Sophos MDR

So erfüllen Sie in einem Paket mehrere Anforderungen für eine Cyberversicherung

Versicherungsunternehmen stellen zunehmend hohe Schutz-Anforderungen als Bedingung für eine Cyberversicherung. Ihr Ziel: Die Wahrscheinlichkeit eines Cybersecurity-Vorfalls verringern und damit das Risiko senken, dass der Versicherungsschutz in Anspruch genommen wird. So mussten im letzten Jahr 54 % der IT-Fachleute mehr Schutz-Anforderungen erfüllen, um eine Cyberversicherung abschließen zu können.*

Mit Sophos MDR können Sie viele Anforderungen von Versicherern erfüllen. Sophos MDR beinhaltet proaktives Threat Hunting mit Bedrohungsbekämpfung durch ein Experten-Team sowie modernste Schutztechnologien:

- **24/7 Threat Hunting, Detection and Response** durch Sophos-Experten
- **Sophos XDR** (Extended Detection and Response) ermöglicht Ihnen Zugriff auf Live-Daten und Daten aus der Vergangenheit zu Ihren Endpoints und Ihrer gesamten Umgebung, für eine Bewertung auf Makroebene und detaillierte Untersuchungen
- **Sophos Endpoint Protection** bietet Ihnen branchenweit führende Cybersecurity für Ihre Geräte und Workloads, die mehr Bedrohungen schneller stoppt

Um Fragen und Ihre individuellen Anforderungen zu besprechen, erreichen Sie unser deutschsprachiges MDR-Team unter mdrsalesdach@sophos.com.

Schutz-Anforderung	So erfüllt Sophos MDR die Anforderung
Endpoint Detection and Response (EDR)	Sophos Endpoint Protection bietet branchenweit führenden Schutz für Ihre Endpoints und Workloads und blockiert 99,98 % der Cyberangriffe, bevor sie ausgeführt werden können [AV-TEST]. Parallel dazu überwachen die Sophos MDR-Experten Ihre Umgebung 24/7 und erkennen, analysieren und beseitigen selbst hochkomplexe, manuell gesteuerte Angriffe.
Web Security	Sophos Endpoint Protection schützt vor schädlichen Downloads und verdächtigen Payloads. Administratoren können Websites basierend auf ihrer Kategorie mit Warnmeldungen versehen oder blockieren, riskante Dateitypen blockieren und Data-Leakage-Kontrollen auf webbasierte E-Mails und File Sharing anwenden. Web-Control-Funktionen für Cloud-Workload-Umgebungen schützen Daten, wenn Benutzer auf virtuelle Desktops zugreifen, die sich nicht hinter einem traditionellen Web Gateway befinden.
Privileged Access Management (PAM)	Sophos XDR zeichnet alle Benutzeraktivitäten auf, inkl. Authentifizierungs- und Microsoft-365-Audit-Protokollen, damit Änderungen an Berechtigungs-Einstellungen sichtbar werden. Enthalten ist zudem Zugriff auf die Windows-Protokolle vom Geräte- und Domain-Controller, um Windows-Ereignisse zu sehen. Sophos Endpoint Protection unterbindet Versuche, Anmelde-Informationen von Benutzern direkt aus dem Speicher abzufangen oder zu stehlen.
Incident-Response-Plan für Cybersecurity-Vorfälle	Sophos MDR umfasst einen Notfall-Service für akute Cyberangriffe. Wenn Sie angegriffen werden, schreiten unsere Experten sofort ein – ohne zusätzliche Kosten.
Hardening-Techniken, einschließlich Remote Desktop Protocol (RDP) Mitigation	Mit Sophos XDR können Sie Sicherheitslücken erkennen und beseitigen, z.B. ungeschützte Geräte, und härten damit Ihre Umgebung. Außerdem können Sie erkennen, wann RDP verwendet wurde, und Sie können die RDP-Richtlinie auf allen verwalteten Geräten einsehen und Änderungen daran erkennen. Per Remote-Terminal-Zugriff können Administratoren die RDP-Richtlinie auf Geräten von überall aus aktivieren/deaktivieren.
Protokollierung und Monitoring	Sophos XDR zeichnet Daten bis zu 90 Tage auf dem Gerät auf. Bis zu 30 Tage zurückliegende Daten werden im Sophos Data Lake gespeichert.
Austausch / Schutz von End-of-Life-Systemen	Mit Sophos XDR können Sie veraltete und nicht unterstützte Software und Systeme erkennen.
Patch- und Schwachstellen-Management	Sophos XDR bietet Zugriff auf alle Anwendungen auf dem Gerät, Versionsinfos, SHA256, Patch-Informationen und Protokolle, inkl. Ausführungsverlauf der Anwendungen, sowie Netzwerkverbindungen, übergeordnete und untergeordnete Prozesse usw. Zudem enthalten sind Abfragen, um installierte Anwendungen auf bekannte Schwachstellen zu prüfen sowie Abfragen zum Ermitteln von Schwächen des Sicherheitsstatus in Registry-Einstellungen.

** Cyber Insurance 2022: Reality from the Infosec Frontline, Sophos*

SOPHOS