Zukunftssichere IT-Sicherheit mit einem ganzheitlichen **Managed SOC Service**

SOPHOS
Cybersecurity as a Service

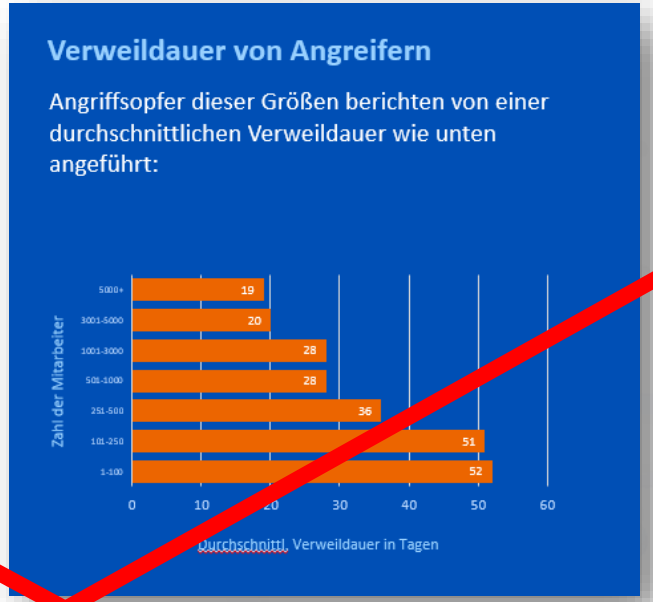
Alexander Polak
Enterprise Account Executive
alexander.polak@sophos.com
+43676 4040102

WKO WIEN
WIRTSCHAFTSKAMMER WIEN

Zahl der Cyberangriffe stieg um 89 Prozent

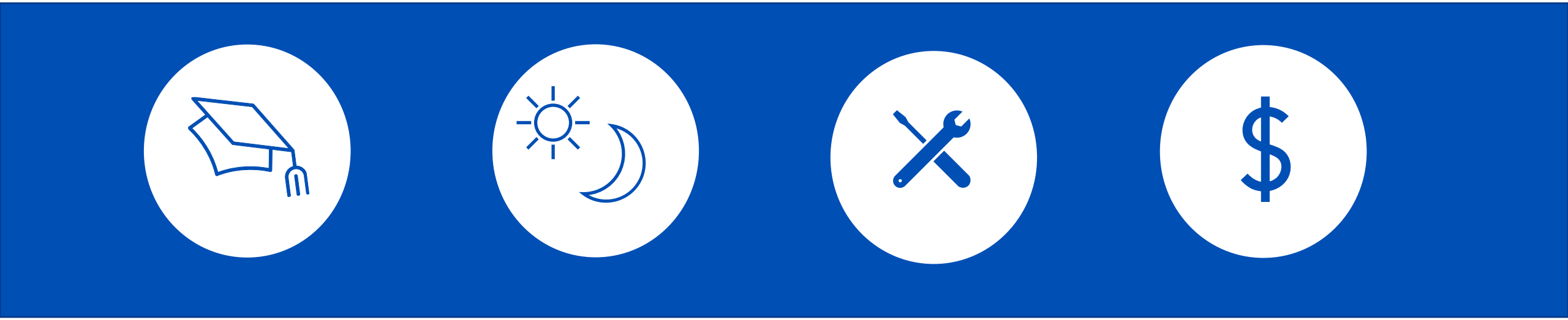
Aktuelle KPMG-Studie zeigt Bedrohungslage für Wiener EPU und KMU – Risikofaktor: fehlende IT-Abteilung – Cyberangriff: eher eine Frage des Wann als des Ob

