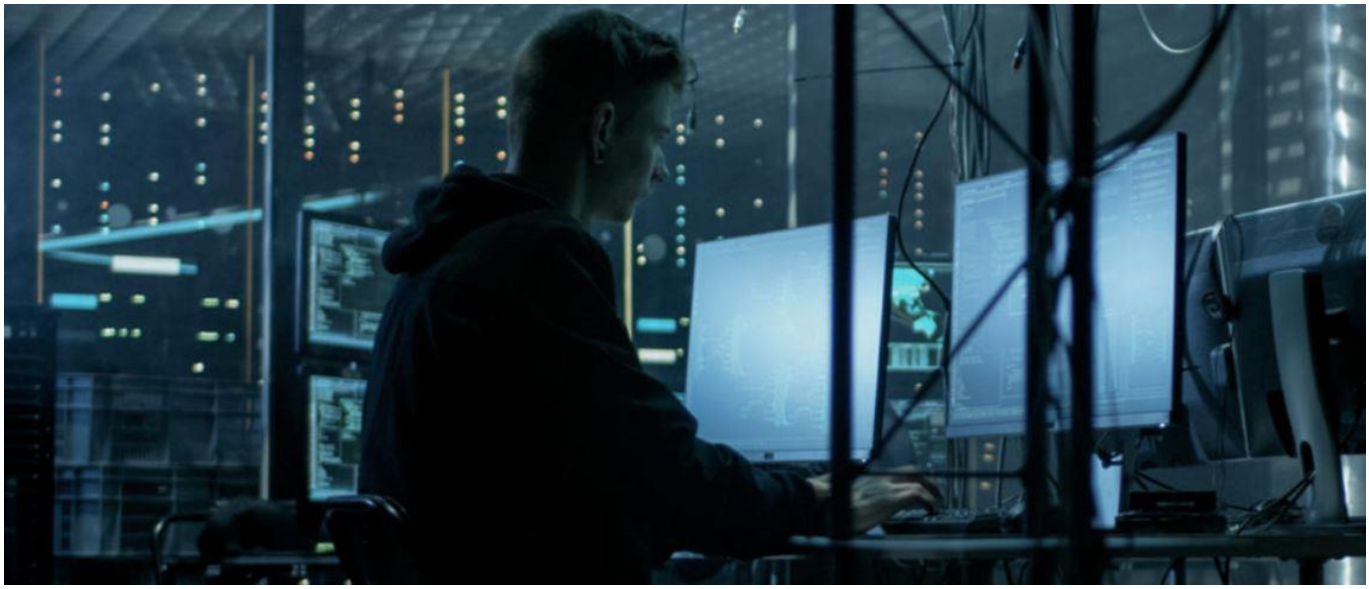
Höchste Sicherheit in industriellen Produktionsnetzwerken

Integrity Event Monitoring mit Belden Tripwire® Industrial Visibility®.



Nur ein sicheres, stabiles Netzwerk und ein detailliertes Wissen darüber, wie genau sich Ihre OT-Infrastruktur im Normalbetrieb verhält, schützt Sie vor Produktionsausfällen infolge unerlaubter, sicherheitskritischer Vorfälle.

Wir gehen davon aus, dass Sie Ihr OT-Netzwrk bereits heute bezüglich Technologie und Budget in einer für Sie optimalen Art und Weise schützen. Und das ist auch gut so. Wir wissen aber, dass auch Sie beim Schutz ihrer OT-Netzwerke viele Kompromisse eingehen müssen: Industrie-Steuerungen oder Messgeräte können ebenso schlecht geschützt werden wie veraltete Betriebssysteme, also müssen Sie mit einem relativ hohen Restrisiko leben.

Unsere Lösung ermögliches es Ihnen, dieses Restrisiko beherrschbar zu machen: Tripwire® Industrial Visibility liest passiv die Daten in Ihrem OT-Netzwerk mit, erstellt automatisch eine detaillierte Liste mit allen Netzwerkteilnehmern und deren Datenverbindungen und entwickelt daraus ein Bild, wie sich Ihr OT-Netzwerk im Normalbetrieb verhält. Auf der Grundlage dieser Daten zeigt Ihnen Tripwire® Industrial Visibility, welche bekannten Schwachstellen sich in Ihrem Netzwerk befinden und meldet unverzüglich alle Vorkommnisse, welche sich vom Normalbetrieb Ihres Netzwerks unterscheiden. So können Sie aktiv Schwachstellen eliminieren und wissen sofort, ob sich in Ihrem Netzwerk etwas Unbekanntes tut. Diese Lösung ist speziell für Ihre OT-Umgebung konzipiert und lässt Sie sicher, ungestört und mit höchster Verfügbarkeit produzieren.

