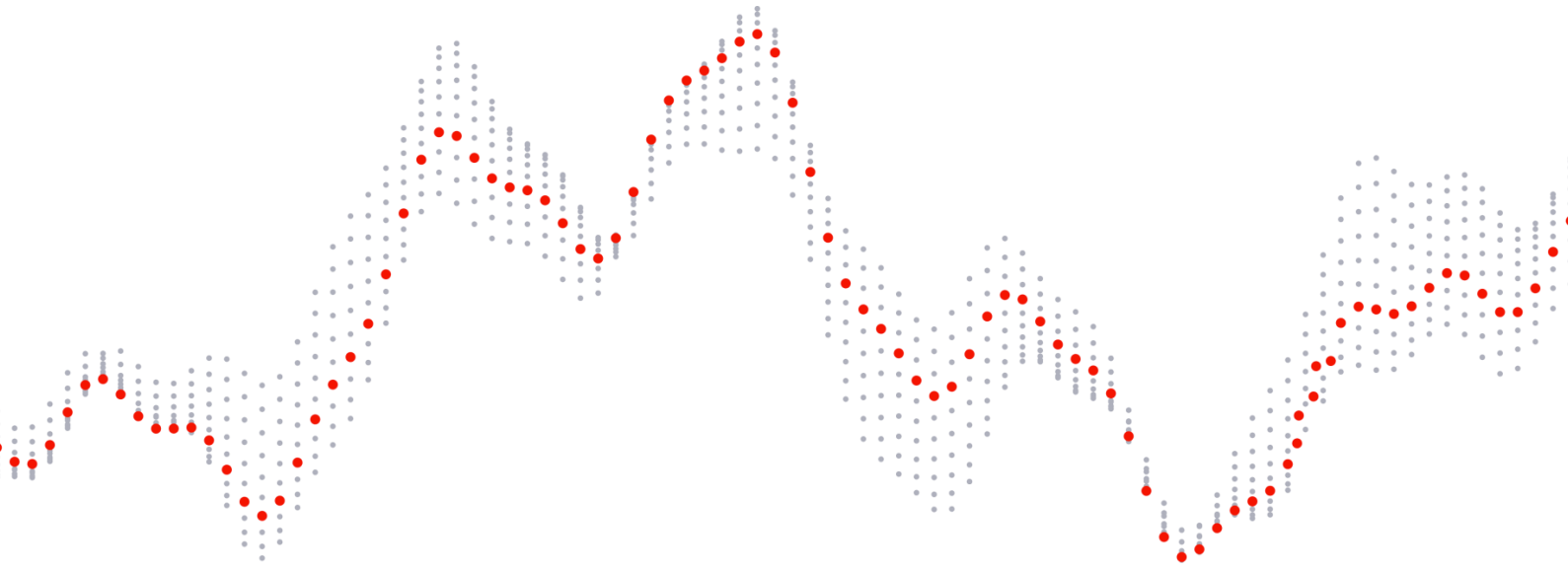
WHITE PAPER

OT Security ohne unnötigen Aufwand

Von Compliance-Anforderungen zu operativer Resilienz

Wie sich die OT-Transparenzlücke schliessen, die Segmentierung validieren und die OT-Sicherheit operationalisieren lässt – ohne zusätzliche SIEM-Komplexität.

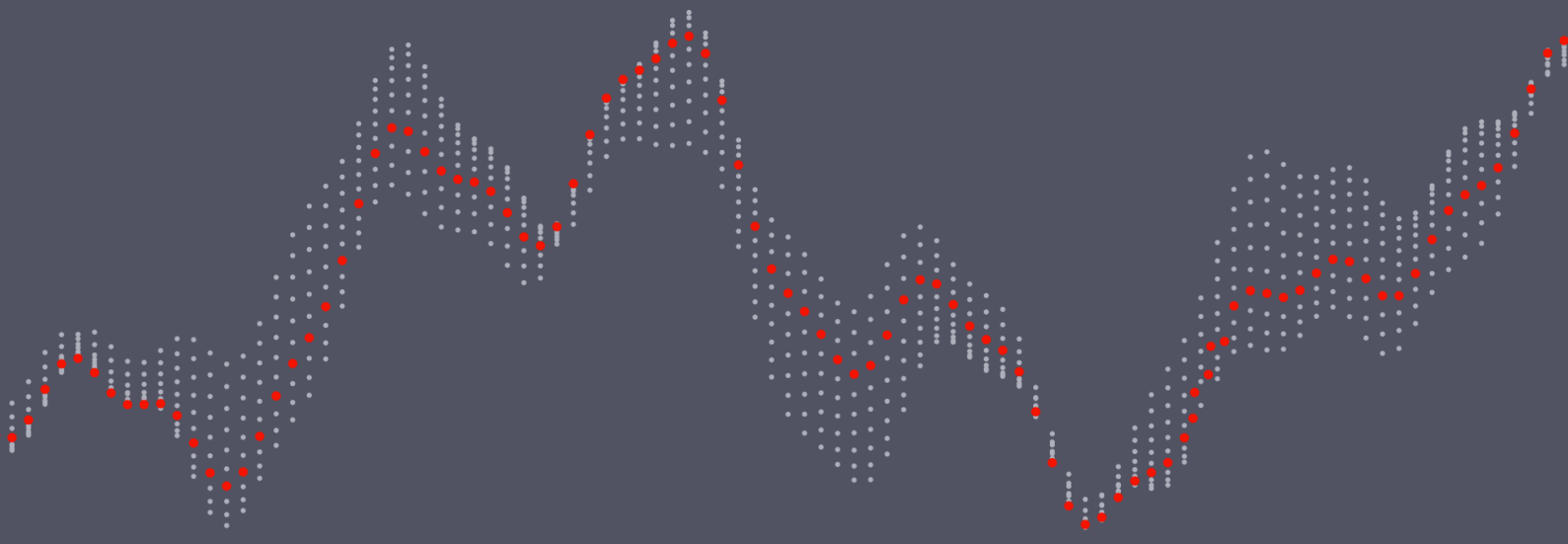


exeon

exeon.com

Table of Contents

Executive Summary



EXECUTIVE SUMMARY

Operational Technology gehört inzwischen zu den exponiertesten und zugleich am wenigsten überschaubaren Bereichen moderner Organisationen. Die Systeme, die Produktionslinien, Energienetze, Wasseraufbereitung, Spitalinfrastruktur und Verkehrsnetze steuern, wurden auf beständige Verfügbarkeit und lange Lebenszyklen ausgelegt, nicht auf eine einfache Integration inin IT-Netzwerke. Auch Remote-Wartungen oder ein einfaches Anpassen an neue regulatorische Frameworks waren bisher nur ein geringes Augenmerk.

Heute müssen Organisationen eine Frage beantworten, für die ihnen häufig die nötige Grundlage fehlt: Kann nachgewiesen werden, dass die OT-Umgebung überwacht und segmentiert ist? Vorgaben wie NIS2 und KRITIS verlangen zunehmend Nachweise für kontinuierliches Monitoring, Asset Visibility und Incident Readiness. Viele Organisationen verfügen jedoch weder über ein verlässliches Inventar ihrer OT-Systeme noch über einen vollständigen Überblick darüber, wie diese kommunizieren.

> **Daraus entsteht ein grundlegendes Paradoxon: Organisationen müssen Systeme schützen, segmentieren und auditieren, die sie nicht vollständig überblicken können.**

Die klassische Antwort sind umfassende Implementierungen von Firewalls, ZTNA und weiteren Security Controls. Solche Projekte sind jedoch oft langsam, teuer und bergen operative Risiken. Viele traditionelle IT-Security-Ansätze, wie zusätzliche Sensoren, aktive Scans oder Endpoint-Agenten, eignen sich für Legacy-Systeme nicht oder nur bedingt, Herstellervorgaben und betrieblichen Anforderungen erschweren ihren Einsatz, kurzum sie sind für eine OT-Umgebung nicht ohne grösseren Aufwand anwendbar. Projekte bleiben deshalb häufig in der Planung stecken und liefern die versprochene Sichtbarkeit nie.

