Tenable erweitert sein Sicherheitsportfolio für Cloud und Applikationen und liefert damit ganzheitliche Einblicke in die Cyber Exposure

Erweiterungen ermöglichen einen durchgängigen DevOps-Prozess

München, 6. Mai 2018 – Tenable™, das Cyber Exposure-Unternehmen, kündigt neue Produkte und Erweiterungen seines Ökosystems rund um Tenable.io® an, der Cloud-basierten Cyber Exposure-Plattform. Tenable.io unterstützt Sicherheitsteams dabei, Cyberrisiken in hochdynamischen Cloud-Umgebungen zu identifizieren, zu messen und zu managen. Diese Cloud-Erweiterungen für den Unternehmenseinsatz sind die ersten ihrer Art und bieten eine einheitliche Sicht auf die Cyber Exposure von Web-Applikationen, Containern und Cloud-Infrastrukturen. Damit beschleunigt Tenable die Einführung von DevOps-Abläufen und senkt Cyberrisiken in Unternehmen.

Mit Public Clouds können Unternehmen diese Infrastruktur als Code nutzen. Das bedeutet, dass sie dadurch verschiedene, verfügbare Bausteine, wie z.B. Speicherdienste, virtuelle Maschinen, Container und das Netzwerk an sich, über Abruf der Public Cloud APIs modifizieren können. Mit Cloud Computing haben Unternehmen enorme Vorteile in Sachen Geschwindigkeit und Agilität. Das wiederum treibt die Entwicklung von DevOps-Abläufen voran – sie erlauben es, täglich oder sogar stündlich, neue Anwendungsfunktionen zu implementieren. Trotz aller Vorteile machen Cloud Computing und DevOps die Arbeit von Sicherheitsteams auch komplexer: z.B. sorgen sie zwar für schnelle Änderungen an Produktionsumgebungen sowie kurzlebige und sogar serverlose Assets, doch verursachen sie gleichzeitig „Tote Winkel“ im Netzwerk, die Sicherheitssysteme nicht einsehen können, was in den meisten Fällen unkontrollierbare Cyberrisiken zur Folge hat.

Unternehmen benötigen sowohl einen umfassenden Sicherheitsansatz als auch Einblick in sämtliche Geräte, Schwachstellen und Risiken. Die neuen Produkte und Erweiterungen des Ökosystems von Tenable bieten einen zusammengefassten Einblick in die Cyber Exposure – über traditionelle IT- und heterogene Cloud-Plattformen hinweg. Damit können Unternehmen die Sicherheit im gesamten Lebenszyklus der Softwareentwicklung integrieren – vom Build bis zur Produktion.

Verbesserungen der neuen Tenable.io-Plattform und des Cloud-Ökosystems:

- **Microsoft Azure und Google Cloud Platform (GCP) Cloud Connectors:** Erkennt und verfolgt automatisiert und kontinuierlich Asset-Änderungen in Azure- und GCP-Cloud-Umgebungen. So stellen Unternehmen sicher, dass alle Cloud-Workloads bekannt sind und auf Schwachstellen untersucht werden. Die Tenable.io Cloud Connectors für Azure und GCP ergänzen den bestehenden Cloud Connector für Amazon Web Services (AWS) und bieten eine einheitliche Sicht auf Cybersicherheitsrisiken auf den drei meistgenutzten Public Cloud (IaaS) Plattformen.

- **Container-Runtime-Scanning:** Einblick in die Cyber Exposure von Containern, die in der Produktion laufen. Tenable.io Container Security erkennt automatisiert neue Container sowie Änderungen an laufenden Containern in der Produktionsumgebung, damit diese auf Schwachstellen untersucht werden können. Dies ergänzt die bestehenden Möglichkeiten für Sicherheitstests von Container-Images während des Buildprozesses und die Identifizierung von Docker-Hosts, die in der Produktion laufen. Tenable.io Container Security und Tenable.io Vulnerability Management integrieren die Sicherheit nahtlos in den End-to-End DevOps-Prozess und bieten gleichzeitig eine konsistente Sicht auf die Daten und ein einheitliches Kundenerlebnis.
- **Web-Applikationen aufspüren:** Identifiziert sowohl die vom Unternehmen selbst eingesetzten Web-Applikationen als auch bisher unbekannte Anwendungen, damit Unternehmen die Cyber Exposure der gesamten Umgebung von Web-Applikationen verstehen. Bisher mussten die Sicherheitsteams festlegen, welche Web-Applikationen gescannt werden, indem sie die Ziel-URLs eingaben. Dabei ist es für die Sicherheit eines Unternehmens entscheidend, dass es erkennt, welche Web-Applikationen sich in seinem Netzwerk befinden. Die Anzahl der eingesetzten Web-Anwendungen ist oft höher, als den Sicherheitsteams bewusst ist. Diese hat erhebliche „Tote Winkel“ zur Folge: das Cyberrisiko steigt.
- **Cloud Security Alliance:** Tenable hat als Mitglied der Cloud Security Alliance (CSA) das CSA STAR (Security, Trust & Assurance Registry) Self-Assessment für Tenable.io durchgeführt. CSA STAR ist das leistungsstärkste Programm der Branche für die Sicherheitzertifizierung in der Cloud.

"Der weitverbreitete Cloud-Einsatz sorgt bei Sicherheitsteams für gefährliche, blinde Flecken oder zwingt sie dazu, Tools einzusetzen, die nur Einblicke auf einzelne Aspekte liefern, die später manuell zu einem vollständigen Bild der Umgebung zusammengefügt werden müssen", sagte Dave Cole, Chief Product Officer, Tenable. "Das ist viel zu viel Arbeit und das Gegenteil der durch Cloud oder DevOps erhofften Geschwindigkeit. Wir wollen es unseren Kunden erlauben, das gesamte Spektrum moderner Risiken schnell und besonders einfach zu managen. Mit Tenable.io können sie diesen neuen Herausforderungen begegnen."

Zusätzliche Informationen

● Lesen Sie auf dem Tenable-Blog einen Beitrag von Renaud Deraison, Mitbegründer und CTO von Tenable, zur Sicherung der Cloud-Infrastruktur.
● Registrieren Sie sich für das gemeinsame Webinar der Cloud Security Alliance und Tenable zum Thema Secure DevOps: Application Security from Development through Runtime – am 5. Juni um 12 Uhr EDT
● Fordern Sie eine Testversion von Tenable.io Vulnerability Management, Container Security oder Web Application Scanning an

Konnektoren für Azure und GCP Cloud und das Container Runtime Scanning sind in der Regel innerhalb von 60 Tagen verfügbar. Einblicke in Web-Applikationen sind ab dem zweiten Halbjahr 2018 verfügbar. Die Cloud Konnektoren sind im Lieferumfang von Tenable.io Vulnerability Management enthalten. Die Container-Laufzeitüberprüfung ist in Tenable.io Container Security enthalten. Die Erkennung von Web-Applikationen ist in Tenable.io Web Application Scanning enthalten.