Tripwire Industrial Visibility

Maximale Verfügbarkeit durch automatisiertes Netzwerk-Mapping für ICS-Umgebungen

Tripwire® Industrial Visibility (TIV) bietet Kunden umfassende Transparenz, kontinuierliche Bedrohungs- und Schwachstellenüberprüfung und detaillierte Einblicke in ihre ICS-Netzwerke (industrielle Steuersysteme). TIV ist speziell dafür konzipiert, die Sicherheit und Zuverlässigkeit des Betriebs in komplexen industriellen Netzwerken mit Lösungen mehrerer Anbieter zu gewährleisten. Somit werden geschäftskritische Prozesse vor Hackern geschützt und der Sicherheitsstatus der Organisation gestärkt.

Die wichtigsten Vorteile

Tripwire Industrial Visibility stellt Kunden regelmäßig aktualisierte Daten und leistungsfähige Funktionen zur Bedrohungserkennung bereit und unterstützt somit:

- eine schnelle Identifizierung von Risiken, die Stärkung der Cybersicherheitsstrategie und die Minimierung ungeplanter Ausfallzeiten
- die Eindämmung der Auswirkungen von Sicherheitsvorfällen auf physische Prozesse und kostspielige industrielle Geräte, zum Schutz von ICS und Mitarbeitern
- die zeitnahe Bereitstellung und Skalierung der Lösung an mehreren Standorten, um die Verwaltungskosten zu reduzieren
- die automatische Erfassung des Zustands der Systeme und Kommunikationen im Netzwerk und die Erarbeitung einer Netzwerksegmentierungsstrategie
- die Bereitstellung umfassender Einblicke in die gesamte ICS-Umgebung, von externen E/A-Geräten bis hin zu den demilitarisierten Zonen, ohne den Betrieb zu stören

Tripwire Industrial Visibility sammelt präzise Informationen über jede Ressource im Netzwerk, erstellt für sämtliche Kommunikation und Protokolle Profile, erfasst anhand detaillierter Verhaltensdaten den Normalzustand des Netzwerkbestands und generiert bei Abweichungen, unerwarteten Änderungen, Bedrohungen und neuen Schwachstellen aussagekräftige Warnmeldungen. All das bildet die Grundlage für eine schnelle, effektive Reaktion auf Cybergefahren und andere Risiken.

Stärkere Sicherheit durch bessere Transparenz

Mit Tripwire Industrial Visibility können Sie die Kommunikation, Protokolle und das Verhalten Ihres ICS-Netzwerks genauestens überprüfen. TIV identifiziert automatisch alle Ressourcen (ob mit oder ohne IP-Addresse, geschachtelt oder mit serieller Verbindung zu anderen Ressourcen), erstellt Profile für die Kommunikation zwischen diesen Ressourcen und legt anhand dieser Daten den Normalzustand des Netzwerks fest. Somit ist TIV in der Lage, unerwartete Änderungen zu erkennen, virtuelle Zonen abzustecken, Bedrohungen rechtzeitig zu identifizieren und praxistaugliche Warnmeldungen zu generieren.

Dabei geht es um mehr als die bloße Identifizierung von Ressourcen im Netzwerk. Im Gegensatz zu anderen Lösungen, die sich darauf beschränken, die Kommunikation zwischen zwei IP-Adressen zu registrieren, kann Tripwire Industrial Visibility diese Kommunikation „verstehen". Das bedeutet, TIV erkennt zum Beispiel den Unterschied zwischen einer speicherprogrammierbaren Steuerung (PLC), die über eine Nutzerschnittstelle einen Lesevorgang durchführt, und einer Engineering-Workstation, die über neue KOP-Sprache eine Konfigurationsdatei hochlädt. Darüber hinaus lassen sich Abweichungen vom Normalzustand identifizieren, wie die Installation einer neuen PLC-Ein- oder Ausgangskarte oder eine Nutzerschnittstelle, über die ein neuer Controller Schreibvorgänge durchführt. In beiden Fällen stellt TIV Sicherheitsteams die nötigen Kontextinformationen zur Verfügung und unterstützt somit eine schnellere Untersuchung und Reaktion auf Vorfälle. Mit solch umfassenden Einblicken in ihre ICS-Netzwerke können Kunden ihre Ressourcen besser verstehen, überwachen und schützen.

