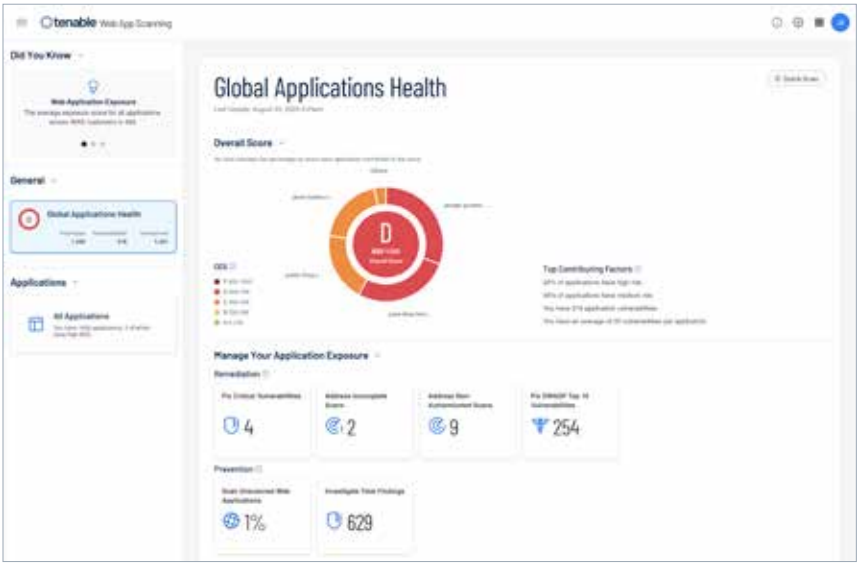
DATENBLATT

EIN EINFACHER UND SKALIERBARER ANSATZ FÜR DYNAMISCHE TESTS DER ANWENDUNGSSICHERHEIT

Angesichts des beispiellosen Tempos bei der Entwicklung zunehmend komplexer Geschäftsanwendungen stellt die Absicherung moderner Webanwendungen für Unternehmen nach wie vor eine Herausforderung dar. Viele Unternehmen veröffentlichen mehrmals am Tag neue oder aktualisierte Webanwendungen, die durchschnittlich gleich mehrere Schwachstellen aufweisen. Nicht selten kommt auf 100 Entwickler nur ein Cybersecurity-Mitarbeiter. Das macht es vielen Sicherheitsteams so gut wie unmöglich, mit der Entwicklung Schritt zu halten. Zahlreiche Webanwendungen werden daher erst dann auf Sicherheitsprobleme geprüft, wenn es bereits zu spät ist. Der Mangel an Qualifikationen und Ressourcen im Bereich Anwendungssicherheit hindert viele Unternehmen daran, sich angemessen vor Cyberbedrohungen zu schützen.

Noch ein weiteres eigenständiges Sicherheitsprodukt einzusetzen, ist jedoch keine Lösung. Sicherheitsverantwortliche müssen im Rahmen einer umfassenden Exposure-Management-Lösung Einblick in die Sicherheit ihrer gesamten Webanwendungen erhalten, damit sie sich ein vollständiges Bild von ihrer Sicherheits- und Compliance-Lage machen können.

Ganz gleich, ob als eigenständiges Modul für Tenable Vulnerability Management oder als zentraler Bestandteil der Exposure-Management-Plattform Tenable One: Tenable Web App Scanning bietet Einblick in die Sicherheit sämtlicher Webanwendungen. Tenable Web App Scanning ist als SaaS-basierte oder als On-Prem-Lösung erhältlich und ermöglicht sicheres, automatisiertes und mühelos skalierbares Schwachstellen-Scanning für das gesamte Portfolio, sodass Sicherheitsexperten ihre Webanwendungen schnell und ohne großen manuellen Aufwand bewerten können. Tenable Web App Scanning bietet hohe Erkennungsraten mit einer minimalen Anzahl falsch-positiver Ergebnisse, um Ihnen ein genaues Verständnis der tatsächlichen Cyberrisiken in Ihren Web-Apps zu vermitteln.



Mit Tenable Web App Scanning können Sicherheitsteams sich die identifizierten Schwachstellen anzeigen lassen, um Sichtbarkeit und die effektive Priorisierung von Behebungsmaßnahmen zu gewährleisten.

Wichtige Vorteile

- **Verbessern der Scan-Zuverlässigkeit**
  Liefert äußerst präzise Ergebnisse mit minimalen Falschmeldungen, damit Sie und Ihre Entwickler wissen, dass auf Ihre Berichte Verlass ist.
- **Reduzieren des manuellen Arbeitsaufwands**
  Dank automatisiertem Scanning mit geringem manuellen Aufwand verschaffen Sie sich einen vollständigen Überblick über die Sicherheitsrisiken von Webanwendungen in Ihrer sich verändernden Umgebung – ohne den normalerweise erforderlichen Arbeits- und Zeitaufwand.
- **Beseitigen sicherheitsrelevanter blinder Flecken**
  Scannen Sie alle Ihre Applikationen – einschließlich solcher, die mit modernen Web-Frameworks wie JavaScript, AJAX, HTML5 und Single-Page-Anwendungen entwickelt wurden.
- **Sicherheitsbewertungen in kürzester Zeit**
  Durch schnelle Scans von Webanwendungen erzielen Sie innerhalb von maximal zwei Minuten einen unmittelbaren Nutzen und decken gängige Probleme der Sicherheitshygiene auf.
- **Weniger separate Einzellösungen**
  Mithilfe der Exposure-Management-Plattform Tenable One bringen Sie die tatsächlichen Cyberrisiken Ihrer modernen Angriffsoberfläche zum Vorschein. So verringern Sie Komplexität und das Ausufern von Produkten.

