tenable | Datenblatt

Tenable OT Security

Beheben von OT-Cyberrisiken – mit der einheitlichen Sicherheitslösung für konvergente OT/IT-Umgebungen

Produktübersicht

Durch die Konvergenz von operativen Technologien (OT) und IT-Systemen – und die parallel dazu rapide zunehmende Nutzung von IoT-Technologien – befinden sich Branchen im Wandel. Diese Konvergenz optimiert Produktionsprozesse, treibt Innovationen voran und steigert Effizienzen durch Datenanalysen in Echtzeit und systemübergreifende Kommunikation. Darüber hinaus vergrößert sie jedoch auch die Angriffsfläche, wodurch neue Schwachstellen und Angriffsvektoren entstehen. Mit der zunehmenden Vernetzung von OT- und IT-Netzwerken steigt auch das Potenzial für Cyberbedrohungen. Dies macht robuste Sicherheitsmaßnahmen erforderlich, um sich vor Cyberangriffen zu schützen und die Integrität und Zuverlässigkeit von kritischen Abläufen zu wahren.

Tenable OT Security bietet Sichtbarkeit, Sicherheit und Kontrolle in Industrieumgebungen, kritischen Infrastrukturen, Gebäudemanagementsystemen und vielen weiteren Bereichen. Die Lösung reduziert Geschäftsrisiken und schützt Unternehmen vor Angriffen auf der gesamten rapide zusammenwachsenden OT/IT-Umgebung von heute. Mit einem patentierten Hybrid-Ansatz zur Erfassung, der Unternehmen auf sichere Weise Einblick in OT-, IT- und IoT-Geräte sowie cyber-physische Systeme verschafft, ermöglicht Tenable OT Security eine gründliche Asset-Inventarisierung und liefert ein detailliertes Lagebild – alles über eine einzige, zentrale Benutzeroberfläche. Von Schwachstellen-Management und Bedrohungserkennung bis hin zu Konfigurationskontrolle und Berichterstattung: Tenable OT Security versetzt Unternehmen in die Lage, Maßnahmen zu priorisieren und die Zusammenarbeit zwischen OT- und IT-Sicherheitsteams zu fördern, um bestehende Sicherheitslücken zu schließen.

Unser Tätigkeitsfeld

- Fertigungsindustrie
- Öl und Gas
- Chemie und Petrochemie
- Wasserversorgung
- Pharma
- Strom- und Energiebranche
- Luft- und Raumfahrt
- Gebäudeautomation
- Lebensmittel und Getränke
- Transportwesen

Wichtige Vorteile

Identifizieren aller OT/IT-Assets in Ihrer konvergenten Umgebung

- **Verschaffen Sie sich einen einheitlichen Überblick** über konvergente OT/IT-Umgebungen. Beseitigen Sie blinde Flecken und bauen Sie Silos ab, über die laterale Bedrohungen sich in OT-, IoT- und IT-Umgebungen ausbreiten können.
- **Decken Sie Schwachstellen in OT- und IT-Assets auf** und stufen Sie potenzielle Bedrohungen entsprechend ein, noch bevor sie zu Exploits werden. Priorisieren Sie Behebungsmaßnahmen und reduzieren Sie Cyberrisiken auf Basis des Schweregrads und der Auswirkungen von Schwachstellen.

Bewerten der kritischen Sicherheitslücken, dielhr Unternehmen in Gefahr bringen

- **Optimieren Sie Erkenntnisse** durch die Kombination von reinem Netzwerk-Monitoring mit hochentwickelten Erkennungsfunktionen, um Richtlinienverstöße zu ermitteln, Verhaltensanomalien zu erkennen und hochriskante Signaturen auf Ihrer gesamten Angriffsfläche zu verfolgen.
- **Untersuchen Sie Konfigurationsänderungen** mithilfe eines umfassenden Audit-Trail, um zu ermitteln, was genau von wem aus welchem Grund und mit welchem Ergebnis verändert wurde.

Beheben der wichtigsten Sicherheitslücken

- **Beseitigen Sie Sicherheitslücken** mit Asset-übergreifenden Vulnerability Priority Ratings (VPR), geführten Behebungsmaßnahmen und erweitertem Konfigurationsmanagement.
- **Übernehmen Sie die Kontrolle** über Ihre konvergente Umgebung und implementieren Sie strategische Abwehrmaßnahmen, um eine laterale Ausbreitung von Bedrohungen über OT- und IT-Bereiche hinweg zu verhindern.

Wichtige Funktionen

Umfassende Asset-Sichtbarkeit

Tenable OT Security automatisiert die Asset-Erfassung und erstellt visuelle Asset-Maps, um eine einheitliche Ansicht der Netzwerk-Assets bereitzustellen, einschließlich Workstations, Servern, Mensch-Maschine-Schnittstellen (Human Machine Interfaces, HMI), Historian-Datenbanken, SPS, RTUs, intelligenten Elektronikgeräten (IED) sowie IoT-Geräten. Connector-Engines zielen speziell auf Anwendungen ab, die IoT-Geräte verwalten, und stellen eine vollständige Inventarisierung sicher. Verwalten Sie Assets, indem Sie Firmware- und Betriebssystemversionen, interne Konfiguration, Anwendungen und Benutzer, Seriennummern und Backplane-Konfiguration für OT- und IT-basierte Geräte nachverfolgen.

