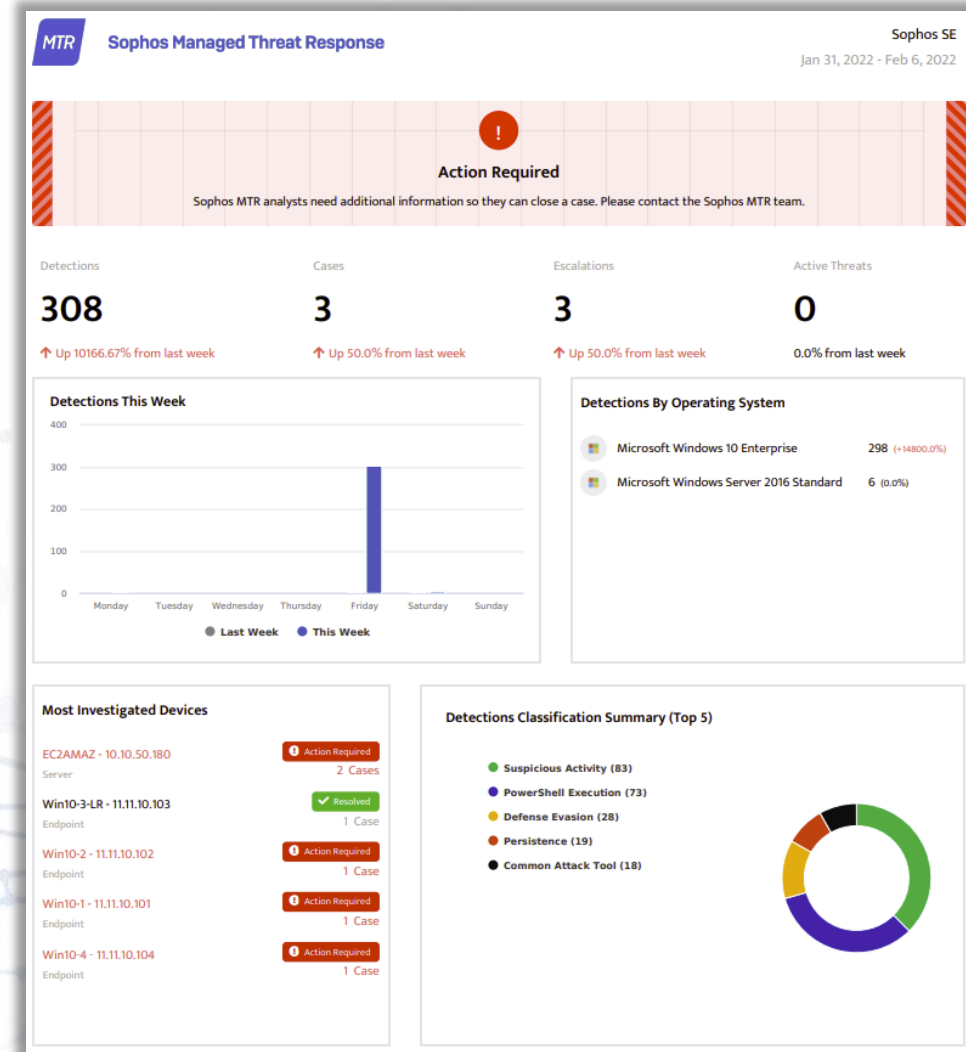


- Automatische Erstellung von Reports

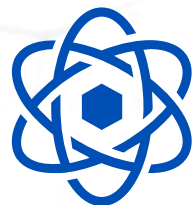
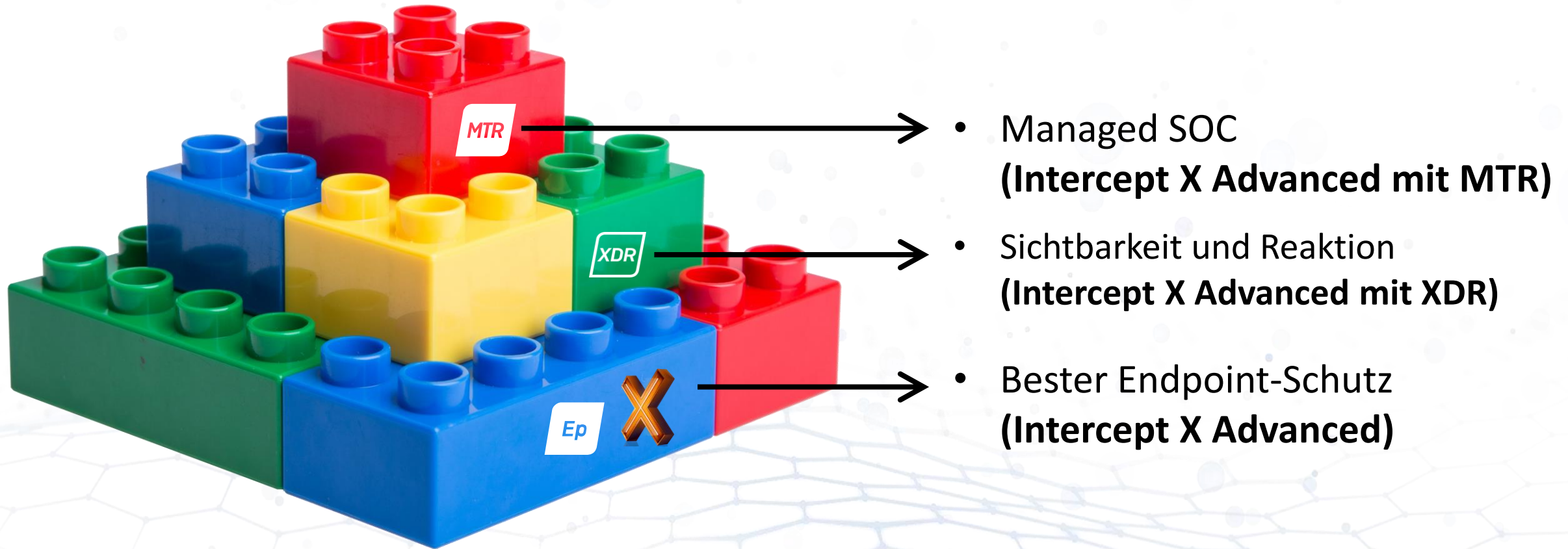
- Monatlich
- Wöchentlich

