Pressemitteilung

API-Sicherheit: Cequence Security verstärkt API-Protection-Plattform mit generativer Künstlicher Intelligenz

Updates für API-Sicherheitstests und zur Betrugsabwehr

München, 28. Juni 2023 – Cequence Security, führender Anbieter von API-Sicherheitslösungen, erweitert seine Unified-API-Protection-Plattform (UAP). Die Updates erleichtern es Kunden, API-Risiken aufzudecken, zu managen und ihre Schnittstellen noch besser zu schützen. Durch neue Module in der End-to-End-Lösung ist es möglich, API-Sicherheitstests mit integrierter generativer KI-Automatisierung einfach zu implementieren, die API-Testergebnisse schneller für die Abwehr von Cyber-Betrug zu nutzen und IT-Security-Prozesse via Low-Code/No-Code-Workflows zu automatisieren.

„Mit unserer erweiterten UAP-Plattform rüsten sich unsere Kunden bestmöglich gegen Bedrohungen und Angreifer im API-Umfeld. Wir sind einer der ersten Anbieter von API-Sicherheitslösungen, der die Vorteile der generativen Künstlichen Intelligenz und der No-Code-Sicherheitsautomatisierung innerhalb einer API-Protection-Lösung nutzt“, sagt Ameya Talwalkar, CEO und Gründer von Cequence Security.

Generative KI-Automatisierung für hohen API-Schutz
Das Unternehmen nutzt das Potenzial von generativen KI-Tools wie ChatGPT und Google Bard und setzt deren Leistungen zum Schutz von Daten und Nutzern vor Cyber-Angriffen ein. Damit nimmt Cequence Security eine Vorreiterrolle im KI-basierten API-Schutz ein. Ein Beispiel dafür ist etwa die neue Funktion „Intelligent Mode“ im Bereich der API-Sicherheitstests. Das Feature ermöglicht es, Pläne für API-Sicherheitstests automatisch zu erstellen und den Low-Code/No-Code-Ansatz auf den API-Testkatalog auszuweiten. Je nach Funktionalität werden so die richtigen APIs automatisch mit den richtigen Testfällen verknüpft. Das reduziert den Zeitaufwand für die Erstellung eines Testplans deutlich – von mehreren Monaten bei herkömmlichen Lösungen auf Minuten bei der UAP-Plattform von Cequence Security.

Durch die API-Testing-Funktion lassen sich zudem Erfahrungswerte über die gesamten Anwendungen und Umgebungen eines Kunden durchgängig sammeln und für die Erhöhung der API-Sicherheit nutzen.

API Spartan: Cyber-Betrug im API-Umfeld abwehren
Updates hat Cequence Security auch für die Plattform-Tools „API Spartan“ und „API Spyder“ vorgenommen. API Spartan ermöglicht es IT-Security-Teams, ihre Schnittstellen vor dem gesamten Spektrum automatisierter API-Angriffe zu schützen. Mit dem neu integrierten Modul zur Betrugsabwehr schützen Unternehmen ihre Endkunden noch effektiver vor Online-Betrug. Im Angriffsfall können sie umgehend Sicherheitsmaßnahmen ergreifen und

zum Beispiel Transaktionen sperren oder Benachrichtigungen für die zuständigen Teams generieren.

API Spyder: API-Sichtbarkeit erhöhen
Als Management-Tool ist API Spyder eine der zentralen Säulen der UAP-Plattform von Cequence Security. Es verschafft IT-Security-, IT-Compliance- und IT-Governance-Teams einen Überblick über ihre öffentlich exponierten APIs und Ressourcen und deckt API-Angriffsflächen auf. Mit den neuen Erweiterungen von API Spyder können Organisationen die APIs, die zwar extern zugänglich, aber nicht vollständig geschützt sind, zuverlässig identifizieren.

Damit ergänzt API Spyder nahtlos das weitere Tool der UAP-Lösung „API Sentinel“. API Sentinel ermittelt alle verwalteten und nicht verwalteten APIs, die in einem Unternehmen betrieben werden. Das versetzt IT-Security-Teams in die Lage, die APIs zu monitoren, Risiken zu bewerten und Bedrohungen zu beheben, die durch Codierungsfehler zu Datenverlust und Geschäftsunterbrechungen führen können.

End-to-End-Lösung für den gesamten API-Protection-Lebenszyklus
Mit der Unified-API-Protection-Plattform bietet Cequence Security eine umfassende End-to-End-Lösung für den gesamten API-Protection-Lebenszyklus – vom Aufdecken über das Monitoren bis hin zum Schützen aller im Unternehmen vorhandenen Schnittstellen. Hyperverbundene Organisationen schützen ihre web-, mobil- und API-basierten Anwendungen vor Betrug, Geschäftsmissbrauch, Datenverlust, Business-Logic-Angriffen, Exploits und unbeabsichtigten Datenlecks.

Mehr Informationen auf www.cequence.ai

Pressekontakt:

Cequence Security
Mario van Riesen
Regional Sales Director DACH & CEE
Tel.: +49 151 7219 3673
Mail: mario@cequence.ai
Web: www.cequence.ai

VOCATO public relations GmbH
Birgit Brabeck /
Friederike Wagner
Tel.: +49 2234 60198 - 18 / - 16
Mail: bbrabeck@vocato.com / fwagner@vocato.com
Web: www.vocato.com

Über Cequence Security
Cequence Security bietet innovative Anwendungssicherheitslösungen für moderne hypervernetzte Unternehmen an. Das US-amerikanische Unternehmen mit Hauptsitz in Sunnyvale, Kalifornien, hat die Unified-API-Protection-Plattform entwickelt, die API-Erkennung, Inventarisierung, Compliance und dynamisches Testen mit Echtzeit-Erkennung von Bedrohungen gegen sich ständig weiterentwickelnde Online-Angriffe in einer Lösung vereint. Hyperverbundene Unternehmen schützen damit ihre web-, mobil- und API-basierten Anwendungen vor Betrug, Geschäftsmissbrauch und Datenverlust. Gegründet 2014, sichert Cequence Security heute mehr als sechs Milliarden API-Transaktionen pro Tag und schützt mehr als zwei Milliarden Benutzerkonten der Fortune-500-Kunden. Weitere Informationen auf www.cequence.ai

Bildmaterial:

Bild: Ameya Talwalkar, CEO und Gründer von Cequence Security.
Bildquelle: Cequence Security