Tenable erweitert seine Partnerschaft mit ServiceNow

München, 09. Mai 2019 - Tenable™, das Cyber Exposure Unternehmen, kündigt eine erweiterte Integration mit ServiceNow an, damit gemeinsame Kunden Schwachstellen besser priorisieren und beheben können. Die Partnerschaft adressiert eine der größten Herausforderungen der Cyber-Sicherheit: Eine Überforderung durch zu viele Schwachstellen.

Schwachstellen lassen sich mithilfe des Common Vulnerability Scoring System (CVSS) nur sehr eingeschränkt priorisieren, da die Mehrheit als „high" oder „critical" eingestuft wird. Tenable hat deshalb kürzlich Vulnerability Priority Ratings (VPR) als Teil von Predictive Prioritization vorgestellt. Mit VPR können sich Unternehmen auf die drei Prozent der Schwachstellen konzentrieren, die am ehesten ausgenutzt werden. Dank der Partnerschaft ist VPR jetzt auch für ServiceNow Security Operations verfügbar. Zum ersten Mal können Security- und IT-Teams VPR-Scores nutzen, um das spezifische Geschäftsrisiko der Schwachstellen zu prüfen, zu sortieren und entscheiden, welche sie priorisiert beheben.

Die neueste Integration ermöglicht es den Kunden, ihre Schwachstellendaten 400 Prozent schneller zu synchronisieren. Dafür werden mehrere Schwachstellen-Datenflüsse von Tenable gleichzeitig – anstatt einzeln – in ServiceNow Vulnerability Response und ServiceNow CMDB eingebunden. Tenable und ServiceNow helfen Security- und IT-Teams somit, schneller auf die gefährlichsten Schwachstellen zu reagieren und ihre Cyber Exposure-Lücke zu verkleinern.

„Mit den erweiterten Integrationen können die IT-Teams sich auf das Wesentliche konzentrieren: Die drei Prozent der Schwachstellen, die die größte Gefahr darstellen", sagt Ray Komar, Vice President of Technical Alliances, Tenable. „Den gemeinsamen Kunden stellen Tenable und ServiceNow die nötigen Mittel bereit, um ihre Cyber-Risiken besser zu verwalten, zu messen und zu reduzieren und strategische Cyber Exposure-Prozesse aufzubauen."

Die Integration führt eine einzelne App sowohl für Tenable.io als auch Tenable.sc (zuvor SecurityCenter) ein. Kunden, die die flexiblen Deployment-Optionen der Tenable

Cyber Exposure-Plattform nutzen, steht damit eine nahtlose Nutzererfahrung und ein nahtloses Interface bereit.

„Die meisten Datenlecks entstehen durch fehlende Patches. Trotzdem kämpfen viele Unternehmen schon mit einem grundlegenden Patching und der Reaktion auf Schwachstellen“, sagt Sean Convery, General Manager von ServiceNow Security Business. „ServiceNow und Tenable stellen die Schwachstellen in einen umfassenden Kontext zu den Auswirkungen und Sicherheitsrisiken. Auf dieser Basis können Unternehmen die Schwachstellen beheben, die den potenziell größten Schaden anrichten.“

Weitere Informationen über die Tenable-ServiceNow-Integration finden Sie hier.

Über Tenable

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Weltweit vertrauen über 27.000 Organisationen auf Tenable, um Cyberrisiken zu verstehen und zu reduzieren. Als Erfinder von Nessus® hat Tenable seine Expertise zunehmend erweitert und stellt die weltweit erste Plattform bereit, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und gesichert werden kann. Der Kundenstamm von Tenable umfasst mehr als 50 Prozent der Fortune 500, über 25 Prozent der Global 2000 und große Regierungsstellen. Weitere Informationen finden Sie unter https://de.tenable.com/