Pressemeldung von SentinelOne vom 24.04.2020

MITRE ATT&CK-Evaluierung zeigt: SentinelOne ist führend bei EDR

Die Singularity-Plattform bietet eine beispiellose kontextbasierte Bedrohungserkennung und sorgt für weniger Zeitverlust und Komplexität in der IT-Sicherheit

München - 24. April 2020 - SentinelOne, das Unternehmen für autonomen Endpunktschutz, veröffentlicht seine Ergebnisse aus dem MITRE ATT&CK™ APT29-Bericht. Von den 29 evaluierten Endgeräteanbietern war SentinelOne in der Kategorie produktgetriebene EDR das Unternehmen mit der genauesten Erkennungsrate von Bedrohungen. Der Anbieter kann jeden Angriff in jeder Sekunde und auf allen wichtigen Angriffsflächen des Unternehmens abwehren, indem es die Effizienz der Sicherheitsteams mit einem verfolgbaren Bedrohungskontext und einer beispiellosen Sichtbarkeit erhöht.
Die Singularity-Plattform von SentinelOne wurde hinsichtlich der Fähigkeit bewertet, Angriffstechniken zu erkennen, die von APT29, einer der russischen Regierung zugeschriebenen Bedrohungsgruppe, eingesetzt werden. Durch die Integration des MITRE-Frameworks mit seiner ActiveEDR eliminiert Singularity die traditionelle und manuelle Arbeit, die Analysten für die Korrelation und Untersuchung ihrer Ergebnisse benötigen. Das Sicherheitspersonal kann automatisch feststellen, woher ein Angriff kommt, was der Angriff zu kompromittieren versucht und wie er zu beheben ist – und zwar autonom und ohne menschliches Eingreifen zur Vorbeugung und Beseitigung der Bedrohung.
Zu den wichtigsten Ergebnissen der MITRE-Evaluierung gehören:

1. Der Anbieter erreichte die höchste Anzahl kombinierter qualitativ hochwertiger Erkennungen und die höchste Anzahl automatisierter Korrelationen. Security-Analysten sind nicht in der Lage, mit ausgeklügelten Angriffsvektoren Schritt zu halten. Singularity hilft dabei, Daten in nachvollziehbare „Geschichten“ zu verwandeln, so dass sich die Analysten auf die Warnungen konzentrieren können, die am wichtigsten sind.
2. Der Anbieter gruppierte alle Daten des dreitägigen MITRE-Tests in nur 11 Konsolenwarnungen, wobei jede Warnung alle darin enthaltenen Details enthielt. Eine derartig effiziente Gruppierung von Alerts ist wichtig, um die Übersicht zu behalten und Nachrichtenmüdigkeit zu vermeiden. Singularity hat erfolgreich relevante, verwandte Daten, Kontext und Korrelationen gruppiert, was es für Analysten einfacher macht, sie zu verstehen und zu handeln.
3. Der Anbieter wies die höchste Anzahl von Erkennungen auf, die nur durch Werkzeuge erfolgen, und die höchste Anzahl von Erkennungen durch Menschen/MDR. Hohe Punktzahlen in diesen beiden Bereichen zeigen, dass Singularity Bedrohungen ohne die Unterstützung zusätzlicher Tools erkennen kann und beweist, dass Vigilance Managed Detection and Response <https://www.sentinelone.com/press/sentinelone-announces-new-vigilance-mdr-offerings/> (MDR) einen erstklassigen SOC-Service auf der Grundlage eines Weltklasseprodukts bietet.

„Die heutigen EDR-Plattformen müssen in der Lage sein, Daten in großem Maßstab aufzunehmen und zu korrelieren, sonst werden sie versagen“, sagt Chris Bates, CISO, SentinelOne. „CISOs wollen oder brauchen nicht mehr Daten – sie wollen Kontext und Intelligenz, um vorhandene Daten innerhalb des MITRE-Frameworks verwertbar und

aussagekräftig zu machen. Die Leistung von Singularity im APT29-Bericht löst unser Versprechen einer konkurrenzlosen Produktinnovation ein, indem sie einen umfassenden Überblick über das gesamte Unternehmen bietet, um Organisationen bei der Abwehr jedes Angriffs in jeder Phase des Bedrohungslebenszyklus durch eine einzige autonome Plattform zu unterstützen."
SentinelOne war eines der ersten Endpoint-Unternehmen, das Warnmeldungen im Produkt <https://www.sentinelone.com/blog/behavioral-indicators-and-mitre-attck-for-enterprise/>mit dem MITRE ATT&CK-Framework <https://www.sentinelone.com/press/sentinelone-integrates-mitre-attck-knowledge-base-next-gen-endpoint-solution/> korrelierte, die MITRE ATT&CK Endpoint Protection Product Evaluation <https://www.sentinelone.com/press/mitre-attck-evaluation/> übernahm und den MITRE ATT&CK-Rahmen als neuen Standard für die Bedrohungsjagd <https://www.sentinelone.com/press/sentinelone-disrupts-the-edr-paradigm-making-mitre-attck-framework-new-hunting-standard/> einbezog, womit das Unternehmen seine Führungsrolle bei der Bereitstellung eines unmittelbaren und erweiterten Bedrohungskontextes und der Sichtbarkeit innerhalb des MITRE-Frameworks unter Beweis stellte.

Über SentinelOne
SentinelOne bietet autonomen Endpunktschutz durch einen einzigen Agenten, der Angriffe über alle wichtigen Vektoren hinweg erfolgreich verhindert, erkennt und darauf reagiert. Die Singularity-Plattform wurde für eine extrem einfache Bedienung entwickelt und spart Kunden Zeit, indem sie KI zur automatischen Beseitigung von Bedrohungen in Echtzeit sowohl für standortbasierte als auch für Cloud-Umgebungen einsetzt. Sie ist die einzige Lösung, die direkt vom Endpunkt aus eine vollständige Transparenz über Netzwerke hinweg bietet. Wenn Sie mehr erfahren möchten, besuchen Sie www.sentinelone.com/de oder folgen Sie uns bei @SentinelOne, auf LinkedIn oder Facebook.

Kontakt

Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de