Neue XDR-Lösung von Sophos synchronisiert Endpoint-, Server-, Firewall- und E-Mail-Sicherheit

Sophos XDR erweitert Next Generation Security-Lösungen um neue EDR-Funktionen und schafft so ein umfassendes und integriertes Threat Detection and Response System

Wiesbaden, 5. Mai 2021 – Sophos stellt heute seine neue Lösung Sophos XDR vor. Dabei handelt es sich um die einzige Extended Detection and Response (XDR)-Lösung der Branche, die Endpoint-, Server-, Firewall- und E-Mail-Sicherheit synchronisiert. Mit diesem umfassenden und integrierten Ansatz bietet Sophos XDR einen ganzheitlichen Überblick über die Security-Umgebung eines Unternehmens, kombiniert mit einem umfangreichen Datensatz sowie tiefgreifenden Analyse-Möglichkeiten zur Erkennung und Untersuchung von Cyberbedrohungen inklusive entsprechender Reaktionsmaßnahmen. So lassen sich selbst raffinierteste Angriffe abwehren – insbesondere solche, die mehrere Zugangspunkte nutzen und sich zunächst unauffällig im Netzwerk bewegen, um der Erkennung zu entgehen.

Detaillierte Bedrohungsanalyse mit umfangreichem Datensatz
Das Herzstück von Sophos XDR ist einer der branchenweit umfangreichsten Datensätze: Es werden zum einen bis zu 90 Tage On-Device-Daten und zum anderen bis zu 30 Tage produktübergreifende Daten im Cloud-basierten Data Lake gespeichert. Der einzigartige Ansatz, On-Device- und Data-Lake-Forensik zu kombinieren, bietet umfassende und kontextbezogene Einblicke. Diese können von Sicherheitsanalysten über Sophos Central und offene Anwendungsprogrammierschnittstellen (APIs) zur Einbindung in folgende Systeme genutzt werden: Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Professional Service Automation (PSA) und Remote Monitoring and Management (RMM).

Der Data Lake enthält wichtige Informationen von Intercept X, Intercept X für Server, Sophos Firewall und Sophos E-Mail. Sophos Cloud Optix und Sophos Mobile werden im Laufe des Jahres ebenfalls in die Datensammlung eingespeist. Dadurch sind Sicherheits- und IT-Teams in der Lage, einfach auf diese Daten zuzugreifen, um produktübergreifende Bedrohungsuntersuchungen durchzuführen und schnell granulare Details zu vergangenen und aktuellen Angriffsaktivitäten zu erhalten. Die Verfügbarkeit des Offline-Zugriffs auf historische Daten schützt zusätzlich vor verlorenen oder beeinträchtigten Geräten.

Neue EDR-Version
Weiterhin hat Sophos eine neue Version seiner branchenführenden Endpoint Detection and Response-Lösung Sophos EDR veröffentlicht. Neue zeitgesteuerte Abfragen und anpassbare kontextbezogene Pivoting-Funktionen bieten Sicherheitsanalysten und IT-Administratoren eine schnelle und präzise Identifizierung und Untersuchung von Sicherheitsproblemen, um schnell und gezielt reagieren zu können. Durch die Integration mit dem Data-Science-Tool SophosLabs Intelix liefert die neue Version vorkonfigurierte Abfragen und leistungsstarke Threat-Intelligence-Funktionen. Sophos EDR-Kunden können im Data Lake auf Daten zugreifen, die sieben Tage in der Cloud gehostet sind (erweiterbar auf 30 Tage). Bei On-Device-Daten ist dies bis zu 90 Tagen möglich.

Sophos Adaptive Cybersecurity Ecosystem
Sophos XDR und EDR sind Teil des Sophos Adaptive Cybersecurity Ecosystem (ACE), einer neuen, offenen Sicherheitsarchitektur zur Optimierung von Threat Prevention, Detection und Response. Sophos ACE nutzt Automatisierung und Analysen sowie den kollektiven Input von

Sophos-Produkten, -Partnern, -Kunden sowie Entwicklern und anderen Security-Anbietern. So schafft diese Architektur einen Schutz, der sich kontinuierlich verbessert; das System lernt ständig dazu und entwickelt sich weiter. Sophos ACE baut auf eine umfangreiche Datensammlung auf und korreliert verwertbare Erkenntnisse aus Sophos-Lösungen und -Services sowie Threat Intelligence aus den SophosLabs, Sophos AI und dem Sophos Managed Threat Response-Team. Offene Anwendungsprogrammierschnittstellen (APIs) ermöglichen es Kunden, Partnern und Entwicklern, Tools und Lösungen zu erstellen, die mit dem System interagieren und die Vorteile bestehender Integrationen nutzen können. Sophos ist mit diesem Ansatz führend in der Branche und arbeitet bereits mit vielen Anbietern zusammen.

Die Wichtigkeit eines interagierenden und auf möglichst vielen Datensätzen beruhenden IT-Security-Systems wird in der neuen Sophos-Studie „Intervention halts a ProxyLogon-enabled attack“ deutlich, die einen Angriff auf ein großes Unternehmen beschreibt. Die Attacke begann damit, dass die Angreifer einen Exchange-Server mit dem aktuellen ProxyLogon-Exploit kompromittierten und sich unbemerkt durch das Netzwerk bewegten. So konnten sie über einen Zeitraum von zwei Wochen Account-Anmeldeinformationen entwenden, Domain-Controller kompromittieren und sich auf mehreren Rechnern einnisten. Dabei verwendeten sie ein kommerzielles Remote-Access-Tool, um den Zugang zu den gehackten Rechnern aufrechtzuerhalten und eine Reihe von bösartigen Programmen zu verteilen. Die Studie zeigt, dass die Angreifer immer wieder zurückkehrten. Dabei setzten sie manchmal das gleiche Tool, wie beispielsweise Cobalt Strike, manchmal aber auch andere Tools auf verschiedenen Rechnern ein. Sie verwendeten ein kommerzielles Fernzugriffsprogramm und nicht das eher standardmäßige RDP, nach dem IT-Security-Spezialisten normalerweise suchen.

Dan Schiappa, Chief Product Officer bei Sophos. „Der Report verdeutlicht die Komplexität von Cyberangriffen, die von Menschen durchgeführt werden, und zeigt, wie schwierig es für IT-Sicherheitsteams ist, mehrstufige Vorfälle mit mehreren Vektoren zu verfolgen und einzudämmen. Oftmals ist es schlicht unmöglich, mit den Angriffsaktivitäten Schritt zu halten, die in allen Teilen des Unternehmens stattfanden. Laut dem Ende April veröffentlichten Sophos-Report State of Ransomware ist dieses Problem weit verbreitet. Mehr als 54 Prozent der befragten IT-Manager gaben an, dass Cyberangriffe zu weit fortgeschritten sind, als dass ihre IT-Teams sie alleine bewältigen könnten. XDR ist hier eine wichtige Verteidigungskomponente.“

Verfügbarkeit
Sophos XDR sowie die aktualisierten EDR-Funktionen für Intercept X Advanced with EDR und Intercept X Advanced for Server with EDR sind ab dem 19. Mai weltweit über Sophos Partner erhältlich. Partner und Kunden können alle XDR- und EDR-Produktlösungen auf der Cloud-basierten Sophos Central-Plattform über eine einzige Benutzeroberfläche einfach verwalten.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de