Sophos stellt ITDR-Schutz vor identitätsbasierten Angriffen vor

Erweiterung des Sophos-SecOps-Portfolios ermöglicht schnellere Erkennung der Risiken von Identitäten und kompromittierten Anmeldeinformationen

Wiesbaden, 21. Oktober 2025 – Sophos kündigt heute sein Sophos Identity Threat Detection and Response (ITDR) für Sophos XDR und Sophos MDR an. Diese neue Lösung überwacht kontinuierlich die Kundenumgebung auf Risiken und Fehlkonfigurationen von Identitäten und durchsucht das Darknet nach kompromittierten Zugangsdaten. Damit ermöglicht sie eine schnelle Erkennung und die Reaktion auf identitätsbasierte Angriffe. Darüber hinaus identifiziert ITDR risikoreiches Benutzerverhalten, welches für ein Unternehmen zur Bedrohung werden könnte.

Die Vorstellung von ITDR ist ein bedeutender Meilenstein für Sophos und ein Resultat aus der Übernahme von Secureworks. Sie ist die erste Secureworks-Lösung, die vollständig in die Sophos.Central-Plattform integriert ist und erweitert damit das umfassende Sicherheitsmanagement für die über 600.000 Sophos-Kunden.

Sophos ITDR richtet sich gegen identitätsbasierte Angriffe, eine der am schnellsten wachsenden Bedrohungen weltweit. Die Sophos X-Ops Counter Threat Unit (CTU) verzeichnete zwischen Juni 2024 und Juni 2025 einen Anstieg von 106 Prozent bei gestohlenen Zugangsdaten, die im Darknet zum Verkauf angeboten wurden – ein klares Zeichen für das wachsende Risiko. Der Sophos Active Adversary Report bestätigt zudem, dass in den in MDR- und Incident-Response-Fällen kompromittierte Zugangsdaten im zweiten Jahr in Folge die Hauptursache für Angriffe waren. In 56 Prozent der Vorfälle meldeten sich Angreifer mit gültigen Konten bei externen Remote-Diensten an.

„Cloud- und Remote-Arbeit haben die Angriffsfläche bei den Identitäten erweitert und neue Möglichkeiten für Angreifer geschaffen“, sagt Rob Harrison, SVP Product Management bei Sophos. „Komplexe Identitäts- und Zugriffsverwaltungssysteme mit ständig wechselnden Einstellungen und Richtlinien schaffen Lücken, die Angreifer ausnutzen. Sophos ITDR hilft, diese Lücken zu schließen, indem es Kunden einen schnellen Einblick in die Risiken von Identitäten bietet, kompromittierte Zugangsdaten überwacht und mit Sophos XDR und Sophos MDR für eine schnelle, analystengeführte Reaktion sorgt.“

Sophos ITDR deckt Risiken von Identitäten auf und ist darauf ausgelegt, alle bekannten MITRE ATT&CK Credential Access-Techniken zu erkennen und dagegen zu schützen. Die Lösung führt über 80 Prüfungen der Cloud-Identitätskonfiguration durch, überwacht kompromittierte Zugangsdaten im Darknet und nutzt KI-gestützte Erkennungen, um identitätsbasierte Angriffe wie Kerberoasting, Privilege Escalation, Account Takeover, Brute Force und Lateral Movement zu identifizieren. Integrierte Response Playbooks in Sophos ITDR sorgen für automatisierte Gegenmaßnahmen wie das Sperren von Konten, Zurücksetzen von Passwörtern, Aktualisieren der Multi-Faktor-Authentifizierung oder das Widerrufen von Sitzungen.

Wichtige Funktionen von Sophos ITDR:

- **Identity Catalog:** Vollständige Sichtbarkeit aller Identitäten in allen Systemen zur Reduzierung blinder Flecken.
- **Identity Posture Dashboard:** Einheitlicher, priorisierter Überblick über Risiken bei Identitäten, einschließlich kompromittierter Zugangsdaten aus dem Darknet, für ein schnelleres Handeln.
- **Continuous Assessments:** Stärkung der Sicherheitslage durch kontinuierliche Erkennung von Fehlkonfigurationen, inaktiven Konten, Schwachstellen und MFA-Lücken.

