

Alarm oder Alltag?

Im Schatten der Routine den Fokus behalten

Sophos MDR erkennt und beseitigt komplexe Cyberangriffe, unter anderem welche, die automatisch nicht gestoppt werden können. Erweitern Sie Ihr Team um Incident-Response Experten, die Bedrohungen 24/7 überwachen und analysieren und sofortige Reaktionsmaßnahmen für Sie ergreifen.



Gabriel Kunzer

Senior Sales Engineer
gabriel.kunzer@sophos.com
+43 732 21032011



Besmir Ferati

Channel Account Executive
besmir.ferati@sophos.com
+43 660 3946043

Sophos auf einen Blick

 \$1.5B+ ARR + One Time	 30,000+ Sophos MDR-Kunden	 Der größte Anbieter von Managed Detection and Response Services (MDR)
 600,000+ Kunden	 300,000+ Sophos Endpoint Kunden	 Der einzigste Anbieter , der von Gartner als Customers' Choice und G2 Leader für EPP, Firewall und MDR ausgezeichnet wurde
 25,000+ Aktive Channel-Partner	 44,000+ Sophos XDR Kunden	 Ein Top-Performer in den MITRE ATT&CK Evals für Enterprise Products und Managed Services
 100+ Strategische Partner (Technologie, Dienstleistungen, etc.)	 300,000+ Sophos Firewall Kunden	 Eine KI-native Plattform die mit praktisch jeder Umgebung kompatibel ist
		 Ein dediziertes Portfolio an erstklassigen Produkten und Managed Security Services

Sophos + Secureworks

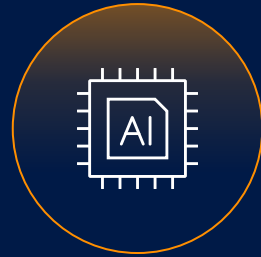


Prevention-First-Ansatz

Blockiert mehr Bedrohungen im Voraus, um das Risiko zu minimieren und den Arbeitsaufwand für Untersuchungen und Reaktionen zu reduzieren



- 99%** Prozentsatz der Bedrohungen, die automatisch blockiert werden
- 15** Jahre in Folge als Gartner Leader



Die größte KI-native offene Plattform

Die KI ist in die gesamte Angriffskette eingebettet und wird über eine der größten Plattformen der Branche bereitgestellt



- 900+** Täglich verarbeitete Terabyte an Daten in Sophos Central
- 50+** Deep Learning und KI-Modelle der Generation



Anpassbar an Ihre Bedürfnisse

Eine Plattform, die mit anderen Produkten kompatibel ist, sowie Dienstleistungen, die in hohem Maße an Ihre Bedürfnisse angepasst werden können



- 350+** Integrationen mit Produkten von Drittanbietern
- 30K+** Kunden mit XDR-Integrationen von Drittanbietern



Synchronized Security

Automatisierte Reaktion stoppt Angriffe, während der produktübergreifende Datenaustausch zuvor verborgene Bedrohungen aufdeckt



- 90%+** Reduzierung des Zeitaufwands für die tägliche Arbeitsbelastung der Sicherheitsadministratoren
- 85%** Reduzierung der Anzahl von Sicherheitsvorfällen



Top-Rated Kundenzufriedenheit

Die einzige Lösung in der Branche, die von Gartner als Customers' Choice für Endpunkte, Firewalls und MDR ausgezeichnet wurde



- 4.9/5.0** Der am besten bewertete und am häufigsten bewertete MDR-Service
- 75+** Industry awards in 2024

NIS2

- Januar 2023 in Kraft getreten.
- Erhöhung der Cybersicherheit in Europa.
- Verbesserung der Resilienz kritischer Infrastrukturen und digitaler Dienste.
- Haftungsrisiken für die Geschäftsführung!
- Frist bis zum 17. Oktober 2024 eingeräumt, um die Sicherheitsvorschriften der NIS2 in nationales Recht umzusetzen.
- Aktuell plant die Bundesregierung eine Umsetzung Ende 2025 / Anfang 2026



Branchenspezifische Anforderungen

C5

- Der **C5**-Standard (Cloud Computing Compliance Controls Catalogue) ist ein vom BSI entwickelter Prüfkatalog
- Bewertet und dokumentiert die Sicherheit und Compliance von Cloud-Diensten nach deutschen und europäischen Anforderungen.

