



Tenable stellt Innovationen für die Cyber Exposure-Analyse vor

München, 04. Juni 2019 – [Tenable](#), das Cyber Exposure Unternehmen, stellt weitere innovative Analyse-Funktionen für Tenable Lumin vor. Diese stützen sich auf Machine Learning und korrelieren Schwachstellen und Bedrohungsdaten mit Informationen zur Asset-Kritikalität. Unternehmen können damit erstmalig die Cyber Exposure exakt bewerten, Trends erkennen und auch messen. All dies geschieht abhängig von der Wahrscheinlichkeit, mit der die verschiedenen Schwachstellen ausgenutzt werden und abhängig davon, wie geschäftskritisch das betroffene Asset ist.

Die neuen, innovativen Funktionen zur Cyber Exposure-Analyse mit Tenable Lumin:

Cyber Exposure Score: Dieser Wert ermittelt die tatsächlichen Cyber-Risiken und stützt sich dafür auf datenwissenschaftliche Messungen zu Schwachstellen, Threat Intelligence und darauf, wie wichtig die verschiedenen Assets für den Geschäftserfolg sind. Lumin erledigt dies automatisch mittels Machine-Learning-Algorithmen. Dafür nutzt die Lösung zum einen das Tenable Vulnerability Priority Rating (VPR), das bestimmt, mit welcher Wahrscheinlichkeit eine Schwachstelle ausgenutzt wird. Zum anderen bestimmt das Tenable Asset Criticality Rating (ACR), wie geschäftskritisch betroffene Assets sind. So können Unternehmen langfristig erkennen, wie effektiv ihre Security-Maßnahmen sind.

Cyber Exposure Benchmarking: Unternehmen können mit dem ermittelten Cyber Exposure Score den Erfolg ihrer Security-Strategien mit denen anderer Branchenplayer vergleichen, und so erkennen, wie gut sie gegen Cyber-Risiken aufgestellt sind. Tenable verarbeitet 1,5 Milliarden Sicherheitsvorfälle pro Woche und kann deshalb auf die umfassendsten Threat-Intelligence-Daten der Branche zurückgreifen. Das daraus gewonnene Wissen kombiniert Tenable mit Data Science, um eine noch umfangreichere Datenbasis für die Auswertung zu erhalten. So können

Unternehmen beispielsweise exakt bestimmen, wie sicher die verschiedenen Abteilungen oder Außenstellen sind.

Remediation Guidance Workflow: Sicherheitsteams erhalten eine Liste wichtiger Empfehlungen, wie sie die Cyber Exposure des Unternehmens verringern können. Für weitere Informationen können die Teams den verschiedenen Schwachstellen und Assets genau auf den Grund gehen und den geschäftlichen wie den technischen Kontext analysieren. Das hilft dabei, Probleme noch effektiver zu beheben.

„Cyber Exposure wird immer wichtiger. Die grundlegende Frage ist dabei, wie sicher sind wir. Mit den innovativen Funktionen erhalten Unternehmen neue Möglichkeiten. Zuvor konnten sie diese Frage nicht anhand der geschäftlichen Folgen oder anhand von Daten über die bestehenden Risiken beantworten“, erklärt Ofer Ben-David, Chief Product Officer bei Tenable. „Wir bauen unsere umfassende Schwachstellen-Expertise noch weiter aus, um objektive Messwerte zu den Cyber-Risiken zu gewinnen. Diese beeinflussen künftig die Art und Weise, wie Security-Technologie entwickelt und Geschäftsentscheidungen gefällt werden.“

Die neuen Funktionen werden ab Q3 2019 als Teil der Beta-Version von Tenable Lumin verfügbar sein. Tenable Lumin wird in der zweiten Hälfte 2019 verfügbar sein.

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/>