SOPHOS

Die NIS2-Herausforderung meistern

Effektives Risikomanagement mit Managed SOC

Michael Veit
Manager Sales Engineering, SOPHOS

Oktober 2024

Warum betrifft mich NIS2?

- Meine Organisation fällt unter NIS2
- Ich bin Zulieferer für eine Organisation, die unter NIS2 fällt
- Weder noch – aber ein Angriff auf mich wird wahrscheinlicher

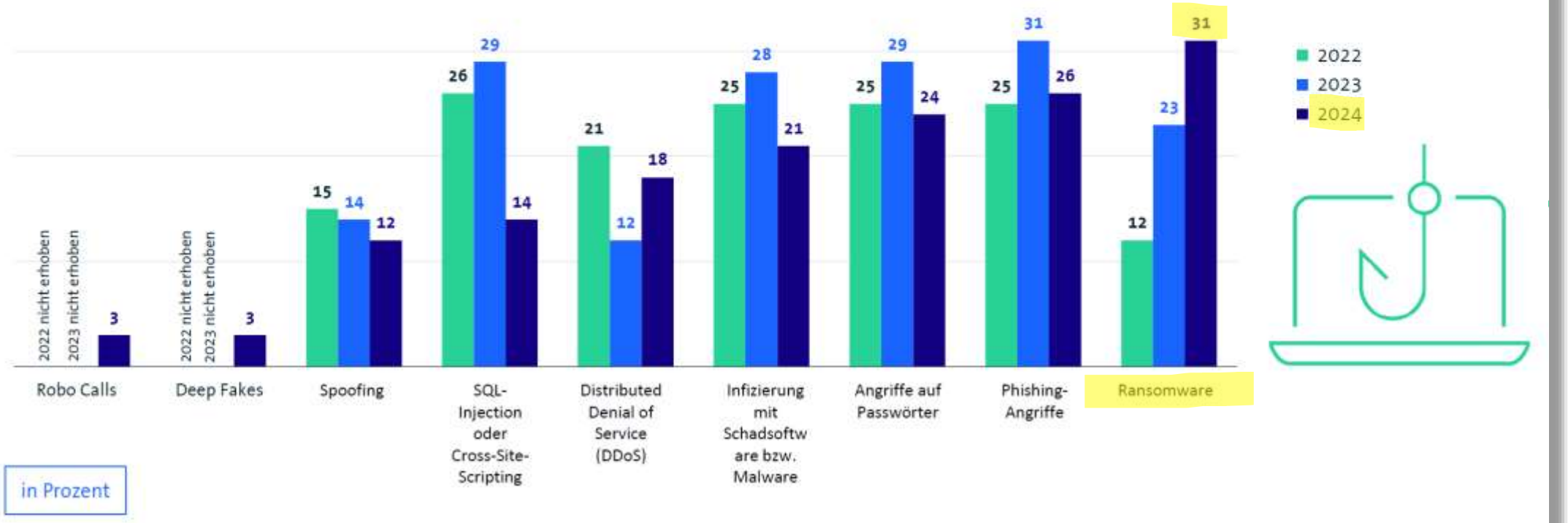
bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024

bitkom

Themen Daten Events Presse Mediathek Bitkom Karriere Mitgliedschaft

Ransomware verursacht häufiger Schäden

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?



in Prozent

Quelle: Dr. Ralf Wintergerst, Bitkom-Präsident im August 2024 (https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf)
Datenbasis: Unternehmen in Deutschland mit mindestens 10 Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr

SOPHOS

Wieso werden Organisationen gehackt?

Flughafen Leipzig im Mai 2024

Mainstream Support Ende 2011
Extended Support Ende 2016

Pflichten nach NIS2

Registrierungspflichten

Risikomanagement-maßnahmen

Nachweispflichten

Meldepflichten

Informationspflichten

Unterrichtungspflichten

Risikomanagementmaßnahmen

Technisch

- Technische Kontrollen
- Verschlüsselung
- Lieferkettensicherheit
- Sicherheitsupdates und Patch-Management
- Multifaktor-Authentifizierung

Organisatorisch

- Richtlinien
- Notfallpläne und Konzepte
- Business Continuity
- Incident Management
- Awareness-Programme

Operativ

- Sicherheitsüberprüfungen
- Risikobewertung
- Dokumentation und Reporting

Kommt Ihnen das bekannt vor?