Beschreibung der Anforderungen	Wichtigkei	CIXE	CIXA	CIMADR	COMPLETE	SVRCIAE	SVRCIAE	PREMIUM	MDRC	LETE
Planbare, wiederkehrende Abfragen	!			x	x			x	x	
Automatische Erkennung von verdächtigem Verhalten (KI gestützt) zur weiteren Untersuchung.	!			x	x			x	x	
Produktübergreifende Abfragemöglichkeit von Datenquellen	!									
Abfragemöglichkeit von Endpoint Daten	!			x	x			x	x	
Abfragemöglichkeit von Server Daten	!			x	x			x	x	
Abfragemöglichkeit von Firewall Daten	!			x	x			x	x	
Abfragemöglichkeit von E-Mail Daten	!			x	x			x	x	
Abfragemöglichkeit von Cloud Security Posture Management	!			x	x			x	x	
Live Response (Remote Terminal Zugriff)	!									
Absicherung des Zugriffs über mehrstufige Authentifizierung	!			x	x			x	x	
Auditierung des Zugriffs	!			x	x			x	x	
Möglichkeit der Nutzung einer Consolen Sitzung mit System-Rechten	!			x	x			x	x	
Verwendung von DOS-, UNIX- oder Linux-Befehle (je nach Betriebssystem des Zielgerätes)	!			x	x			x	x	
KI gestützte Erkennungen	!									
priorisierte Liste verdächtiger Aktivitäten und anfälliger Konfigurationen	!			x	x			x	x	
Zuordnung der Aktivitäten zu den TTPs aus dem MITRE ATT&CK Framework	!			x	x			x	x	
Risiko Einstufung verdächtiger Aktivitäten (Skala von 1 bis 10)	!			x	x			x	x	
Managed Detection and Response (MDR)	!									
Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen	!				x				x	
Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen	!				x				x	
Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung	!				x				x	
Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen	!				x				x	
Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen	!				x				x	
24/7 indizienbasierte Bedrohungssuche (Bei dieser Art der Bedrohungssuche werden kausale und angrenzende Ereignisse (schwache Signale) aggregiert und analysiert, um neue „Indicators of Attack (IoA)“ und „Indicators of Compromise (IoC)“ zu enttarnen, die bislang nicht erkannt werden konnten)	!				x				x	
Security Health Check (proaktive Untersuchungen von Betriebsbedingungen und empfohlene Konfigurations-Verbesserungen)	!				x				x	
Aktivitätsreports (Zusammenfassungen der Aktivitäten im Rahmen von Wochen und Monatsreports)	!				x				x	
Angriffserkennung (Erkennung von Angriffs Taktiken, Techniken und Prozessen (TTPs))					x				x	
24/7 indizienlose Bedrohungssuche (Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten werden verschiedene Informationen kombiniert, um das Verhalten von Angreifern vorherzusagen und neue Angriffsindikatoren (IoA) zu identifizie	!				x				x	
Optimierte Telemetriedaten (Bedrohungsanalysen werden um Telemetriedaten ergänzt)	!				x				x	
Proaktive Verbesserung des Sicherheitsstatus	!				x				x	
Dedizierter Ansprechpartner	!				x				x	
Direkter Telefon-Support	!				x				x	
Monatliches Briefing zu aktuellen Bedrohungen	!				x				x	
Stoppen und Eindämmen von Bedrohungen	!				x				x	
Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen	!				x				x	
Korrelieren aller vorliegenden Informationen, um Ausmaß und Schwere zu bestimmen	!				x				x	
Bewertung der Auswirkungen auf das Netzwerk	!				x				x	
Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Bed gsaktivität zu bekämpfen	!				x				x	
Ergreifen von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von ungen	!				x				x	
Vollständiges Incident-Response: komplette Neutralisierung von Bed gen	!				x				x	
Vollständige Ursachenanalyse	!				x				x	
Asset-Erkennung (Asset-Informationen über Betriebssy versionen, Anwendungen und Schwachstellen bis hin zur Identifizierung verwalteter und nicht verwalteter Assets)	!				x				x	
Zielzeit für Fallerstellung 2 Minuten nach Erke	!				x				x	
Zielzeit für die erste Reaktionsmaßnah inuten nach der Fallerstellung	!				x				x	
Die Antwortzeiten sind in einem S evel-Argement definiert	!				x				x	
Breach Protection Warrant e von bis zu 1 Mio. US-Dollar für Reaktionsmaßnahmen	!				x				x	
90 Tage Datenspeich er beteiligten Komponenten (inkl. potentieller Integrationen)	!				x				x	