Hochentwickelte Scanfunktionen

Anforderungen und Betriebsprozesse unterscheiden sich von Organisation zu Organisation, doch Tripwire Industrial Visibility lässt sich an jedes Netzwerk individuell anpassen. Durch auf Portspiegelung (auch Switched Port Analyzer oder SPAN genannt) basierte passive Überwachung, aktives Scanning

oder auch eine Kombination dieser Ansätze (mithilfe einer Analyse von Projektdateien) behält TIV Ihre kritischen industriellen Systeme stets im Auge, ohne den Betrieb zu beeinträchtigen.

Erweiterte Bedrohungserkennung

Tripwire Industrial Visibility nutzt modernste Funktionen zur Anomalieerkennung, um Abweichungen vom Normalzustand frühzeitig zu erkennen. Somit kann TIV den gesamten Angriffszyklus überwachen und von Ausspähaktivitäten bis zu Angriffsversuchen auf industrielle Steuer-systeme (ICS) und -prozesse in jeder Phase entsprechende Warnmeldungen generieren. Das erleichtert Sicherheitsteams insbesondere die Erkennung und Abwehr ICS-spezifischer Malware, denn TIV stellt ihnen ergänzend relevante Gefahrenindikatoren zur Verfügung und unterstützt Snort- und YARA-Regeln. Mit solch umfassen-den Kontextinformatio-nen und Abwehrtaktiken gewappnet können Teams schnell und flexibel auf Bedrohungen und Angriffsversuche reagieren und deren Auswirkungen auf den Betrieb minimieren.

Wichtige Alleinstellungsmerkmale unserer Lösungsind die kontextreichen Warnmeldungen und Bedrohungsdaten, die kontinuierlich automatisch aktualisiert werden. Dadurch sind SOC-Teams immer auf dem neuesten Stand und können Probleme in Zusammenarbeit mit den Betriebsteams schneller beheben.

Änderungen mit Handlungsbedarf: Schnelle Erkennung von Änderungen an kritischen Systemen oder Ressourcen, die den Betrieb beeinträchtigen könnten.

Bekannte und unbekannte Bedrohungen: Identifizierung von Verhaltensanomalien und anderen Hinweisen auf Angreiferaktivitäten im Netzwerk.

Proaktives Schwachstellen-monitoring

Tripwire Industrial Visibility bietet Kunden einen umfassenden Einblick in ihre ICS-Umgebungen, sodass sie potenzielle Schwachstellen rasch erkennen und patchen können.

Präziser CVE-Abgleich: Ermöglicht die Identifizierung bekannter Schwachstellen und Einfallstore (Common Vulnerabilities and Exposures, CVE) in Ressourcen, zum Beispiel risikoreiche Firmwareversionen für industrielle Geräte. Diese CVEs werden in einer zentral verwalteten, öffentlich zugänglichen Liste zusammengefasst, die wir regelmäßig um vorab überprüfte und verifizierte Schwachstellen erweitern.

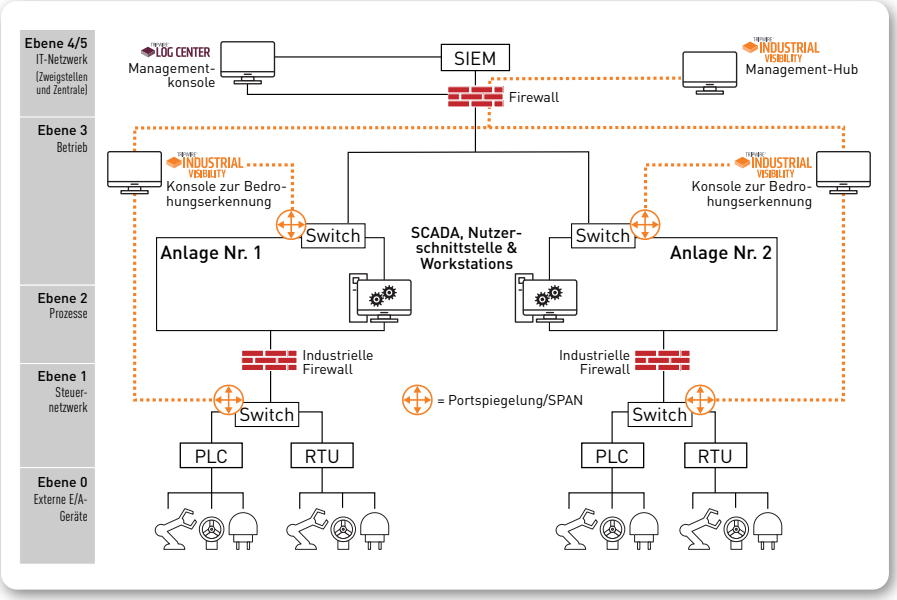

Abb. 1: Tripwire Industrial Visibility bietet Kunden durch im gesamten OT-Netzwerk installierte Sensoren umfassende Transparenz in ihren ICS-Umgebungen und unterstützt somit die Integrität und Zuverlässigkeit der Systeme.

