Tenable erweitert das Cyber Exposure Ecosystem

München, 29. Mai 2019 – Tenable™, das Cyber Exposure Unternehmen, erweitert sein Cyber Exposure Ecosystem um 19 neue und tiefer gehende Technologie Integrationen. Die Integrationen umfassen branchenführende Lösungen für Mobile Device Management (MDM), public Cloud Infrastrukturen, SIEM sowie IT Service Management. Sie bieten bessere Transparenz über die moderne Angriffsfläche plus integrierte Security und IT Workflows, sodass Kunden Probleme schneller erkennen und lösen können.

„Wir haben das Cyber Exposure Ecosystem gemeinsam mit erstklassigen Partnern aufgebaut, damit digitale Unternehmen ihre Cyber Risiken ganzheitlich und schnell verstehen und reduzieren können –über die gesamte Angriffsfläche hinweg“, sagt Ray Komar, Vice President of Technical Alliances, Tenable. „Wir verknüpfen punktuelle Lösungen und Datenquellen, damit unsere Kunden ihre Risiken effizient verwalten und reduzieren können.“

Partner verschiedenster Größe können ihre Lösungen mit der offenen Tenable Plattform einfach in das Cyber Exposure Ecosystem integrieren. Eine Auswahl der neuen Integrationen für Tenable.sc (ehemals SecurityCenter) und Tenable.io:

MDM:
Tenable hat neue Integrationen für Tenable.io mit BlackBerry Manager und Microsoft Intune veröffentlicht. Außerdem wurden die Integrationen mit **Microsoft ActiveSync**, **Airwatch by VMware**, **MobileIron** und **IBM MaaS360** erweitert – sowohl für Tenable.io als auch Tenable.sc. Die Integrationen sammeln mobile Asset Daten aus ihren jeweiligen MDM Anwendungen und sorgen so für bessere Einblicke und Assessments von Schwachstellen auf Mobilgeräten.

Public Clouds:

Die Tenable.io Cloud Connectors für **Amazon Web Services (AWS)**, **Google Cloud Platform (GCP)** und **Microsoft Azure Cloud Connectors** liefern jetzt erweiterte Funktionen wie Multi Account Auto Discovery. Diese gibt eine schnelle und vollständige Übersicht über die Accounts auf den drei beliebtesten public Cloud (IaaS) Plattformen. Tenable.io Cloud Connectors unterstützt nun außerdem die Rollenverteilung für AWS, um bessere, sicherere Authentifizierung zu ermöglichen.

SIEM:

Tenable hat die Integrationen von Tenable.sc und Tenable.io mit Splunk Produkten erweitert. Dies verbessert die Korrelation der Schwachstellen mit Maschinendaten. Außerdem vereinfachen sie Reporting und Dashboards. Darüber hinaus können Tenable und Splunk Kunden die relevanten Schwachstellendaten von Tenable in Splunk Enterprise Security (ES) nutzen. Das löst automatische Abläufe aus, die mit Splunk Phantom über den gesamten Workflow hinweg orchestriert werden können- vom Erkennen, über das Anreichern, Beurteilen, bis zur Behebung und dem Reporting. Splunk Phantom ist eine Security Orchestration Automation and Response (SOAR) Lösung. Für Kunden steht damit eine leistungsstarke, einzigartige und risikobasierte Methode bereit, mit der sie ihre Alerts besser sammeln und priorisieren können. Gleichzeitig beschleunigt die Automatisierung die Problemlösung erheblich.

Tenable ist das erste Unternehmen, dass seine Schwachstellen Management-Lösung mit Chronicle integriert. Die Integration mit Tenable.io reichert die Schwachstellendaten von Tenable mit Assets sowie Alarmen aus Chronicle an und stellt so nicht nur tiefgreifendere Einblicke in Security Probleme bereit, sondern ermöglicht auch schnellere Reaktionszeiten.

IT Service Management:

Tenable erweiterte kürzlich seine Integration mit ServiceNow und fügte sein Vulnerability Priority Rating (VPR) zu ServiceNow Security Operations hinzu. Gemeinsame Kunden können so Schwachstellen auf Basis des tatsächlichen Geschäftsrisikos priorisieren, filtern und einsehen. Zudem synchronisieren sie Schwachstellendaten 400 Prozent schneller. Dafür werden gleichzeitig mehrere Schwachstellen Datenflüsse von Tenable in ServiceNow Vulnerability Response und

ServiceNow CMDB eingebunden. Mit der erweiterten Integration stellt Tenable eine einzelne App sowohl für Tenable.io als auch Tenable.sc (zuvor SecurityCenter) vor.

Darüber hinaus hat Tenable die bestehende Tenable.io Integration mit **Atlassian Jira Core**, **Jira Software** und **Jira Service Desk** erweitert und auch Tenable.sc integriert. Damit werden automatisch Tickets für Schwachstellen geöffnet, die Tenable identifiziert, und wieder geschlossen, wenn sie behoben sind. Das sorgt für einen konsistenten und nachvollziehbaren Lösungsprozess.

Weitere Informationen darüber, wie Sie ein Tenable Technologiepartner werden können finden Sie unter www.tenable.com/partners/technology.

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/