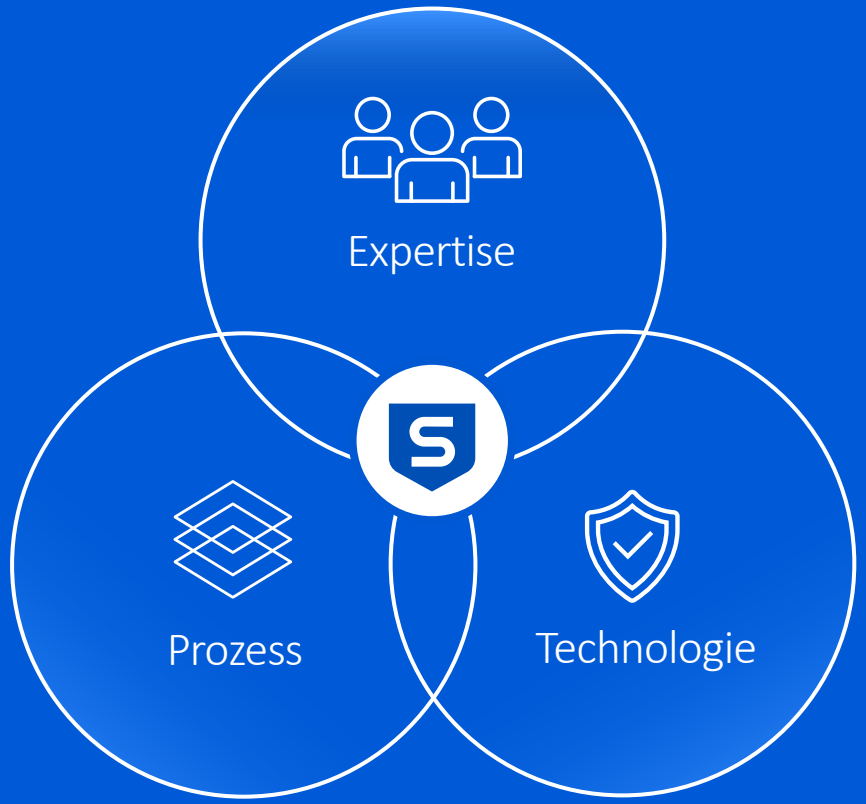
SOPHOS

Herausforderungen in der effektiven Verwaltung der IT-Sicherheit?



Wie kann Sophos unterstützen?