Granulare Risikobewertung: Mit der Risikobewertung von Tripwire Industrial Visibility können Netzwerkbereiche und Ressourcen in verschiedene Kategorien aufgeteilt werden. Der selbstlernende Algorithmus von TIV ermöglicht die Erkennung risikoreicher Netzwerksegmente, eine detaillierte Analyse der potenziellen Gefahren und somit eine effektivere Fehlerbehebung und Bedrohungsabwehr. Anhand dieser Analyse werden Ressourcen und Bereiche dann mit einer hohen, mittleren oder niedrigen Risikobewertung versehen.

Praxistaugliche Konfigurationseinblicke: TIV unterstützt Sicherheitsteams dabei, Netzwerkkonfigurations- und andere Probleme schnell zu erkennen, die Angriffsfläche proaktiv zu reduzieren und die Zuverlässigkeit der Betriebsprozesse zu steigern. Des Weiteren zieht die Lösung detaillierte Konfigurationsdaten aus Windows-Endpunkten und Kontextinformationen aus AV-Lösungen für WMI, SNMP, WSUS und McAfee/Symantec für ihre Analysen hinzu.

Proaktives Netzwerkpatching: Mit TIV lassen sich Probleme wie Softwareschwachstellen, Fehlkonfigurationen im Netzwerk, in Klartext gespeicherte Passwörter oder unsichere Verbindungen, die den Betrieb gefährden könnten, schnell identifizieren und beheben.

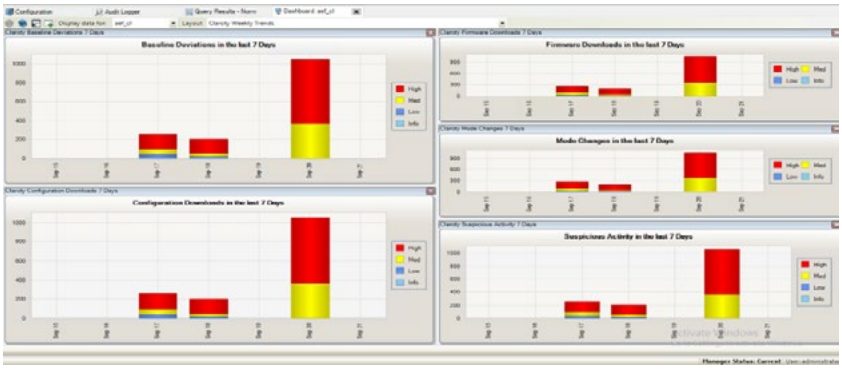

Abb. 2: Tripwire Industrial Visibility ermöglicht eine effektive Verwaltung von Logdateien und sorgt dafür, dass Ihre ICS Best Practices und branchenspezifische Cybersicherheitsstandards wie IEC 62443 und NIST SP 800.82 einhalten.

Netzwerksegmentierung – Richtlinien- und Zonenmanagement

Tripwire Industrial Visibility nutzt proprietäre Algorithmen, um Ressourcen je nach Kommunikationsverhalten automatisch in logische Segmente aufzuteilen und ein virtuelles, individualisiertes Netzwerkmodell zu erstellen. Dieses können Sicherheitsteams verwenden, um auf Ports, Protokollen oder Anwendungen basierte Firewallrichtlinien zu implementieren oder um das Netzwerk anhand von VLANs zu segmentieren.

Automatisierung grundlegender Cybersicherheitskontrollen

Tripwire Industrial Visibility stellt Kunden ein breites Portfolio an Funktionen bereit, um die Betriebseffizienz zu steigern, darunter das Änderungsmanagement, die Ereignisprotokollierung, passive Überwachung und aktives Scanning.

Erkennung und Verwaltung von Änderungen: Tripwire erkennt Änderungen an der Controllerkonfiguration sowie am Normalzustand von Firmware und Ressourcenkommunikation. Sicherheitsteams können dann entscheiden, ob es sich dabei um unerwartete oder unautorisierte Änderungen handelt und anhand von Änderungsmanagementrichtlinien ihre Betriebsumgebungen vor Angriffen schützen.

