Tenable und ServiceNow formen Security-Allianz, um Cyberrisiken zu bekämpfen

München, 01. März 2018 – Tenable Network Security und ServiceNow, Inc. (NYSE: NOW) geben eine strategische Security-Allianz zwischen der Tenable Cyber-Exposure-Plattform und ServiceNow® Security Operations bekannt. Sie vereinfacht und beschleunigt es für Unternehmen und staatliche Einrichtungen, Cyberrisiken zu verstehen, zu managen und zu reduzieren.

Die digitale Transformation führt zu einer stark wachsenden Zahl von Technologien und Computing-Plattformen in Unternehmen. Dadurch entstehen übermäßig viele „blinde Flecken" in Netzwerken – diese zu verstehen, überschreitet oft die die Fähigkeiten von Unternehmen. Erschwerend kommt hinzu, dass Security- und IT-Teams häufig isoliert arbeiten. Sie können deshalb den neuen Problemen nicht begegnen. Zwar identifizieren die Verantwortlichen die Sicherheitslücken, diese werden aber nicht rechtzeitig behoben.

Tenable und ServiceNow ermöglichen Unternehmen die gesamte IT, Cloud- sowie IoT-Assets automatisiert zu erfassen und einen allgemeinen Einblick zu erhalten. Systeme werden kontinuierlich auf Schwachstellen überprüft, Assets nach ihrer geschäftlichen Bedeutung beurteilt und darauf basierend Probleme priorisiert sowie beschleunigt behoben. Gemeinsame Kunden können automatisierte Workflows nutzen, um ihre anfälligsten Assets als erstes zu sichern. Das spart nicht nur Zeit, sondern reduziert auch potenzielle Exposures, die mit der Schwachstelle zusammenhängen. Darüber hinaus kann mit der Integration ein automatisches Re-Assessment des Assets eingerichtet werden, um sicherzustellen, dass die Probleme behoben sind. Tenable und ServiceNow stellen Kunden somit einen umfassenden und abgeschlossenen Lösungsweg bereit.

„Wir freuen uns mit ServiceNow zusammenzuarbeiten, um unseren gemeinsamen Kunden eine erweiterte Sichtbarkeit und tiefere Einblicke in ihre Cyber Exposure zu liefern. Mit dieser können Anwender Cyberrisiken über die ganze Angriffsoberfläche hinweg, von IT, Cloud und Containern bis IoT-Geräte, verstehen und reduzieren", kommentiert Dave Cole, Chief Product Officer bei Tenable, die Zusammenarbeit. „Den Graben zwischen Security und IT zu überbrücken, ist die einzige Möglichkeit, um dem wachsenden Problem komplexer Angriffsoberflächen in digitalen Unternehmen zu begegnen."

„Security-Teams können Probleme nicht als ‚gelöst' vermerken, wenn sie lediglich die Sicherheitslücke gescannt haben", sagt Sean Convery, General Manager of ServiceNow's Security Business. „Zusammen geben Tenable und ServiceNow ihren Kunden die Möglichkeit, geschäftliche Auswirkungen und Sicherheitsrisiken zu verstehen. Dann wirken sich Patching und andere reaktive Maßnahmen bestmöglich aus und Sicherheitslücken werden schneller behoben."

Die Integration von Tenable SecurityCenter und ServiceNow Security Operations ist ab sofort im ServiceNow Store erhältlich. Die Integration von Tenable.io und ServiceNow Security

Operations folgt im Laufe 2018. Beide Unternehmen wollen Use Cases für verbesserte Fehlerbehebung, Konfigurations-Compliance und erweitertes Asset-Support unterstützen.

Über ServiceNow

ServiceNow verbessert die Arbeit im gesamten Unternehmen. Simple Aufgaben zu erledigen kann einfach sein und komplexe, mehrstufige Tätigkeiten ebenso. Unsere Anwendungen automatisieren, prognostizieren, digitalisieren und optimieren Geschäftsprozesse und Aufgaben, von der IT zum Kundenservice, Security Operations bis zu Human Resources. Gleichzeitig verbessert sich die Nutzererfahrung von Mitarbeitern, Anwendern und Kunden, während das Unternehmen transformiert wird. ServiceNow (NYSE:NOW) definiert, wie Arbeit erledigt wird. Für weitere Informationen besuchen Sie: www.servicenow.de.

Über Tenable

Tenable ist ein Cyber Exposure-Unternehmen. Weltweit vertrauen über 24.000 Unternehmen auf Tenable, um Cyberrisiken zu verstehen und zu reduzieren. Die Erfinder von Nessus haben ihre Expertise im Bereich Vulnerabilities in Tenable.io kombiniert und liefern die branchenweit erste Plattform, die Echtzeit-Einblick in alle Assets auf jeder beliebigen Computing-Plattform gewährt und diese Assets sichert. Der Kundenstamm von Tenable umfasst mehr als 50 Prozent der Fortune 500, über 20 Prozent der Global 2000 und große Regierungsstellen. Mehr auf: https://de.tenable.com/

Forward-Looking Statements

This press release contains forward-looking statements about the expectations, beliefs, plans, intentions and strategies relating to ServiceNow and Tenable's Strategic Security Alliance. Such forward-looking statements include statements regarding future integrations and offerings. The forward-looking statements in this press release are subject to various risks and uncertainties that could cause actual outcomes and results to differ materially and adversely from those expressed in such forward-looking statements. These risks and uncertainties include, without limitation, the company's ability to realize benefits from strategic partnerships and gain customer acceptance of new offerings and integrations. The information in this press release on new offerings, features, or functionality is intended to outline our general product direction and should not be relied upon in making a purchasing decision.