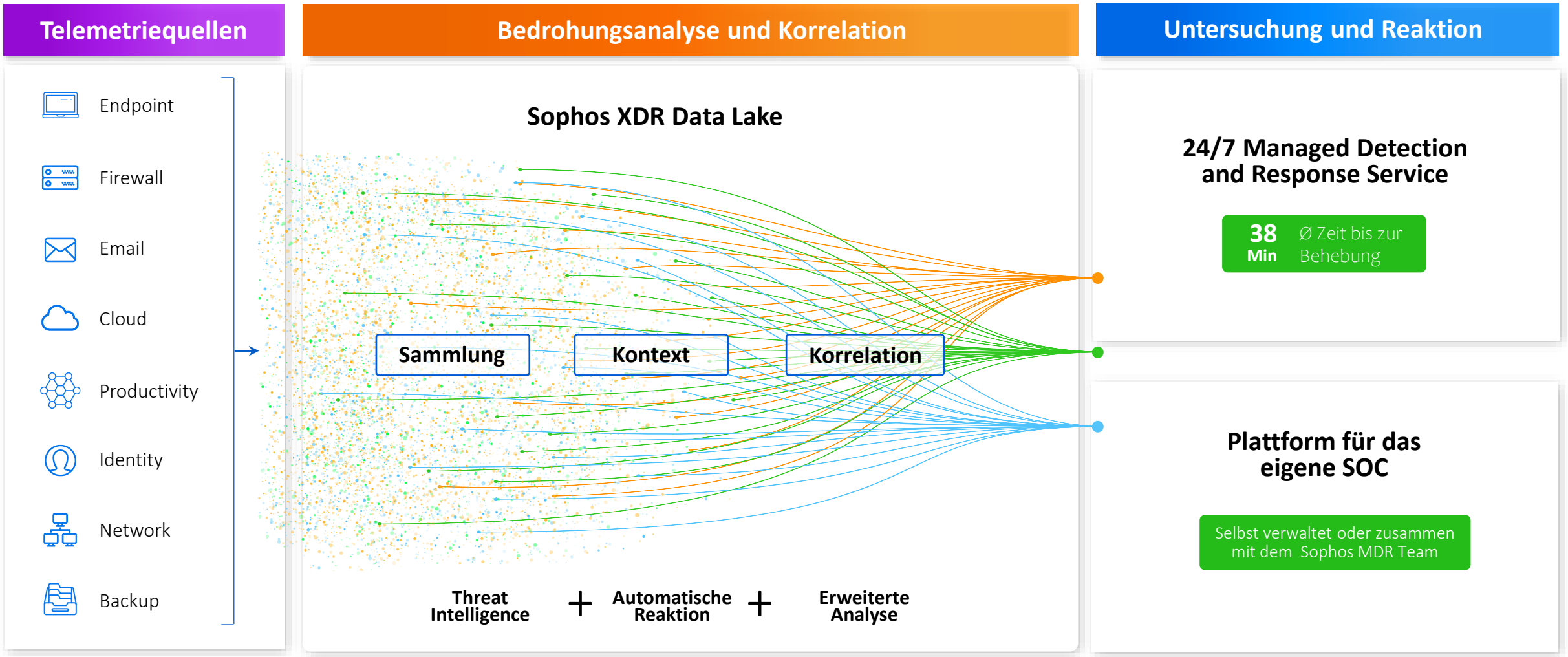
Was kann ich tun?

Warum brauche ich nochmal Telemetrie?