INDUSTRIAL CYBERSECURITY

NETWORKCOMPETENCECENTER
by YELLO NETCOM & DDS NETCOM

Wenn Sie für die Sicherheit eines industriellen Produktionsnetzwerks (OT) verantwortlich sind, wissen Sie, wie schwierig es ist, sich ein vollständiges, lückenloses Bild davon zu machen, was in Ihrem Netzwerk eigentlich genau passiert. Dieses Bild soll neben den aktiven Netzwerkkomponenten auch alle Ihre Steuer- und Messgeräte umfassen - besonders, wenn Sie sowohl ältere als auch moderne Geräte haben. Unsere Tripwire® Industrial Visibility-Lösung hilft Ihnen bei dieser großen operativen Herausforderung und bietet Ihnen als Ergebnis eine tiefe, detaillierte und transparente Übersicht über das, was in Ihrem industriellen Produktionsnetzwerk überhaupt passiert. Damit können Sie Ihre sensibelsten Anlagen automatisch vor unerlaubten, sicherheitskritischen Änderungen schützen. Diese Lösung schützt die Kernintegrität und Cyberresilienz Ihrer gesamten OT-Umgebung und sorgt durch passives Scannen und Erkennen dafür, dass Sie sicher, ungestört und mit höchster Verfügbarkeit arbeiten können.

Unsere Cybersecurity- Lösungen

Network infrastructure	Log management	Change detection / Integrity monitoring
Integrated • Network access control • Network segmentation • Zones & conduits	**Passive** • Syslog data collection • Log filtering & management • Investigation analytics & reporting	**Continuous** • Real-time change detection • Best practice assessment & remediation • Compliance analytics & reporting

Unsere Belden Tripwire® Industrial Visibility®- Lösung

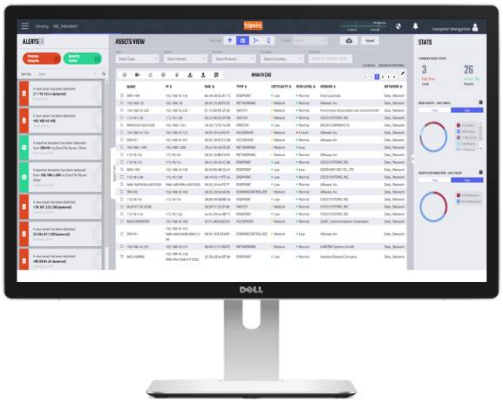
Die Tripwire® Industrial Visibility- Lösung von Belden sammelt Informationen über Bedrohungen in Ihrem Netzwerk, indem mit "Deep Packet Inspection" der gesamte Netzverkehr analysiert und überwacht wird. Dafür kennt Tripwire® Industrial Visibility über 40 der bekanntesten Industrieprotokolle, angefangen bei Siemens-S7 über GOOSE bis zu OPC DA/UA. Deep Packet Inspection (DPI) wird verwendet, um den Datenverkehr in Ihrem Netzwerk zu extrahieren und zu analysieren. Es nutzt die gesamte Netzwerkkommunikation, indem es über einen speziellen SPAN-Port von Routern und Switches, die mit dem Netzwerksegment verbunden sind, mithört, Datenpakete öffnet und Protokolle interpretiert, ohne den normalen Betrieb zu unterbrechen. Diese SPAN-

Ports werden zum Beispiel von Hirschmann-Switches mit HiOS- Betriebssystem zur Verfügung gestellt. Ältere OT-Netzwerke können empfindlich auf Latenzzeiten und Bandbreitenänderungen reagieren - deshalb verwendet Tripwire® Industrial Visibility agentenloses Monitoring und passive Asset-Discovery, um Ihr Produktionsnetzwerk ungestört arbeiten zu lassen.

Was macht nun Tripwire® Industrial Visibility mit den gesammelten Daten?

