FORESCOUT

Optimale Sicherheit für ICS-Netzwerke

Reduzieren Sie Risiken und behalten Sie die Kontrolle über Ihr ICS-Netzwerk mit integriertem IT-OT-Visibility-Management und hochmoderner Bedrohungserkennung.

Zusammenfassung

Es ist offiziell: Unternehmen sind nicht mehr konkurrenzfähig, wenn sie Informationstechnologie (IT) und Betriebstechnik (OT) getrennt betreiben. Aber sie näher zusammenzubringen, führt zu enormer Komplexität bei der eingesetzten Technik. Das gilt auch für die Anzahl und die unterschiedlichen Fähigkeiten der Mitarbeiter, die nötig sind, um das konvergente Netzwerk effektiv zu betreiben und zu schützen.

Betriebstechnikleiter waren bisher mit einer steigenden Flut von Herausforderungen konfrontiert, weil die zunehmende Komplexität die Kosten nach oben getrieben hat, Cyber- und Betriebsrisiken gestiegen sind, die Arbeitsbelastung zunahm und die Compliance-Anforderungen wuchsen. Die Grundursache für all ihre Probleme? Sichtbarkeit – oder besser gesagt, fehlende Sichtbarkeit. Schließlich können sie nicht schützen und pflegen, was verborgen ist. Und obwohl bestehende Sicherheitslösungen das auf der IT-Seite gut im Griff haben, ist das bei der Betriebstechnik (OT) etwas ganz anderes.

Dieses Whitepaper beschreibt den optimalen Ansatz für ICS-Sichtbarkeit: die Nutzung einer fortschrittlichen und nicht-invasiven Netzwerküberwachung und Situationsanalyse für industrielle Netzwerke. Es erklärt auch, wie Sie und Kollegen – die die Zeichen erkannt haben und solche Lösungen unterstützen – Ihre Arbeit erheblich vereinfachen und gleichzeitig einen Mehrwert für Ihre Unternehmen schaffen können, indem Sie echte Cyber-Resilienz etablieren.

Die Vorteile konvergenter Netze als Chance nutzen

Um wettbewerbsfähig zu bleiben, müssen industrielle Fertigungs- und Versorgungsunternehmen die potenziellen Vorteile einer engeren Integration zwischen Informationstechnologie (IT) und Betriebstechnik (OT) nutzen. Zu diesen Vorteilen gehören eine höhere Effizienz und eine Reduzierung der Ausfallzeiten durch vorbeugende Instandhaltungslösungen, die die Geräte überwachen und mögliche Ausfälle erkennen, bevor sie auftreten.

Die für die Realisierung solcher Vorteile erforderliche Netzwerkkonvergenz führt jedoch zu immer höheren Komplexitätsgraden für IT- und OT-Manager. Im Laufe der Jahre haben diese neuen Geschäftsanforderungen die Öffnung von zuvor isolierten ICS-Netzen (Industrial Control System) für eine immer breitere Palette von IT-Technologien erforderlich gemacht (siehe Abbildung 1).

DIE ISOLATION ÜBERWINDEN

In den letzten Jahren haben neue Geschäftsanforderungen die Öffnung von zuvor isolierten Industrial-Control-System-Netzen (ICS) notwendig gemacht.

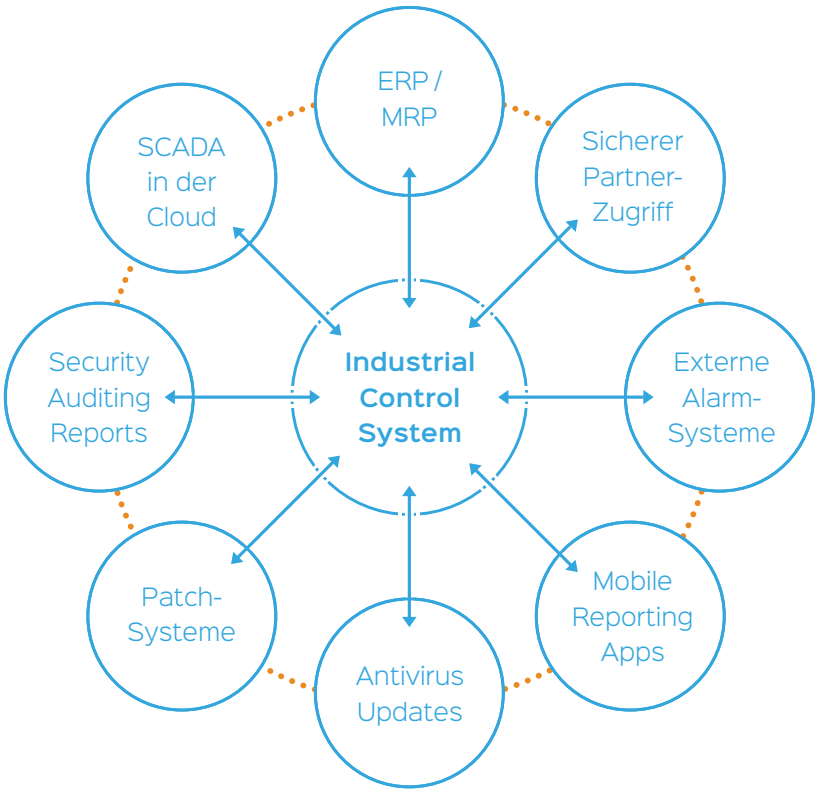
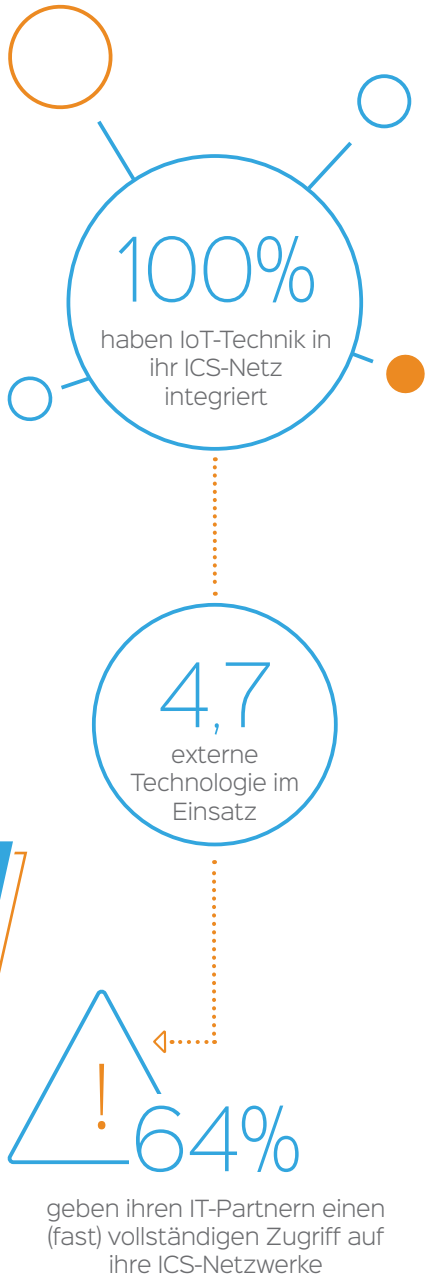


