tripwire

HOPF
PARTNER | SOLUTIONS | COMPONENTS

Tripwire Industrial Solutions Katalog

Cybersecurity für moderne industrielle Steuerungssysteme






GRUNDLEGENDE KONTROLLEN FÜR
SICHERHEIT, COMPLIANCE & IT/OT OPERATIONS

Erkennen, stoppen und überwachen, von der Cloud bis zur Werkshalle

Unabhängig davon, ob Ihre Sicherheitsstrategie von komplexen Compliance-Standards wie NERC CIP, NIST und NEI bestimmt wird, ob Ihr Unternehmen die Best Practices der Branche wie die CIS Controls des Center for Internet Security befolgen möchte oder ob Sie gerade erst damit beginnen, die Implementierung von Cybersecurity-Strategien für Ihre OT-Umgebung zu validieren - Tripwire bietet eine Reihe von zuverlässigen Sicherheitslösungen für Ihre industriellen Steuerungssysteme.

Tripwire und seine Muttergesellschaft Belden, der die Hälfte der Fortune-500-Unternehmen vertrauen, verfügen über mehr als 20 Jahre Erfahrung in der Entwicklung führender globaler Cybersicherheitslösungen - und über 100 Jahre Erfahrung in der Unterstützung der größten Industrieunternehmen der Welt.

Die drei Prinzipien der ICS-Sicherheit

- **Transparenz**: Sie müssen wissen, was sich in Ihrem Netzwerk befindet, um es abzusichern. Tripwire-Lösungen bieten hervorragende Transparenz und Asset-Erkennung, lesen 135 Industrieprotokolle und bilden Protokollkommunikationsmuster ab.
- **Prävention**: Tripwire-Lösungen setzen Sicherheitskontrollen durch, um Ihr ICS gegen anomales Verhalten zu härten und die Konformität mit Standards wie ISO27001 und IEC 62443 zu gewährleisten.
- **Überwachung**: Tripwire-Lösungen lesen Konfigurations- und Protokolländerungen unterbrechungsfrei aus und liefern umsetzbare Warnmeldungen in Echtzeit, damit Sie immer wissen, was in Ihrem Netzwerk passiert.

Tripwire-Compliance-Richtlinien unterstützen die Frameworks von über 42 Standards, darunter:

