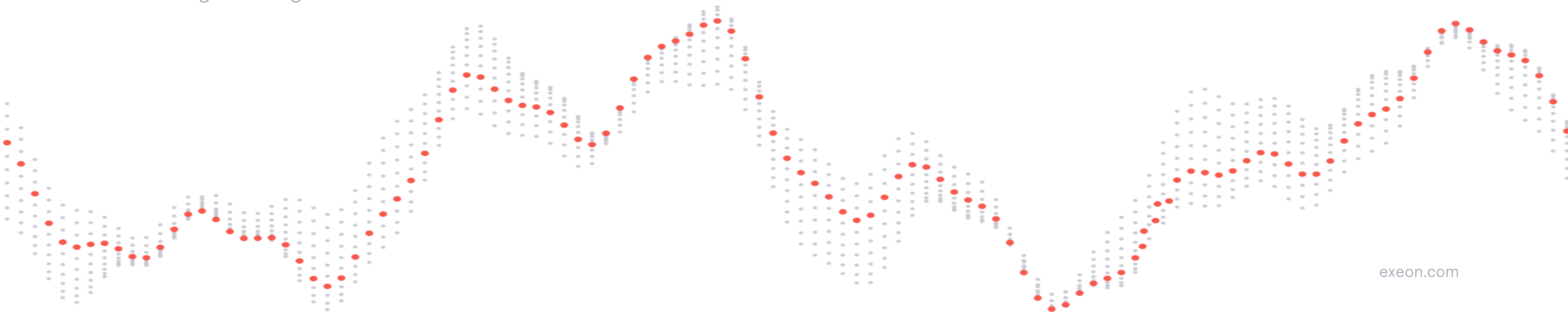
exeon

LEITFADEN ZUR EVALUATION VON OT SECURITY

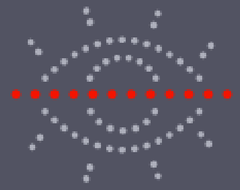
Mehr OT-Sicherheit ohne zusätzlichen Betriebsaufwand

Wenn Organisationen OT-Sicherheits-Ziele verfolgen, wie etwa Ihren Überblick über kommunizierende Assets zu verbessern, Ihre Netzwerksegmentierung zu validieren oder Ihre bestehenden OT-Sicherheitsinvestitionen besser nutzen möchten, kommen viele Aspekte ins Spiel.

Dieser Leitfaden dient Verantwortlichen für OT-Sicherheit bzw. Security Operations oder operativer Resilienz, die die Positionierung ihrer Organisation evaluieren möchten.



DIE FEHLENDE EBENE IN VIELEN OT-SECURITY-ARCHITEKTUREN



Die Evaluation Ihrer OT-Security beginnt in Industrieunternehmen selten bei Null. Firewalls, Switches, Remote-Access-Controls und Monitoring-Technologien sind oft bereits vorhanden. Manche Organisationen nutzen spezialisierte OT-Intrusion-Detection-Technologien oder Deep Packet Inspection (DPI), viele leiten ausgewählte Events zudem an ein zentrales SIEM oder externes SOC weiter.

Trotzdem bleiben grundlegende Fragen überraschend schwierig zu beantworten. Welche Geräte kommunizieren tatsächlich? Welche Verbindungen führen über Netzwerkzonen hinaus? Wurde aus einem temporären Wartungszugriff unbemerkt eine permanente Verbindung? Und kann ein SOC Analyst einen OT-Alert verstehen, ohne dass ein Engineer den gesamten Kontext manuell rekonstruieren muss?

Das bedeutet nicht zwingend, dass bestehende Tools versagt haben. Häufig sieht jedes Tool einen relevanten Ausschnitt, jedoch bleibt das operative Gesamtbild fragmentiert. Dies erschwert es Analysten erheblich, den Überblick über alle Technologien, Standorte und Teams zu behalten. Ein gezielter Ausbau der OT-Sicherheitssysteme greift hier ein: Vorhandene Tools werden um eine weitere Ebene ergänzt, die bestehende Telemetriedaten verbinden kann. Diese Ebene sollte die Arbeit des SOC mit zusätzlichen Analysekapazitäten unterstützen und einen Überblick über das Netzwerk und tiefere Einblicke in das Kommunikationsverhalten einzelner Endpoints geben. Damit können bereits installierte Sensoren für Security Operations besser nutzbar gemacht werden.

Der beste Ansatz

Identifizieren Sie zuerst die Lücken in Ihrer bestehenden Architektur und vergleichen Sie erst danach Produktfunktionen. Entscheidend ist nicht nur, welche Lösung am meisten sieht, sondern welcher Ansatz die fehlende Sichtbarkeit und den notwendigen Kontext mit vertretbaren Kosten, angemessener Komplexität und geringem operativem Risiko ergänzt.

