Tenable-Lösung sichert kritische Infrastrukturen in konvergierten IT/OT-Umgebungen

München, 14. Juni 2018 – Tenable™, das Cyber Exposure-Unternehmen, veröffentlicht die branchenweit erste Lösung, die das Cybersicherheitsrisiko in den konvergierten IT/OT-Umgebungen von heute reduziert. Zudem kündigt Tenable eine Erweiterung für seine Tenable.io®-Plattform und Industrial Security an, eine Lösung, die Assets und Schwachstellen in Operational Technology (OT)-Systemen erkennt. Tenable stellt Industrial Security in Zusammenarbeit mit Siemens bereit und ermöglicht es Unternehmen, die Cyber Exposure ganzheitlich über IT und OT hinweg zu managen und Schwachstellen nach unternehmenskritischen Assets zu bewerten sowie effizient zu priorisieren.

OT- und kritische Infrastruktursysteme wurden ursprünglich so konzipiert, dass sie isoliert vom Netzwerk arbeiteten und von externen Cybersicherheitsbedrohungen abgeschirmt sind. Doch die Digitale Transformation hat auch diese isolierten Systeme erreicht, sie in vernetzte Geräte verwandelt und zu wertvollen Zielen für Angreifer gemacht. Laut der Warnung des FBI-Departments und des Department of Homeland Security vor russischen Angriffen auf kritische Infrastruktur in den USA, beginnen Angriffe auf OT-Assets tatsächlich oft damit, IT-Systeme zu kompromittieren und sich anschließend durch diese hindurchzuarbeiten. Konvergente Umgebungen enthalten eine Mischung aus IT- und OT-Geräten sowie -Systemen, die einen ganzheitlichen Ansatz für Cybersicherheit erfordern, so dass Unternehmen Cybersicherheitsrisiken präzise managen, messen und reduzieren können.

Zu den Erweiterungen gehören:

- Smart Scanning: Smart Scanning bildet eine smarte Ebene mithilfe von aktivem Scannen und passiver Netzwerküberwachung, um IT- und OT-Systeme in einem einzigen Workflow zu bewerten. In bestimmten Situationen kann das aktive Scannen bei empfindlichen OT-Systemen das System überlasten und letztendlich zu Systemstörungen führen. Smart Scanning stoppt das aktive Scannen von IT-Assets, wenn es diese als OT-Geräte identifiziert.
- Erweitertes OT Asset Coverage: Tenable weitet seine Bewertungsmöglichkeiten auf ein noch breiteres Spektrum von OT-Assets aus. Der erweiterte Support umfasst dabei über 250 zusätzliche Geräte und Anwendungen von Siemens, Schneider und Rockwell/Allen-Bradley und stellt den Kunden eine größere Transparenz ihrer OT-Anlagen und gemischten IT/OT-Technologie-Umgebungen bereit.
- Interaktive Topologiekarten: Neue 2D- und 3D-Topologiekarten zeigen die Verknüpfungen zwischen IT- und OT-Assets als Teil eines konvergenten Systems. Diese neue Ebene der IT- und OT-Asset-Intelligenz, kombiniert mit unserem tiefgehenden Wissen über Schwachstellen, bietet Kunden eine risikobasierte Heat Map, die sich auf unternehmenskritische Assets und Schwachstellen stützt und es so ermöglicht, diese effizient zu priorisieren und schneller zu beheben.

„Die Sicherheitsherausforderungen, denen Unternehmen mit operativen Technologien gegenübersehen, können nie überschätzt werden. IT- und OT-Assets allein – und auch zusammen als konvergierte Systeme - bilden einen Teil der modernen Angriffsfläche und stellen somit ein Cybersicherheitsrisiko dar. Unternehmen, die ihren Sicherheitsstatus einschätzen, aber OT-Assets vernachlässigen und nicht als Teil der Angriffsfläche betrachten, haben nicht die kritische Sichtbarkeit, um ihre Cyber Exposure zu verstehen“, sagt Dave Cole, Chief Product Officer, Tenable. „Mit Tenable.io, einschließlich unseres speziell für die OT-Sicherheit entwickelten Angebots für industrielle Sicherheit, bricht Tenable mit den versteckten Silos und liefert einen einzigartigen Überblick in die gesamte Cyber Exposure in konvergierten IT/OT-Umgebungen.“

Die Ankündigung folgt auf die Entdeckung einer kritischen Schwachstelle bei der Remotecode-Ausführung in zwei Applikationen von Schneider Electric, die in den Bereichen Produktion, Öl und Gas, Wasser, Automatisierung sowie Wind- und Solarenergie eingesetzt werden und unterstreicht das Engagement des Unternehmens für wegweisende Lösungen für die Cybersicherheit in OT und kritischen Infrastrukturen. Weitere Informationen, wie Tenable Unternehmen hilft, Cyberrisiken in konvergierten IT- und OT-Umgebungen zu verstehen und zu reduzieren, finden Sie unter: https://www.tenable.com/solutions/iot

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/