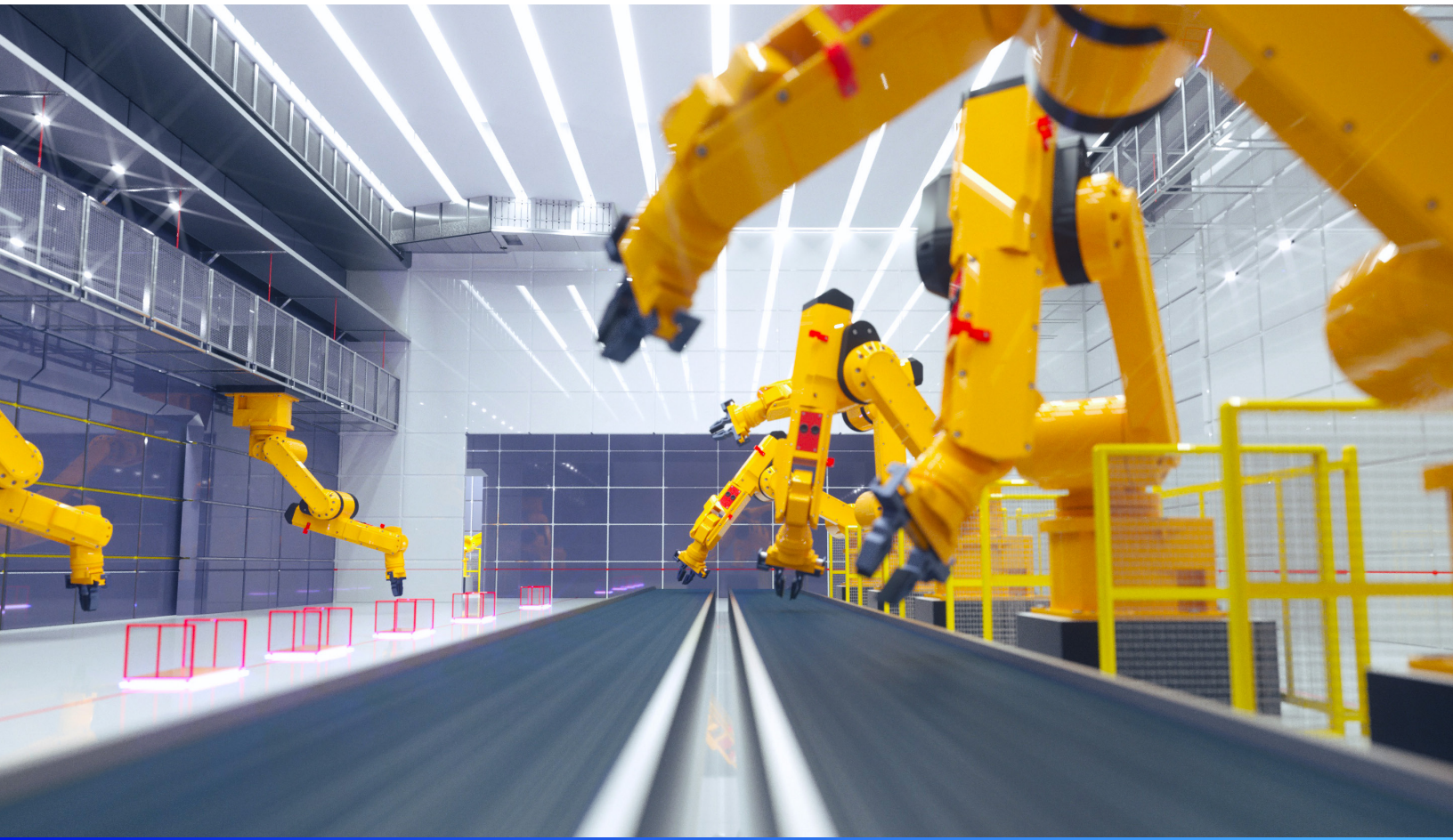
IEC · NEI Nuclear Energy Institute · ISO 27001 · American Water Works Association · NERC North American Electric Reliability Corporation · NIST

TRIPWIRE®
ENTERPRISE

Tripwire Enterprise ist eine branchenführende Security Configuration Management (SCM)-Suite, die eine vollständig integrierte Lösung für die Verwaltung von Konfigurationsrichtlinien, Dateiintegrität und Korrekturmaßnahmen bietet. Mit Compliance-Richtlinien, die den Rahmen von mehr als 42 Standards unterstützen, ermöglicht die Suite IT- und OT-Cybersecurity-, Compliance- und IT/OT-Betriebsteams, in ihren IT- und OT-Infrastrukturen schnell ein grundlegendes Sicherheitsniveau zu erreichen, indem die Angriffsfläche reduziert, die Systemintegrität erhöht und eine kontinuierliche Compliance gewährleistet wird.

Die Suite verfügt über eine noch nie dagewesene Anzahl von Konfigurationsrichtlinien aus regulatorischen und industriellen Richtlinien wie IEC 62443, NIST 800-53, ISO 27001 und vielen anderen. Um einen ganzheitlichen Überblick über die in Ihrem ICS laufenden Anlagen zu erhalten, ist Tripwire Enterprise in Rockwell Automation FactoryTalk AssetCentre, MDT Autosave und KEPServerEX integriert und unterstützt industrielle Protokolle wie Modbus TCP und Ethernet/IP CIP. Dies schließt auch die Nutzung anderer agentenloser Datenerfassungsmechanismen mit SNMP und Web-Benutzeroberflächen ein.