Bevor Sie Produktfeaturelisten vergleichen, machen Sie sich zunächst ein Bild von den tatsächlichen Bedürfnissen Ihrer Sicherheitsarchitektur. Eine sinnvolle Ergänzung Ihrer Sicherheitsarchitektur zeichnet sich dadurch aus, dass sie gezielt die identifizierten Sicherheitslücken schliesst und notwendige Klarheit schafft. Von diesem Ansatz aus können Sie gezielt eine Lösung suchen, die weder Kosten- noch Komplexitätsrahmen sprengt, und sich risikoarm in Ihren bestehenden operativen Kontext einpasst.

EINE PRAXISNAHE EVALUATIONSABFOLGE

Die Evaluation einer Lösung sollte sich an der Art und Weise wie OT-Sicherheitsinfrastruktur ihre Wirkung in der Praxis entfaltet orientieren. Zunächst muss eine Organisation sich ein Bild über ihre Assets und Kommunikationspfade machen. Basierend auf dieser Übersicht können Organisationen dann ihre bestehenden Zonenkontrollen validieren. Die gesammelten Informationen dienen dann in Vorfalluntersuchungen oder Workflows als Grundlage, auf der Organisationen ihre Response aufbauen können. Eine passende Lösung unterstützt Organisationen belastbare Informationen über ihr Netzwerk für die gemeinsame Entscheidungsfindung zu gewinnen.

SEE

Assets, Flows und Abhängigkeiten

→

VALIDATE

Zonen, Policies und Abweichungen

→

OPERATIONALIZE

Kontext, Korrelation und Workflows

→

RESPOND

gemeinsame Entscheidungen und Nachweise

1. ZUERST DIE LÜCKE DEFINIEREN

Eine OT-Umgebung kann über ausgereifte Controls verfügen und trotzdem keinen verlässlichen Gesamtüberblick bieten. Asset Inventories können veralten, im Netzwerkdiagramm sind nur geplante Verbindungen hinterlegt, es zeigt nicht tatsächlich kommunizierende Verbindungen. Informationen verschiedener Anbieter lassen sich nur schwer zusammenführen. Verteilte Produktionsstandorte, Umspannwerke und isolierte Segmente verschärfen das Problem, weil dieselbe Sensorarchitektur nicht überall wirtschaftlich oder ohne Betriebsrisiko ausgerollt werden kann.

Dokumentieren Sie zunächst, was die bestehende Architektur nicht oder nicht zuverlässig zeigen und unterstützen kann. So konzentriert sich die Evaluation auf einen konkreten operativen Bedarf und Sie führen kein neues Tool mit unnötigen Überlappungen ein.

Fragen zur Abgrenzung des Scopes

Welche Standorte, Segmente, Assets oder Remote-Verbindungen sind unzureichend sichtbar?

Können die Teams notwendige Kommunikation von unerwarteten oder veralteten Pfaden unterscheiden?

Funktioniert Ihre Segmentierung auch ausserhalb eines Audits?

Wie viel manuelle Zusammenarbeit erfordert die Untersuchung eines OT-Events?

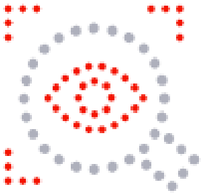
Welche Umgebungen unterstützen keine Agents, Active Scans, zusätzliche Sensoren oder Cloud-Processing?

Welche Daten aus der Netzwerkinfrastruktur und bestehenden OT-Security-Tools sind bereits verfügbar?

EVALUATIONSFRAGE

Kann die vorgeschlagene Lösung die definierte Lücke schliessen und gleichzeitig bestehende Investitionen und funktionierende Prozesse erhalten?

2. SEE: VISIBILITY OHNE PRODUKTIONSRISIKO



Visibility bildet die Basis der Evaluation, doch der Weg dorthin ist ebenso wichtig wie das Ergebnis. In Produktionsumgebungen hat jede neue Appliance, jede Netzwerkänderung und jedes Wartungsfenster operative Folgen. Ein Design kann eine umfassende Abdeckung versprechen und trotzdem kurzfristig kaum Mehrwert liefern, wenn Beschaffung und Implementierung Monate dauern.

Ein passiver, metadaten-basierter Ansatz bietet einen anderen Ausgangspunkt. Network Flows, Firewall Logs, Switch-Telemetrie und Daten aus bestehender Security-Infrastruktur zeigen dynamisch, welche Assets kommunizieren, wie Systeme voneinander abhängen und wo Traffic Zonengrenzen überschreitet. Da die Analyse auf bereits vorhandenen Daten basiert, lässt sich häufig eine nützliche Abdeckung erreichen, bevor zusätzliche Hardware an jedem Standort eingeführt wird.

