SophosLabs Intelix: Cloud-basierte Cyber-Threat-Intelligence-Plattform für alle

- *On-Demand-Zugriff auf Cyber-Threat-Expertise via APIs*
- *Bedrohungs- und Analyseplattform für Entwickler und alle, die auf der Suche nach validen Bedrohungsinformationen sind*

Wiesbaden, 3. Dezember 2019 – Sophos gibt die Verfügbarkeit von SophosLabs Intelix bekannt. Die Cloud-basierte Threat-Intelligence- und Analyseplattform ermöglicht es Anwendern, sicherere Anwendungen zu entwerfen. Programmierer haben via APIs Zugriff auf die Intelix Plattform, um mit aktuellem Cyber-Bedrohungs-Know-how Dateien, URLs und IP-Adressen zu bewerten. Auf der Plattform aktualisiert und sammelt Sophos kontinuierlich Petabytes an Echtzeit- und historischer Intelligenz, etwa Telemetriedaten der Sophos Endpoint-, Netzwerk- und mobilen Sicherheitslösungen, Daten von Sophos-Honeypots und Spam-Fallen sowie Wissen aus über 30 Jahren Bedrohungsforschung. Darüber hinaus stehen prädiktive Erkenntnisse aus Machine- und Deep-Learning-Modellen und vieles mehr zur Verfügung. SophosLabs Intelix steht über den AWS Marketplace zur Verfügung und beinhaltet ein kostenloses Starter-Kit. Pay-as-you-go-Optionen für umfangreiche Recherchen sind ebenfalls verfügbar und Teil des Sophos Cloud-Security-Provider (CSP)-Programms für Vertriebspartner.

Direkter Zugriff für Analysen und Abfragen
Durch die Verwendung von RESTful-APIs können Entwickler direkt und vor allem sicher auf die Plattform zugreifen, um Dateien für statische und dynamische Analysen zu übertragen oder Abfragen von Datei-Hashes, URLs, IP-Adressen und Android-Anwendungen (APKs) zu tätigen. Auf diese Weise erhalte sie Antworten auf Fragen wie "Ist diese Datei sicher? Was passiert, wenn ich sie öffne oder ausführe?", "Ist dieser Link sicher?“ oder „Was passiert, wenn ich diese URL aufrufe?".

Globale Community für die Entwicklung sicherer Anwendungen
„Sophos baut eine globale Community auf, um die Innovationskraft von Entwicklern mit Hilfe der APIs anzuregen. Durch die direkte Bereitstellung einer Vielzahl von Informationen aus den SophosLabs über RESTful APIs machen wir es einfacher als je zuvor, Bedrohungsinformationen schnell und einfach in neue und bestehende Anwendungen und Abläufe zu integrieren“, sagt Joe Levy, CTO von Sophos. „Mit SophosLabs Intelix erleichtern wir die Durchführung von Analysen für jeden, der eine Anwendung oder Plattform entwickelt. Darüber hinaus ist die Informationsbreite und -tiefe auf der Plattform wertvoll für IT-Administratoren, Forscher, Sicherheitsanalysten oder Studenten, die auf der Suche nach validen Bedrohungsinformationen sind."

Die drei Kernfunktionen von SophosLabs Intelix sind:

- **Echtzeitsuche**: Ermöglicht die schnelle Klassifizierung von Artefakten mit direktem Zugriff auf jüngste Erkenntnisse der SophosLabs durch Abfrage von Datei-Hashes, URLs, IPs oder Android-Anwendungsverlusten. Reputationsbewertungen (ReputationScores) identifizieren bekannte schlechte und gute Dateien sowie solche in der Grauzone.

- **Statische Dateianalyse:** Nutzt mehrere Modelle des Machine Learning, globale Reputation, Deep File Scan und mehr, ohne dass die Datei in Echtzeit ausgeführt werden muss.
- **Dynamische Dateianalyse:** Bietet dynamische Dateianalyse- und Klassifizierungsfunktionen durch die Ausführung und Instrumentierung der eingereichten Dateien in einer Sandbox. Dabei werden die jüngsten Techniken zur Laufzeiterkennung verwendet, um das tatsächliche Verhalten potenzieller Bedrohungen zu ermitteln.

Weitere Informationen stehen bereit unter:
https://api.labs.sophos.com/
https://www.sophos.com/intelix

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 47.000 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, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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