DAS PROBLEM – UND UNSERE LÖSUNG

Die moderne Angriffsoberfläche wächst, verändert sich ständig und ist verflochtener als je zuvor. Als Reaktion darauf setzen Security-Teams eine Vielzahl von Sicherheitstechnologien ein – jede mit ihren eigenen Analysen und ohne einheitliche Berichterstattung. Gänzlich verschiedene Tools können zu doppeltem Aufwand und ineffektiven Programmen führen, ohne dass sich ein klarer Weg bietet, um das Risiko spürbar zu verringern oder die Sicherheitslage eines Unternehmens schnell und präzise zu kommunizieren. Noch gravierender ist, dass die Verteidiger durch diesen reaktiven, auf „Brandbekämpfung" ausgelegten Ansatz für Cybersicherheit stark im Nachteil sind.

Cybersecurity-Teams benötigen eine einheitliche, prädiktive und proaktive Methode, um Gefährdungen auf der gesamten Angriffsoberfläche zu managen. Die Exposure Management-Plattform Tenable One vermittelt ein kontextbezogenes Risikobewusstsein und macht es möglich, von einer reaktiven zu einer präventiven Vorgehensweise überzugehen – damit Cybersecurity-Teams Bedrohungen vorhersehen und abwehren können, bevor diese Schäden verursachen.

ZAHLEN UND FAKTEN

GEGRÜNDET
2002

STANDORTE
- Columbia, Maryland, USA
- Internationaler Hauptsitz in Dublin, Irland
- Präsenz in mehr als 40 Ländern

MARKTSTELLUNG
- Mehr als 40.000 Kunden
- Über 60 Prozent der Fortune 500-Unternehmen
- Über 40 Prozent der Global 2000-Unternehmen

UNTERNEHMENSLEITUNG
Amit Yoran, Chairman und CEO
Nico Popp, Chief Product Officer
Glen Pendley, Chief Technology Officer
Steve Vintz, Chief Financial Officer
Bridgett Paradise, Chief People and Culture Officer
Mark Thurmond, Chief Operating Officer
Brian Goldfarb, Chief Marketing Officer
Dave Feringa, Chief Revenue Officer
Terry Dolce, EVP, Operations, Global Business Development and Channels
Michela Stribling, Chief Communications Officer
Robert Huber, Chief Security Officer
Patricia Grant, Chief Information Officer
Matt Olton, Senior Vice President of Corporate Development and Strategy

ÜBER TENABLE

Tenable® ist das Unternehmen für Exposure Management. Rund 40.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen ca. 60 Prozent der Fortune 500-Unternehmen, ca. 40 Prozent der Global 2000 sowie große Regierungsbehörden. Weitere Informationen finden Sie auf de.tenable.com.

TENABLE ONE – DIE EXPOSURE MANAGEMENT-PLATTFORM

Tenable One soll Unternehmen dabei helfen, Sichtbarkeit auf ihrer gesamten modernen Angriffsoberfläche zu erzielen, Maßnahmen auf das Verhindern wahrscheinlicher Angriffe zu fokussieren und Cyberrisiken präzise zu kommunizieren, um eine optimale Unternehmensleistung zu unterstützen. Die Tenable One-Plattform bietet umfassende Schwachstellen-Abdeckung über IT-Assets, Cloud-Ressourcen, Container, Web-Apps und Identitätssysteme hinweg.

TENABLE BIETET:

Cloud-Sicherheit
Tenable ermöglicht umfassende Sichtbarkeit und Sicherheit für Multi-Cloud-Umgebungen und liefert einen einheitlichen Überblick über Schwachstellen, Fehlkonfigurationen und Drift in einer zentralen Ansicht. Priorisieren Sie Maßnahmen im Handumdrehen – mit risikobasiertem Scoring, Compliance-Reporting sowie automatisierten Behebungsmaßnahmen, die die mittlere Zeit bis zur Reaktion (Mean Time to Respond, MTTR) um bis zu 99 % senken.

Web-App-Sicherheit
Webanwendungen sind allgegenwärtig, geschäftskritisch und verändern sich ständig. Tenable bietet benutzerfreundliches, umfassendes und automatisiertes Schwachstellen-Scanning für moderne Webapplikationen. Nutzer können Web-App-Scans konfigurieren und verwalten und erhalten handlungsrelevante Ergebnisse binnen weniger Minuten.

Active Directory-Sicherheit
Hinter nahezu jeder Datenpanne in den Schlagzeilen steckt ein Angriff auf Active Directory (AD), der es Angreifern ermöglicht, die Zugriffsrechte zu erhöhen und sich im Netzwerk seitwärts fortzubewegen. Tenable versetzt Nutzer in die Lage, in ihrer AD-Umgebung alles zu sehen, vorherzusagen, was wichtig ist, und Risiken zu beseitigen, um Angriffspfade zu versperren, bevor Angreifer sie ausnutzen können.

Risikobasiertes Schwachstellen-Management
Herkömmliche Tools für das Schwachstellen-Management (Vulnerability Management, VM) können mit der IT-Landschaft von heute nicht mithalten. Risikobasiertes Schwachstellen-Management macht Schluss mit Rätselraten und gibt eindeutige Antworten auf die Frage, welche Schwachstellen zuerst behoben werden müssen.

External Attack Surface Management
Sichtbarkeit ist für Cybersecurity von grundlegender Bedeutung, doch nur wenige Unternehmen haben dieses Problem im Griff. External Attack Surface Management (EASM) bildet das gesamte Internet ab und ermittelt sämtliche Domänen Ihres Unternehmens. Identifizieren und schützen Sie zuvor unbekannte Assets mit Internetanbindung, um blinde Flecken zu beseitigen.

Sicherheit für operative Technologien
Durch die digitale Transformation der Industrie werden Kontrolle, Effizienz, Produktion und Sicherheit gesteigert, aber dies ist nicht ohne Risiken. Tenable bietet umfassende Transparenz, einheitliche Sicherheit und Priorisierung des Bedrohungsmanagements, um Risiken in einer integrierten IT- und OT-Landschaft zu minimieren.

Basierend auf Nessus – dem Goldstandard in Sachen Schwachstellenbewertung
Ein genaues Verständnis von Schwachstellen ist für Exposure Management von grundlegender Bedeutung – und Nessus ist das Herzstück von Tenable One. Nessus unterstützt Nutzer bei der Bewertung ihrer modernen Angriffsoberflächen und liefert ein genaues Bild, damit sie schnell und effektiv arbeiten können.