Abbildung 1: Neue Geschäftsanforderungen treiben die Öffnung von ICS-Netzwerken für verschiedene Technologien voran.

In der Vergangenheit half die Integration von ERP-Systemen den Unternehmen, die Ressourcennutzung besser an die Produktion anzupassen. Seitdem erfordern zunehmende Sicherheitsvorfälle und die wachsende Bedeutung mobiler Technologie im Betriebsmanagement, dass mehrere Alarm-, Berichts- und Aktualisierungssysteme Zugang zum ICS-Netzwerk erhalten. Aktuell haben laut Forrester [1] (Januar 2018) 100% der Unternehmen IoT-Technik mit ihren ICS-Netzwerke verbunden. Durchschnittlich sind das 4,7 IoT-Systeme. Darüber hinaus gaben 64% der befragten Unternehmen an, Drittanbietern von IT-Systemen einen (fast) vollständigen Zugang zu ihren ICS-Netzwerken zu gewähren. Weitere Systeme, die zukünftig in ICS-Netzwerke integriert werden, sind Cloud-basierte Supervisory Control And Data Acquisition-Systeme (SCADA). Sie werden eine weitere Komplexitätsebene hinzufügen.



Neben den erhöhten Arbeitsbelastungen und Belastungen für OT-Manager erhöht diese Komplexität auch das Risiko von Cyberangriffen. So schaffen die neuen Schnittstellen zwischen IT- und OT-Systemen neue Angriffspunkte für Cyberkriminelle, die diese natürlich auszunutzen versuchen. Und mehr Komplexität führt auch zu mehr möglichen Fehlfunktionen, Fehlkonfigurationen und Bedienungsfehlern.

> „Diese Komplexität erhöht das Risiko von Cyber-Angriffen auf IT- und Betriebstechnik."

Gleichzeitig wird eine Vielzahl an Teams und Rollen benötigt, darunter Führungskräfte auf C-Level, Business Manager, Ingenieure sowie IT-, OT- und Security-Experten, um das Netzwerk in seiner Gesamtheit zu spezifizieren. Die meisten dieser Stakeholder haben keinen tiefen Einblick in die jeweiligen Technologien und Prozesse ihrer Kollegen. Darüber hinaus hat keiner von ihnen ein vollständiges Bild aller mit dem konvergenten Netzwerk verbundenen Ressourcen. Und was nicht sichtbar ist, kann nicht geschützt oder effizient gewartet werden. Insbesondere ist das Wissen über den aktuellen Zustand der ICS-Assets in Bezug auf Schwachstellen, Status und Konfiguration – bekannt als ICS-Sichtbarkeit oder ICS-Visibility – eher gering. Das Gleiche gilt für die Fähigkeit, potenzielle Vorfälle zu erkennen und zu verhindern, bevor sie dem Netzwerk und dem Unternehmen schaden.

Die folgenden Abschnitte zeigen die Herausforderungen und Risiken, die mit der mangelnden Transparenz der Ressourcen in einem konvergenten IT-OT-Netzwerk verbunden sind.

Sechs Chancen und Risiken der IT-OT-Konvergenz

1. Steigende Kosten

2. Ungeplante Ausfallzeiten

3. Steigende Cyber-Angriffe

4. IT-OT Netzwerk-Puzzle

5. Limitierte Ressourcen / Steigende Workloads

6. Aufwendige Compliance Anforderungen

1. Steigende Kosten

DIREKTE UND INDIREKTE KOSTEN

- Zusätzliche Arbeitsstunden
- Umsatzeinbußen
- Image-Schaden

JE WENIGER SIE SEHEN, UM SO MEHR ZAHLEN SIE

Vor allem die beschriebene fehlende Ressourcen-Transparenz verursacht Kosten, da es die Bewältigung der nachfolgend beschriebenen Herausforderungen und Risiken erschwert. Das können direkte Kosten sein, weil Überstunden nötig sind, um in komplexeren Umgebungen alle Richtlinien einhalten zu können oder Umsatzeinbußen, weil ein nicht erfasstes Netzwerkgerät ungeplant ausfällt. Sie können aber auch indirekt sein, wie ein Image-Schaden durch ein Sicherheitsleck, das vorher übersehen wurde. Zusammen können das Millionen Euros ungeplanter Mehrkosten werden.

