



Sophos stellt weitere KI-Ressourcen in den Dienst der Open-Source-Gemeinde

Machine-Learning-Toolkit ermöglicht Programmierenden das automatische Generieren von Regeln für das plattformübergreifende Klassifizierungsprogramm YARA

Das [SophosAI-Team](#) für künstliche Intelligenz hat ein auf maschinellem Lernen basierendes Tool entwickelt, das YARA-Regeln zur Erkennung bestimmter Arten von Bedrohungen generiert. Das von VirusTotal verwaltete, plattformübergreifende Klassifizierungstool ist eines der wichtigsten Tools für Forscherinnen und Forscher zum Aufspüren und Klassifizieren von Malware. Obwohl das Erstellen eigener YARA-Regeln für die Analyse unerlässlich ist, gestaltet sich diese Arbeit sehr zeitaufwändig.



Aus diesem Grund hat SophosAI die Leistungsfähigkeit des maschinellen Lernens in YARA eingebracht. Mit dem neuen YaraML-Tool, das als Open-Source-Tool unter Apache 2.0 veröffentlicht wurde, können Incident-Response und Malware-Forscher gebrauchsfertige YARA-Regeln bereitstellen, die aus einem Datensatz mit als böartig/gutartig gekennzeichneten Daten generiert werden. Joshua Saxe, Chef des SophosAI-Teams, hat YaraML so entwickelt, dass das Tool ohne vorherige Erfahrung mit maschinellem Lernen verwendet werden kann. Gleichzeitig ermöglicht es fortgeschrittenen Benutzern, die bereits Erfahrungen mit maschinellen Lernprojekten haben, benutzerdefinierte Parameter festzulegen.

YaraML analysiert einen Datensatz gutartig und böartig gekennzeichnete Zeichenfolgenartefakte, um YARA-Regeln zu erstellen und Muster zu extrahieren, die zum Identifizieren schädlicher Zeichenfolgenartefakte mit YARA verwendet werden können. Nähere Einzelheiten zur Analyse und Nutzung des Tools gibt es in einem umfangreichen [Blogeintrag](#) zu dem Thema.

Mit der aktuellen Initiative setzt Sophos seine Offensive zur herstellerübergreifenden Förderung gemeinsamer Innovationen im Bereich IT-Sicherheit weiter fort. Im Dezember 2021 wurden bereits vier neue Entwicklungen im Bereich offener Künstliche Intelligenz (KI) für Open-Source-Anwender veröffentlicht, die dazu beitragen, den Schutz gegen Cyberangriffe branchenweit zu optimieren.

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 Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198