Diese Software "lernt" über einen gewissen Zeitraum die Daten kennen, die im Normalbetrieb auf Ihrem Produktionsnetzwerk transportiert werden, und erstellt daraus eine sogenannte "Baseline", die dann als sichere Grundlage zum Entdecken von Anomalien genutzt wird. Während dem Analysieren des Netzwerk-Traffics isoliert Tripwire® Industrial Visibility jeden Netzwerkteilnehmer und bildet den Datenfluss zwischen diesen Teilnehmern ab. Aus diesen Daten wird eine grafische Netzwerk-Map erstellt, die eine einfache Visualisierung der Datenströme erlaubt und so ungeplante und unerlaubte Änderungen bemerkt, bevor ein Schaden eintritt. Tripwire® Industrial Visibility kann sogar Angriffe auf kritische Bereiche simulieren, um Ihnen zu helfen, deren Eingenschaften zu verstehen und deren Gefährdung zu erkennen.

Sobald Sie genau wissen, wie Ihr Produktionsnetzwerk bezüglich Netzwerk-Traffic und bezüglich aller angeschlossenen Geräte funktioniert, können Sie Tripwire® Industrial Visibility verwenden, um häufige Schwachstellen und Risiken (CVEs) aufzuspüren und zu analysieren. Diese CVEs sind öffentlich zugänglich und werden in einer zentralen Anlaufstelle kontinuierlich aktualisiert, wo auftretende Schwachstellen veröffentlicht und verifiziert werden. Wenn Sie eine bestimmte Firmware oder eine Geräte-Version verwenden, werden Sie automatisch mit aussagekräftigen Informationen über alle diesbezüglich bekannten Cybersicherheitsrisiken informiert.



Im Gegensatz zu IT-Netzwerken werden in OT-Netzwerken mehrheitlich kleine, sich zyklisch wiederholende Datenpakete vermittelt, die ein vorhersehbares, konsistentes Verhalten des gesamten Netzwerks zur Folge haben. Dieses Verhalten erleichtert das Unterscheiden zwischen normalem und abnormalem Verhalten erheblich. Tripwire® Industrial Visibility nutzt maschinelles Lernen, um zu verstehen, wie sich Ihr Netzwerk-Traffic in einem normalen Zustand verhält. Aufgrund dieses normalen Zustands wird eine sichere Baseline erstellt und als Folge daraus werden automatisch verwertbare Warnmeldungen generiert, wenn unerwartetes, nicht normales Verhalten auftritt. Konfigurationsänderungen und daraus entstehende ungewöhnliche Daten oder Befehle werden mit der erstellten Baseline verglichen, um unerlaubte Änderungen durch eigenes Personal oder durch Eindringlinge schnell und sicher identifizieren zu können. Wenn zum Beispiel Datenpakete nicht mehr feststellbar sind, die normalerweise zyklisch vermittlet wurden, oder plötzlich unbekannte Daten in einem ungewöhnlichen Umfang auftauchen, wird automatisch ein

Alarm ausgelöst. Dieser "Baselining"-Ansatz ermöglicht es Ihnen, schnell und zielsicher ungewöhnliche und unerlaubte Aktionen zu erkennen. Social Engineering und andere Methoden für das Entwenden von Passwörtern erschweren es, unautorisierte Benutzer zu erkennen. Tripwire® Industrial Visibility kann Eindringlinge erkennen, selbst wenn sie erfolgreich legitime Anmeldeinformationen gestohlen haben. Ihre Login-Informationen mögen unauffällig aussehen, aber ihr Verhalten weicht von Ihrem normalen Basiszustand ab.

Angreifer auf industrielle Produktionsnetzwerke haben eine Reihe von Motiven. Das bedeutet, dass Sie auf eine Vielzahl von Verletzungsszenarien vorbereitet sein müssen, wie z.B. verärgerte Mitarbeiter, die die Produktivität gefährden wollen, Wettbewerber, die versuchen, geistiges Eigentum zu stehlen, und sogar staatliche oder organisierte kriminelle Angriffe auf Ihre kritischen Infrastrukturen. Tripwire® Industrial Visibility hilft Ihnen, Ihre sensibelsten Objekte zu lokalisieren und zu verstehen, wie sie über verschiedene Angriffsvektoren in Ihrem Netzwerk erreicht werden können.

So weiß beispielsweise jemand, der eine Werkstatt in einer Ölraffinerie leitet, dass seine sensibelste Anlage das System ist, das die Öltemperaturen aufrechterhält. Ein Hacker knackt nun einen diesem Mitarbeiter unbekannten E-Mail-Server, der im IT-Netzwerk des Unternehmens steht. Wie kommt der Hacker nun von diesem E-Mail-Server zu seinem Ziel im OT-Netzwerk? Der Hacker muss einen Weg zu seinem Ziel von der IT zur OT gehen und dabei knackbare Geräte als Sprungbrett verwenden. Aus diesem Grund benötigen Sie eine genaue Netzwerkübersicht, die die bekannten Schwachstellen der einzelnen Geräte in Ihrem Produktionsnetzwerk detailliert beschreibt. Sie können diese Informationen verwenden, um den Weg des Hackers zu Ihren sensibelsten Anlagen zu blockieren. So können Sie die Bedrohungsmodellierungsfunktion von Tripwire® Industrial Visibility nutzen, um zu erfahren, welche Geräte direkt oder indirekt mit Ihren sensiblen Anlagen verbunden sind. Aufgrund dieser Informationen können Sie diejenigen Verbindungen besonders schützen oder sogar unterbrechen, die Ihre Gegner nutzen könnten, um diese Anlagen zu erreichen.

Tripwire Industrial Visibility arbeitet mit Funktionen und Lösungen aus dem Änderungsmanagement (Change-Management), aus dem Event Logging (Ereignisprotokollierung) und aus dem passive scanning (passive Abtastung).

Change Management:

Tripwire Industrial Visibility bemerkt Konfigurationsänderungen, schon während sie durchgeführt werden, und protokolliert und meldet diese sofort. Sie können eine verdächtige Änderung - wie z.B. die Eskalation von Berechtigungen - erkennen, bevor sie zu einer echten Beeinträchtigung des Prozesses und des Produkts Ihrer OT-Umgebung führt.

Event Logging:

Die Protokollierung von Änderungsereignissen ermöglicht es, ein durchdrungenes System schnell in seinen letzten bekannten, "sicheren" Zustand zurückzusetzen, was die durchschnittli-

che Reparaturzeit erheblich verkürzt. Die Tripwire® Industrial Visibility-Lösung beinhaltet automatisch das Tripwire Log Center™, das Ereignisprotokolle über mehrere Geräte hinweg sammelt und aggregiert. Tripwire Log Center™ normalisiert die Daten, die von verschiedenen Geräten und Syslog-Zuflüssen übertragen werden. Es korreliert dann Ereignisse aus diesen Daten und zeigt umsetzbare Erkenntnisse in einer klaren Dashboard-Ansicht an.

Passive scanning:

Unsere Lösung verwendet passives Scannen, auch um zu vermeiden, dass sensible, ältere Systeme in ihrer Funktion gestört werden. Diese Strategie sorgt dafür, dass auch ältere Systeme trotz Einführen von Sicherhetsmechanismen vollumfänglich funktionstüchtig bleiben. Im Gegensatz zu traditionellen Schwachstellenmanagement-(VM) und Sicherheitskonfiguration Management (SCM)- Produkten verwendet es "berührungsloses Abtasten", das verwendet werden muss, damit auch ältere oder weniger leistungsfähige Systeme beim Abruf von Daten nicht einfach abstürzen.

Zusammengefasst hilft Ihnen Tripwire® Industrial Visibility, alle Vorgänge in Ihrem Produktionsnetzwerk vollständig sichtbar zu machen und trägt damit wesentlich - auf die OT optimiert - zur Sicherheit Ihrer Produktion bei. Tripwire® Industrial Visibility ermöglicht Ihnen eine vollständige Übersicht über alle Geräte und Aktivitäten in Ihrem OT-Netzwerk. Mithilfe von Änderungsmanagement, Ereignisprotokollierung und Bedrohungsmodellierung können Sie Ihre sensibelsten Anlagen vor unerlaubten, sicherheitskritischen Änderungen schützen. Diese Lösung schützt die Kernintegrität und Cyberresilienz Ihrer gesamten OT-Umgebung und sorgt durch passives Scannen und Erkennen dafür, dass Sie ungestört und mit höchster Verfügbarkeit arbeiten können.

Wir zeigen Ihnen gerne unsere Lösungen und freuen uns auf Ihre Kontaktaufnahme.