2. Ungeplante Ausfallzeiten (Downtime)

DURCHSCHNITTLICHE KOSTEN BEI AUSFÄLLEN (PRO STUNDE)

€ 26.000 ⟷ € 1.150.000

WENN DIE PRODUKTION STEHT, GALOPPIERT DIE PANIK

Laut eines aktuellen Berichts des Technologie-Marktforschungsspezialisten Vanson Bourne [2] hat die Vermeidung jedweder ungeplanter Ausfallzeiten bei fast drei Vierteln (72%) der befragten Unternehmen auf Vorstandsebene höchste Priorität. Dies überrascht kaum angesichts der großen finanziellen Verluste bei Betriebsunterbrechungen. Laut Quellen wie der Aberdeen Group [3] liegen die durchschnittlichen Kosten pro Downtime-Stunde je nach Branche zwischen 26.000 und 1,15 Millionen Euro.

Leider steigt das Risiko ungeplanter Ausfallzeiten, die durch die oben beschriebene Netzwerkkomplexität und insbesondere durch mangelnde Transparenz der Anlagen verursacht werden. Im Bericht von Vanson Bourne heißt es, dass ein gewisse Unkenntnis über das Netzwerk-Inventar aufgrund fehlender Transparenz etwa 70% der Unternehmen betrifft.

3. Steigende Cyber-Angriffe

In den letzten Jahren ist die Zahl der Internet-Geräte, die auf OT-Netzwerke zugreifen, dramatisch gestiegen. Deswegen müssen OT-Netzwerke, proprietäre und veraltete Systeme, die in der Vergangenheit nicht von Cyber-Vorfällen betroffen waren, vor Bedrohungen aus dem Internet geschützt werden. Sensoren, WLAN-fähige Controller und die neuesten Cloud-basierten industriellen Steuerungssysteme wie SCADA-as-a-Service bieten potenzielle Angriffspunkte für Gegner. Tatsächlich ergab die genannte Forrester-Umfrage, dass 79% der SCADA/ICS-Verantwortlichen einen Verstoß in den letzten 2 Jahren gemeldet haben. Jeder dieser Verstöße kann die Sicherheit der Mitarbeiter und die finanzielle Stabilität der betroffenen Unternehmen gefährden.

79%

der SCADA/ICS-Verantwortlichen haben in den letzten 2 Jahren einen Vorfall gemeldet

> „Viele der mit der Infrastruktur verbundenen Komponenten sind für OT-Manager unsichtbar."

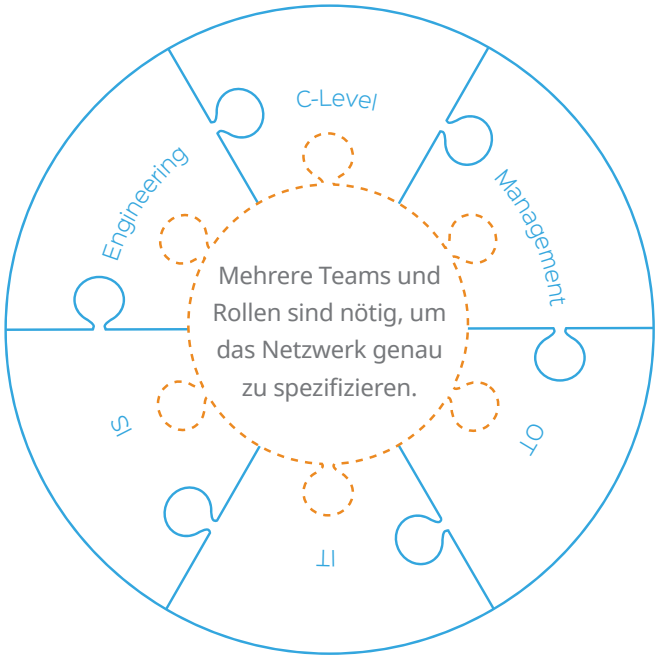
Die mangelnde Transparenz über die Ressourcen erhöht auch die Anfälligkeit eines Unternehmens für Cyber-Bedrohungen. In einer aktuellen Umfrage des SANS Institute[5] gaben 44% der Befragten an, dass ihre größte Sorge in Bezug auf Cyber-Bedrohungen darin besteht, dass Geräte und „Dinge" (die sich nicht selbst schützen können) in ihr Netzwerk aufgenommen werden. Wie bereits erwähnt, können die finanziellen Folgen der Ausfallzeiten – verursacht durch eine direkte und indirekte Verletzung – äußerst schwerwiegend sein.

4. Das IT-OT-Netzwerk-Puzzle

TOP IT-PRIORITÄT
Datenschutz

TOP-OT-PRIORITÄT
Schutz der Verfügbarkeit und Integrität der industriellen Prozesse

Oft sind IT und OT sehr unterschiedliche Abteilungen mit sehr unterschiedlichen Strukturen. Die oberste Priorität der IT ist der Schutz der Daten. Die oberste Priorität von OT ist die Verfügbarkeit und Integrität der industriellen Prozesse. Die heutige Geschäftsumgebung erfordert jedoch, dass IT- und OT-Manager zusammenarbeiten, um das ICS-Netzwerk zu schützen. CIOs und CISOs müssen nun auch die Verantwortung für unerwartete Ausfallzeiten, Geräteschäden und Sicherheitsrisiken in ihrer Produktionsumgebung übernehmen, die durch Cyber-Vorfälle verursacht werden. Dafür brauchen Sie einen detaillierteren Einblick in das ICS-Netzwerk-Inventar.



5. Limitierte Ressourcen und steigende Arbeitslast

ZU VIEL ARBEIT, ZU WENIG ZEIT

IT- und OT-Manager haben auch ohne die zusätzliche Komplexität der IT-OT-Konvergenz bereits eine hohe Arbeitsbelastung. Dazu kommt, dass existierende IT- und OT-Netzwerktransparenzlösungen selten gut zusammenpassen. Das manuelle Zusammenfügen von Informationen aus solchen Lösungen ist fehleranfällig und daraus dann noch Erkenntnisse zu gewinnen, ist enorm schwer – überlastete Teams kann das komplett überfordern. Wenn es nicht gelingt, eine vollständige Transparenz und Kontrolle über alle Abläufe im jeweiligen Umfeld herzustellen, werden ihre Aufgaben unvermeidlich noch schwieriger und stressiger. Selbst wo IT-Transparenz schon herrscht, ist oft die OT-Transparenz das Problem.

6. Aufwendige Compliance-Anforderungen

COMPLIANCE WIRD ERSCHWERT DURCH

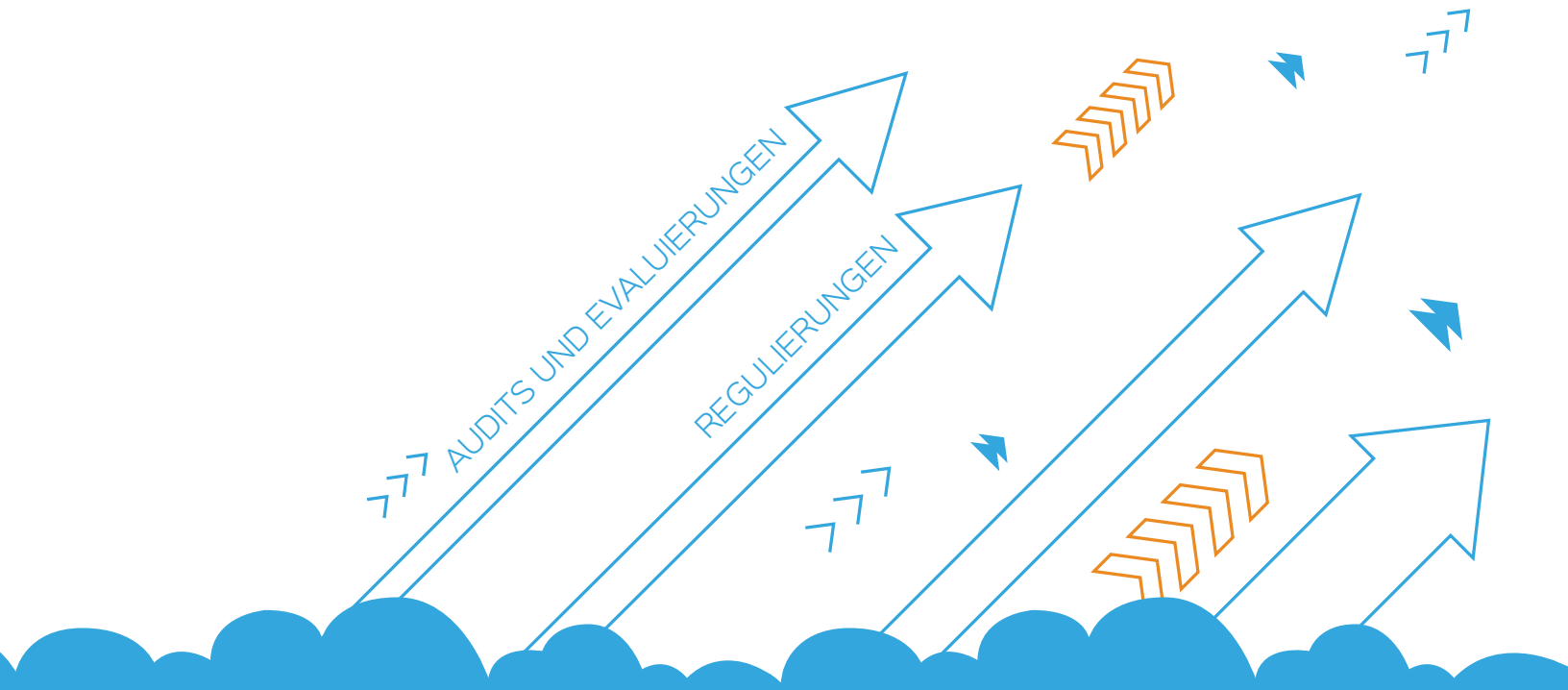
- Netzwerk-Komplexität
- Änderung interner Richtlinien
- Externe Vorschriften

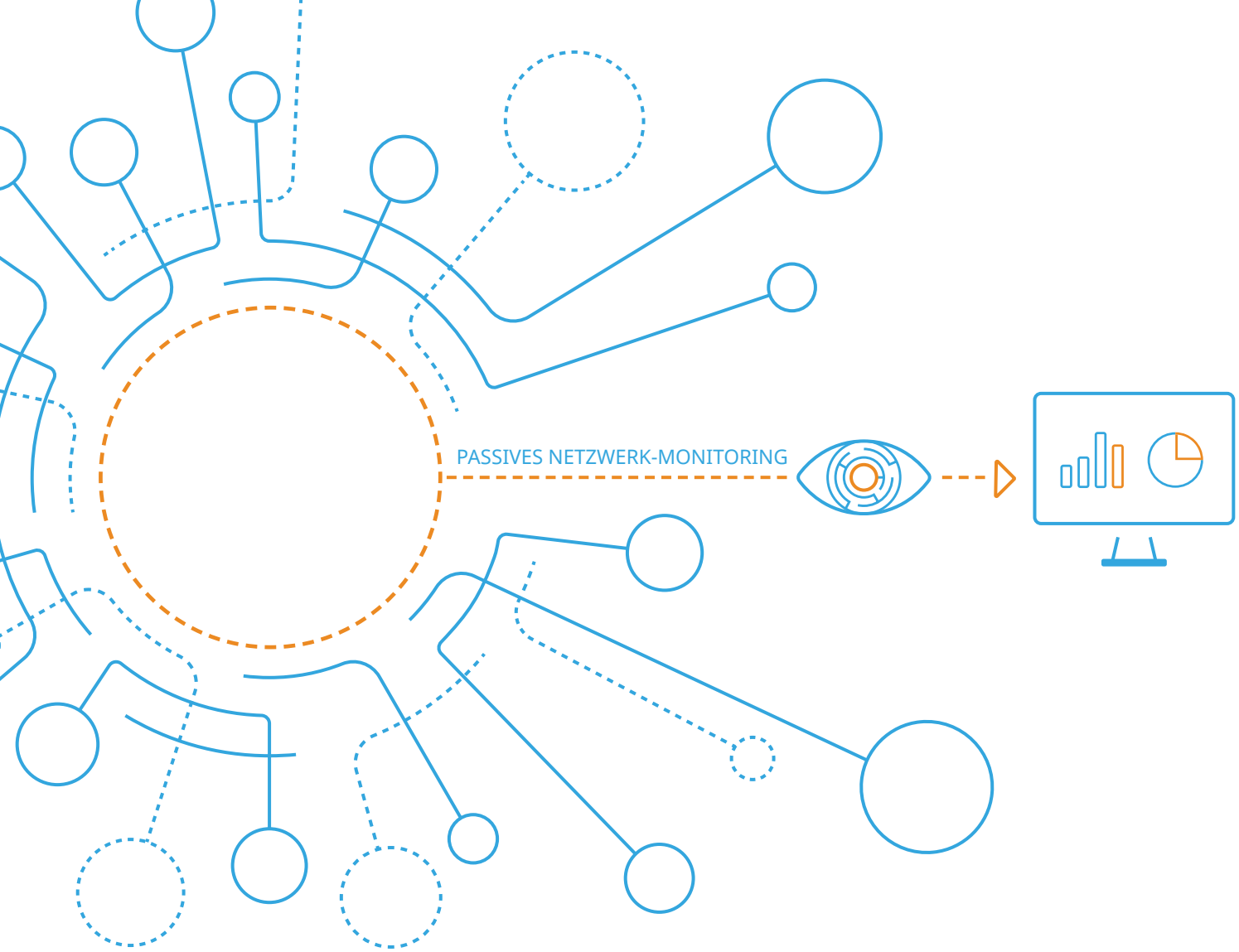
Jeder Rechtsrahmen zur Einhaltung der Vorschriften erfordert als Grundlage ein solides Asset-Management und eine Bestandsübersicht. Die zunehmende Netzwerkkomplexität sowie sich ständig ändernde interne Richtlinien und externe Vorschriften machen diese Aufgabe schwieriger und zeitaufwendiger, was die beschriebenen Herausforderungen an Ressourcen und Arbeitsbelastung weiter verschärft.

Trotz der kostspieligen und arbeitsintensiven Compliance-Bemühungen vieler Unternehmen ist die Gefahr von Bußgeldern relativ groß. Mehr noch: Die zukünftigen Compliance-Kosten und -Aufwände dürften noch steigen. Eine Ursache zeigt der kürzlich erschienene Bericht des Ponemon Institute: Zwei Drittel der führenden IT-Sicherheitsfachleute erwarten, dass die Häufigkeit von Audits und Evaluierungen zunehmen wird, wobei die Vorstandsmitglieder sich stärker in den Prozess der effizienten IT-Sicherheit einbringen werden. Ein weiterer Grund ist das zunehmende Menge und die Verschärfung von Vorschriften, wie die NIS-Richtlinie, das IT-Sicherheitsgesetz oder IEC 62443. Diese Faktoren stützen die Ergebnisse des Ponemon-Institute-Berichts [6], der auch die Zusammenhänge zwischen Compliance-Vereinfachung und gesteigerter Sicherheit beleuchtet. Er ermittelte eine 90%-ige Zunahme der Zahl der Befragten gegenüber dem Vorjahr, die glauben, dass eine Verringerung der Compliance-Belastung zu einer stärkeren Cybersicherheit führt.

2/3

der leitenden IT-Sicherheits-verantwortlichen erwarten eine Zunahme von Audits und Evaluierungen





Die gesteigerte Transparenz von ICS-Assets und -Bedrohungen ist entscheidend

Eine Umfrage des SANS-Instituts aus 2017 hat ergeben, dass 40% der ICS-Sicherheitstechniker Transparenz und ausreichende Informationen über ihr ICS-Netzwerk fehlen. Wie können Unternehmen also fundierte Entscheidungen darüber treffen, wie sie Ausgaben priorisieren und Sicherheitspläne erstellen können, die ihre Mitarbeiter, ihren Ruf und ihr Geschäft schützen? Sie müssen sich einen umfassenden Überblick über ihre Netzwerkressourcen und Schwachstellen verschaffen. Traditionelle Ansätze führen aber oft nicht zum Ziel. So kann etwa ein einfaches Scannen des Netzwerks zu Unterbrechungen oder Systemausfällen und damit zu finanziellen Verlusten führen. Im Extremfall kann es sogar die Produktionstechnik schädigen oder zu Verletzungen von Mitarbeitern führen, wenn Schutzvorrichtungen dadurch fehlerhaft arbeiten. Die manuelle Erfassung ist zwar sicherer, aber extrem arbeitsintensiv, zeitaufwendig, teuer und fehleranfällig.

TRADITIONELLE ANSÄTZE FÜR MEHR TRANSPARENZ

- Einfaches Scannen des Netzwerks
- Manuelle Erfassung

OPTIMALER ANSATZ

- Störungsfreie Netzwerküberwachung

Glücklicherweise gibt es eine Technik, die Anlagen präzise, sicher und kostengünstig identifizieren kann: Die störungsfreie Netzwerküberwachung.

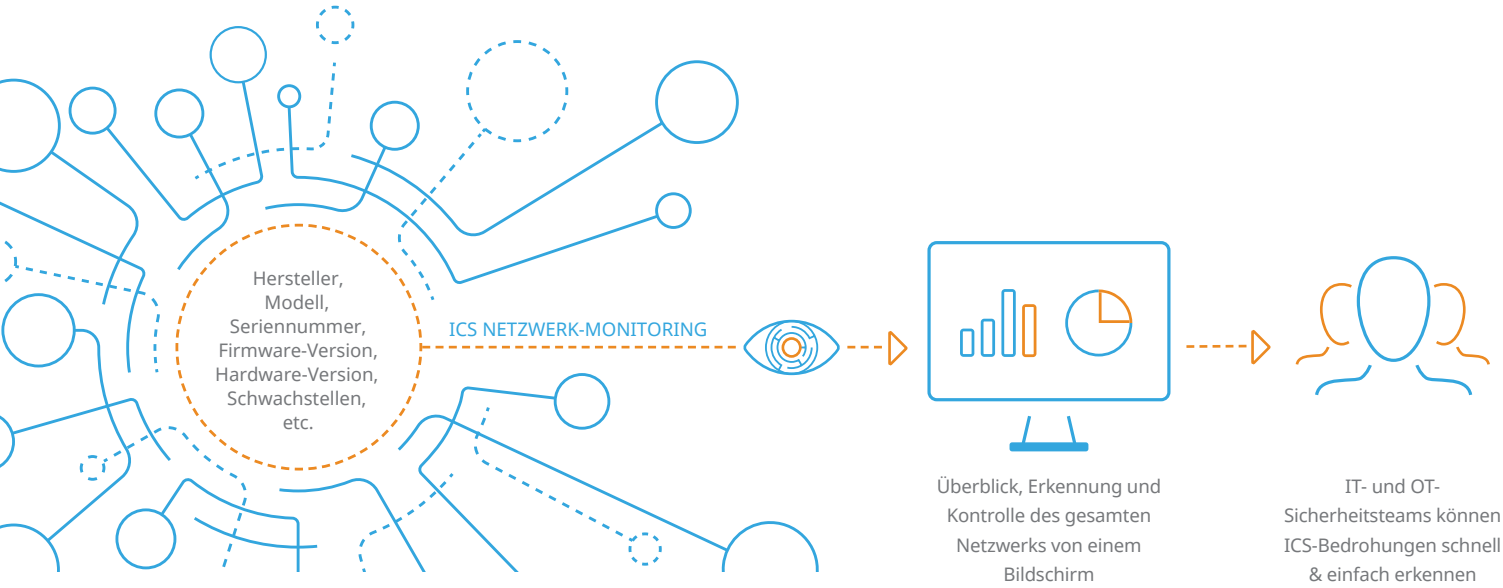
Der optimale Weg zum ICS-Visibility-Management

Das ICS-Sichtbarkeitsmanagement zu optimieren, gewährleistet, dass Unternehmen ein umfassendes Verständnis der ICS-Umgebung und ihrer Verbindungen haben. Dies erleichtert es unter anderem, effektive Sicherheitsarchitekturen zu entwerfen, Angriffsvektoren zu identifizieren und blinde Flecken zu finden. Eine verbesserte Transparenz ermöglicht es OT-Managern auch, unbekannte und ungeprüfte betriebliche Sicherheitsprobleme zu lösen. Dazu gehören Schwachstellen, Fehlkonfigurationen, Verstöße gegen Zugriffsrichtlinien, fehlerhaftes Design in Form von schwachen Sicherheitskontrollen sowie spontane oder nicht autorisierte Änderungen.

Der optimale Weg zur Verbesserung der ICS-Sichtbarkeit ist die Einführung einer ausgereiften, nicht-invasiven Netzwerküberwachungs- und Intelligence Plattform für industrielle Steuerungssysteme. Diese Netzwerküberwachungslösung sist für das Netzwerk unsichtbar und hat keinen Einfluss auf laufende Prozesse. Sie sammeln Asset-Informationen wie Typ, Version und Standort, indem sie den bereits laufenden Datenverkehr analysiert. Aufgrund dieser automatisierten, passiven Art und Weise können Anwender kontinuierlich Anlageninformationen und -verhalten erfassen. Das steigert die Effizienz einer sonst teuren Erfassung der Bestände im Netzwerk deutlich.

Optional kann der Betreiber entscheiden, zusätzliche, nicht-invasive, aktive Module einzusetzen. Durch das passive System gesteuert, können diese Module bestimmte Netzwerkknoten für zusätzliche Informationen detaillierter abfragen – ohne das Netzwerk zu beeinträchtigen.

ICS-NETZWERK-MONITORING
ist die Erfassung von Asset-Informationen wie Typ, Version und Standort durch Mithören des laufenden Netzwerk-Datenverkehrs, wahlweise kombiniert mit aktiven Modulen zur erweiterten Auswertung.



Lösungen wie diese nutzen leistungsstarke Machine-Learning-Fähigkeiten und vollständige Deep-Packet-Inspection (DPI). Sie verfügen auch über umfangreiche Datenbanken ICS-spezifischer Bedrohungsindikatoren und Schwachstellen, um proprietäre und Standardprotokolle aller großen Prozessleittechnik-Hersteller analysieren zu können. Dazu gehören:

- Bestandsaufnahme und -verwaltung, einschließlich dynamischer Klassifizierung von Betriebsmitteln
- OT-Schwachstellenmanagement, einschließlich solcher mit und ohne CVE-Identifier
- Anomalie-Erkennung, um nicht nur neue Cyberangriffe und -techniken, sondern auch Abweichungen vom normalen Prozessverhalten zu erkennen
- API-Integration mit IT-Security-Management-Tools
- Umfassende ICS-Protocol-Unterstützung

DEEP PACKET INSPECTION (DPI)
Die Fähigkeit, jedes einzelne Netzwerkpaket zu untersuchen und jede Kommunikation zwischen ICS-Netzwerkknoten (also Befehle, Variablen, überwachte Parameter, Knotenmerkmale und mehr) zu analysieren.

Diese Funktionen ermöglichen es den nicht invasiven ICS-Überwachungslösungen, operative Gefahren und Probleme wie Netzwerkverbindungsabbrüche, Gerätefehlfunktionen und Fehlkonfigurationen, gefährliche Prozessabläufe, die Verwendung unsicherer Protokolle und Anmeldedaten sowie hochentwickelte Cyberangriffe und Exploits zu erkennen. Warnmeldungen über potenzielle Bedrohungen, die den Betrieb beeinträchtigen könnten, werden in Echtzeit an eine zentrale Visibility-Management-Plattform übermittelt. Von dort aus können sie innerhalb der Organisation entsprechend eskaliert werden.

Durch die Kombination sensorbasierter Informationen aus dem Netzwerk mit anderen Datenquellen (wie der Steuerungskonfiguration und dem Asset Management) kann ein umfassendes, visuelles und interaktives Modell erstellt werden. Dies eröffnet OT-Managern die vollständige ICS-Transparenz und einen klaren Entwicklungspfad zu echter Widerstandsfähigkeit gegen Cyberangriffe.

„Dies eröffnet OT-Managern die vollständige ICS-Transparenz und einen klaren Entwicklungspfad zu echter Widerstandsfähigkeit gegen Cyberangriffe."

5 Vorteile eines optimalen ICS-Visibility-Managements

Das ICS-Visibility-Management ermöglicht es OT-Managern, Herausforderungen und Risiken zu beherrschen, die mit zunehmender Konvergenz der IT-OT-Infrastruktur einhergehen. Die Vorteile reichen von Kosteneinsparungen über geringere Arbeitsbelastung bis hin zu vereinfachter Compliance.

1. Deutliche Kostensenkungen

2. Geringere Ausfallzeiten

3. Verbesserte Widerstandsfähigkeit gegen Cyberangriffe

4. Geringere Arbeitslast und bessere IT-OT-Collaboration

5. Vereinfachte interne und externe Compliance

1. Deutliche Kostensenkungen

KOSTENEINSPARUNGEN DURCH

- Verbesserte Wartung
- Weniger Vor-Ort-Besuche
- Geringere Ausfallzeiten

Durch erhöhte Transparenz können potenzielle Bedrohungen schnell und kostengünstig identifiziert und behoben werden. Wenn Sie zum Beispiel alle Anlagen im Blick haben, kann der Besitzer prüfen, ob die richtige Anlage überwacht wird und ob die Wartung ohne teure Vor-Ort-Besuche wie erwartet verläuft. Das optimiert die Kosten und den Aufwand für die Untersuchung von Angriffen und Schwachstellen sowie für die Fehlersuche, -behebung und -vermeidung. Weitere Kosteneinsparungen lassen sich durch die Vermeidung von Ausfallzeiten, Service- oder Lieferunterbrechungen und dem Image-Verlust infolge erfolgreicher Angriffe beziffern.

2. Geringere Ausfallzeiten

Laut des zitierten Berichts von Vanson Bourne glauben 49% der Befragten, dass Maschinen hilfreich wären, die zur Vermeidung von Ausfallzeiten automatisch Unterstützung anfordern. 45% möchten auch Ingenieuren Zugriff auf historische Anlagendaten ermöglichen. Ein optimierter, nicht invasiver Überwachungsansatz für das ICS Visibility Management liefert dafür die richtigen Werkzeuge.

Kontinuierliche Zustandstests des Netzwerks geben dem OT-Manager auf einen Blick ein vollständiges Bild des aktuellen Status.

Automatische Warnungen helfen Managern, potenzielle Probleme früh zu erkennen und die nötigen Informationen für eine schnelle Reaktion zu sammeln.

Zusätzlich werden alle Konfigurationsänderungen protokolliert und können dazu dienen, Probleme und Effekte schnell und einfach zu analysieren.

NIE WIEDER PRODUKTIONS-PANIK

Außerdem können die bei Vorfällen gewonnenen Erkenntnisse Manager dabei unterstützen, zukünftige Schwachstellen zu erkennen. Potenzielle Probleme lassen sich dadurch früh beheben – bevor sie zu Ausfallzeiten und damit verbundenen Betriebs-, Finanz- und Image-Schäden führen.

> „Das Wissen aus früheren Vorfällen kann Managern dabei helfen, zukünftige Schwachstellen, Leistungs-engpässe und schlechte Wartung zu erkennen."

3. Verbesserte Widerstandsfähigkeit gegen Cyberangriffe

Die umfassende Kenntnis aller ICS-Ressourcen, Schwachstellen, Erweiterungen und Änderungen sorgt dafür, dass OT-Manager nicht mehr im Blindflug unterwegs sind. Dies hilft ihnen, sicher zu entscheiden, welche Kontrollen sie zur Risikominderung implementieren und wie sie Sicherheits- und Wartungspläne sowie -ausgaben priorisieren können. Zudem kann eine ganzheitliche Sicht auf die gesamte Angriffsfläche einer Firma – inklusive Schwachstellen in IT- und OT-Netzwerken sowie virtuellen und Multi-Cloud-Netzwerken – potenzielle Angriffspunkte sichtbar machen. Insgesamt steigert eine verbesserte Cyber-Wartung und Früherkennung die Fähigkeit von Unternehmen, ICS-Cybervorfälle zu verhindern und/oder zu erkennen und darauf zu reagieren.

4. Verringerte Arbeitslast und verbesserte IT-OT-Collaboration

Die Verwendung einer optimierten, nicht invasiven Inventarisierungslösung gibt OT-Managern den nötigen Überblick, um im Unternehmen das Netzwerk genau zu spezifizieren und diese Netzwerkstruktur dauerhaft zu erhalten. Die dadurch entstehende Synergie macht eine enge Zusammenarbeit mit den IT- und IS-Kollegen möglich und hilft allen Beteiligten, die Wechselwirkung mit dem Umfeld zu verstehen, die größten Risiken zu erkennen und zu planen, wie man damit umgeht. All dies hilft dem Unternehmen, die Netzwerkintegrität zu schützen und eine breite Widerstandsfähigkeit gegen Cyberangriffe zu erreichen. Und da eine verbesserte ICS-Transparenz die Kontrolle und den Schutz des Netzwerks erleichtert, können OT-Manager besser verdeutlichen, welche Wertsteigerung sie dem Unternehmen bringen – mit weniger Aufwand und geringeren Kosten.

SYNERGIEN ZWISCHEN IT UND OT
helfen Unternehmen, die Netzwerkintegrität zu sichern und Widerstandsfähigkeit gegen Cyberangriffe zu erzielen
MIT WENIGER STRESS
GEMEINSAM MEHR ERREICHEN

5. Vereinfachte interne und externe Compliance

Die vollständigen Bestandsinformationen und -kontrollmöglichkeiten, die eine optimierte ICS-Netzwerküberwachung bereitstellt, vereinfachen und reduzieren die Kosten für die Einhaltung von Standards und Rahmenbedingungen wie dem NIST Cybersecurity Framework, NERC CIP, IEC 62443 und FISMA. Die Bestandsdaten werden durch leistungsstarke automatisierte Berichtsfunktionen bereitgestellt, die eine fehleranfällige und kostspielige manuelle Dateneingabe überflüssig machen. Die Daten beinhalten wichtige Informationen wie: Hersteller, Modell, Seriennummer, Teil/Typ (z.B. IO-Karte, Kommunikationsmodul), Firmware-Version, Hardware-Version, Gerätename, Schwachstellen, Änderungen, Purdue-Netzwerk-Level und NERC-CIP-Klassifizierung. Eine umfassende Inventarliste und eine interaktive Netzwerkübersicht, die Geräte und Kommunikationswege nach Gerätetyp und Netzwerk gruppiert, ermöglicht zudem ein präzises Reporting und Auditing, und hilft, mögliche Strafen mit minimalem Aufwand zu vermeiden.

EINHALTUNG VON STANDARDS UND COMPLIANCE-VORGABEN WIE:

- NIST CSF
- NERC CIP
- IEC 62443
- FISMA

NACHHALTIGE ERLÖSUNG VOM COMPLIANCE-LEID

Fazit

Die Nutzung einer konvergierten OT- und IT-Infrastruktur bietet einen Wettbewerbsvorteil, aber nur, wenn die ICS-Sichtbarkeit effizient gestaltet wird und mögliche Cyber- oder Betriebsvorfälle identifiziert und verhindert werden können. Während bestehende Security-Management-Tools nur die IT-Seite der IT-OT-Gleichung abdecken, benötigt die ICS-Welt eine dedizierte Lösung. Ein optimierter, nicht-invasiver Überwachungsansatz für das ICS-Visibility-Management ist die beste Lösung.

Zu den Vorteilen der ICS-Transparenz gehören: vollständige Asset-Übersicht, eine deutliche Reduzierung des Arbeitsaufwands und der Kosten für das OT-Management, ein geringeres Geschäftsrisiko durch Prävention von Cyber- und Betriebsstörungen sowie eine vereinfachte Compliance. Letztendlich ermöglicht das ICS-Visibility-Management Industrie-, Öl-, Gas- und Versorgungsunternehmen, alle Vorteile der IT-OT-Konvergenz zu nutzen und gleichzeitig die Kosten und den Aufwand für eine echte Cyber-Resilienz deutlich zu senken.

Weiterführende Informationen

1. Forrester Research for Fortinet 2017 – "INDEPENDENT STUDY PINPOINTS SIGNIFICANT SCADA /ICS CYBERSECURITY RISKS " https://hub.fortinet.com/whitepapers/independent-study-pinpoints-significant-scada-ics-cybersecurity-risks
2. Vanson Bourne "After The Fall: Cost, Causes and Consequences of Unplanned Downtime, Oct 2017"
3. Aberdeen http://www.aberdeenessentials.com/techpro-essentials/stat-of-the-week-the-rising-cost-of-downtime/
4. Forrester Research 2018 – "Protecting Industrial Control Systems And Critical Infrastructure From Attack"
5. SANS Institute 2017 – https://www.sans.org/reading-room/whitepapers/ICS/securing-industrial-control-systems-2017-37860
6. Ponemon Institute 2018 "2018 STUDY ON GLOBAL MEGATRENDS IN CYBERSECURITY"
7. EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html

Über Forescout

Forescout befähigt Betreiber kritischer Infrastrukturen sowie Fertigungsunternehmen, industrielle Bedrohungen und Fehler zu erkennen, zu analysieren und darauf zu reagieren, um so die Kosten für die Fehlerbehebung und unerwartete Ausfallzeiten zu minimieren. Wir nutzen ICS-spezifisches Know-how, um Einblick in kritische Systeme und deren Aktivitäten zu gewinnen und operative Probleme und Cyber-Sicherheitsrisiken zu erkennen. Unsere revolutionäre und umfassende Netzwerküberwachungsplattform wird von Kunden weltweit erfolgreich eingesetzt. Und im Gegensatz zu einigen anderen Anbietern bieten wir bereits heute die Flexibilität, um IT- und OT-Ressourcen in mehreren branchenspezifischen Nutzungsszenarien vollständig und effektiv zu schützen. Im Jahr 2018 wurde Forescout von Frost & Sullivan für seine wegweisende industrielle Cybersicherheitslösung ausgezeichnet und erhielt den Global Customer Value Leadership Award 2018 für den Schutz der Systemnetzwerke von Industrieunternehmen im Bereich der Informations- und Betriebstechnik (IT & OT) vor Malware und Zero-Day-Angriffen.

Sie möchten mehr erfahren?

Mehr über SilentDefense von Forescout und seine Vorteile finden Sie unter www.forescout.com/silentdefense.

Oder kontaktieren Sie uns noch heute per E-Mail: info-ot@forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com