Die Datenstrategie evaluieren, nicht nur das Dashboard

Anbieter sollten transparent zeigen, aus welchen Quellen sie Daten ziehen, welchen Beitrag jede Quelle leistet und welche Blind Spots bestehen bleiben. Eine brauchbare Visibility entsteht, wenn kommunizierende Assets, Protokolle, Verbindungen, Datenvolumen, externe Kommunikation und Veränderungen über Zeit abgedeckt sind. Ebenso wichtig sind nicht verwaltete und Legacy-Geräte, die in Endpoint-basierten Inventaren fehlen.

Metadatenanalyse und Deep Packet Inspection beantworten unterschiedliche Fragen. Flow- und Logdaten schaffen breite und skalierbare Sichtbarkeit über Kommunikationsverhalten, auch wenn eine Payload-Analyse nicht verfügbar oder nicht erwünscht ist. DPI ergänzt Details auf Protokollebene, die in ausgewählten kritischen Segmenten erforderlich sein kann. Eine sinnvolle Sicherheitsarchitektur kombiniert beide Ansätze gezielt: Sie nutzt bestehende DPI-Investitionen und ergänzt verhaltensbasierte Inspektion dort, wo der Use Case sie rechtfertigt, statt einen Ansatz als universell ausreichend zu behandeln.

Worauf Sie achten sollten

- Passive Datenerfassung ohne Agents, Active Scanning oder Traffic Injection in Produktionsnetzwerke
- Unterstützung bestehender NetFlow-, Firewall-, Switch-, Network-Log-, DPI- und OT-Telemetrie
- Erkennung kommunizierender Assets und Abhängigkeiten in verteilten und segmentierten Umgebungen
- Transparenz über Grenzen des Ansatzes, einschliesslich einer Auflistung in welchen Bereichen gezielte DPI oder eine weitere Datenquelle erforderlich bleibt
- Ein schneller Weg zu erster nützlicher Visibility, ohne einen vollständigen Rollout in der gesamten Umgebung vorauszusetzen

EVALUATIONSFRAGE

Wie viel der benötigten Sichtbarkeit lässt sich aus vorhandener Telemetrie gewinnen und was muss ergänzt werden, um die verbleibenden Lücken zu schliessen?

3. VALIDATE: SEGMENTIERUNG IN DER PRAXIS PRÜFEN

Segmentierung ist ein zentraler Bestandteil jeder OT-Sicherheitsarchitektur, vom Purdue-Modell bis hin zu Zonen und Conduits. Eine Firewall-Regel beschreibt jedoch nur, was erlaubt sein soll, während ein Netzwerkdiagramm den vorgesehenen Zustand zeigt. Keines von beiden beweist, dass die aktuelle Kommunikation dem Design entspricht.

Reale Umgebungen verändern sich. Eine Ausnahme für Remote Maintenance bleibt nach Abschluss der Arbeiten aktiv. Unter Produktionsdruck wird eine Verbindung eingerichtet und nie dokumentiert. Ein neues System kommuniziert über eine Grenze hinweg, die niemand erwartet hat. Mit der Zeit gehen Policy und tatsächliche Aktivität auseinander. Jährliche oder projektbezogene Kontrollen erfassen nur einen Zeitpunkt, nicht die Abweichungen zwischen zwei Reviews.

Kontinuierliche Validierung macht diese Lücke anhand der beobachteten Netzwerkaktivität sichtbar. Teams erkennen unerwartete Kommunikation zwischen Zonen, neue Protokolle, nicht dokumentierte Pfade und Veränderungen, die überprüft werden müssen. Damit wird Segmentierung von einer statischen Designübung zu einer Kontrollmetrik, an der sich die operative Realität kontinuierlich messen lässt.

Validierung unterstützt auch Governance

OT Operations, IT Security und Compliance beurteilen Netzwerkänderungen aus unterschiedlichen Perspektiven. Operations schützt Verfügbarkeit und Prozesssicherheit, Security betrachtet Policies und mögliche Angriffspfade, Compliance benötigt Nachweise dafür, dass Controls überwacht und überprüft werden. Eine gemeinsame temporale Ansicht der Kommunikation liefert die Sachgrundlage, um zu entscheiden, ob eine Änderung erwartet, autorisiert und akzeptabel war.

