Ein Ausblick auf das Security Operation Center der Zukunft

Das KI-gestützten SOC als neues Maß der Dinge

Eine Einschätzung von Joshua Saxe, Chief Scientist und KI-Experte bei Sophos

Heutzutage gibt es zwei Arten von benutzerorientierten Softwareprodukten: Produkte, die maschinelles Lernen und Automatisierung verwenden, um sich an die Ziele der Benutzer anzupassen und diese zu verwirklichen, und Produkte, die von Unterbrechungen geprägt sind und sorgfältig auswendig gelernte und sich wiederholende Interaktionen erfordern. Google Search, Siri und Spotify gehören zur erstgenannten Produktkategorie. Die heutigen Security Operations Center (SOC)-Plattformen gehören zur letzteren, nicht anpassungsfähigen, disruptiven Kategorie.

In den nächsten fünf Jahren wird sich das ändern. Erfolgreiche Sicherheitsprodukte werden bei der Empfehlung relevanter Sicherheitsinformationen so versiert sein wie Google und Facebook und die Absicht hinter sicherheitsorientierten Anfragen in natürlicher Sprache so präzise wie Alexa und Siri vorhersagen. Sie werden auch Technologien der künstlichen Intelligenz mit den Arten von Systemintegrationen kombinieren, die Smart-Home-Ökosysteme erreicht haben und Sicherheitsrichtlinien aktualisieren – genau wie Smart Homes Sicherheitskameras einschalten und Türen auf Benutzerwunsch verriegeln.
Dieses neue „KI-unterstützte SOC“ wird sich den heutigen SOCs genauso dramatisch überlegen anfühlen, wie die heutige Google-Suche im Vergleich zu Altavista aus den 1990er Jahren. Mit der KI-Verbesserung, die das Wissen einer globalen „Crowd“ von SOC-Analysten zu einer Art Co-Pilot für Sicherheits-Workflows destilliert, SOC-Analyst-Workflows automatisch vervollständigt und die Absicht von SOC-Analysten vorwegnimmt, wird das Sicherheitspersonal erheblich effektiver sein.

Natürlich wird diese Veränderung nicht aus einem Vakuum heraus entstehen, sondern das Ergebnis des Zusammenwachsens mehrerer aktueller Technologietrends sein: Der erste davon ist die zunehmende Integration aller relevanten Sicherheitsdaten über den gesamten Anwenderkreis hinweg durch Extended Detection and Response (XDR)-Anbieter. Diese stellen erstmals die notwendigen Trainingsdaten für die unterstützenden maschinellen Lernmodelle des zukünftigen KI-gestützten SOC bereit. Der zweite Trend ist die technologieübergreifende KI-Innovation, bei der die Forschung weiterhin bessere Algorithmen, Tools und Cloud-KI-Infrastrukturen für maschinelles Lernen (ML) entwickelt, die Möglichkeiten für die ML-Fähigkeiten des KI-gestützten SOC bieten.
Der dritte Trend ist die programmierbare Sicherheitslage, bei der IT-, Cloud- und Sicherheitsprodukte zunehmend robuste Management-APIs bereitstellen. Da ein immer größerer Teil der IT-Landschaft über APIs steuerbar wird, ergeben sich vermehrt Möglichkeiten, SOAR-Funktionen (Security Orchestration, Automation and Response) für KI-gestützte SOCs bereitzustellen, die sich wie Smart-Home-Ökosysteme verhalten, die Sicherheitslage von Unternehmen aktualisieren und Vorfälle via Automatisierung per Knopfdruck beheben.

Alles deutet zurzeit darauf hin, dass die Entwicklung von Benutzerschnittstellen hin zu einer nahtlosen und ausgeklügelten Integration von KI-Modellen, die die Nutzerabsicht erkennen können, immer wichtiger wird, und mehrere Technologiebereiche diesen Status bereits erreicht haben. Diese Entwicklung lässt sich in den nächsten Jahren auch bei Anbietern von SOC-Softwareprodukten erwarten - oder sie werden zunehmend irrelevant. Tatsächlich scheint eine „Empfehlungs-Engine für Sicherheitsoperationen“ sehr wahrscheinlich, deren

Nutzerfreundlichkeit mit der von Dienstprogrammen konkurriert, die wir von Google, Amazon oder Netflix kennen.

Der gesamte Artikel von Joshua Saxe mit weiteren, technischen Details kann hier nachgelesen 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/
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