Dieses Whitepaper präsentiert eine andere Reihenfolge: Zuerst passive Sichtbarkeit schaffen, danach die Segmentierung kontinuierlich validieren und bereits vor einem Vorfall klar festlegen, wer auf dem Shopfloor welche Entscheidungen trifft.

EXECUTIVE SUMMARY

Auch Organisationen mit bestehenden OT-Security-Plattformen stehen vor einer Herausforderung: Der Operationalisierung dieser Plattformern. Alerts verteilen sich auf verschiedene Tools, OT-Engineers fehlt eine zentrale Sicht auf Security-Informationen und dem SOC häufig der notwendige OT-Kontext. Klassische SIEMs können dafür zu teuer, komplex oder ungeeignet sein. Es fehlt nicht an einem weiteren OT-Sensor, sondern an einer praktikablen Möglichkeit, OT-Security-Daten zu konsolidieren, zu kontextualisieren und für konkrete Massnahmen nutzbar zu machen.

Das Ziel ist nicht Perfektion. Es ist nachweisbare Resilienz, die sich innerhalb von Wochen statt Jahren aufbauen lässt.

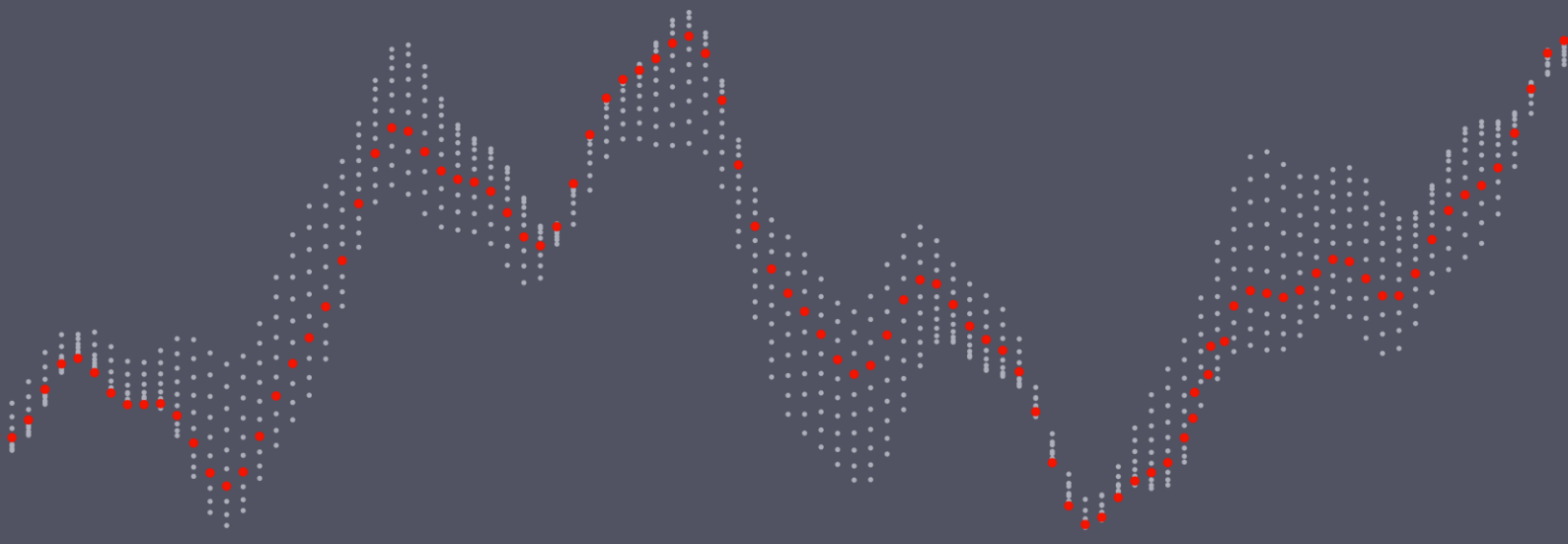
DER NEUE STANDARD

Die Frage lautet nicht mehr “Verfügen Sie über Sicherheitskontrollen?”, sondern “Können Sie belegen, dass sie funktionieren – über Systeme hinweg, die Sie auch wirklich einsehen können?”

01

ABSCHNITT 01

Das Compliance-Paradoxon: Schützen, was man nicht sieht



Rechtliche Anforderungen haben sich deutlich verschärft.

Rechtliche Anforderungen haben sich deutlich verschärft. NIS2 erweitert die Cybersecurity-Pflichten auf wesentlich mehr wichtige und besonders wichtige Einrichtungen. KRITIS-Vorgaben in Deutschland und vergleichbare nationale Regelwerke verpflichten Betreiber kritischer Infrastrukturen zu Monitoring und Reporting. DORA stellt Anforderungen an die operative Resilienz und Meldung von Vorfällen im Finanzsektor und bei dessen Dienstleistern. Gemeinsam ist diesen Vorgaben die Nachweispflicht: Organisationen müssen belegen, dass ihre Umgebungen überwacht werden und Vorfälle innerhalb enger Fristen erkannt und gemeldet werden können.

NIS2 **KRITIS** **DORA**

Viele OT-Umgebungen scheitern bereits an dieser Voraussetzung. Ein nie inventarisiertes Asset lässt sich nicht zuverlässig in ein Reporting aufnehmen. Die Segmentierung zwischen unbekannten Zonen kann nicht nachgewiesen werden. Und ohne eine Baseline für normales Verhalten lässt sich eine Meldefrist von 24 Stunden kaum einhalten. Compliance setzt eine Sichtbarkeit voraus, die in vielen OT-Umgebungen in der Praxis fehlt.

Warum OT nicht IT ist

Viele Securityteams versuchen zunächst, bekannte IT-Security-Ansätze auf OT-Umbgebungen zu übertragen. Auf dem Shopfloor stossen diese jedoch schnell an ihre Grenzen:

- **Patching ist oft nicht möglich.** Viele Systeme nutzen alte Betriebssysteme, zertifizierte Konfigurationen oder herstellergebundene Software. Ein Patch kann den Supportanspruch aufheben oder eine erneute Zertifizierung erfordern.

- **Aktive Scans sind häufig zu riskant.** Active Scanning und authentifizierte Abfragen können fragile OT-Systeme beeinträchtigen oder zum Absturz bringen.
- **Downtime ist ausgeschlossen.** Eine Produktionslinie, ein Umspannwerk oder ein Spitalsystem kann nicht einfach für ein Security-Projekt abgeschaltet werden. Verfügbarkeit hat höchste Priorität.
- **Lebenszyklen werden in Jahrzehnten gemessen.** Anlagen, die vor zwanzig Jahren installiert wurden, sind teilweise noch immer im Einsatz. Sie haben keine integrierte Security-Funktionen und es gibt keinen realistischen Ersatz oder kurzfristige Alternativen für sie.

Das sind keine Ausreden, sondern technische und operative Realitäten. Ein glaubwürdiger OT-Security-Ansatz muss sich an diese Umgebung anpassen.

KERNFRAGE FÜR CISOs

Könnten Sie heute nachweisen:

- welche Assets vorhanden sind?
- wie diese miteinander kommunizieren?
- ob die Segmentierung tatsächlich funktioniert?
- was während eines Vorfalls geschehen ist?