- **Compromised Credential Monitoring:** Schutz der Benutzer durch Erkennung und Benachrichtigung, wenn gestohlene Zugangsdaten in Datenbanken für gestohlene Identitäten auftauchen.
- **Dark Web Intelligence:** Proaktive Überwachung von Untergrundmärkten auf geleakte Zugangsdaten, um Angreifern immer einen Schritt voraus zu sein.
- **User Behavior Analytics (UEBA):** Früherkennung interner Bedrohungen und anomaler Aktivitäten zur Verhinderung von Kontoübernahmen und lateralen Bewegungen.
- **Advanced Identity Detections:** Erkennung komplexer Identitätsangriffe wie Kerberoasting, Account Compromise, Password Spray, Brute Force und Impossible Travel.
- **Identity Response Actions:** Sofortiges Eingreifen bei Identitätsbedrohungen durch integrierte Maßnahmen wie das Deaktivieren von Konten, Zurücksetzen von Sitzungen oder Passwörtern sowie das Markieren von kompromittierten Benutzern in Microsoft Entra ID.

Sophos ITDR integriert sich nahtlos in Sophos XDR sowie Sophos MDR und erzeugt automatisch Fälle, wenn identitätsbasierte Bedrohungen oder hohe Risiken identifiziert werden. Im Zusammenspiel mit Sophos MDR untersuchen Sophos-Sicherheitsanalysten die Vorfälle und ergreifen für den Kunden Reaktionsmaßnahmen, was die Behebung beschleunigt und das Risiko senkt.

Sophos-Partner erhalten Schulungsmaterialien und Vertriebsunterstützung im Sophos Partner Portal.

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/
X/Twitter: @sophos_info

Über Sophos
Sophos ist ein führender Anbieter im Bereich Cybersicherheit und schützt weltweit über 600.000 Unternehmen und Organisationen mit einer KI-gestützten Plattform und von Experten bereitgestellten Services. Sophos unterstützt Unternehmen und Organisationen unabhängig von ihrem aktuellen Sicherheitsniveau und entwickelt sich mit ihnen weiter, um Cyberangriffe erfolgreich abzuwehren. Die Lösungen von Sophos kombinieren maschinelles Lernen, Automatisierung und Echtzeit-Bedrohungsinformationen mit der menschlichen Expertise der Sophos X-Ops. So entsteht modernster Schutz mit einer 24/7 aktiven Erkennung, Analyse und Abwehr von Bedrohungen. Das Sophos-Portfolio beinhaltet branchenführende Managed Detection and Response Services (MDR) sowie umfassende Cybersecurity-Technologien – darunter Schutz für Endpoints, Netzwerke, E-Mails und Cloud-Umgebungen, XDR (Extended Detection and Response), ITDR (Identity Threat Detection and Response) und Next-Gen-SIEM. Ergänzt wird das Angebot durch Beratungs-Services, die Unternehmen und Organisationen helfen, Risiken proaktiv zu reduzieren und schneller zu reagieren – mit umfassender Transparenz und Skalierbarkeit, um Bedrohungen immer einen Schritt voraus zu sein. Der Vertrieb der Sophos-Lösungen erfolgt über ein globales Partner-Netzwerk, das Managed Service Provider (MSPs), Managed Security Service Provider (MSSPs), Reseller und Distributoren, Marketplace-Integrationen und Cyber Risk Partner umfasst. So können Unternehmen und Organisationen flexibel auf vertrauensvolle Partnerschaften setzen, wenn es um die Sicherheit ihres Geschäfts geht. Der Hauptsitz von Sophos befindet sich in Oxford, Großbritannien. Weitere Informationen finden Sie unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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