



## **Bedrohungen mit neuen KI-Funktionen in Sophos XDR noch schneller erkennen und abwehren**

Bei der Erkennung und Neutralisierung von Bedrohungen kann für Sicherheitsexperten, darunter auch Managed Service Provider (MSP), jede Minute entscheidend sein. Um die Reaktionsfähigkeit und forensische Untersuchungen weiter zu optimieren, hat Sophos jetzt seine [Extended Detection and Response \(XDR\)-Plattform](#) mit einer neuen Künstlichen Intelligenz (KI) erweitert. Die [neuen generativen KI-Funktionen](#) beschleunigen und vereinfachen die Untersuchungen, womit selbst weniger erfahrene Analysten die nötigen Sicherheitsoperationen gezielt durchführen und Gegner schneller neutralisieren können. Zu den wichtigsten neuen Funktionen zählen:

### **Optimierte Suche**

Die Funktion 'AI Search' unterstützt Sicherheitsexperten bei der Durchsuchung großer Mengen an sicherheitsrelevanten Daten mithilfe natürlicher Sprache. Dies erleichtert Untersuchungen, da beispielsweise keine fortgeschrittene, technische SQL-Kenntnis erforderlich ist.

### **Überblick und Transparenz**

Die Funktion 'AI Case Summary' bietet einen leicht verständlichen Überblick über die Erkenntnisse einer Untersuchung. Damit haben Sicherheitsexperten eine valide Informationsbasis, um schnell und effizient Entscheidungen für die nächsten Schritte treffen zu können.

### **Granulare Command-Analyse**

Bei der Untersuchung potenziell bösartiger Befehle verschafft 'AI Command Analysis' Sicherheitsexperten tiefe Einblicke in das Verhalten der Angreifer. Die Funktion entschlüsselt den Code und reduziert damit die Komplexität und den Zeitaufwand, die zur Beurteilung einer Erkennung erforderlich sind.



### **Gezielte Untersuchung**

Wenn Sicherheitsexperten und Forensiker die Details einer Untersuchung betrachten, profitieren sie jetzt von der aktualisierten und vereinfachten Benutzeroberfläche des 'Pivot-Menüs'. Mit dieser Funktion lassen sich wichtige Informationen einer Entdeckung auswählen und diese als Ausgangspunkt für eine eingehendere Untersuchung und die Einleitung sofortiger Maßnahmen verwenden.

Sophos kombiniert KI und menschliches Fachwissen, um die unterschiedlichsten Bedrohungen zu stoppen, wo immer sie auftreten. Die neuen generativen KI-Funktionen sind für alle Partner und lizenzierten Sophos XDR-Kunden optional erhältlich und können in Sophos Central aktiviert werden.

## **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

## **Pressekontakt:**

Sophos

Jörg Schindler, Senior PR-Manager EMEA Central  
[joerg.schindler@sophos.com](mailto: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](mailto:sophos@tc-communications.de)