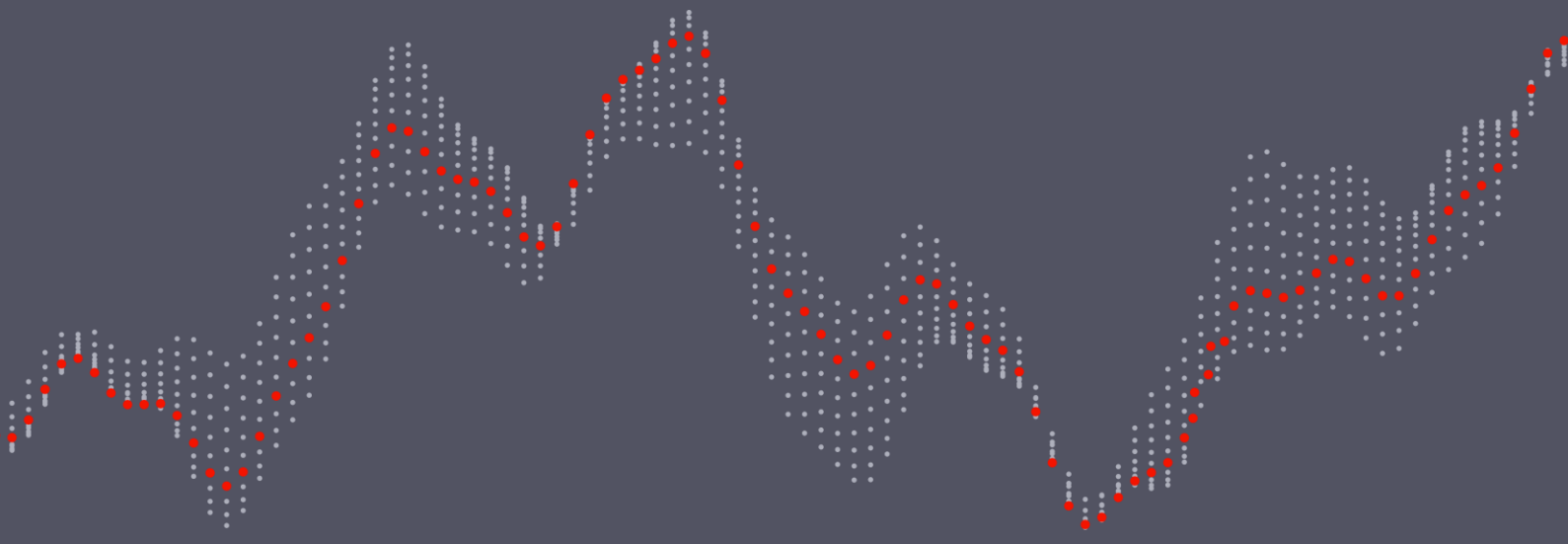
The Reporting-Lücke

Richtliniengerechtes Reporting setzt eine Baseline voraus. Um eine Abweichung, Anomalie oder einen Vorfall zu melden, muss bekannt sein, wie normales Verhalten aussieht. Ohne eine aktuelle Übersicht über Assets und Kommunikationswege müssen OT-Verantwortliche die Antworten auf regulatorische Fragen nach einem Vorfall unter Zeitdruck und aus unvoll- ständigen Daten rekonstruieren: Was ist passiert, wann ist es passiert, welche Systeme waren betroffen und wie wurde der Vorfall eingedämmt? Die Baseline muss vor dem Vorfall bestehen, sie kann nicht erst im Nachgang rekonstruiert werden. Die Frage lautet nicht mehr: «Verfügen Sie über Security Controls?» Sondern: «Können Sie nachweisen, dass die Security Controls funktionieren, und zwar für alles Systeme, die Sie tatsächlich auch sehen?»

02

ABSCHNITT 02

Warum OT-Security-Projekte in der Planung stecken bleiben



Bei vielen grossen OT-Security-Initiativen zeigt sich dasselbe Muster

Fragen Sie nahezu jeden OT-Sicherheitsverantwortlichen nach seiner letzten grossen Initiative, und es zeigt sich ein vertrautes Muster. Das Projekt startet ambitioniert: vollständige Sensorabdeckung, Firewalls an jeder Zonengrenze, ZTNA für Remote Access und Agents, wo immer sie eingesetzt werden können. Der Business Case verspricht nahezu vollständige Abdeckung. Dann folgt unweigerlich die harte Landung in der Realität.

Sensorintensive Implementierungen erfordern Hardwarebeschaffung, Netzwerk-änderungen, Freigaben durch Change Advisory Boards, Wartungsfenster, Koordination mit Herstellern und sorgfältige Tests, um sicherzustellen, dass die Produktion nicht beeinträchtigt wird. Jeder Schritt braucht Zeit, und jede Änderung muss angesichts des operativen Risikos begründet und vorab geplant werden. Monate vergehen, während das Budget bereits durch Planung und Integration gebunden ist, ohne dass Einsehbarkeit in die OT-Netzwerke entsteht. Prioritäten ändern sich. Das Projekt, das nach 18 Monaten eine Abdeckung von 98 Prozent versprochen hat, befindet sich nach 12 Monaten noch immer in der Planung.

DER NEUE STANDARD

In der OT-Sicherheit ist das Perfekte der Feind des Guten. 80 % Transparenz heute sind mehr wert als 98 % Transparenz, die nie zustande kommen.

Die Kosten des Wartens

Während das Grossprojekt stagniert, bleibt die Umgebung weitgehend unüberwacht. Shadow- OT wächst weiter: Nicht verwaltete Geräte, vergessene Remote-Access-Pfade, Laptops externer Dienstleister, alle bauen nicht dokumentierte Verbindungen auf. Die «blinden Flecken», die das Projekt überhaupt notwendig gemacht haben, bleiben während der gesamten Planungsphase bestehen. Das Streben nach Vollständigkeit führt paradoxerweise dazu, dass die Organisation länger ungeschützt bleibt.

Eine bessere Reihenfolge begreift Sichtbarkeit nicht als Endpunkt einer langen Implementierung, sondern als schneller und risikoarmer erster Schritt. Die gewonnenen Einsichten zeigen anschliessend, wo umfassendere Investitionen den grössten Nutzen bringen.

Erst sehen. Dann investieren.

TRADITIONELLES OT-SECURITY-PROJEKT

Planung	Beschaffung	Implementierung	Integration

✓ Sichtbarkeit

VISIBILITY-FIRST-ANSATZ

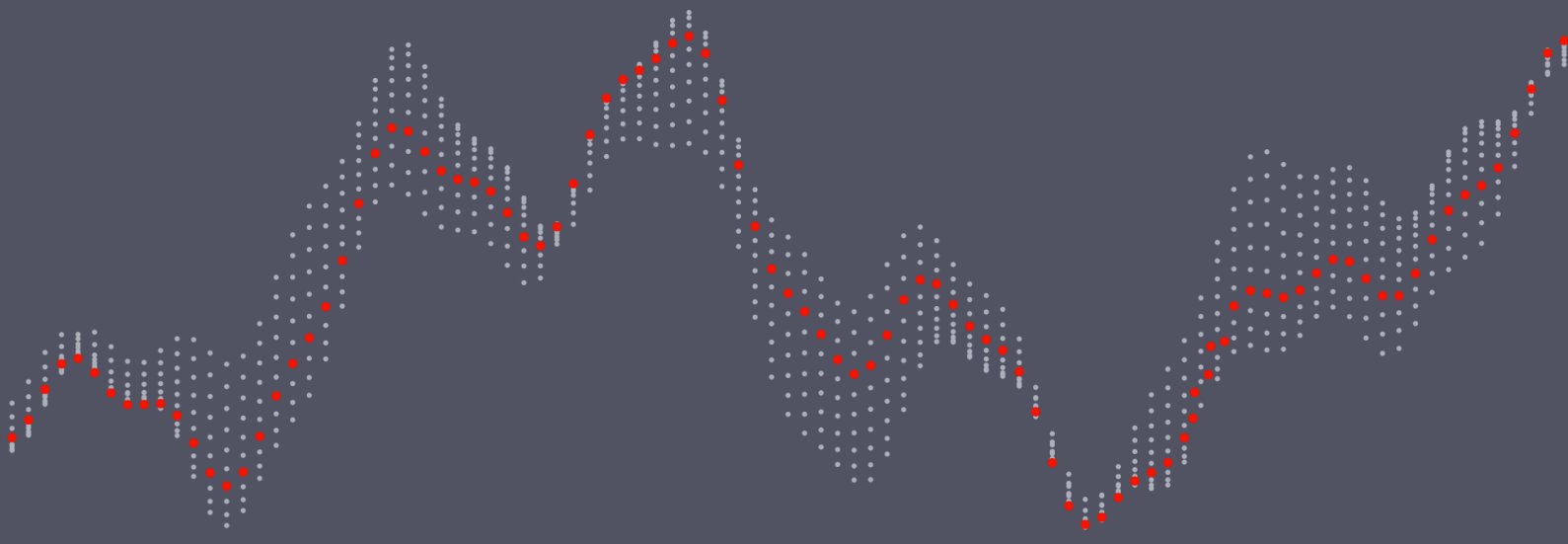
Passive Sichtbarkeit	Asset Inventory	Validierung der Segmentierung	gezielte Security-Investitionen