- MDR Team sendet Benachrichtigungen bei besonderen Ereignissen

- Log4Shell
- ProxyLogon
- ProxyShell
- ...



Sophos ACE - Funktionspyramide



Sophos Central

XDR 3rd Party Integrations - Zukunft

Firewall Connector

- Palo Alto Networks
- Fortinet
- Cisco

Cloud Connector

- Azure
- AWS
- Google Cloud

Endpoint Connector

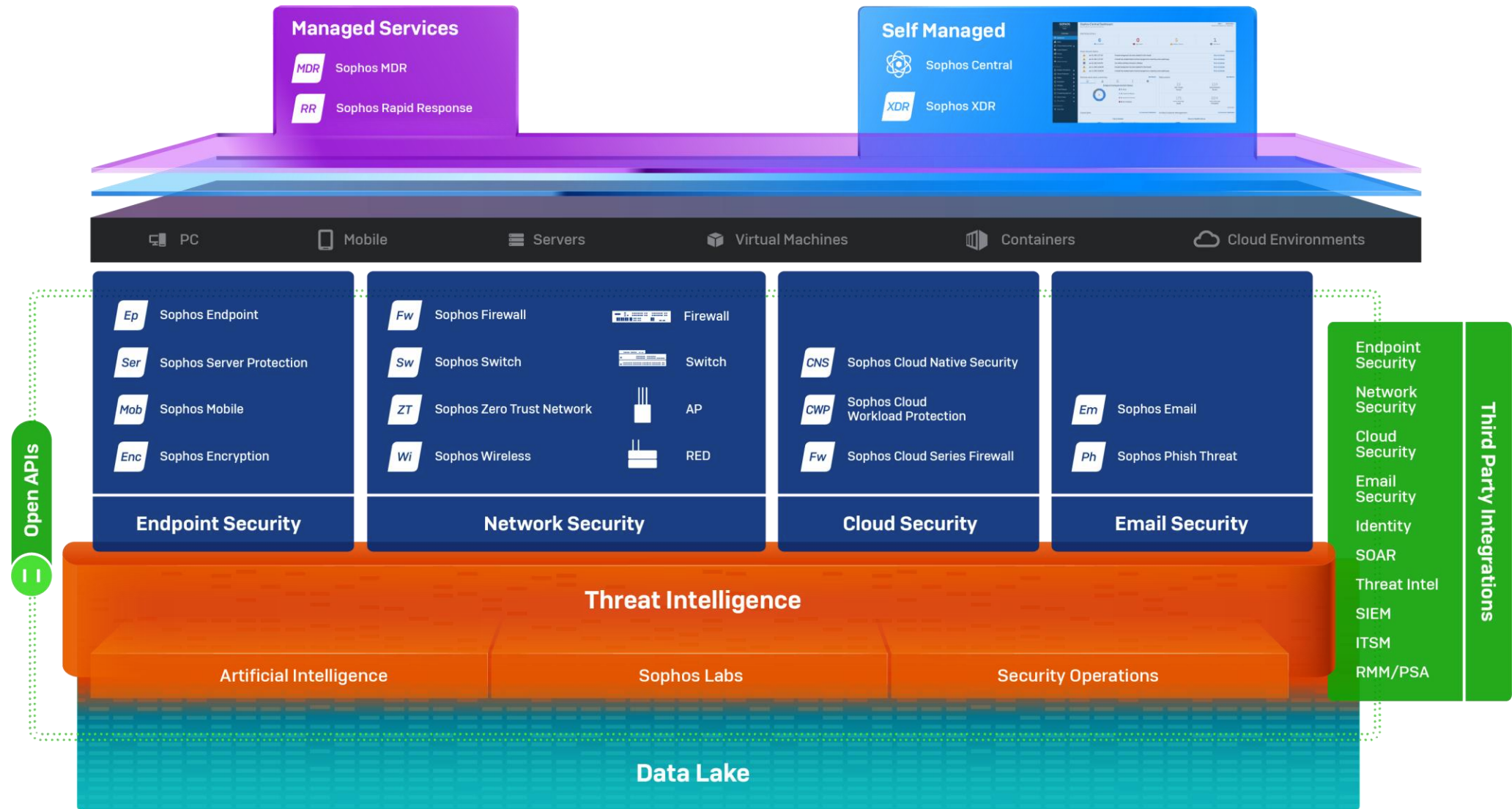
- Microsoft
- McAfee
- Symantec

Email Connector

- Microsoft
- Trend Micro
- Proofpoint



Adaptive Cybersecurity Ecosystem - ACE



Sophos Rapid Response

Blitzschnelle Unterstützung bei
aktiven Bedrohungen durch ein
weltweites Expertenteam von
Spezialisten

rapidresponse@sophos.com
+49 611 711 86766



SOPHOS