Wichtige Funktionen

Webanwendungen verstehen

Tenable Web App Scanning bietet Ihnen Einblick in die Seitenstruktur und das Layout Ihrer Webanwendungen, sodass Sie ein gründliches Verständnis Ihres Risikos entwickeln können und wissen, welche Schwachstellen zuerst gepatcht werden müssen. Ob als SaaS-basierte oder als On-Prem-Lösung: Sie erhalten umfassende und präzise Schwachstellenanalysen für moderne Webanwendungen.

Erweiterte Dashboard-Funktionen

Dashboards in Tenable Web App Scanning machen gescannte Webanwendungen auf einen Blick sichtbar. Die Exposition durch Schwachstellen lässt sich basierend auf dem jeweiligen Tenable One-Scoring betrachten, z. B. nach Vulnerability Priority Rating (VPR), Asset Criticality Rating (ACR) und Asset Exposure Score (AES). Darüber hinaus können Sie schnell zu den Top-10-Sicherheitsproblemen des OWASP sowie zu kritischen Schwachstellen und Scan-Behebungsmaßnahmen übergehen und vorbeugende Maßnahmen ergreifen – mittels Pivot-Funktionen (Quick Pivots), um ungescannte Webanwendungen anzuzeigen und Funde näher zu untersuchen.

Sicheres Scannen von Webanwendungen

Um Leistungsverzögerungen und Unterbrechungen zu verhindern, ist es wichtig, dass Sicherheitsteams die Teile kritischer Webanwendungen definieren, die gefahrlos gescannt werden können, sowie diejenigen, die niemals gescannt werden sollten. Mit Tenable Web App Scanning können Sie Teile der zu scannenden Webanwendung ausschließen, indem Sie die URLs oder Dateierweiterungen angeben, die ausgenommen werden sollen. So stellen Sie sicher, dass der Scanner nicht ins System eingreift.

Automatisiertes Scannen von Webanwendungen

Angesichts des Mangels an erfahrenen Sicherheitsfachkräften (und der damit verbundenen Kosten) sind Lösungen gefordert, die Automatisierungsmöglichkeiten bieten, sodass unterbesetzte Sicherheitsteams entlastet werden können. Mit Tenable Web App Scanning bewerten Sie Ihre gesamten Webanwendungen schnell und mühelos – dank einer hochgradig automatisierten Lösung, die den manuellen Arbeitsaufwand verringert.

Abdeckung moderner Frameworks für Webanwendungen

Ältere Web-App-Scanner sind für die modernen Anwendungen, die in der heutigen Entwicklungsumgebung Standard sind, nicht mehr geeignet. Tenable Web App Scanning scannt nicht nur herkömmliche HTML-Webanwendungen, sondern unterstützt neben dynamischen Web-Apps, die mit HTML5-, JavaScript- und AJAX-Frameworks entwickelt wurden, auch Single-Page-Anwendungen.

Rasche Erkennung von problematischer Cyberhygiene

Tenable Web App Scanning bietet zwei vorgefertigte Scanvorlagen für gängige und potenziell kostspielige Fehlkonfigurationen von Webanwendungen. Der SSL/TLS-Scan prüft auf ungültige, ablaufende oder unsachgemäß ausgestellte Zertifikate, die Warnmeldungen im Browser auslösen und die Absprungrate unter Besuchern erhöhen. Der Config Audit Scan prüft auf allzu umfangreiche Antworten auf HTTP-Aufrufe, die potenziellen Hackern im Zuge der Auskundschaftung wertvolle Informationen liefern. Beide Scans sind innerhalb weniger Minuten abgeschlossen und bieten damit quasi sofortige Ergebnisse.

Scannen von Drittkomponenten

Webanwendungen bestehen zu bis zu 85 % aus Drittanbieter- und Open Source-Komponenten, darunter Content Management-Systeme, Webserver und Sprach-Engines, die in vielen Fällen gefährliche Schwachstellen aufweisen.

Tenable Web App Scanning kann Komponenten von Drittanbietern in einer Anwendung identifizieren und diese im Rahmen eines umfangreichen Scans auf Schwachstellen prüfen.

Einheitliches Scannen von Web-Apps und Exposure-Management

Tenable Web App Scanning ist als eigenständige Anwendung oder als Bestandteil der Exposure-Management-Plattform Tenable One erhältlich. Als Teil von Tenable One bietet Ihnen die Lösung einen einheitlichen Überblick über Risiken bei sämtlichen Arten von Assets – von IT bis OT, von der Cloud bis hin zum Code und von Web-Apps bis hin zu Active Directory. Dadurch können Sie die tatsächliche Sicherheitslage besser nachvollziehen und Defizite, die in einer siloisierten Umgebung mit mehreren Anbietern unter Umständen unbemerkt bleiben, schnell identifizieren und beseitigen.

Weitere Informationen: Besuchen Sie de.tenable.com.
Kontakt: Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact.