Integriertes Exposure Management

Tenable gilt als Vorreiter des Vulnerability Managements, hat mit seiner Exposure-Management-Plattform, die einen kompletten Überblick über alle Cyberrisiken ermöglicht, aber viel mehr zu bieten. Patrick Michel, Principal Consultant bei BOLL Engineering, gibt im Interview Auskunft über die Lösungen und deren Vorteile.

Patrick Michel ist Principal Consultant bei BOLL.

Tenable – wer ist das?
Patrick Michel: Das 2002 gegründete Unternehmen Tenable hat sich zu Beginn mit der Lösung Nessus dem Vulnerability Management verschrieben. Heute bietet Tenable eine komplette, analyseorientierte Exposure-Management-Plattform an, die praktisch alle Aspekte der Cybersecurity abdeckt und eine umfassende und gleichzeitig detaillierte Übersicht über die Cyberrisiken, die ein Unternehmen bedrohen können, verschafft.

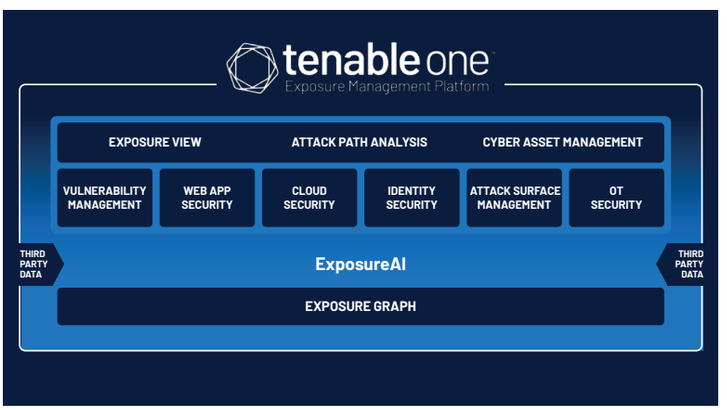
Was unterscheidet Tenable von Anbietern vergleichbarer Lösungen?
Wie andere Cybersecurity-Anbieter hat Tenable im Lauf der Jahre mehrere Produkte und Cybersecurity-Firmen dazugekauft. Tenable hat es jedoch auf einzigartige Weise geschafft, die verschiedenen Lösungen so zu integrieren, dass sich eine einheitliche Plattform bildet, die mit einer einzigen, einheitlichen Sicht der Angriffsoberfläche aufwarten kann.

Wie heisst diese Plattform, und wie ist sie aufgebaut?
Sie nennt sich Tenable One. Nebst einer speziell angepassten Version von Nessus ermöglichen drei Kernkomponenten eine fundierte Bewertung und Priorisierung aller Cyberrisiken, damit das Wichtigste zuerst angegangen wird:

- «Asset Inventory» bietet eine zentralisierte Sicht auf alle Assets im Unternehmensnetz. Vor dem Hintergrund, dass viele Unternehmen nicht wissen, welche Systeme überhaupt vorhanden sind, ein zentraler Aspekt.
- «Lumin Exposure View» fasst die Risiko-Insights anschaulich zusammen.
- «Attack Path Analysis» hilft, die wichtigsten und somit die gefährlichsten Schwachstellen innerhalb eines Angriffspfads zu finden. Das hilft bei der Priorisierung der zu schliessenden Schwachstellen.

Das Ganze wird unterstützt durch die integrierte generative KI ExposureAI und durch Exposure-Informationen des Tenable-Research-Teams. Darauf aufbauend bietet die Plattform Lösungen für unterschiedliche technische Bereiche.

Welche Bereiche werden abgedeckt?
Tenable One maximiert die IT-Security einerseits durch ein klassisches, allgemeines Vulnerability Management, bietet andererseits aber weit mehr. So sorgen dedizierte Komponenten für die Sicherheit von Web-Apps sowie von einfachen bis komplexen Cloud- und Multi-Cloud-Umgebungen (inklusive Kubernetes und Container-Umgebungen). Zudem unterstützt die Lösung die Sicherung der Authentizität von Identitäten (etwa im Active Directory), ermöglicht die Sicherung von OT-Systemen und erlaubt ein übergreifendes Management der Angriffsoberfläche.



Wie lässt sich Tenable One nutzen?
Die Plattform arbeitet cloudbasiert und kann somit ohne On-Premises-Installation genutzt werden. Sie ist zudem mandantenfähig und steht als Managed Service zur Verfügung – attraktiv auch für Partner, die ihren Kunden eine umfassende Cybersecurity-Plattform erster Güte mit geringstmöglichem Aufwand anbieten möchten.

Für welche Unternehmen eignet sich die Plattform?
Tenable zielt mit seinen Lösungen – wie die meisten US-amerikanischen Anbieter – verstärkt auf das Enterprise-Segment und hat Kunden mit bis zu 150 000 Mitarbeitenden. Tenable One ist jedoch sehr gut skalierbar und kann seine Vorteile auch in mittelgrossen Unternehmen ausspielen, zum Beispiel in einem KMU mit 100 oder 200 Mitarbeitenden. Dies gilt in ganz besonderem Mass für die Managed-Service-Variante, die sich sehr flexibel einsetzen lässt.

Was zeichnet Tenable weiter aus?
Der hervorragende Support, der Partnern und deren Kunden das Leben erleichtert und sich fundiert und zeitgerecht um Probleme kümmert. Eine derart hohe Supportqualität ist erfahrungsgemäss nicht bei allen Mitbewerbern gegeben. Ein klarer Vorteil der integrierten Plattform ist zudem die Bereitstellung belastbarer Risikoinformationen, die für die Einhaltung der unternehmenseigenen Compliance und regulatorischer Vorgaben unabdingbar sind.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 I 5430 Wettingen
056 437 60 60 I info@boll.ch
www.boll.ch