Laden Sie das Tripwire Enterprise-Datenblatt herunter



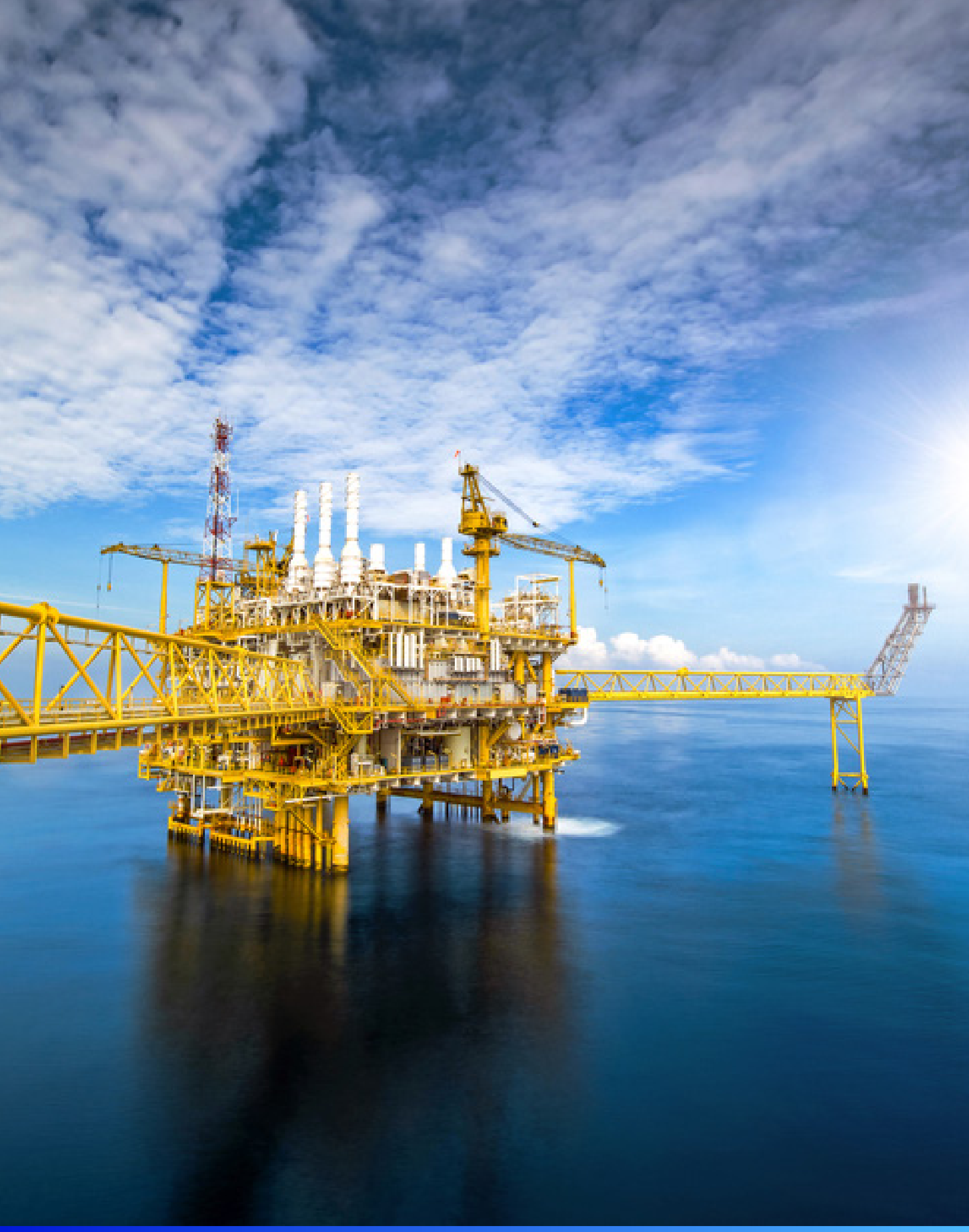
TRIPWIRE®
INDUSTRIAL VISIBILITY

Tripwire Industrial Visibility sammelt Bestands- und Bedrohungsdaten, um die Sicherheit und Verfügbarkeit Ihrer OT-Umgebung zu verbessern. Dazu analysiert es den Netzwerkverkehr und führt eine Protokolldekonstruktion durch, um Anlagen zu inventarisieren, eine Netzwerktopologie zu erstellen und vieles mehr. Tripwire Industrial Visibility beherrscht über 135 der in ICS üblichen nativen Industrieprotokolle und macht so die Datenflut verständlich, die alle verbundenen Industriegeräte erzeugen.

