Tenable stellt branchenweit erste integrierte Lösung für konvergierte IT/OT Umgebungen vor

Die Lösung deckt zudem zusätzlich tausende neue Geräte führender Industriehersteller ab

München, 27. Februar 2019 – Tenable™, das Cyber Exposure-Unternehmen, stellt die branchenweit erste integrierte Cyber Exposure-Lösung vor, die einen einheitlichen Blick auf Cyberrisiken in IT-Netzwerken, Operational Technology (OT), Enterprise-Anwendungen sowie industriellen Kontrollsystemen bietet. Dafür integriert Tenable Industrial Security™ in Tenable.sc™ (zuvor SecurityCenter). Security-Verantwortliche können damit zum ersten Mal Cyberrisiken über eine einzelne Plattform erfassen, verwalten und reduzieren – sowohl für IT- als auch für OT-Umgebungen.

Die digitale Transformation beendet die Zeiten isolierter OT-Assets weitgehend, weil moderne OT-Umgebungen zunehmend mit der IT vernetzt sind. Daraus entsteht eine komplexe, sensible und stark wachsende Angriffsoberfläche. Da ein effektives Risikomanagement ein ganzheitliches Verständnis der IT-/OT-Angriffsoberfläche erfordert, verlagern viele Unternehmen die Verantwortung für die OT-Sicherheit zum Chief Information Security Officer (CISO). Doch ergibt sich hier ein neues Problem: Traditionellen IT-Sicherheitslösungen fehlt die Möglichkeiten, sensible OT-Assets fortlaufend zu identifizieren und zu bewerten. Umgekehrt funktionieren viele OT-Lösungen nicht in der Welt der IT. Durch diesen fehlenden ganzheitlichen Einblick entstehen sicherheitskritische blinde Flecken, die eine Gefahr für wichtige Systeme darstellen – diese können kompromittiert oder ausgeschaltet werden. Der Angriff auf ein wertvolles OT-Asset könnte beispielsweise damit beginnen, über ein traditionelles IT-Asset ins System einzudringen und sich von dort aus auszubreiten.

Gemeinsam mit Industrial Security eingesetzt, löst Tenable.sc dieses Problem, indem es bisher unerreichte Einblicke in konvergierte IT-/OT-Umgebungen bereitstellt. Tenable.sc setzt branchenführende Nessus®-Scanner ein, um zahlreiche sicherheitsrelevante Informationen über IT-basierte Assets in OT- und IT-Netzwerken zu sammeln. Diese Informationen verbindet Tenable.sc dann mit passiv erfassten Daten zu Assets und Schwachstellen aus Industrial Security. Anwendern bietet die Lösung so sichere, zuverlässige Asset-Erkennung und Schwachstellenmanagement speziell für OT-Umgebungen. Der Vorteil: Als OT-fokussierte Lösung wählt Industrial Security einen Ansatz für

das Schwachstellenmanagement, der Prozesse im Unternehmen nicht stört. Deshalb können Anwender OT-Risiken identifizieren, priorisieren und ihre kritischen Produktions-Assets sichern, ohne dabei deren Funktionen einzuschränken. Die Integration von Tenable.sc und Industrial Security bietet das erste Gesamtbild der IT- und OT-Assets, identifiziert Risiken und Schwachstellen im gesamten Unternehmen. Das hilft den Verantwortlichen, Cybersicherheit mit Blick auf geschäftliche Risiken zu priorisieren und zu verwalten.

Zusätzliche Verbesserungen für die integrierte Lösung umfassen:

- **Integration mit dem Tenable Cyber Exposure Technology Ecosystem**, um Fehlerbehebung und Reaktionsprozesse sowohl für IT- als auch für OT-Umgebungen zu verbessern. Zu Tenables marktführenden Integrationspartnern im Ökosystem gehören einige der am meisten genutzten Security- und IT-Technologien, darunter Lösungen für Privileged Access Management, SIEM, IT Ticketing und Configuration Management Database (CMDB). Mit den integrierten Lösungen können Probleme schneller entdeckt und gelöst werden, weil sie einen besseren Überblick über die moderne Angriffsoberfläche, tiefergehende Analysen sowie integrierte Daten und Workflows bieten. Auf dieser Basis können Security- und IT-Operations-Teams besser zusammenarbeiten.

- **Mehr OT-Assets werden abgedeckt**, darunter einige tausend neue Geräte führender Industriehersteller, wie Yokogawa und Emerson. Diese Hersteller stoßen zu den Top-10 der Industriehersteller hinzu, deren Geräte bereits von Industrial Security abgedeckt werden – dazu gehören etwa Siemens, Schneider, Rockwell/Allen-Bradley, Honeywell, Mitsubishi.

„Die Vernetzung digitaler Infrastruktur bedeutet, dass sich die Sicherheit der IT direkt auf der OT auswirkt und umgekehrt. Ohne einen einheitlichen Blick auf konvergierte IT-/OT-Umgebungen tappen CISOs bei der Verteidigung ihres Unternehmens im Dunkeln. Der fehlende Blick auf das große Ganze ist also eine schlechte Cyber-Strategie und gefährdet das Unternehmen“, sagt Renaud Deraison, Mitgründer und Chief Technology Officer. „Tenable.sc ist eine Plattform, die von Tausenden CISOs und Security-Teams für ihr On-Premise Schwachstellenmanagement geschätzt wird. Die Integration mit Industrial Security für einen ganzheitlichen Blick auf IT und OT ist der naheliegende nächste Schritt, um unsere führenden Fähigkeiten im Bereich Schwachstellenmanagement weiter auszubauen.“

Weitere Informationen über die Integration finden Sie unter http://lookbook.tenable.com/it-ot-convergence-gartner/industrial-security-overview.

Über Tenable

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Weltweit vertrauen über 24.000 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/