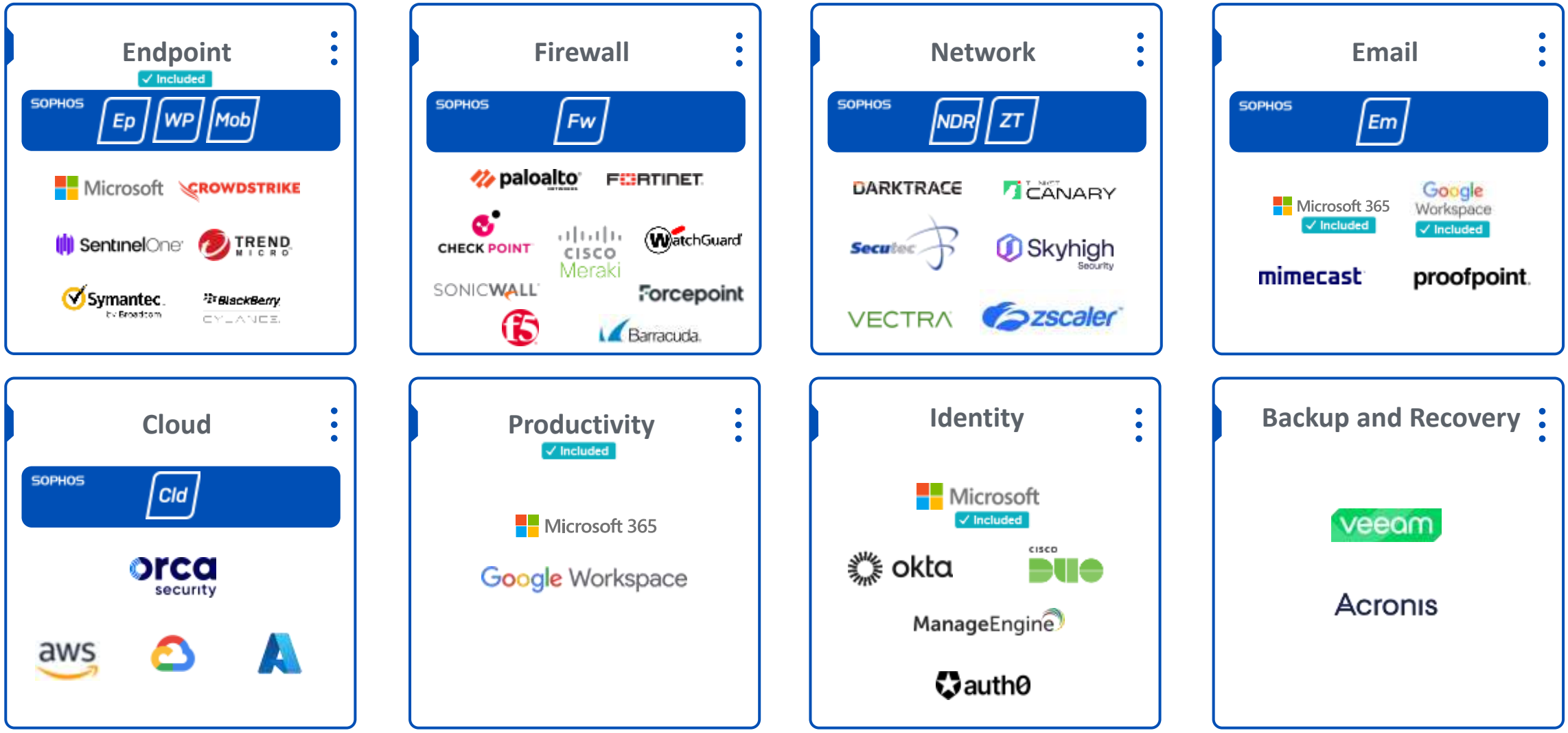
Und das ist nur für den „Heimgebrauch“

Telemetrie bei den Profis

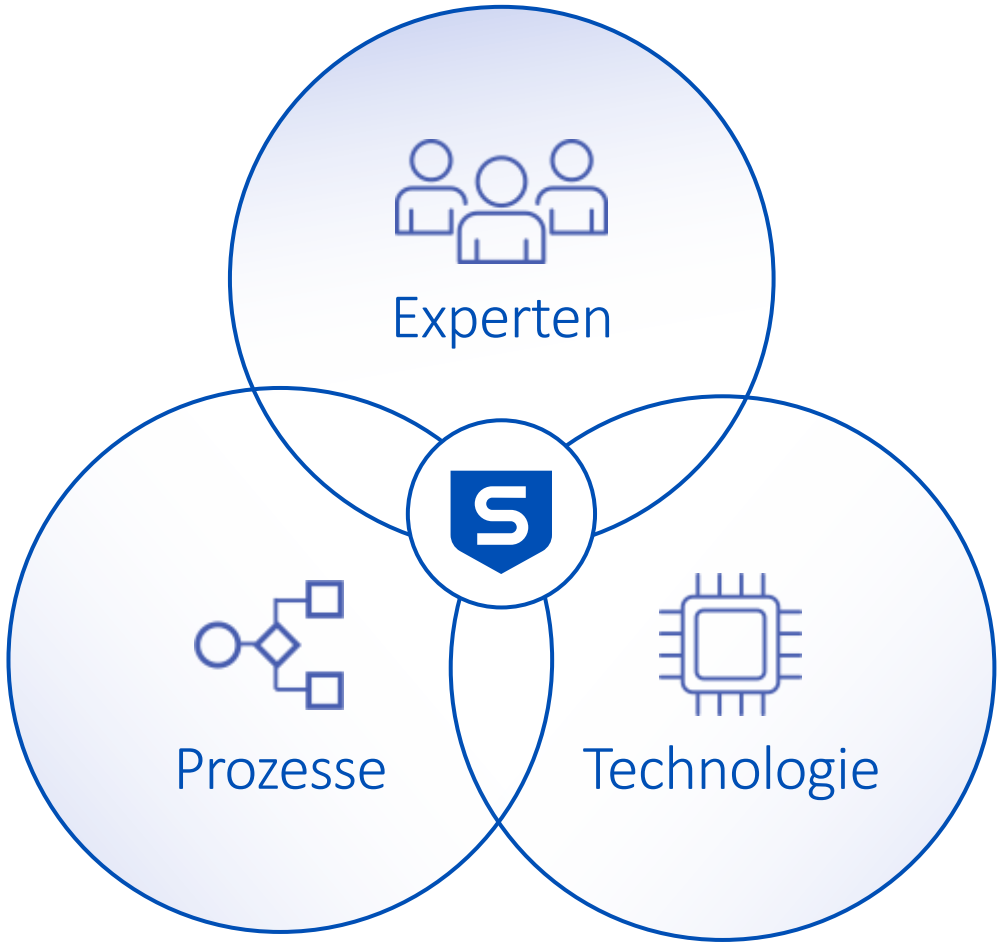
Herausforderung Detection and Response



Sophos XDR und MDR schützen Ihre Investitionen



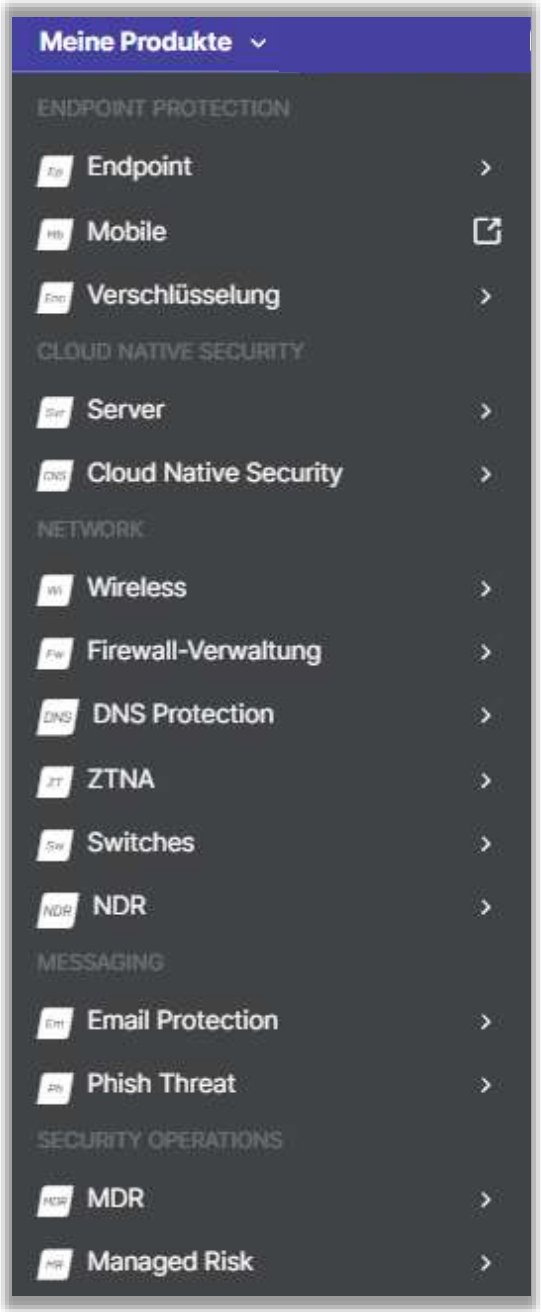
SOPHOS MDR – weil das Ergebnis zählt



- 24/7 Erkennung und Reaktion durch Analysten
- Analysten nutzen Erkenntnisse von
  - 40+ Herstellern im Bereich Firewall, Endpoint, Email, Cloud, NDR, Identity, Backup, Microsoft 365
  - Sophos Managed Risk Schwachstellenmanagement
- Vollständige Ursachenanalyse + Incident Response
- Mehr als 23.000 Sophos MDR Kunden
- Breach Protection Warranty bis 1 Mio €
- All-inclusive Service – keine versteckten Kosten