Ereignisprotokollierung: Durch die regelmäßige Protokollierung von Ereignisdaten ist es einfacher, den früheren, als problemfrei bekannten Zustand eines infiltrierten Systems ohne größeren Zeit- und Ressourcenaufwand wiederherzustellen. TIV wird in einem Lösungspaket mit Tripwire Log Center™ angeboten, unserem Tool zur Erfassung und Zusammenführung von Logdateien aus verschiedenen Geräten. Die gesammelten Gerätedaten sowie über Syslog im Netzwerk versendete Daten werden normalisiert, zueinander in Beziehung gesetzt und schließlich als klare, praxistaugliche Erkenntnisse im Dashboard bereitgestellt.

Weitere Funktionen

Sichere Cloud-Konnektivität: Tripwire führt Daten aus verschiedenen Kundenstandorten und -netzwerken zusammen, um hinsichtlich branchenspezifischer Bedrohungen, Angreifertaktiken und Sicherheitstrends stets auf dem neuesten Stand zu sein. Diese Kontextinformationen werden anonymisiert, an zentraler Stelle gesammelt und regelmäßig aktualisiert, damit wir unseren Kunden den besten Service bieten, die Problembehebung beschleunigen und Vorfällen vorbeugen können.

Normalerweise wird die Cloud-Konnektivität in hochsicheren OT-Umgebungen meist nicht erlaubt. Doch mit leistungsfähigen Funktionen zur Richtliniendurchsetzung und Netzwerksegmentierung nach Risikobewertung ist Tripwire Industrial Visibility eine Ausnahme wert. Zumal Sicherheitsteams durch eine Cloud-Integration von regelmäßigen Updates zu den neuesten Bedrohungssignaturen und Schwachstellen profitieren, mit denen sie ihren ohnehin schon starken Sicherheitsstatus weiter verbessern können. Außerdem werden sämtliche an die Cloud geschickten Daten mit SSL verschlüsselt.

Angriffssimulation und Risikoanalyse: Mit TIV können Nutzer risikoanfällige Ressourcen auswählen und erhalten eine Liste potenzieller Angriffsvektoren. Um diese zu erstellen, identifiziert und analysiert unsere Lösung mögliche Schwachstellen und Wege, über die Angreifer an kritische Ressourcen im ICS-Netzwerk gelangen könnten. Dadurch erhalten SOC- und andere Sicherheitsteams einen Überblick über Einfallstore und Angriffspfade und können Patching-Maßnahmen effektiv priorisieren.

Skalierbare Architektur: Tripwire Industrial Visibility kann selbst in ICS-Umgebungen bereitgestellt werden, die auf viele verschiedene Remote-Standorte auf der ganzen Welt verteilt sind. Da einige Standorte extremen klimatischen Bedingungen ausgesetzt sind oder besondere branchenspezifische Anforderungen haben, sind unsere Sensoren so

Anwendungsszenarien

- Tripwire Industrial Visibility stellt SOC-Teams integrierte Funktionen für SIEM, das Ressourcenmanagement, die Ticketerstellung und die Logdateiverwaltung sowie nahezu in Echtzeit generierte Warnmeldungen und Tools für die proaktive Bedrohungssuche und -abwehr zur Verfügung.
- Betriebsteams können ihr Netzwerk mit TIV auf unautorisiertes Verhalten oder Änderungen an der speicherprogrammierbaren Steuerung überprüfen und neu hinzugefügte Geräte überwachen.
- Sicherheitsteams können das gesamte industrielle Netzwerk überwachen, mit TIV automatisch Schwachstellen wie nicht unautorisierte oder unbekannte Geräte identifizieren und diese dann patchen, bevor sie zu einer schwerwiegenden Cybersicherheitsgefahr werden.
- Sicherheitsarchitekten unterstützt Tripwire Industrial Visibility bei der Optimierung und Beschleunigung von Netzwerksegmentierungsprojekten.

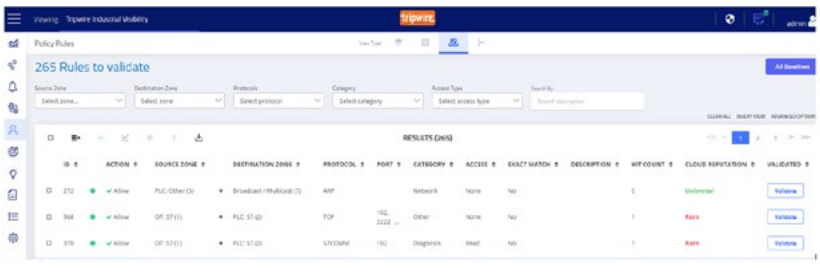

Abb. 3: Kunden, die sich für Cloud-Konnektivität entscheiden, erhalten Zugang zu regelmäßig automatisch aktualisierten Bedrohungsdaten und Datenanalysen.

konzipiert, dass sie selbst bei begrenzter Rechenleistung, wenig Platz und Kommunikation über Netzwerke mit einer geringen Bandbreite funktionstüchtig bleiben. Das ist besonders für Kraftwerke oder Fertigungsorganisationen mit mehreren Anlagen von Nutzen.