PCI DSS

- PCI DSS (Payment Card Industry Data Security Standard) ist ein globaler Sicherheitsstandard, der Unternehmen verpflichtet, technische und organisatorische Maßnahmen zum Schutz von Kreditkartendaten umzusetzen, wenn sie diese speichern, verarbeiten oder übertragen.

SOC2

- SOC 2 (System and Organization Controls 2) ist ein US-amerikanischer Prüfstandard, der die Einhaltung von Datenschutz, Verfügbarkeit, Integrität, Vertraulichkeit und Sicherheit bei Dienstleistern bewertet, insbesondere in der Cloud- und IT-Branche.

TISAX

- **TISAX** (Trusted Information Security Assessment Exchange) ist ein branchenspezifisches Prüf- und Austauschverfahren für Informationssicherheit in der Automobilindustrie
- Basiert auf ISO/IEC 27001 und ist speziell auf Anforderungen wie Datenschutz und Prototypenschutz zugeschnitten.

Sophos Compliance und Zertifizierungen

Sophos überwacht kontinuierlich, welche regulatorischen Standards weltweit festgelegt werden.

Wir integrieren die neuesten relevanten Kontrollen in unsere Organisation,

unsere Produkte und Technologien, um unseren Kunden bei der Erfüllung ihrer Compliance-Verpflichtungen zu unterstützen.

ISO-Standards

- ISO 27001:2022
- ISO 27017:2015
- ISO 27018:2019

Cloud & Services

- SOC2 Type2
- C5 Testat



Branchenspezifisch

- PCI DSS
- HIPAA



Datenschutz

- DSGVO

Bewerten des Compliance Reifegrades

- Bevor es an die Umsetzung geht, sollte ein Unternehmen zunächst alle Anforderungen ermitteln
- Relevante Anforderungen identifizieren
- Erhebung des IST-Zustands
- Identifikation der Risiken und Priorisierung
- Implementation der Maßnahmen
- Überwachung und Audits
- Korrekturen implementieren

NIS-2 Assessment

- Sophos stellt ein kostenloses NIS-2 Assessment bereit
- **Identifizieren Sie Lücken:** Identifizieren Sie Bereich, in denen Ihre Cybersicherheit verbessert werden muss
- **Risiken mindern:** Reduzieren Sie die Wahrscheinlichkeit von Cyberangriffen und deren potenziellen Auswirkungen
- **Konformität nachweisen:** Beweisen Sie Aufsichtsbehörden und Interessenvertretern, dass Sie Maßnahmen wirksam umsetzen
- **Verschaffen Sie sich einen Wettbewerbsvorteil:** Zeigen Sie Kunden und Partnern, dass Sie Datenschutz priorisieren.

The screenshot displays the 'NIS2 Directive Assessment' interface. On the left is a navigation menu with items like 'Profil', 'Risikomanagement', 'Plan zur Bearbeitung von Vorfällen', 'Geschäftskontinuität', 'Lieferkette', 'Lebenszyklus der Systemsicherheit', 'Bewertung der Wirksamkeit', 'Cyberhygiene', 'Kryptografische Maßnahmen', 'Personalwesen', 'Authentifizierung und Kommunikation', 'Berichtspflichten', 'Zertifizierungssysteme', and 'Ergebnis der Bewertung'. The main content area is titled 'Risikomanagement' and contains a list of 9 questions related to risk management. Each question has three buttons: 'Nicht begonnen', 'Begonnen', and 'Abgeschlossen'. The progress status for each question is as follows:

Frage	Nicht begonnen	Begonnen	Abgeschlossen
1. Werden die Mitarbeitenden Ihrer Organisation regelmäßig über Best Practices im Bereich Cybersicherheit informiert und geschult?	Abgeschlossen		
2. Berücksichtigt Ihre Organisation das Thema Cybersicherheit in der Personalarbeit?	Abgeschlossen		
3. Haben Sie in Ihrer Organisation eine klare Governance-Struktur für die Cybersicherheit eingerichtet?	Abgeschlossen		
4. Haben Sie eine bestimmte Person oder ein Team, das für die Überwachung der Cybersicherheitsrichtlinien und -praktiken verantwortlich ist?		Begonnen	Abgeschlossen
5. Haben die Leitungsorgane Ihrer Organisation die geltenden Maßnahmen zum Cybersicherheitsrisikomanagement offiziell genehmigt?		Begonnen	Abgeschlossen
6. Gibt es dokumentierte Nachweise (z. B. Sitzungsprotokolle, offizielle Genehmigungen) für die Beteiligung des Leitungsorgans am Genehmigungsprozess?	Nicht begonnen	Begonnen	Abgeschlossen
7. Überwacht das Leitungsorgan die Umsetzung von Maßnahmen zum Management von Cybersicherheitsrisiken?		Begonnen	Abgeschlossen
8. Gibt es etablierte Verfahren für die regelmäßige Berichterstattung und Überprüfung dieser Maßnahmen an das Leitungsorgan?		Begonnen	Abgeschlossen
9. Ist das Leitungsorgan aktiv an der Bewertung der Wirksamkeit dieser Maßnahmen beteiligt?		Begonnen	Abgeschlossen