Sophos hilft Ihnen, folgende Themen zu lösen

- Schutz vor Ransomware und Betriebsausfall
- NIS2
- SOC
- Personal
- Kosteneffizienz
- Konsolidierung der IT-Sicherheit



SOPHOS

Sophos Whitepaper

Die NIS-2-Richtlinie

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) war der erste EU-weite Rechtsakt zur Cybersicherheit und trat 2016 in Kraft. Um die innerhalb des derzeitigen Rahmenwerks festgestellten Einschränkungen zu adressieren und auf die zunehmenden Cybersecurity-Bedrohungen in der EU infolge der Digitalisierung und der COVID-19-Pandemie zu reagieren, hat die Europäische Kommission die NIS-Richtlinie durch die NIS-2-Richtlinie ersetzt. Diese sieht strengere Aufsichtsmaßnahmen für nationale Behörden und strengere Durchsetzungsvorschriften vor und soll die Sanktionsregelungen zwischen den Mitgliedstaaten harmonisieren. Die NIS-2-Richtlinie ist am 16. Januar 2023 in Kraft getreten und die Mitgliedstaaten haben 21 Monate Zeit, um die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen.

Die NIS-2-Richtlinie soll die Sicherheitsanforderungen in der EU erhöhen, indem ihr Anwendungsbereich auf weitere Sektoren und Einrichtungen ausgeweitet wird; dabei werden Maßnahmen wie Risikoanalyse und Sicherheitsrichtlinien für Informationssysteme, Bewältigung von Sicherheitsvorfällen und die Sicherheit von Lieferketten berücksichtigt und unter anderem die Berichtspflichten gestrafft. Bei Nichterfüllung der Pflichten müssen die Mitgliedstaaten gemäß NIS 2 hohe Geldbußen auferlegen: 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist) für wesentliche Einrichtungen und 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist) für wichtige Einrichtungen. NIS 2 verpflichtet die Leitungsorgane unmittelbar zur Umsetzung und Überwachung der Einhaltung der Rechtsvorschriften durch ihre Organisation. Bei Verstößen gegen diese Richtlinie kann die Ausübung von Leitungsaufgaben auf Geschäftsführungs- bzw. Vorstandsebene der Einrichtung vorübergehend untersagt werden.

In diesem Dokument wird erläutert, wie Sophos-Lösungen Unternehmen und Einrichtungen bei der Umsetzung von Kapitel IV der NIS-2-Richtlinie, Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit, unterstützen und ihnen bei der Einhaltung der NIS-2-Richtlinie helfen.

https://www.sophos.com/de-de/content/nis2-compliance

NIS-2-Richtlinie – Kapitel IV, Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
Kapitel IV, Artikel 20, Governance		
2. Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.	Sophos Phish Threat	Bietet simulierte Phishing-Cyber-Angriffe und Security-Awareness-Trainings für die Endbenutzer von Unternehmen und Einrichtungen. Das Kursangebot deckt die Bereiche Phishing und Cybersecurity ab: Unsere Trainingsmodule behandeln Themen wie Verhinderung von Datenverlust, Passwort-Schutz und mehr.
	Sophos-Trainings und -Zertifizierungen	Trainingskurse und Zertifizierungen, die Partnern und Kunden dabei helfen, das Potenzial ihrer Sophos-Sicherheitsimplementierungen voll auszuschöpfen; Zugang zu neuestem Know-how und Expertise für Security Best Practices.
Kapitel IV, Artikel 21, Risikomanagementmaßnahmen im Bereich der Cybersicherheit		
2. Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme…die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen… 2. Die in Absatz 1 genannten Maßnahmen müssen […] zumindest Folgendes umfassen: a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;	Sophos Endpoint	Bietet modernsten Schutz vor Ransomware und komplexen Angriffen. Innovative Schutzfunktionen, darunter KI-basiertes Deep Learning, Anti-Exploit, lückenloser Ransomware-Schutz mit automatischem Rollback und adaptive Abwehrmechanismen, die automatisch auf Angreifer reagieren und selbst hochkomplexe Angriffe stoppen.
	Sophos Firewall	Bietet branchenführenden Netzwerkschutz, optimiert für das moderne verschlüsselte Internet und verteilte Benutzergruppen. Umfassende SD-WAN-Funktionen binden verteilte Büros und Standorte sicher an, während das integrierte ZTNA einen sicheren, benutzerbasierten Zugriff von jedem Standort ermöglicht. In Kombination mit Sophos Endpoint, Sophos ZTNA, Sophos Switches und Wireless Access Points sowie Sophos XDR und Sophos MDR kann die Sophos Firewall automatisch auf Bedrohungen reagieren und Angriffe stoppen, bevor sie sich ausbreiten. Kompromittierte Hosts werden automatisch isoliert. So werden laterale Bewegungen und externe Kommunikationen unterbunden, bis eine Bedrohung analysiert und beseitigt wird.
	Sophos Managed Detection and Response (MDR)	Überwacht kontinuierlich Signale aus der gesamten Sicherheitsumgebung (u. a. von Netzwerk-, E-Mail-, Firewall-, Identity-, Endpoint- und Cloud-Technologien), damit wir potenzielle Cybersecurity-Vorfälle schnell und präzise erkennen und darauf reagieren können. Das proaktive Threat Hunting erkennt Bedrohungen, bevor sie das Unternehmen oder die Organisation beeinträchtigen.