✓ Sichtbarkeit

03

ABSCHNITT 03

Der simple Ansatz: 90 Prozent Sichtbarkeit in wenigen Wochen



Passive Sichtbarkeit verändert die Kostenstruktur

Passive Sichtbarkeit verändert die Kostenstruktur von OT Security. Statt tief eingreifende Agents oder aktive Scanner einzusetzen, können Organisationen vorhandene Netzwerk-Telemetrie aus Firewalls, Switches und bestehender Security-Infrastruktur nutzen. Daraus entsteht ein umfassendes Bild der OT-Assets und Kommunikationsflüsse. Weil keine zusätzliche Infrastruktur in die OT-Umgebung eingebracht wird, ist die Implementierung schneller, einfacher und deutlich weniger störend. Es werden keine Daten oder Abfragen in das OT-Netzwerk eingebaut, wodurch die Produktion unberührt bleibt und praktisch kein Downtime-Risiko entsteht.

Aus den passiv erfassten Metadaten entsteht häufig innerhalb weniger Tage ein erstaunlich vollständiges Bild:

- **Asset Inventory:** Aktive und kommunizierende Geräte werden sichtbar, auch wenn sie in keiner Tabelle erfasst sind.
- **Kommunikationsflüsse:** Es wird erkennbar, welche Systeme über welche Protokolle und Zonengrenzen hinweg miteinander kommunizieren.
- **Shadow OT:** Nicht verwaltete Assets oder unerwartete Verbindungen werden sichtbar, einschliesslich Remote-Access-Pfaden, die vorgesehene Controls umgehen.
- **Anomalien:** Sobald eine Verhaltens-Baseline besteht, lassen sich Abweichungen wie neue Verbindungen, ungewöhnliche Datenmengen oder unerwartete externe Kommunikation erkennen.

90%

SICHTBARKEIT IN ~2 WOCHEN

Das ist was «90 Prozent in zwei Wochen» in der Praxis heisst. Statt monatelang auf eine perfekte Implementierung zu warten, können Organisationen Risiken sofort reduzieren und ihre Security-Fähigkeiten schrittweise ausbauen. Investiert wird dort, wo die gewonnene Sichtbarkeit den grössten Effekt erwarten lässt.

Sichtbarkeit ist die Grundlage, nicht das Ziel

Passive Sichtbarkeit ersetzt weder Segmentierung noch Access Control oder Incident Response. Sie schafft die Grundlage, um diese Massnahmen gezielt umzusetzen und ihre Wirksamkeit nachzuweisen. Zudem kann sich so Segmentierung an den tatsächlich beobachteten Kommunikationsflüssen, Access Policies an realen Abhängigkeiten, und die Erkennung von Anomalien an einer belastbaren Baseline orientieren. Nachfolgende Controls lassen sich schneller planen und besser begründen, weil sie auf Nachweisen statt Annahmen beruhen.

OT Security Maturity Journey

Sehen

Asset Inventory · Kommunikationsflüsse · Legacy-Systeme

↓

Validieren

Segmentierung · Policies · Compliance

↓

Operationalisieren

gemeinsame Untersuchungen · SOC-Kontext · Datenkorrelation

↓

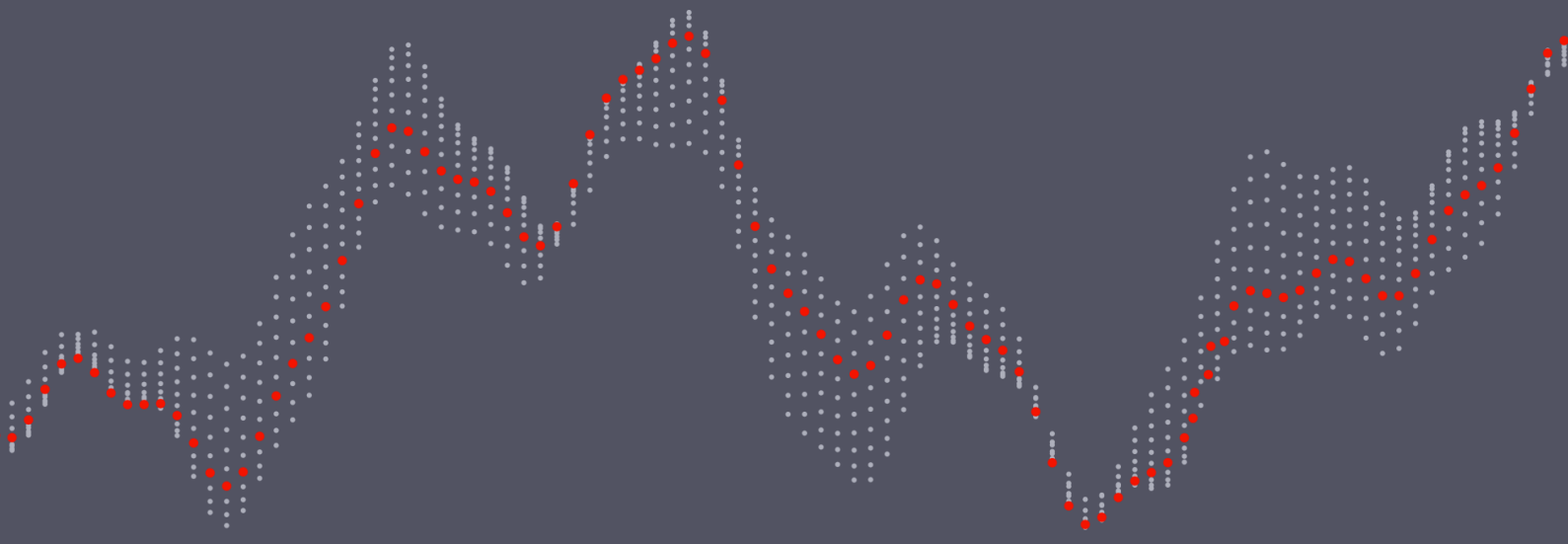
Reagieren

Incident Workflows · Nachweise · Reporting

04

ABSCHNITT 04

Warum OT-Security-Tools operativen Kontext brauchen



Neither side has the complete picture

Viele Organisationen haben bereits in OT-Security-Plattformen investiert, um industrielle Assets, Protokolle und Anomalien besser zu verstehen. Diese Lösungen liefern wertvolle Erkenntnisse und sind ein wichtiger Bestandteil moderner OT-Security-Architekturen.

Sichtbarkeit allein macht OT Security jedoch noch nicht operativ nutzbar.

Security-Informationen verteilen sich häufig auf mehrere Plattformen: OT IDS, Firewalls, Switches, Remote-Access-Lösungen und bestehende IT-Security-Tools. Jedes System liefert einen Teil des Bildes, aber keines den vollständigen operativen Kontext, der für Untersuchungen, die Validierung von Controls und Security Operations erforderlich ist.

Das Resultat wurde bereits erläutert: OT-Teams verstehen die Produktionsumgebung, SOC Teams die Cyberbedrohungen. Beide verfügen über wertvolle Informationen, aber keiner über das Gesamtbild.

KERNFRAGE FÜR SOC TEAMS

Kann Ihr SOC einen OT-Vorfall untersuchen, ohne dass das OT-Team die Ereignisse manuell rekonstruieren muss?

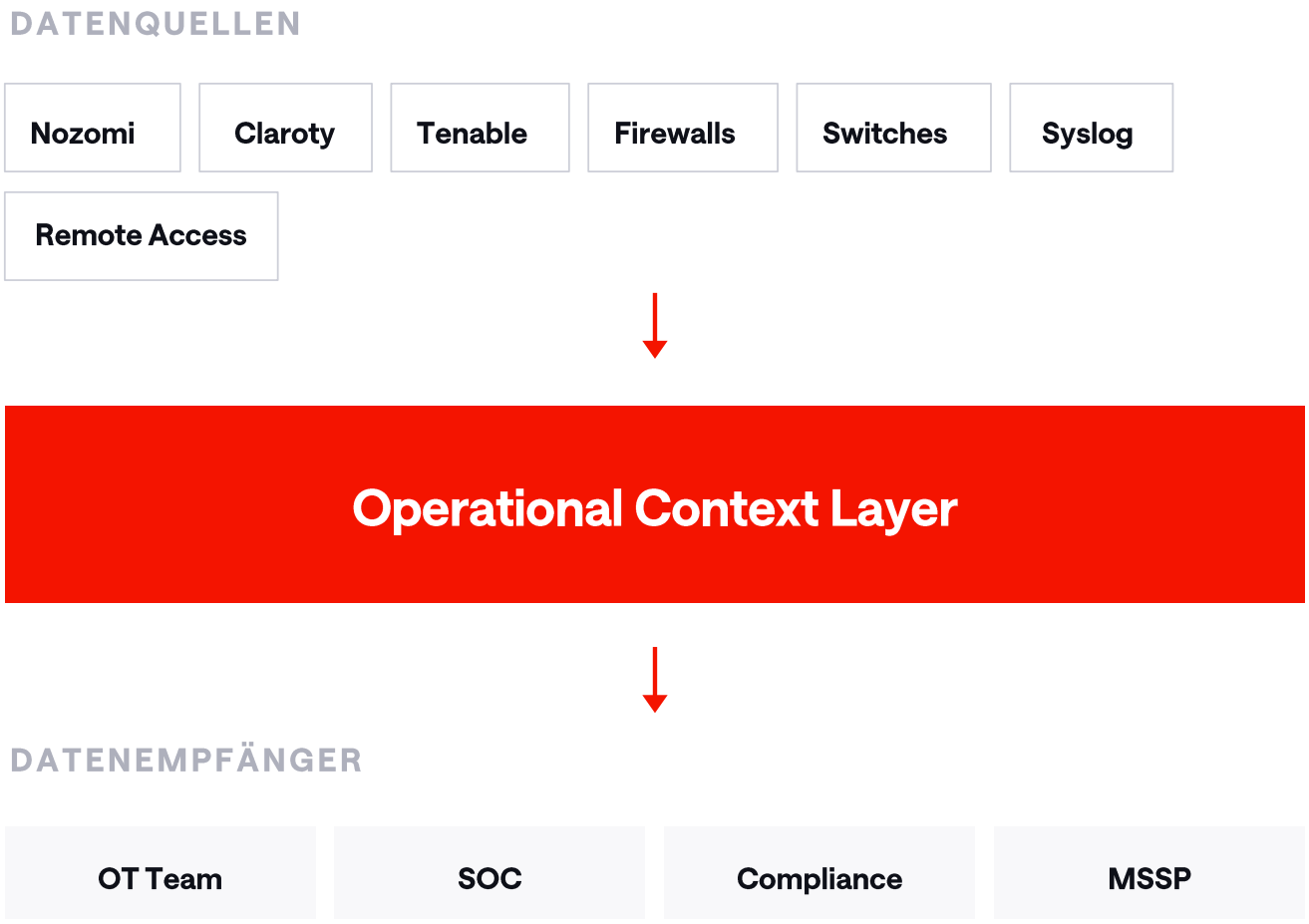
Über die Erkennung hinaus

Eine häufige Reaktion ist die Einführung eines SIEM. In vielen OT-Umgebungen lassen sich klassische SIEM-Plattformen jedoch nur schwer rechtfertigen. Sie können teuer im Betrieb und komplex in der Wartung sein und orientieren sich oft an IT-zentrierten Workflows statt an den Realitäten industrieller Prozesse.

Operative Resilienz braucht deshalb nicht noch eine weitere Monitoring-Plattform, die zusätzliche Daten erzeugt. Sie braucht eine zentrale Sicht auf bereits vorhandene Security-Informationen, die Ereignisse aus IT und OT zusammenführt, korreliert und den notwendigen operativen Kontext für Investigationen, Incident Response und Compliance bereitstellt.

> **Es geht nicht darum, bestehende OT-Security-Lösungen zu ersetzen, sondern den vollen Wert aus ihnen zu ziehen.**

Bestehendes verbinden

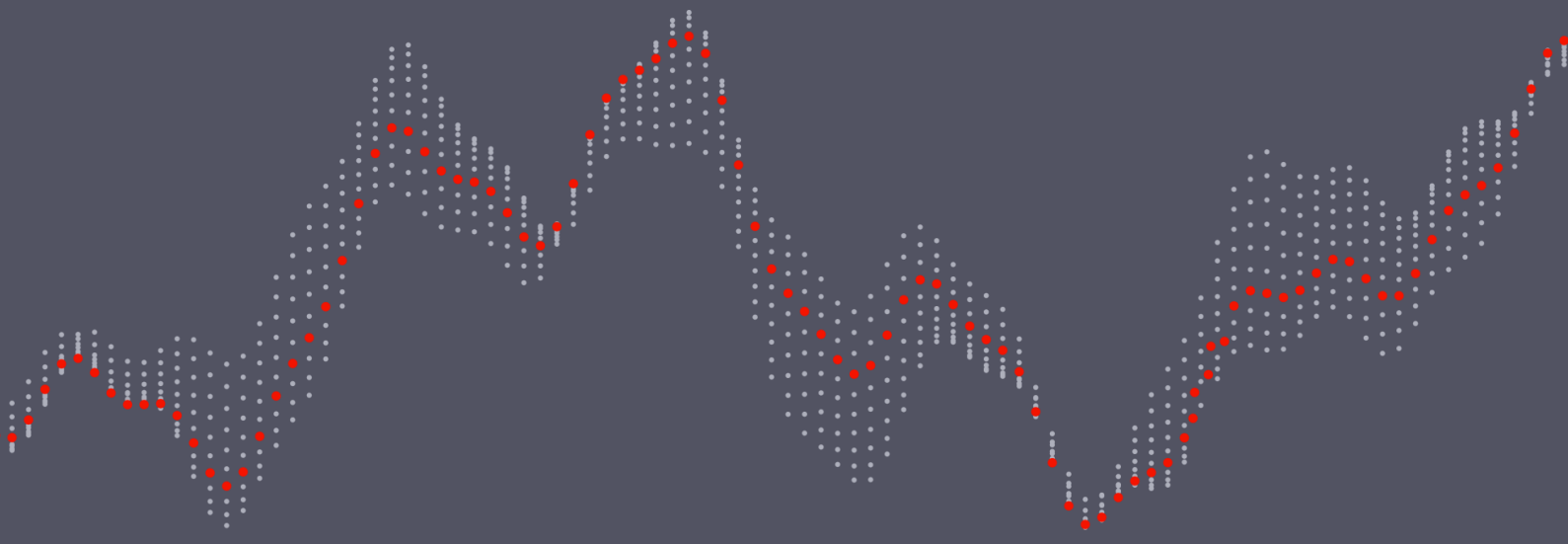


Bestehende Tools erzeugen wertvolle Informationen. Operative Resilienz entsteht, wenn diese Informationen verbunden werden.

05

ABSCHNITT 05

Wenn Firewall-Regeln täuschen: Segmentierung kontinuierlich validieren



Segmentations-Drift

Segmentierung ist das Rückgrat einer OT-Sicherheitsarchitektur. Sie liegt dem Purdue-Modell, Zone-and-Conduit-Designs und vielen regulatorischen Erwartungen zugrunde. Doch Segmentierung kann sich schleichend verschlechtern. Eine Firewall-Regel für ein temporäres Wartungsfenster wird nicht entfernt. Unter Zeitdruck entsteht eine «Any-Any»-Regel, die später vergessen geht. Ein neues System wird angeschlossen, ohne die Policy anzupassen. Dokumentierte Architektur und tatsächlicher Traffic entwickeln sich langsam auseinander.

Dieser Segmentations-Drift ist besonders gefährlich, weil er unsichtbar bleibt. Das Netzwerkdiagramm zeigt weiterhin eine saubere Trennung der Zonen, während der reale Traffic ein anderes Bild vermittelt. Ein jährliches Audit erfasst nur eine Momentaufnahme, nicht die Veränderungen in den elf Monaten dazwischen.

> **Eine Firewall-Regel beschreibt, was erlaubt ist. Netzwerk-Metadaten zeigen, was tatsächlich passiert. Die Lücke dazwischen ist Ihr Risiko.**

Von punktueller zu kontinuierlicher Kontrolle

Die passive Sichtbarkeit, die das Asset Inventory ermöglicht, kann gleichzeitig die Segmentierung fortlaufend validieren. Durch den Vergleich beobachteter Kommunikationsflüsse mit den vorgesehenen Policies lässt sich jederzeit prüfen, ob Traffic unerlaubt Zonengrenzen überschreitet, verbotene Protokolle genutzt werden, die dokumentierte Segmentierung in der Praxis also tatsächlich besteht. Damit wird aus einem statischen Architekturdiagramm ein lebender, kontinuierlich überwachter Sicherheitskontrollmechanismus.

Who Is Allowed to Change What?

Segmentation Drift ist nicht nur ein technisches, sondern auch ein Governance-Problem. Die Verantwortung für Änderungen im OT-Netzwerk verteilt sich meist auf Teams mit unterschiedlichen Prioritäten: OT-Operations verantwortet Verfügbarkeit und Produktionsprozesse, IT-Security die Policies und das Threat Model, und Compliance Model, die Audit Trails und regulatorischen Anforderungen. Ohne eine gemeinsame, aktuelle Sicht auf das Netzwerk können gut gemeinte Änderungen die gesamte Security-Posture schwächen.

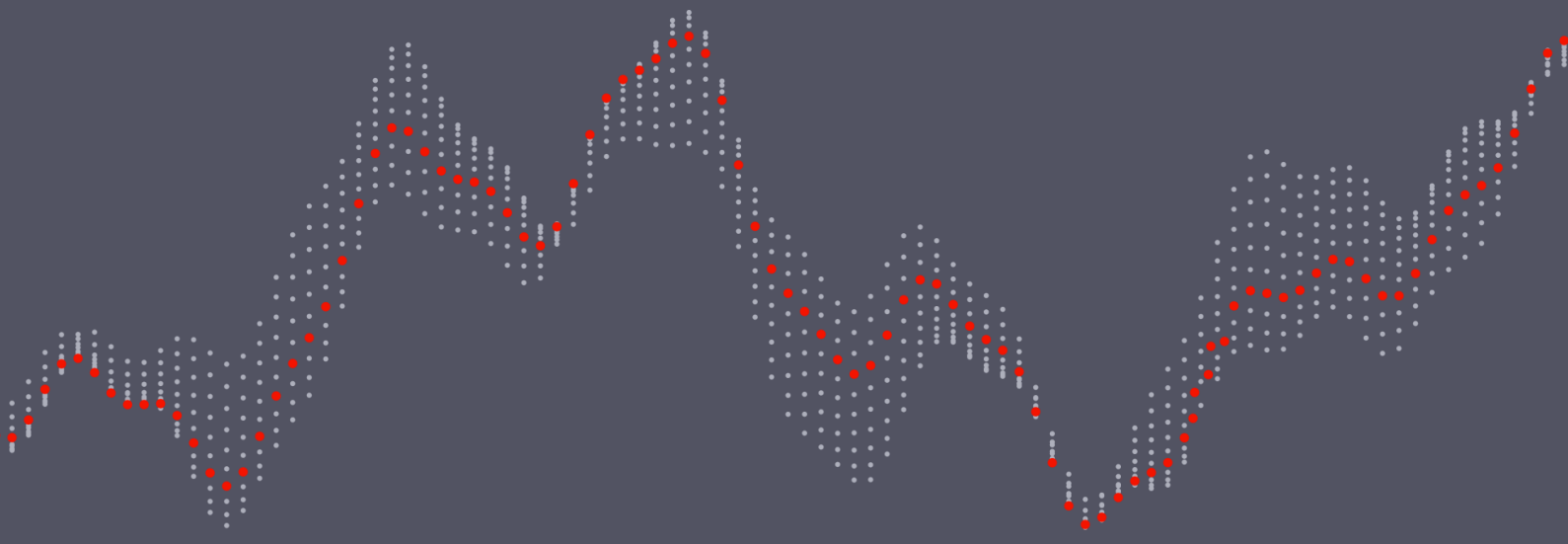
Kontinuierliche Validierung gibt allen drei Gruppen dieselbe verlässliche Datengrundlage. Änderungen werden sichtbar, zuordenbar und überprüfbar. Die Frage «Wer hat was geändert und war dies zulässig?» lässt sich damit anhand von Daten beantworten, statt von Erinnerung oder Wohlwollen abzuhängen.

TEAM	HAUPTANLIEGEN	WAS DIE VALIDIERUNG LIEFERN MUSS
OT Operations	Verfügbarkeit und Prozesskontinuität	Sicherheit, dass Änderungen die Produktion nicht beeinträchtigen
IT Security	Threat Model und Durchsetzung von Policies	Kontinuierlicher Nachweis, dass Policy und Realität übereinstimmen
Compliance / Risk	Audit Trail und regulatorische Readiness	Nachweisbare, zeitgestempelte Belege für die Wirksamkeit der Controls

06

ABSCHNITT 06

Wer entscheidet? OT Incident Response in der Praxis



The containment decision

Jeder OT-Security-Vorfall führt irgendwann zu einer kritischen operativen Entscheidung: Wie lässt sich der Vorfall eindämmen, ohne ein noch grösseres Betriebsrisiko zu schaffen? Anders als in der IT-Umgebung ist es oft nicht möglich, ein betroffenes System einfach zu isolieren. Abhängigkeiten in der Produktion, Sicherheitsanforderungen und Verbindungen innerhalb der Supply Chain können verlangen, dass Systeme auch während einer Untersuchung verfügbar bleiben. Die richtige Massnahme hängt vom Prozess, vom operativen Kontext und von den geschäftlichen Folgen ab. Dieses Wissen liegt bei Operations, nicht beim SOC.

In der OT ist die Containment-Entscheidung nicht allein eine Sicherheitsentscheidung. Sie ist eine Betriebs- und Sicherheits-entscheidung, die die IT-Security nicht im Alleingang treffen kann

Das hybride Playbook

Eine effektive OT Incident Response ist immer eine gemeinsame Aufgabe. OT-Teams verstehen den physischen Prozess, seine Abhängigkeiten und sichere Betriebszustände. IT Security Teams kennen Forensik, Angriffsverhalten und Containment-Techniken. Keine Seite kann alleine angemessen reagieren. Organisationen, die OT-Vorfälle wirksam bewältigen können, haben deshalb im Voraus und schriftlich festgelegt, wie beide Seiten zusammenarbeiten: Wer wird konsultiert, wer entscheidet und unter welchen Bedingungen hat die Produktionskontinuität Vorrang vor dem Containment oder umgekehrt?

In vielen Organisationen ist diese Zusammenarbeit schwierig. Ein zentrales oder externes SOC empfängt Alerts, verfügt aber nicht über den OT-Kontext, um die operativen Auswirkungen einzuschätzen. Gleichzeitig kennen OT Engineers die betroffenen Systeme, arbeiten jedoch selten mit den Prozessen und forensischen Tools des SOC. Diese Trennung verlangsamt Untersuchungen, erschwert Entscheidungen und schafft gerade dann Unsicherheit, wenn schnelles und koordiniertes Handeln entscheidend ist.

Ein gemeinsames operatives Lagebild

Wirksame Zusammenarbeit braucht eine gemeinsame, verlässliche Datengrundlage. Sind relevante Informationen auf mehrere Plattformen verteilt, beginnt jede Untersuchung damit, Daten aus verschiedenen Teams und Tools zusammenzutragen, bevor die eigentliche Analyse überhaupt starten kann. Wenn OT Operations, Security Teams und externe SOC Provider mit demselben operativen Kontext arbeiten, verkürzen sich Untersuchungen und Entscheidungen werden fundierter. Gleichzeitig basiert regulatorisches Reporting auf konsistenten Informationen statt auf einer manuellen Rekonstruktion.

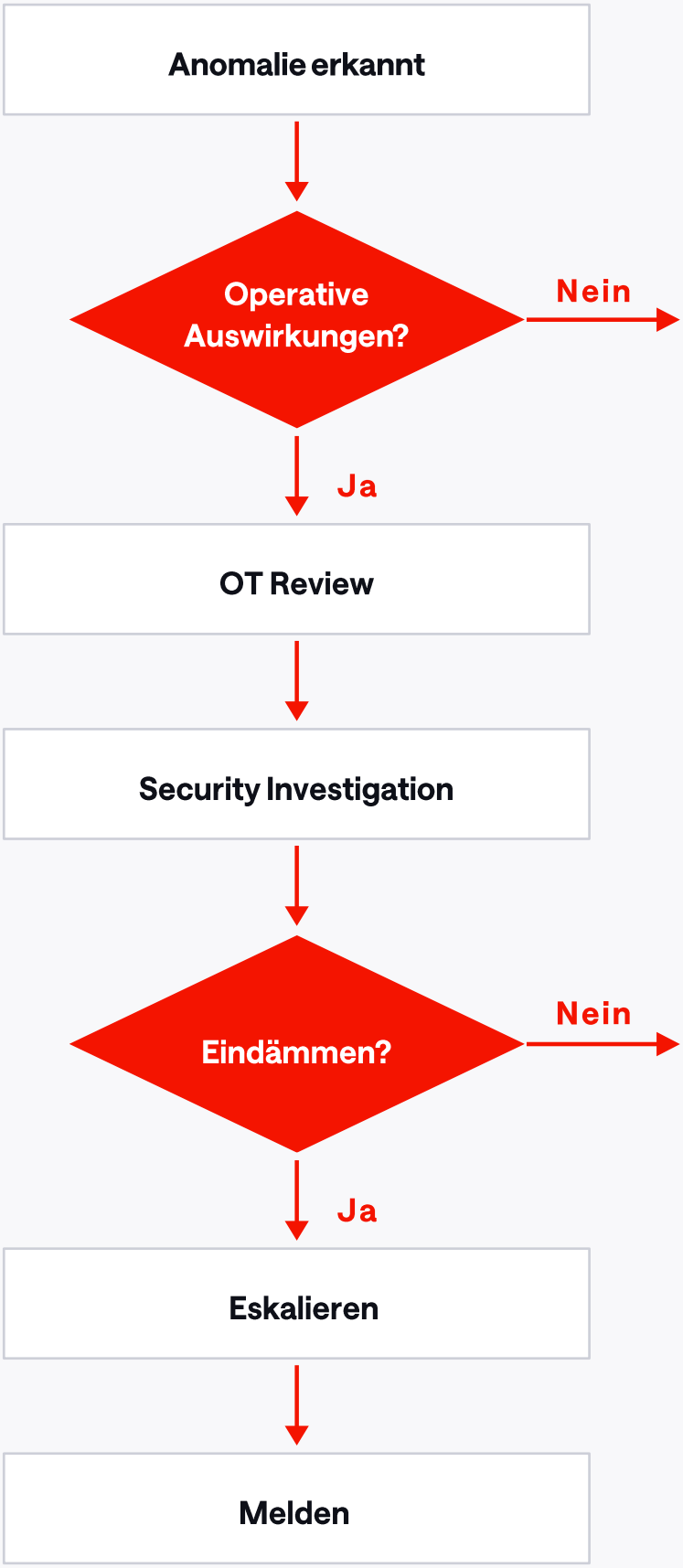
Ein klarer Eskalationsweg

Neben einem Playbook braucht Incident Response eine eindeutige Eskalationskette. So werden zum richtigen Zeitpunkt die richtigen Personen einbezogen und regulatorische Fristen eingehalten:

1. Operations erkennt eine Anomalie oder erhält einen Alert und bewertet die unmittelbaren Auswirkungen auf Betrieb und Sicherheit.
2. Security untersucht und klassifiziert die Bedrohung und beurteilt mögliche Containment-Massnahmen.
3. OT und Security bewerten gemeinsam die operativen Folgen, bevor ein System isoliert oder eine andere Massnahme umgesetzt wird.
4. Das Management entscheidet bei wesentlichen Folgen für Betrieb, Sicherheit oder Geschäft.
5. Sicherheitsbehörden werden innerhalb der durch NIS2, KRITIS oder branchen-spezifische Vorgaben definierten Fristen informiert. Dafür müssen die vorherigen Schritte entsprechende Nachweise liefern.

Ohne Einsehbarkeit funktioniert auch dieser Prozess nicht. Eine Eskalationskette ist nur so wirksam wie die Informationen, die über sie fliesst. Ein Team, das Assets, Kommunikationsflüsse und Anomalien sieht, kann einen Vorfall schneller einordnen und sicher eskalieren. Ohne diesen gemeinsamen Kontext werden selbst klar definierte Prozesse langsamer, unkoordiniert und schwieriger umsetzbar.

ENTSCHEIDUNGSBAUM

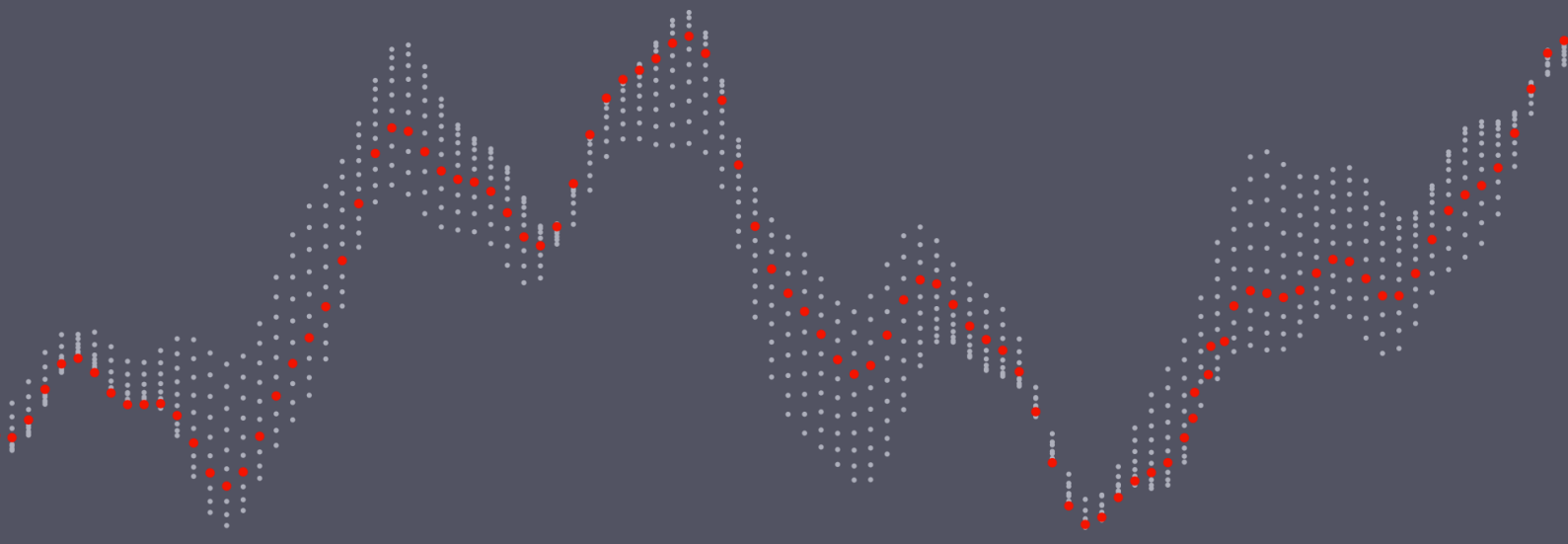


Im OT-Umfeld ist Containment keine reine Security-Entscheidung. Es ist eine operative und sicherheitskritische Entscheidung, die Security-Teamsnicht allein treffen kann.

07

ABSCHNITT 07

Von Compliance zu echter Resilienz



Eine Resilienz-orientierte Reihenfolge

Das zentrale Anliegen dieses Whitepapers ist eine Neuordnung der Prioritäten. OT Security wurde lange als Implementierungsproblem verstanden: Welche Sensoren, Firewalls und Agents müssen installiert werden? Dieser Ansatz führt zu langen Projekten, hohen Kosten und blockierten Initiativen, während die ursprünglichen Blind Spots bestehen bleiben. Ein Resilience-First-Ansatz kehrt die Reihenfolge um:

Zuerst Sichtbarkeit schaffen. Innerhalb weniger Wochen entsteht eine breite, passive Sicht auf Assets und Kommunikationsflüsse – ohne die Produktion zu beeinträchtigen.

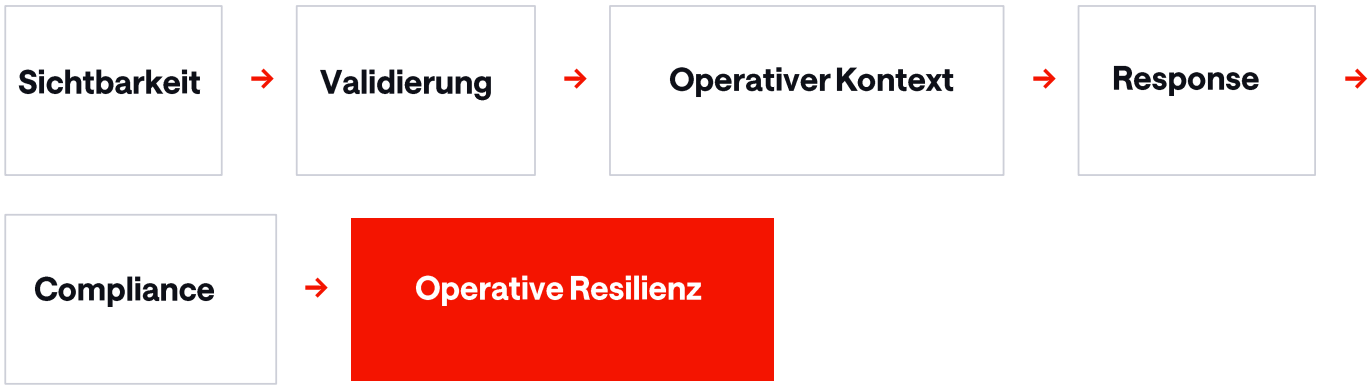
Kontinuierliches Validieren. Die tatsächlich stattfindende Kommunikation wird kontinuierlich mit den geltenden Policies verglichen. So wird die Netzwerksegmentierung überprüft, anstatt lediglich vorausgesetzt zu werden.

Die Reaktion vorbereiten. Bereits vor einem Vorfall werden funktionsüber-greifende Playbooks, klare Eskalationswege und ein gemeinsames operatives Lagebild definiert. Dadurch handeln OT-Teams, SOCs und externe Provider auf derselben Informationsbasis, statt unter Zeitdruck improvisieren zu müssen.

Gezielte Investitionen. Umfassendere Sicherheitskontrollen wie Firewalls, ZTNA oder Agents dort einsetzen, wo die gewonnene Sichtbarkeit die grösste Risikoreduktion bewirkt.

Diese Reihenfolge ersetzt umfassende Controls nicht, sondern schafft die Grundlage für ihren gezielten Einsatz. Gleichzeitig können Organisationen Mehrwert aus bestehenden Tools ziehen. OT-Security-Plattformen, Firewalls und Infrastruktur-Telemetrie liefern nützliche Signale. Resilienz entsteht jedoch erst, wenn diese Signale in einem gemeinsamen operativen Bild verbunden werden, das Teams untersuchen, validieren und langfristig speichern können.

Compliance-Nachweise entstehen dadurch als Ergebnis wirksamer Security, nicht als separate Checkbox-Aufgabe. Gleichzeitig wird etwas möglich, das Regulatoren, Boards und Betreiber zunehmend verlangen: nachweisbare Resilienz, beginnend heute.



Resilienz ist kein weiteres Security-Produkt. Sie entsteht, wenn Sichtbarkeit, Validierung und Operations miteinander verbunden werden.

Wo Exeon ansetzt

Organisationen müssen ihre bestehenden OT-Security-Investitionen nicht ersetzen, um ihre Resilienz zu verbessern. Spezialisierte OT-Security-Plattformen bleiben wichtig, etwa für die Erkennung industrieller Assets, Protokollanalysen und OT-spezifische Threat Detection. Die Herausforderung besteht darin, die Informationen dieser Tools operativ nutzbar zu machen.

Die Herausforderung besteht darin, die Informationen dieser Tools operativ nutzbar zu machen.

Exeon ergänzt bestehende OT-Security-Lösungen, indem Metadaten, Firewall Logs, OT-Security-Alerts und Infrastruktur-Telemetrie in einem gemeinsamen operativen Bild konsolidiert werden. OT Teams, Security Operations und Compliance-Verantwortliche können Vorfälle dadurch mit mehr Kontext untersuchen, Segmentierung kontinuierlich validieren, historische Nachweise aufbewahren und operative Resilienz belegen.

Statt eine weitere isolierte Security-Plattform einzuführen, bündelt Exeon vorhandene Informationen. Dies ermöglicht eine Integration der OT in den bestehenden Security Betrieb und erhöht den Wert bestehender OT-Security-Investitionen.

Das Ergebnis ist ein pragmatischer und herstellerunabhängiger Ansatz zur Operationalisierung von OT Security. Er verbessert Sichtbarkeit, Zusammenarbeit und Resilienz und berücksichtigt gleichzeitig die operativen Realitäten industrieller Umgebungen.

CHECKLISTE

Können Sie OT-Resilienz nachweisen?

- Kennen Sie alle kommunizierenden OT-Assets?
- Können Sie nicht verwaltete und Legacy-Geräte identifizieren?
- Können Sie die Segmentierung kontinuierlich validieren?
- Können Sie die Segmentierung kontinuierlich validieren?
- Sind OT-Security-Informationen zentral konsolidiert?
- Können Sie einen Vorfall auch sechs Monate später rekonstruieren?
- Können Sie erforderliche Nachweise für Audits nach NIS2 oder IEC 62443 bereitstellen?
- Arbeiten OT und IT mit demselben operativen Lagebild?
- Können externe SOC Provider OT-Alerts im richtigen Kontext verstehen?
- Können Sie die Sichtbarkeit verbessern, ohne die Produktion zu beeinträchtigen?

exeon

exeon.com