Erweiterte Bedrohungs- und Anomalieerkennung

Tenable OT Security nutzt eine fortschrittliche Multi-Detection-Engine, die Netzwerkanomalien identifiziert, Sicherheitsrichtlinien durchsetzt und lokale Änderungen auf Geräten mit hochriskanten Ereignissen verfolgt – alles mit granularer Präzision. Dank einer gerätebasierten Bedrohungserkennung können Unternehmen Probleme auf inaktiven Geräten identifizieren, um riskante Ereignisse in OT-/IT-Umgebungen zu erkennen und zu entschärfen. Nutzer können Erkennungsmethoden flexibel an die spezifischen Anforderungen ihrer Umgebung anpassen und entsprechend optimieren. Funktionen zur Reaktion auf Bedrohungen werden um kontextreiche Warnmeldungen und einen umfassenden Audit-Trail für Incident Response und forensische Untersuchungen ergänzt.

Konfigurationsänderungen verfolgen

Mit der Konfigurationskontrolle von Tenable OT Security können Sie Änderungen nachverfolgen, die von Malware und Benutzern über Ihr Netzwerk oder direkt auf einem Gerät vorgenommen wurden. Tenable stellt eine Zeitachse der Änderungen an Gerätekonfigurationen bereit, einschließlich spezifischer Leiterlogiksegmente, Diagnosepuffer und Tag-Tabellen. Erstellen Sie einen Backup-Snapshot, der den „zuletzt als funktionierend bekannten Zustand“ festhält, um eine schnellere Wiederherstellung zu ermöglichen und die Einhaltung von Branchenvorschriften zu gewährleisten.

Risikobasiertes Schwachstellenmanagement für OT/IT

Tenable OT Security nutzt mit dem Vulnerability Priority Rating (VPR) ein ausgefeiltes Scoring-System, um Schwachstellen basierend auf ihrem Kontext und ihren potenziellen Auswirkungen zu bewerten und auf diese Weise die Priorisierung von Behebungsmaßnahmen zu ermöglichen. Jedes Asset wird anhand umfassender Daten analysiert, darunter Firmware-Versionen, proprietäre Forschungsdaten und Erkenntnisse zu Asset-Beziehungen, Sicherheitslücken, Berechtigungen und Angriffspfaden. Dadurch verfügen Sicherheitsteams über die notwendigen handlungsrelevanten Informationen, um fundierte Entscheidungen zu treffen und Maßnahmen zur Risikominderung zu beschleunigen.

Automatisiertes Asset-Management

Tenable OT Security vereinfacht das Asset-Management durch bessere Sichtbarkeit und kontextbezogene Erkenntnisse. Die hybride Erfassung mit Abfragen in natürlicher Sprache bietet ein störungsfreies Bestandsmanagement und ermöglicht dabei eine rasche Identifizierung von Assets und kritischen Sicherheitslücken. Die Asset-Zuordnung deckt komplexe Beziehungen zwischen physisch verbundenen und kommunikationsfähigen Geräten auf, um robuste Abwehrstrategien zu entwickeln.

Maximierung bestehender Sicherheitsinvestitionen

Tenable OT Security ist für eine Anpassung an diverse Infrastrukturen und nahtlose Interoperabilität innerhalb dieser Infrastrukturen konzipiert. Die Lösung ist mit den übrigen Produkten von Tenable sowie führenden IT-Sicherheitstools wie SIEM-Systemen, SOAR und Next-Generation-Firewalls integrierbar. Tenable tauscht außerdem Daten mit Configuration Management Databases, Inventarisierungsplattformen, Änderungsmanagement-Tools u. a. aus. Unsere RESTful API unterstützt die Datenextraktion bei Nutzung proprietärer Tools. Auf diese Weise entsteht ein kohärenteres Bild der IT- und OT-Umgebungen in einer einheitlichen Ansicht.

Über Tenable

Tenable®, das Unternehmen für Exposure Management, identifiziert und schließt Sicherheitslücken, die den Wert, die Reputation und die Vertrauenswürdigkeit von Unternehmen gefährden. Die KI-gestützte Exposure Management-Plattform von Tenable bietet umfassende Sichtbarkeit und handlungsrelevante Erkenntnisse entlang der gesamten Angriffsfläche und ermöglicht es Unternehmen, sich vor Cyberangriffen zu schützen – von IT-Infrastrukturen über Cloud-Umgebungen bis hin zu kritischen Infrastrukturen und allen dazwischen liegenden Bereichen. Mehr als 44.000 Kunden weltweit verlassen sich auf Tenable, wenn es darum geht, Sicherheits- und Geschäftsrisiken zu minimieren. Weitere Informationen finden Sie auf de.tenable.com.

Kontakt

Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact.

072924