https://www.sophos.com/de-de/content/nis2-compliance

SOPHOS

ANFORDERUNGEN DER NIS-2-RICHTLINIE	SOPHOS-LÖSUNG	FUNKTIONEN UND VORTEILE
	Sophos Network Detection and Response (NDR)	Analysiert Datenverkehr kontinuierlich auf verdächtige Muster. In Kombination mit Sophos-verwalteten Endpoints und Firewalls überwacht Sophos NDR Netzwerkaktivitäten und erkennt verdächtige und schädliche Muster. Sophos NDR erkennt ungewöhnliche Datenverkehrsflüsse von nicht verwalteten Systemen und IoT-Geräten, nicht autorisierte Assets, interne Bedrohungen, bisher unbekannte Zero-Day-Angriffe und ungewöhnliche Muster tief im Netzwerk.
	Sophos Cloud Optix	Ermöglicht Unternehmen und Organisationen, Public-Cloud-Umgebungen nach Best Practices-Sicherheitsstandards von Amazon Web Services, Microsoft Azure und Google Cloud Platform einzurichten und zu verwalten. Sophos Cloud Optix sorgt für ein kontinuierliches Monitoring der Konfigurationsstandards, um Abweichungen zu erkennen. So können Sie versehentliche oder mutwillige Manipulationen in der Ressourcenkonfiguration verhindern, erkennen und automatisch korrigieren.
	Synchronized Security in Sophos-Produkten	Ermöglicht durch den Austausch von Telemetrie- und Statusdaten ein koordiniertes Erkennen, Isolieren und Beseitigen von Bedrohungen auf Servern, Endpoints und Firewalls. So können auch komplexe Angriffe gestoppt werden.
2. b) Bewältigung von Sicherheitsvorfällen;	Sophos Endpoint	Erkennt und blockiert automatisch 99,98 % aller Angriffe. Forensikbasierte Bereinigungsfunktionen entfernen sowohl den Schadcode als auch die von der Malware erstellten Registry-Schlüssel-Änderungen.
	Sophos Firewall	Die umfangreichen On-Box- und cloudbasierten Protokollierungs- und Reporting-Tools bieten direkt in Handlungen umsetzbare Erkenntnisse, um die Reaktion auf Vorfälle zu steuern und zu beschleunigen, einschließlich umfassender Informationen zu Netzwerkaktivitäten und einfachem Protokollzugriff für forensische Analysen. Die automatisierte Reaktion auf Bedrohungen (in Zusammenarbeit mit anderen Sophos-Produkten) reduziert die Reaktionszeit von Minuten auf Sekunden und stoppt Angriffe, bevor sie sich ausbreiten können.
	Sophos Managed Detection and Response (MDR) Complete	Umfasst standardmäßig eine unbegrenzte umfassende Vorfallsreaktion durch rund um die Uhr aktive Incident-Response-Experten. Umfasst eine komplette Ursachenanalyse und Reporting. Im Schnitt analysieren und beheben wir Vorfälle in nur 38 Minuten nach der Erkennung.
	Sophos Network Detection and Response (NDR)	Wenn Sophos NDR einen Indicator of Compromise, eine aktive Bedrohung oder einen Angreifer erkennt, werden die Analysten sofort benachrichtigt. So können sie direkt einen Bedrohungsfeed an die Sophos Firewall senden, um automatische Reaktionsmaßnahmen zum Isolieren des kompromittierten Hosts einzuleiten.

https://www.sophos.com/de-de/content/nis2-compliance

SOPHOS

itsa EXPO CONGRESS

SOPHOS

Halle 7 Stand 227