Tripwire Industrial Visibility analysiert die Netzwerkkommunikation, indem es den Mirror- oder SPAN-Port Ihrer Industrie-Switches abhört und die Protokolle interpretiert. Ältere OT-Netzwerke können empfindlich auf Latenz- und Bandbreitenänderungen reagieren - deshalb nutzt Tripwire Industrial Visibility diese Technologie.

Tripwire Industrial Visibility bietet ICS-Betreibern einen ganzheitlichen Einblick in die Geräte und die Aktivitäten in ihrem Netzwerk. Die Lösung kann Konfigurations- und Modusänderungen von Controllern erkennen, verfügt über Ereignisprotokollierungsfunktionen und führt Bedrohungsmodellierung durch, um Ihre sensibelsten Anlagen vor Eindringlingen zu schützen. Diese Lösung schützt die Kernintegrität und die Cyber-Resilienz Ihrer OT-Umgebung, indem sie hochentwickelte Überwachungs- und Erkennungsfunktionen einsetzt, um Ihre Verfügbarkeit und den Betrieb aufrechtzuerhalten.

Laden Sie das Datenblatt zu Tripwire Industrial Visibility herunter



TRIPWIRE® LOG CENTER

Tripwire Log Center™ sammelt, analysiert und korreliert Protokolldaten von Geräten, Servern und Anwendungen. Warum ist dies in einem ICS-Kontext wichtig? Das Tripwire Log Center hilft Ihnen, das Grundrauschen zu durchbrechen und sich nur auf das Wesentliche zu konzentrieren, indem es die Daten vorverarbeitet, bevor sie in Ihr Sicherheitsinformations- und Ereignisverwaltungssystem (SIEM) weitergeleitet werden. Diese Daten sind bei der Erstellung einer proaktiven Wartungsstrategie äußerst hilfreich - zum Beispiel wird eine Warnung versandt, wenn ein Patchkabel kurz vor dem Ausfall steht.

Mit der passiven Asset-Erkennungsfunktion von Tripwire Log Center können Sie zuvor nicht identifizierte Assets durch die Analyse ihrer Logdaten aufdecken. Danach können die Assets für die weitere Überwachung Ihren Security-Lösungen hinzugefügt werden.

Betrachten Sie Tripwire Log Center als Cyber-Archivar für das industrielle Netzwerk betrachten, da es Log-Diagnose- und Cybersicherheitsinformationen erfasst und analysiert, die Ihnen helfen, den Betrieb aufrechtzuerhalten. Die Log-Verwaltung ist eine Best Practice, auf die in vielen ICS-Cybersicherheits-Frameworks und -Richtlinien verwiesen wird (einschließlich, aber nicht beschränkt auf IEC62443, ISO27001 und NIST SP 800-82).

Laden Sie den *Beginner's Guide to Industrial Tripwire Log Center Deployments* herunter

TRIPWIRE® IP360

Während Ihre Anlagen in den unteren Ebenen des Purdue-Modells (Zellen-/Bereichszonen) möglicherweise nicht für aktive Scan-Techniken geeignet sind, profitieren Geräte wie HMIs und Engineering-Workstations in der Fertigungszone und DMZ von einem eingehenden Schwachstellen-Scan durch ein Schwachstellen-Management-Tool wie Tripwire IP360™.

Die einzigartige Scan-Methode von Tripwire IP360 liefert die granularste und genaueste Priorisierung von Schwachstellen auf dem Markt. Die Verwendung mehrerer Scoring-Systeme ermöglicht ein zielgruppenspezifisches Reporting und bietet eine offene API für individuelle Integrationen.