MANAGED DETECTION AND RESPONSE



SOPHOS

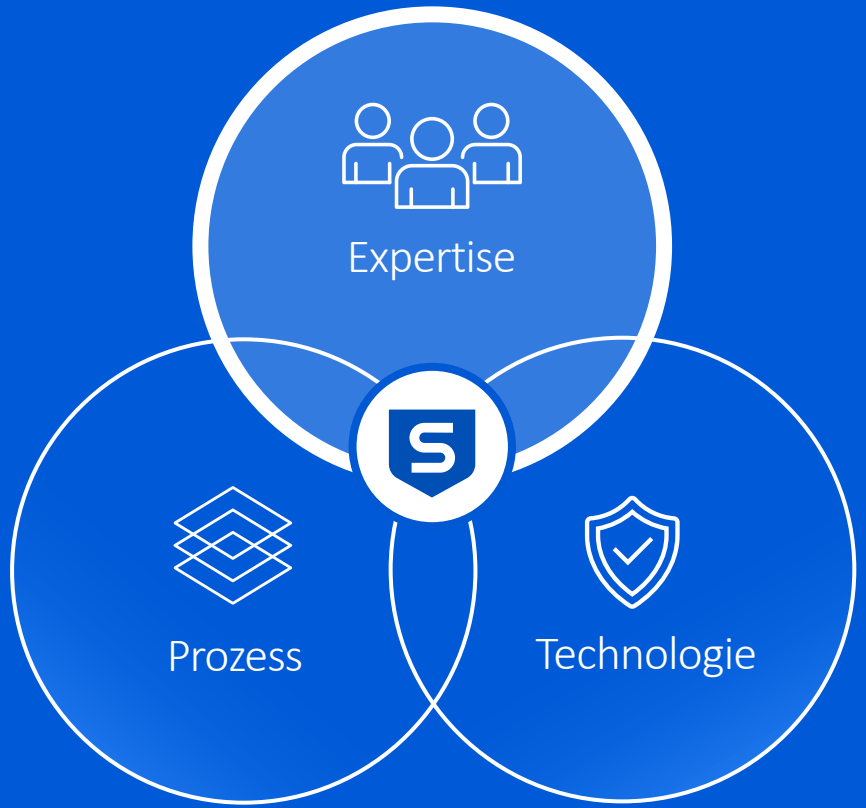
Security Operations Center

650+ MDR Spezialisten 24/7

Individuelle Zusammenarbeit

18.000+ MDR Kunden

MANAGED DETECTION AND RESPONSE



SOPHOS

SOPHOS

XDR Sophos XDR | Fw Sophos Firewall | Cld Sophos Cloud | NDR Sophos NDR | Em Sophos Email | Ep Sophos Endpoint

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- O365 Security & Compliance Center
- Microsoft Sentinel
- Office 365 Management Activity

Endpoint

Symantec. A Division of Broadcom
CROWDSTRIKE
SentinelOne
TREND MICRO
BlackBerry CYLANCE

Firewall

paloalto NETWORKS
FORTINET
CHECK POINT
CISCO
SONICWALL
WatchGuard

Network

DARKTRACE
THINKST CANARY
VECTRA
Skyhigh Security

Email

mimecast
proofpoint

Identity

okta
DUO
ManageEngine

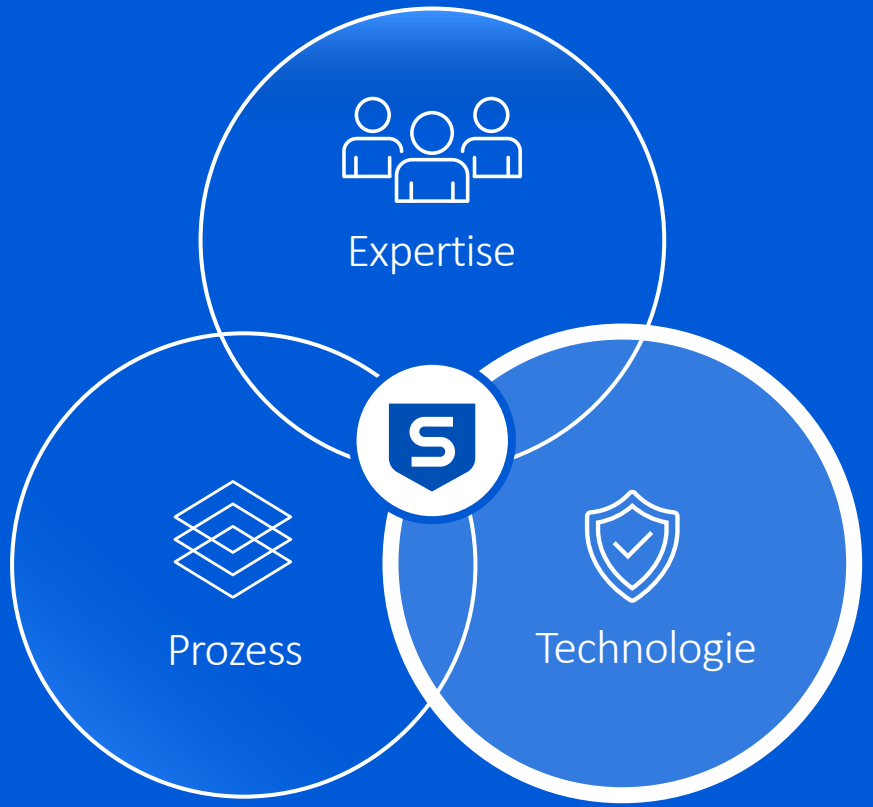
Public Cloud

aws
orca security

Productivity

Google Workspace

MANAGED DETECTION AND RESPONSE



SOPHOS

Incident Response Flatrate

Vollständige Ursachenanalyse

Umfängliche Berichterstattung

Bereicherung von KI/ML etc.

MANAGED DETECTION AND RESPONSE

Dominik Achleitner

Head of IT

NÖM AG

Ingomar Schmickl

Head of IT

St. Anna Kinderkrebsforschung


Kahoot!

SOPHOS

Cybersecurity delivered.