Nahtlose Integration: Dank der Integrationsfreundlichkeit von Tripwire Industrial Visibility können Sie unsere Lösung problemlos in Ihre Infrastruktur einbinden und mit vorhandenen Prozessen, Schulungsprogrammen und Technologien wie SOC-Tools und anderen kritischen IT-/OT-Systemen kombinieren. Wie bereits erwähnt lässt sich TIV nahtlos mit Tripwire Log Center integrieren; doch auch die Zusammenarbeit mit Next-Generation Firewalls zur Implementierung von Sicherheitskontrollen und Abwehr schädlicher Kommunikationen ist ganz einfach Darüber hinaus erstellt TIV auf Risikobewertungen und Netzwerksegmentierung basierte Firewallrichtlinien und ergänzt diese mit kontextreichen Protokolldaten zu Quell- und Ziel-IP- oder MAC-Adressen.

Moderne Nutzerschnittstelle und Dashboards: Sämtliche Analyseergebnisse und Informationen zum Systemzustand wie Hard-und Software leistung oder Datenerfassungsquellen können schnell und übersichtlich visuell aufbereitet und angezeigt werden.

Tripwire Industrial Visibility unterstützt über 100 native industrielle Protokolle (darunter Profinet, Modbus TCP, EtherNet/IP CIP und DNP3), was eine umfassende Analyse industrieller Netzwerke ermöglicht.

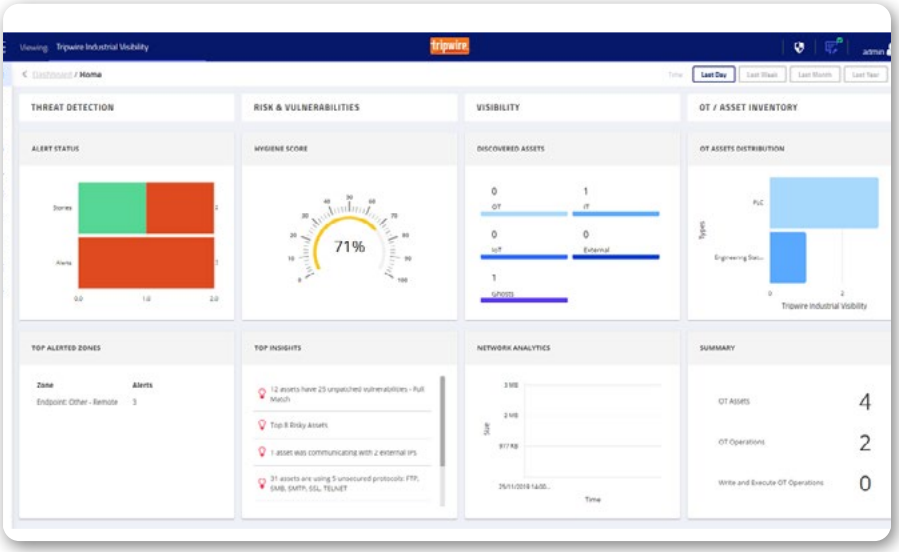

Abb. 4: Die vier Bereiche eines TIV-Dashboards.

Haben Sie Interesse an einer Demo?

Erleben Sie Tripwire Industrial Visibility in Aktion und stellen Sie uns Ihre Fragen.
Näheres erfahren Sie unter **tripwire.com/contact/request-demo**.

Tripwire, ein Unternehmen der Belden-Gruppe, ist der ideale Cybersicherheitspartner zum Schutz von IT- und OT-Umgebungen. Unsere Lösungen lassen sich nahtlos mit Ihren vorhandenen industriellen Produkten wie Tofino-Firewalls oder Switches von Hirschmann integrieren.

Tripwire stellt Kunden branchenführende Produkte zur Stärkung ihrer Cybersicherheit zur Verfügung. Wir schützen prominente Unternehmen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und 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, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere für Ihre 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

TIVDS4a 2006

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc