tenable™

Nessus NM™ Manager

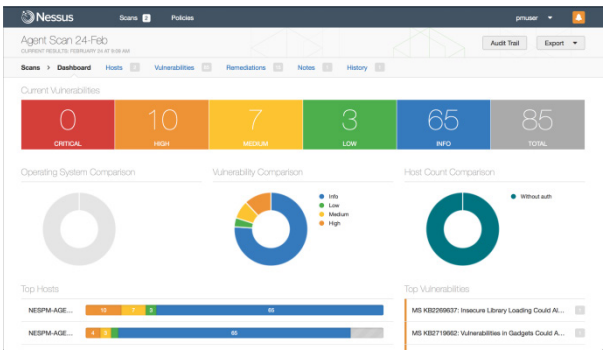
Nessus Manager stellt die Leistung von Nessus für Sicherheits- und Audit-Teams mit zentral verwaltetem, verteiltem Scanning bereit

Vulnerability-Management für Teams

Nessus® Manager kombiniert die leistungsstarken Erkennungs-, Scanning- und Auditingfunktionen von Nessus, dem weltweit meistgenutzten Schwachstellen-Scanner mit umfangreichen Schwachstellen-Management- und Kooperationsfunktionen, um Ihre Angriffsfläche zu reduzieren.

Nessus Manager ermöglicht die gemeinsame Nutzung von Ressourcen, darunter Nessus Scanner, Scan-Terminpläne, Richtlinien und Scan-Ergebnissen, durch mehrere User und Gruppen. User können Ressourcen und Verantwortlichkeiten mit ihren Mitarbeitern, Systembesitzern, internen Auditoren, Risiko- und Compliance-Mitarbeitern, IT-Administratoren, Netzwerkadministratoren und Sicherheitsanalysten teilen. Diese kollaborativen Funktionen reduzieren den Zeit- und Kostenaufwand für Sicherheitsscanning und Compliance-Auditing durch Sanierung und Vereinfachung des Scannings sowie der Malware- und der Fehlerkonfigurations-Erkennung.

Nessus Manager schützt physische, virtuelle, Mobile und Cloud-Umgebungen. Nessus Manager steht für den Einsatz vor Ort zur Verfügung. Das Tenable.io Schwachstellenmanagement steht Organisationen zur Verfügung, die nach einer Cloud-gehosteten Lösung suchen. Nessus Manager unterstützt die breiteste Palette an Systemen, Geräten und Assets, sowohl mit Bereitstellungsoptionen ohne und mit Nessus Agent, die Sie problemlos auf mobile, vorübergehende und andere schwer zugängliche Umgebungen erweitern können.



Multi-Scanner-Unterstützung

Nessus Manager ermöglicht die Steuerung mehrerer Nessus Scanner, die eine Erweiterung der Scannerabdeckung über komplexe Netzwerke, Cloud-Implementierungen und geografisch verteilte Standorte vereinfachen. User können Scans planen, Richtlinien durchsetzen und Scan-Ergebnisse mehrerer Scanner über eine einzige zentrale Konsole einsehen.

Integration

Nessus Manager stimmt sich mit Patch-Management-Lösungen von IBM, Microsoft, Red Hat und Dell ab. So wird sichergestellt, dass Software-Updates auf Systemen und Beständen hinsichtlich ihrer Priorisierung innerhalb Organisation angewendet werden.

Nessus Manager stimmt sich ebenfalls mit Mobilgeräte-Management (MDM)-Lösungen von Microsoft, Apple, Good, MobileIron und AirWatch ab, sodass Organisationen ihrem Schwachstellenmanagement-Programm Mobilgeräte hinzufügen können.

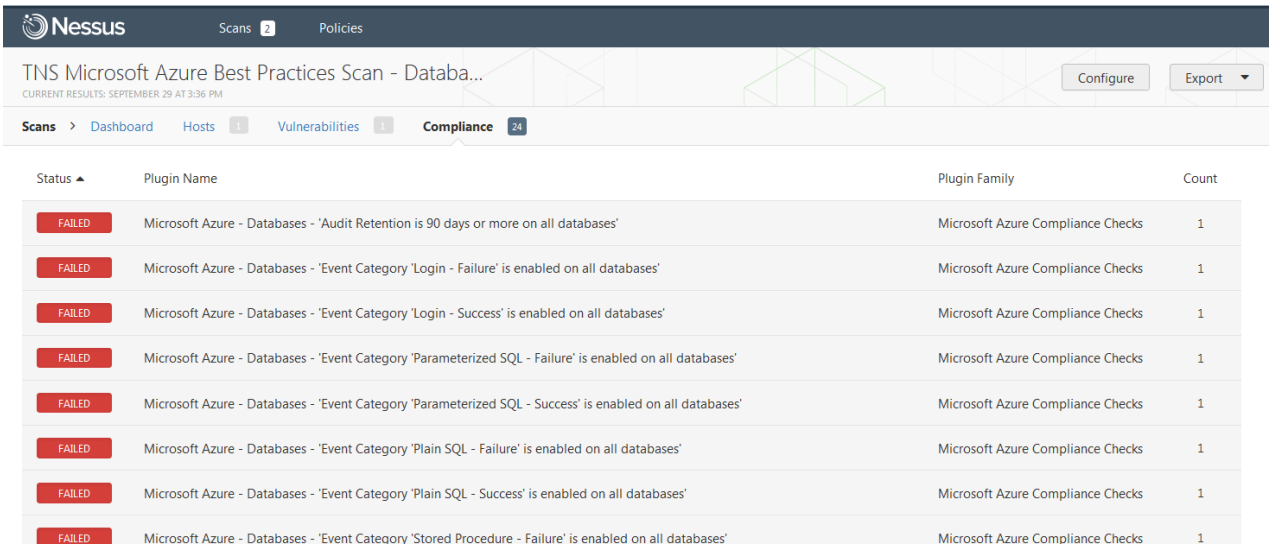
Die Password-Vault-Integration mit CyberArk erleichtert die Bereitstellung von Credential-Management für Organisationen, die die CyberArk-Lösung verwenden.

Nessus Manager reduziert die Angriffsfläche und hilft bei der Compliance durch Auditing und Scanning von Cloud-Implementierungen wie Microsoft Azure, AWS und Rackspace.

Entscheidende Vorteile

- Genaues, bewährtes und vollständig unterstütztes Scanning: Basierend auf dem Nessus Schwachstellenscanner
- Geteilte Ressourcen für mehr Teameffizienz: Weisen Sie Scanner, Richtlinien und Zeitpläne zu und melden Sie den Zugriff auf mehrere User oder Gruppen
- Erweiterter Scanumfang: Verwenden Sie Nessus Agents, um vorübergehende Geräte wie Laptops oder Bestände zu scannen, für die Sie über keine Host-Berechtigungsnachweise verfügen
- Verbesserte Risikoanalyse: Schließen Sie Kontext aus bestehenden Infrastruktur- und Partner-Frameworks mit ein
- Integration mit Kerntechnologien: Mit Nessus Manager können Sie Ihre Investition in komplementäre Technologien wie Patch und Mobilgeräte-Management wirksam einsetzen

SC MAGAZINE



Nessus Manager enthält eine Reihe von Konfigurations-Audits für Cloud-Implementierungen wie Microsoft Azure, Amazon Web Services, Rackspace und andere.

Rollenbasierte Userebenen

Nessus Manager ermöglicht das Hinzufügen von mehreren Usern und stellt vier Userrollen vor: System Administrator, Administrator, Standard und Read-Only. Jedem User können basierend auf individuellen oder Gruppenberechtigungen verschiedene Ebenen des Zugriffs auf Ressourcen zugeordnet werden. Der Systemadministrator und der Administrator haben die Berechtigung, User und Gruppen zu verwalten. Gruppen können auf der Grundlage von Abteilungen, Job-Funktion, Aufgaben und Verantwortlichkeiten, Standort und anderem eingerichtet werden – je nach den spezifischen Anforderungen Ihres Unternehmens.

Forschungsteam

Schwachstellen und neue Bedrohungen sind permanent existent. Daher stellt das Tenable Research Team häufige Updates für Nessus Manager zur Verfügung, um Organisationen bei der Bekämpfung von fortschrittlichen Bedrohungen, Zero-Day-Schwachstellen und neuen Arten von regulatorischen Compliance-Konfigurationen zu unterstützen.

Der Nessus-Vorteil

Kunden wählen Nessus, denn es bietet:

- Hochpräzises Scanning mit wenigen Falschmeldungen
- Umfassende Scanning-Möglichkeiten und Funktionen
- Skalierbarkeit für hunderttausende Systeme
- Einfache Installation und Wartung
- Geringe Kosten für Verwaltung und Betrieb

Nessus Agents

Nessus Agents sind mit Tenable.io sowie dem Nessus Manager verfügbar und beseitigt Probleme beim traditionellen Netzwerk-Scanning, z. B. dem Erhalt von Anmeldeinformationen. Dabei vereinfacht es das Scannen einer breiteren Palette von Beständen, einschließlich Offline-Assets.

Die meisten Organisationen werden in ihrer Nessus-Umgebung eine Mischung aus Agent-basiertem und Agent-freiem Scanning verwenden. Nessus Agents sind in einer Reihe von Szenarien attraktiv, darunter:

- **Vorübergehende Geräte**: Scanning von Laptops oder anderen vorübergehenden Geräten, die nicht immer mit dem lokalen Netzwerk verbunden sind.
- **Scanning ohne Host-Anmeldeinformationen**: Assets, die Sie ohne Credentials scannen möchten oder müssen.
- **Schnelles Scanning**: Einmal installiert, verwenden Agents lokale Host-Ressourcen für das Scanning. Netzwerkressourcen werden nur dazu verwendet, um Ergebnisse zurück zum Nessus Manager zu senden. Dadurch wird das schnelle Scannen großer Mengen von Anlagen vereinfacht.

Schulungen

Tenable bietet Schulungen für alle neuen Nessus-Anwender, die Kenntnisse und Fähigkeiten zur Nutzung des Produkts maximieren wollen. Für fortgeschrittene User gibt es fokussierte Themen wie das Compliance-Auditing. Kurse sind auf Anfrage über die Tenable-Website verfügbar.

tenable™

Für weitere Informationen: Besuchen Sie tenable.com

Kontakt: Bitte mailen Sie uns an subscriptionsales@tenable.com oder besuchen Sie tenable.com/contact