



Geballte Threat-Intelligenz: Sophos kündigt Sophos X-Ops an

Sophos X-Ops vereint SophosLabs, Sophos SecOps und Sophos AI unter einem Dach. Kombination von drei etablierten Sophos Cybersecurity-Experten-Teams hilft Unternehmen, sich noch effektiver gegen Cyberattacken zu schützen.

Wiesbaden, 20. Juli 2022 – Sophos kündigt heute [Sophos X-Ops](#) an, eine neue funktionsübergreifende Einheit aus SophosLabs, Sophos SecOps und Sophos AI. Die drei etablierten Cybersecurity-Experten-Teams werden vereint, damit Unternehmen noch effektiver gegen die sich ständig ändernden und immer komplexeren Cyberattacken verteidigt werden können. Sophos X-Ops vereint die prädiktiven, realitätsnahen und detailliert recherchierten Bedrohungsdaten aller Teams, um gemeinsam stärkere und innovativere Schutz-, Erkennungs- und Reaktionsfunktionen bereitzustellen.

Sophos veröffentlicht heute zudem die Studie „[OODA: Sophos X-Ops Takes on Burgeoning SQL Server Attacks](#)“. Darin geht es um die Zunahme von Angriffen auf ungepatchte Microsoft SQL-Server. Die Ergebnisse beschreiben, wie Angreifer eine gefälschte Download-Seite und Graumarkt-Tools für den Fernzugriff nutzen, um Ransomware zu verbreiten. Sophos X-Ops hat die Angriffe identifiziert und vereitelt, indem die Experten die Kenntnisse über die Vorfälle kombiniert, analysiert und Maßnahmen ergriffen haben. Bereits in der Vergangenheit tauschten die Experten-Teams Informationen aktiv aus. Der Schritt hin zu einem integrierten Sophos X-Ops Team beschleunigt und straft die Vorgehensweise, um ebenso schnell agierenden Angreifern zu begegnen.

„Moderne Cybersicherheit setzt auf hochgradig interaktives Teamwork. Mit der Weiterentwicklung der Branche haben sich die notwendigen Spezialisierungen in den Bereichen Analyse, Technik und Ermittlungen etabliert. Für skalierbare End-to-End-Operationen werden Softwareentwickler, Automatisierungingenieure, Malware-Analysten, Reverse-Ingenieure, Cloud-Infrastruktur-Ingenieure, Incident-Responder, Dateningenieure und -wissenschaftler sowie zahlreiche andere Experten benötigt. Diese wiederum erfordern eine Organisationsstruktur, die Silos vermeidet. Wir haben drei weltweit anerkannte und erfahrene Teams innerhalb von Sophos zusammengeführt, um diese Bandbreite an kritischem Fach- und Prozesswissen bereitzustellen. Sophos X-Ops kombiniert die Stärken aller Teams – darunter die Analyse weltweiter Telemetriedaten von mehr als 500.000 Kunden, Funktionen zur Bedrohungserkennung, -reaktion und -beseitigung sowie künstliche Intelligenz – und verbessert so die Erkennung und Reaktion auf Bedrohungen messbar“, sagt Joe Levy, Chief Technology and Product Officer bei Sophos. „Moderne Angreifer sind oft zu gut organisiert und zu fortschrittlich, um sie ohne die kombinierte Expertise und operative Effizienz einer gemeinsamen Task Force wie Sophos X-Ops zu bekämpfen.“

„Effektive Cybersicherheit erfordert eine solide Zusammenarbeit auf allen Ebenen, sowohl intern als auch extern. Nur so können Cyberkriminelle schnell und in großem Umfang entdeckt, analysiert und bekämpft werden. Die Zusammenführung der separaten Teams in Sophos X-Ops zeigt, dass Sophos dieses Prinzip verstanden hat und bereit ist, danach zu handeln“, sagt Michael Daniel, President und CEO, [Cyber Threat Alliance](#).



Sophos X-Ops bietet darüber hinaus eine stärkere funktionsübergreifende Grundlage für Innovationen, die aufgrund der aggressiven Fortschritte in der organisierten Cyberkriminalität eine wesentliche Komponente der Cybersicherheit darstellen. Durch die Verflechtung des Fachwissens der Gruppen leistet Sophos [Pionierarbeit für das Konzept eines durch künstliche](#)

Intelligenz (KI) unterstützten Security Operations Centers (SOC), das die Voraussagen von Sicherheitsanalysten antizipiert und entsprechende Abwehrmaßnahmen bereitstellt. Sophos ist davon überzeugt, dass dieser Ansatz im SOC der Zukunft die Sicherheitsabläufe dramatisch beschleunigen und die Fähigkeit verbessern wird, neuartige Anzeichen für eine Kompromittierung schneller zu erkennen und darauf zu reagieren.

Für mehr Informationen über Sophos X-Ops und die Bedrohungsforschung, abonnieren Sie die Sophos X-Ops Blogs und folgen Sie Sophos X-Ops auf Twitter.

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

Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Anwendern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter <http://www.sophos.de/>.

Pressekontakt:

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

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