Der Weg zum strukturierten Plan

Vorbereitet sein – Incident Response

- Ein Incident Response Plan ist ein strukturierter und dokumentierter Prozess, um auf Cyberangriffe reagieren zu können.
- Ermöglicht eine schnellere Reaktion und dadurch eine Minimierung von Schäden
- Erforderlich für die Einhaltung von gesetzlichen und regulatorischen Anforderungen
- Sollte mehrere Szenarien abbilden
 - Phishing Angriff
 - C2 / APT
 - Kompromittierter Server / Endpoint
 - Datendiebstahl
 - Ransomware
 - Insider Threat

Incident Response Planner

- Kostenloses Tool zum Erstellen eines Incident Response Plans
- Basierend auf Richtlinien und Empfehlungen von NIST und CISA
- Dient als wesentliches Instrument zur effektiven Bewältigung und Eindämmung von Sicherheitsvorfällen
- Durch einen strukturierten Ansatz hilft dieser Plan Ausfallzeiten zu reduzieren und Schäden zu minimieren





Tabletop Exercises

- Ein förmlich existierender Incident Response Plan garantiert keinen reibungslosen Ablauf
- Wie auch abseits der IT muss für einen Notfall regelmäßig geübt werden
- Hierfür eignen sich Tabletop Exercises
- Tabletop Exercises helfen
 - Kommunikationswegen zu überprüfen
 - Lücken im Plan zu identifizieren
 - Zusammenarbeit zu verbessern
 - Routine aufzubauen
- Sophos unterstützt Sie gerne bei der Durchführung von Tabletop Exercises

Wie kann Sophos helfen?

Risk Management and Compliance

IT Operations and Management

Security Operations

Network Security and Infrastructure Management

Bedrohungen automatisch stoppen

- Ep** Sophos Endpoint
- DNS** Sophos DNS Protection
- Fw** Sophos Firewall
- Em** Sophos Email
- ZT** Sophos Zero Trust Network Access
- Mob** Sophos Mobile

Untersuchen und auf Bedrohungen reagieren

- MDR** Sophos MDR
- XDR** Sophos XDR
- RR** Sophos Rapid Response

Neue Bedrohungen erkennen

- MDR** Sophos MDR
- XDR** Sophos XDR

Risiko eines Angriffs verringern

- CNS** Sophos Cloud Native Security
- Ph** Sophos Phish Threat
- MR** Sophos Managed Risk
- NDR** Sophos Network Detection and Response

Aktive Bedrohungen stoppen

- MDR** Sophos MDR
- IR** Sophos Incident Response Services
- XDR** Sophos XDR
- RR** Sophos Rapid Response

Built-in Threat Intelligence
Adaptive Technologies
AI-Native



SOPHOS CENTRAL PLATFORM

Verwaltet vom Kunden | Verwaltet vom Partner | Verwaltet von SOPHOS

Nutzt SOPHOS Lösungen oder Daten von Drittherstellern

Microsoft 	Endpoint 	Firewall 	Identity 	Cloud 	Email 	Network 	Backup
----------------------	---------------------	---------------------	---------------------	------------------	------------------	--------------------	-------------------

HOLEN SIE SICH HILFE

Sophos Emergency Incident Response Hotline

Wir sind 24/7 für Unternehmen da, die einen Cyberangriff erleben

Australia	+61 272084454	Italy	+39 02 94752 897
Austria	+43 732 655 755 20	Switzerland	+41 445152286
Canada	+1 7785897255	United Kingdom	+44 1235635329
France	+33 186539880	United States	+1 4087461064
Germany	+49 61171186766	Email: EmergencyIR@sophos.com	



