Multi-Cloud-Bedrohungserkennung mit Sophos XDR

Sophos erweitert seine Next Generation Security-Lösung XDR um neue Funktionen für Microsoft Azure und Google Cloud Platform (GCP) und schafft so ein umfassendes und integriertes Threat Detection and Response System

Sophos hat seine Extended Detection and Response (XDR)-Lösung erweitert und fügt neben Aktivitätsprotokollen von Amazon Web Services (AWS) auch die von Microsoft Azure (Azure) und Google Cloud Platform (GCP) hinzu. So erhalten IT- und Sicherheitsteams einen umfassenden Überblick über die Sicherheit ihrer Public-Cloud-Umgebungen. Durch die Integration von Daten aus der Sophos-Cloud-Security-Management-Lösung Cloud Optix ermöglicht Sophos XDR die Erkennung, Bewertung und Absicherung von Sicherheitsfehlkonfigurationen und Schwachstellen in den Cloud-Workloads und bei Benutzerzugriffen.

Mit den neuen Cloud-Optix-Datenquellen in Sophos XDR können Security-Administratoren jetzt ganz einfach Aktivitäten auf API-, CLI- und Managementkonsolen in AWS-, Azure- und GCP-Cloud-Umgebungen untersuchen. Mithilfe vorkonfigurierter und anpassbarer SQL-Abfragen lassen sich Zugriffsversuche über kompromittierte Rollen oder neu erstellte Benutzerrollen und Ressourcen, die auf dauerhafte Kompromittierungen sowie Taktiken zur Privilegienerweiterung und Exfiltration hinweisen, aufdecken.

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 über offene Anwendungsprogrammierschnittstellen (APIs) zur Einbindung in weitere Systeme genutzt werden – darunter Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Professional Service Automation (PSA) oder Remote Monitoring and Management (RMM).

Der Data Lake enthält Informationen von Intercept X, Intercept X für Server, Sophos Firewall, Sophos E-Mail und Sophos Cloud Optix. Sicherheits- und IT-Teams sind 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. Diese vernetzte Multi-Cloud-Sicherheit von einer zentralen Konsole aus hilft den Teams bei Untersuchungen das Gesamtbild zu sehen, Risiken schnell zu erkennen und Sicherheitsvorfälle proaktiv zu verhindern.

Erweiterungen in Cloud Optix
Die aktualisierte Version von Sophos Cloud Optix enthält außerdem eine Reihe von Ergänzungen für eine verbesserte Cloud-Sicherheitsüberwachung:

- **AWS activity nomalies** – Neue SophosAI-Modelle analysieren kontinuierlich die Benutzeraktivitätsprotokolle von AWS CloudTrail. Dadurch kann Cloud Optix ein Bild der Aktivitäten einzelner Benutzerrollen erstellen, um sowohl versehentliche Änderungen als auch böswillige Aktivitäten von kompromittierten Rollen zu identifizieren. Es bietet eine

klare und detaillierte Zeitleistenansicht von AWS CloudTrail-Ereignisse und identifiziert risikoreiche Anomalien, etwa Aktionen, die außerhalb der normalen Arbeitszeiten durchgeführt werden, oder solche, die noch nie zuvor durchgeführt wurden. Mit diesem Update lässt sich die Anzahl der Warnmeldungen für Sicherheitsteams drastisch reduzieren, so dass diese sich auf die Untersuchung von risikoreichen Verhaltensmustern, konzentrieren können.

- **Multiple Jira integration instances** – Sicherheits-Administratoren können damit mehrere Jira-Instanzen zu einem Cloud Optix-Konto hinzufügen. Dabei wird jede Cloud-Umgebung mit einer Jira-Instanz verknüpft. Dies kann eine separate Jira-Instanz pro Umgebung oder eine gemeinsame Jira-Instanz sein, die von vielen Umgebungen genutzt wird.

- **Azure IAM vizualisation** – Damit lasse sich Beziehungen zwischen IAM-Rollen, IAM-Nutzern und Diensten visualisieren, um die Verwaltung komplexer, miteinander verwobener IAM-Rollen für mehrere Azure-Abonnements und Azure AD zu vereinfachen.

- **Custom policy allerts** – Damit können Sicherheitsteams benutzerdefinierte Warnmeldungen auf der Grundlage von erweiterten Suchabfragen in Cloud Optix erstellen. Künftige Sicherheits-Benchmark-Scans lösen dann in Cloud Optix Warnungen aus, wenn die Kriterien der Abfrage erfüllt sind.

Die jüngsten Updates von Sophos Cloud Optix und eine Zusammenfassung aller Verbesserungen sind hier zu finden. Ein 30-Tage-Textversion von Cloud Optix ist unter diesem Link erhältlich

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

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