Die Qualität der gesammelten Daten bildet das Herzstück eines jeden Schwachstellenmanagement-Tools. Tripwire IP360 findet Schwachstellen mit größter Genauigkeit und zeigt Ihnen genau, wie das Tool jede Schwachstelle erkannt hat. Die automatisierte Erkennung, Profilerstellung und Überprüfung spart Sicherheitsteams Zeit und Ressourcen.

Die umsetzbaren Analysen und Berichte, die in Tripwire IP360 verfügbar sind, werden von einem engagierten, erstklassigen Vulnerability and Exploit Research Team (VERT) unterstützt.

Laden Sie das Tripwire IP360 Datenblatt herunter

Tofino Xenon Industrial Security Appliance

Tofino Xenon ist eine Klasse für sich, vielseitig, robust und eine ideale Lösung für den Schutz von industriellen Steuerungssystemen und dabei so viel mehr als eine industrielle Firewall. Sie können nicht nur Deep Packet Inspection (DPI) auf Industrieprotokollen durchführen, um sicherzustellen, dass z. B. Modbus-Datenverkehr in die richtigen Register geschrieben und gelesen wird, sondern auch Protokollanomalien zu erkennen, ohne dass Signatur-Updates erforderlich sind. Dies hilft Zero-Day-Angriffe zu verhindern. Von der Erstinstallation bis zum laufenden Betrieb besteht der Zweck darin, den industriellen Prozess am Laufen zu halten. Änderungen an der Netzwerkarchitektur sind nicht erforderlich, da der Tofino Xenon auf der Datenverbindungsschicht (Layer 2 des OSI-Netzwerkmodells) arbeitet und daher im Netzwerk transparent ist. Betreiber können Regeln definieren, die festlegen, welche Geräte kommunizieren und welche Protokolle sie verwenden dürfen.

Datenblatt der Tofino Xenon Industrial Security Appliance herunterladen

ICS Professional Services von Tripwire

Vielen Industrieunternehmen fehlten Resourcen im Sicherheitsteam. Ressourcen, die für die Implementierung und Aufrechterhaltung strenger ICS-Sicherheitskontrollen unabdingbar sind. Tripwire bietet eine Reihe von Dienstleistungen an, die speziell auf industrielle Umgebungen zugeschnitten sind.

Industrielle Sicherheitsbeurteilungen

Die Durchführung einer Schwachstellenanalyse im Netzwerk Ihres Industrieunternehmens hat sich von einer empfehlenswerten Aktivität zu einer Notwendigkeit gewandelt. Das erfahrene Ingenieursteam von Tripwire identifiziert Schwachstellen und priorisiert sie. Wir sammeln Daten von automatisierten Schwachstellen-Scannern, proprietären Tools und manuellen Bewertungen, um eine Liste der identifizierten Schwachstellen zu erstellen.

Laden Sie die Kurzbeschreibung Industrial Cybersecurity Assessment herunter

Penetrationstests

Penetrationstests - auch Pen-Tests genannt - sind eine Art von ethischem Hacking, mit dem die Sicherheit eines Netzwerks regelmäßig überprüft wird. Unser Team aus hochqualifizierten Cybersecurity-Experten nutzt eine Kombination aus taktischen und strategischen Ansätzen, um mittels Penetrationstests Schwachstellen in Ihren IT-Systemen zu entdecken, auszunutzen und Ihr Sicherheitsprogramm zu bewerten.

Laden Sie die Kurzbeschreibung der Penetration Testing Assessments herunter

Ortsansässige Techniker

Die „Resident Engineers" von Tripwire sind Experten, die vor Ort für die Verwaltung Ihrer Tripwire-Lösung zuständig sind. Unsere Techniker konzentrieren sich darauf, sicherzustellen, dass Sie den größten Nutzen aus Ihrer Tripwire-Investition in Bezug auf Ihre Geschäfts-, Sicherheits- und Compliance-Ziele ziehen.

Laden Sie die Tripwire Professional Services Overview herunter

Demo anfordern

Wollen Sie mehr erfahren? Wir führen Sie gerne durch eine Demo unserer industriellen Sicherheitslösungen, zeigen Ihnen die Funktionen und beantworten alle Ihre Fragen.
Besuchen Sie tripwire.com/contact/request-demo






Tripwire Produktauswahl

Merkmal	Tripwire Enterprise	Tripwire Industrial Visibility	Tripwire Log Center	Tripwire IP360	Beschreibung
Asset-Discovery und Inventarisierung					
Aktive Datenerfassung	✓	✓		✓	**Tripwire Enterprise** nutzt eine aktive Datenerfassung durch Erkennung und Inventarisierung von Geräten über native Protokolle, SSH, WMI, Modbus TCP und Ethernet/I¬P. Tripwire Industrial Visibility erreicht dies ebenfalls durch mehr als sechs Industrieprotokolle.
Passive Datenerfassung		✓			**Tripwire Industrial Visibility** analysiert eine Kopie des Netzwerkverkehrs über ein SPAN, einen Mirror-Port oder einen Netzwerk-TAP.
Hybride Datenerfassung	✓	✓			**Tripwire Enterprise** durch Integrationen mit Rockwell Automation FactoryTalk AssetCentre, Kepware und MDT Autosave.
Schwachstellenerkennung	✓	✓		✓	**Tripwire Enterprise** erreicht dies durch die Integration mit FactoryTalk AssetCentre. **Tripwire Industrial Visibility** erreicht dies durch passive und hybride Datenerfassung. **Tripwire IP360** ist eine aktive Scan-/Polling-Technologie und eine umfassende Lösung für das Schwachstellenmanagement.
Konfigurationsdokumentation oder Konfigurationshärtung	✓				**Tripwire Enterprise** kann die Konfiguration z.B. gegen die Richtlinen IEC 62443, NIST 800-53, ISO 27001 und die CIS Controls bewerten.
Erkennen von Veränderungen	✓	✓			**Tripwire Industrial Lösung:** Tripwire Enterprise erkennt alle Änderungen an überwachten Assets. **Tripwire Industrial Visibility:** Konfigurations- und andere Änderungen im Netzwerkverkehr werden von Tripwire Industrial Visibility erkannt.
Log-Verwaltung		✓	✓		**Tripwire Log Center** sammelt und speichert Protokollmeldungen, einschließlich derer, die von **Tripwire Industrial Visibility** bereitgestellt werden.
Netzwerkgeräte & SCADA-Systeme	✓	✓			Netzwerkgeräte lassen sich mit **Tripwire Enterprise** aktiv scannen. Syslogs werden mit **Tripwire Log Center** gesammelt. **Tripwire Industrial Visibility** erkennt den Datenstrom durch ein Netzwerk und die damit zusammenhängenden Aktivitäten.
Berichte und Analysen	✓	✓	✓	✓	**Tripwire Enterprise** (Tripwire Industrial Solution) und **Tripwire Log Center** (Tripwire Industrial Visibility) verfügen über vorgefertigte Reports. Der **Tripwire Whitelist Profiler** (eine Erweiterung von Tripwire Enterprise, Teil der Tripwire Industrial Solution) enthält zusätzliche Tripwire Enterprise-Reports.
Zentrales Management	✓	✓			**Tripwire Industrial Lösung:** FIM- und SCM-Daten von Tripwire Enterprise und Tripwire Whitelist Profiler. **Tripwire Industrial Visibility:** : Logdaten und Netzwerkwarnungen von Tripwire Log Center und Tripwire Industrial Visibility.

Tripwire bietet seinen Kunden branchenführende Lösungen an, um deren Cybersicherheit zu stärken. Wir schützen führende Organisationen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen. Weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar. Tripwire schützt digitale Infrastrukturen, dabei decken wir Bedrohungen auf und wehren diese ab, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere Ihrer Systeme. **Weitere Informationen erhalten Sie unter tripwire.com.**

The State of Security:
Aktuelles, Trends und interessante Einblicke finden Sie unter tripwire.com/blog
Folgen Sie uns auf LinkedIn, Twitter und Facebook

BRTISC2b 1906