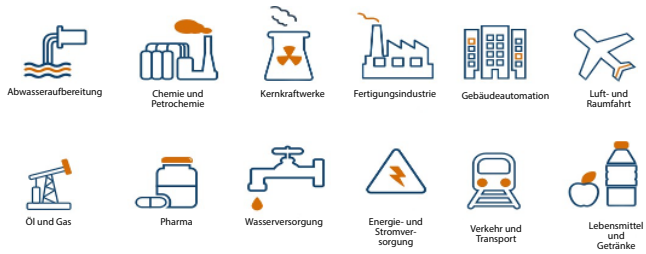
DATENBLATT

TENABLE.OT™

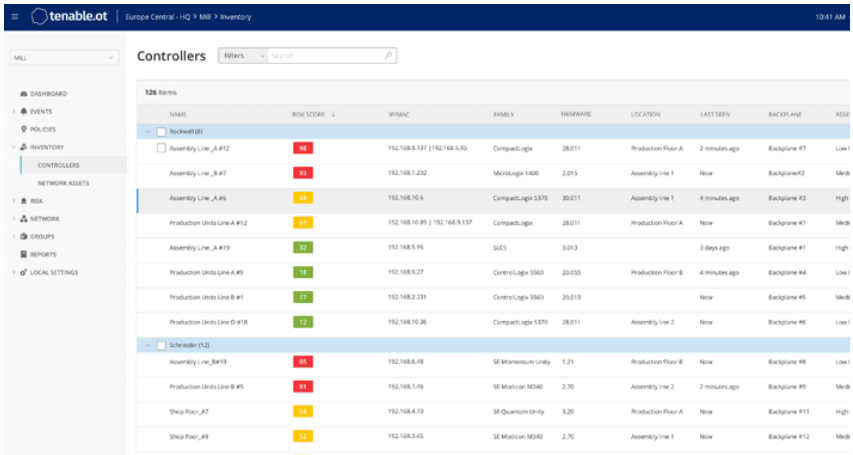
PRODUKTÜBERSICHT

Den Kern jeder Industrieanlage bildet ein Netzwerk aus industriellen Steuerungssystemen mit zweckbestimmten Controllern. Diese speziell für die industrielle Nutzung konzipierten Geräte, die mitunter auch als speicherprogrammierbare Steuerungen (SPS) und Fernwirkstationen (Remote Terminal Units, RTUs) bezeichnet werden, bilden das Fundament aller industriellen Prozesse. Die heutigen hochentwickelten Umgebungen für operative Technologien (OT) weisen eine große Angriffsoberfläche mit zahlreichen Angriffsvektoren auf. Wenn in konvergenten IT- und OT-Systemen keine vollständige Sichtbarkeit, Sicherheit und Kontrolle herrscht, ist es daher nur eine Frage der Zeit, bis es zu einem Angriff kommt.

Tenable.ot™ schützt Industrienetzwerke vor Cyberbedrohungen, böswilligen Insidern und menschlichem Fehlverhalten. Von vollständiger Transparenz über die gesamte Angriffsoberfläche über Bedrohungserkennung und Asset-Verfolgung bis hin zu Schwachstellen-Management und Konfigurationskontrolle – unsere Sicherheitsfunktionen für industrielle Steuerungssysteme (ICS) maximieren die Sicherheit und Zuverlässigkeit von OT-Umgebungen. Die Lösung liefert ein klares Lagebild für alle Standorte sowie deren IT- und OT-Umgebungen.



Speicherprogrammierbare Steuerungen (SPS) sind unabdingbar für den Betrieb kritischer Infrastruktur, die in immer mehr Unternehmen und Branchen zum Einsatz kommt.



WICHTIGE VORTEILE

- **Verschafft vollen Einblick** in den konvergenten IT/OT-Betrieb. Beseitigen Sie blinde Flecken, hinter denen sich möglicherweise Bedrohungen verbergen, die sich in IT- und OT-Umgebungen lateral ausbreiten können.
- **Erkennt Bedrohungen für Netzwerke und Geräte** mit Auswirkungen auf kritische Abläufe und den Betrieb von Anlagen durch eine Kombination mehrerer Erkennungsmethoden. Suchen Sie aktiv nach Bedrohungen, indem Sie Angriffsvektor-Technologie einsetzen.
- **Identifiziert und verfolgt IT- und OT-Assets** Gewinnen Sie detaillierte situationsbezogene Erkenntnisse zum Betrieb und Zustand jedes einzelnen Geräts.
- **Reduziert Risiken** durch die Identifizierung und Ersteinschätzung von Schwachstellen und potenziellen Bedrohungen, bevor sie zu Exploits werden und industrielle Betriebsabläufe beeinträchtigen.
- **Verfolgt Konfigurationsänderungen** mit vollständigen Audit Trail-Funktionen. Stellen Sie fest, wer warum welche Änderungen vorgenommen hat und zu welchem Ergebnis diese Änderungen geführt haben.

WICHTIGE FUNKTIONEN

Konvergente Sichtbarkeit

Tenable.ot bietet unternehmensweite Sichtbarkeit durch die Integration mit den übrigen Produkten von Tenable sowie führenden IT-Sicherheitstools wie SIEM-Systemen, SOAR, Next-Generation-Firewalls, Firewalls auf Basis von Datendioden und mehr. Die Plattform tauscht außerdem Daten mit CMDB, Inventarisierungsplattformen, Änderungsmanagement-Tools u. a. aus. Unsere RESTful API unterstützt die Datenextraktion selbst bei Nutzung proprietärer Tools. Auf diese Weise entsteht ein koheränteres Bild der IT- und OT-Umgebungen – mit allen Informationen auf einen Blick.

Bedrohungserkennung

Tenable.ot erkennt und warnt vor Bedrohungen aus externen und internen Quellen – unabhängig davon, ob diese von Personen oder Malware ausgehen. Unter Einsatz mehrerer Erkennungsmethoden identifiziert Tenable.ot ungewöhnliches Netzwerkverhalten, setzt Richtlinien für Netzwerksicherheit durch und verfolgt lokale Änderungen an Geräten. Darüber hinaus kann Tenable.ot eine gerätebasierte Bedrohungserkennung durchführen und dadurch Sicherheitsprobleme vor der Ausbreitung eines Angriffs sowie bei inaktiven Geräten identifizieren, die nicht über das Netzwerk kommunizieren. Dies ermöglicht es Unternehmen, riskante Ereignisse in OT-Umgebungen zu erkennen und einzudämmen. Kontextbezogene Warnmeldungen enthalten erweiterte Informationen und einen umfassenden Audit Trail für schnelle Vorfallsreaktionen und forensische Untersuchungen.

Asset-Verfolgung

Mit seinen automatisierten Funktionen zur Asset-Erfassung und -Visualisierung ermöglicht Tenable.ot eine umfassende, stets aktuelle Bestandsaufnahme sämtlicher Netzwerk-Assets, einschließlich Workstations, Server, Mensch-Maschine-Schnittstellen (Human Machine Interfaces, HMI), Historian-Datenbanken, SPS, RTUs, intelligente Elektronikgeräte (IED) und Netzwerkgeräte. Funktionen zum aktiven Scannen von Geräten ermöglichen die Erfassung von Geräten in den nicht einsehbaren Bereichen des Netzwerks sowie in nur lokal vorliegenden Daten. Die Bestandsdaten bieten eine einzigartige Asset-Informationstiefe: Firmware- und Betriebssystemversionen werden ebenso nachverfolgt wie interne Konfiguration, ausgeführte Software und Benutzer, Seriennummern und die Backplane-Konfiguration von IT- und OT-Geräten.

Schwachstellen-Management

Tenable.ot generiert Risikostufen für jedes Asset in Ihrem ICS-Netzwerk, wobei es sich auf unsere Funktionen für umfassende und detaillierte Asset-Verfolgung stützt. Die ausgegebenen Berichte enthalten Risikobewertungen und ausführliche Erkenntnisse sowie Vorschläge zur Risikominderung. Unsere Schwachstellenbewertung basiert auf zahlreichen Parametern, darunter Firmware-Versionen, relevante CVEs, eigene Forschungserkenntnisse, Default-Passwörter, offene Ports, installierte Hotfixes und mehr. So können autorisierte Mitarbeiter neue Schwachstellen schnell identifizieren und Risikofaktoren im Netzwerk effektiv beseitigen.

Konfigurationskontrolle

Tenable.ot verfolgt und protokolliert sämtliche von Anwendern oder Malware vorgenommenen Konfigurationsänderungen – unabhängig davon, ob diese über das Netzwerk oder direkt auf dem Gerät erfolgen. Die Lösung stellt einen vollständigen Verlauf aller Änderungen bereit, die im Lauf der Zeit an Gerätekonfigurationen vorgenommen wurden, darunter detailgenaue Informationen zu Kontaktplansegmenten, Diagnosepuffern, Tag-Tabellen und mehr. Damit sind Anwender in der Lage, Backup-Snapshots mit dem „letzten als funktionierend bekannten Zustand" für eine schnellere Wiederherstellung und zum Nachweis der Einhaltung von Branchenbestimmungen zu erstellen.

NUTZEN SIE DAS „ECOSYSTEM OF TRUST" VON TENABLE

Nutzen Sie Ihre bestehenden Sicherheitsinvestitionen. Tenable.ot kann vollständig mit Tenable.sc und Tenable.io integriert werden und bietet dadurch lückenlose Transparenz, Sicherheit und Kontrolle für Ihren gesamten konvergenten Betrieb. In Verbindung mit Tenable.ad identifiziert Tenable.ot Fehlkonfigurationen und Bedrohungen in Active Directory, die zu Ransomware-Angriffen in OT-Umgebungen führen können. Tenable.ot kann auch vollständig in IT-Sicherheitstechnologien eingebunden werden, die Sie bereits nutzen, wie beispielsweise IT-Service-Management, Next-Generation Firewalls (NGFW) und SIEM-Anbieter.

Dank der Integration und Interoperabilität zwischen Tenable-Produkten sowie führenden IT- und OT-Sicherheitssystemen erhalten Sie vollständige situationsbezogene Erkenntnisse, die zur Absicherung Ihres Betriebs gegen moderne IT-/OT-Bedrohungen notwendig sind.

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf de.tenable.com.

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