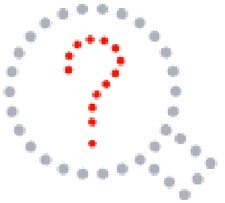
Worauf Sie achten sollten

- Visibility auf die tatsächliche Kommunikation zwischen definierten Zonen und Conduits
- Vergleich der beobachteten Aktivität mit vorgesehenen Policies oder genehmigten Kommunikationsmustern
- Erkennung neuer Pfade, verbotener Protokolle und zunehmender Abweichungen in der Segmentierung
- Genügend Historie und Kontext, um zu erkennen, wann eine Änderung erstmals auftrat und wie sie sich entwickelte
- Findings, die OT Operations und Security gemeinsam beurteilen können

EVALUATIONSFRAGE

Zeigt die Lösung kontinuierlich, wo sich die dokumentierte Segmentierung vom tatsächlichen Netzwerkverhalten unterscheidet, oder nur während eines Audits?

4. OPERATIONALIZE: OT-KONTEXT MIT SECURITY OPERATIONS VERBINDEN



Mehr Daten allein machen Sichtbarkeit noch nicht operativ nutzbar. OT-Security-Informationen verteilen sich häufig auf IDS- oder DPI-Tools, Firewalls, Netzwerkinfrastruktur, Remote-Access-Systeme und IT-Security-Plattformen. Bei einer Untersuchung müssen Teams deshalb oft einzelne Informationen von mehreren Verantwortlichen zusammentragen, bevor eine Timeline entsteht.

Eine ergänzende Analyseebene sollte diese Signale normalisieren und korrelieren. Dabei bleibt der Wert spezialisierter OT-Tools erhalten und wird um den Netzwerk- und Verhaltenskontext erweitert, der für Untersuchungen erforderlich ist. Ein IDS-Alert wird beispielsweise deutlich aussagekräftiger, wenn der Analyst gleichzeitig das betroffene Asset, dessen letzte Kommunikationspartner, eine neue Verbindung, die überschrittene Zonengrenze und die Veränderungen vor dem Alert sieht.

OT-Expertise bleibt weiterhin notwendig. Der Ansatz reduziert jedoch die Zeit für das Sammeln grundlegender Fakten und hilft dem SOC, bessere Fragen zu stellen. Ziel ist ein gemeinsames operatives Lagebild: Security Analysts verstehen die Aktivität, während OT Engineers die Folgen für Produktion und Sicherheit beurteilen können.

Detection Quality muss erklärbar sein

Verhaltensanalyse kann Abweichungen erkennen, die Signaturen und bekannte Indicators nicht erfassen. Ein nicht erklärbarer Score schafft in einer operativen Umgebung jedoch wenig Vertrauen. Analysts müssen nachvollziehen können, warum eine Detection ausgelöst wurde, welche Aktivitäten dazu beigetragen haben und wie sich das Verhalten von der etablierten Baseline unterscheidet. Eine klare Begründung verbessert die Triage und gibt OT-Spezialisten konkrete Informationen, die sie bestätigen oder hinterfragen können.

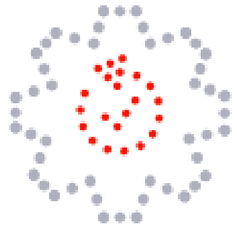
Worauf Sie achten sollten

- Herstellerunabhängige Einspeisung, Normalisierung und Anreicherung bestehender Telemetrie
- Korrelation des Netzwerkverhaltens mit Alerts spezialisierter OT-Security-Tools
- Verhaltens-Baselines, die neue oder ungewöhnliche Kommunikationsmuster erkennen
- Erklärbare Detections mit sichtbaren Assets, Aktivitäten und Timelines
- Integration in bestehende SIEM-, SOC-, MSSP- und Incident-Management-Workflows

EVALUATIONSFRAGE

Kann ein Analyst von einem OT-Alert zu einer belastbaren Darstellung der umgebenden Aktivität gelangen, ohne Daten aus mehreren Systemen manuell zusammenzuführen?

5. RESPOND: GEMEINSAME ENTSCHEIDUNGEN UNTERSTÜTZEN



Die Reaktion auf einen OT-Vorfall unterscheidet sich vom klassischen IT Containment. Die Isolation eines Geräts kann einen Produktionsprozess unterbrechen, die Sicherheit beeinträchtigen oder grössere geschäftliche Folgen verursachen als der vermutete Vorfall. Containment ist deshalb keine reine Security-Entscheidung, sondern erfordert operatives Wissen und klare Zuständigkeiten.

Technologie sollte diese Zusammenarbeit unterstützen, nicht vollständig wegautomatisieren. Eine geeignete Lösung stellt SOC und OT Operations dieselben Fakten zur Verfügung, dokumentiert die relevante Aktivitätssequenz und fügt sich in den vereinbarten Eskalationsprozess ein. Das OT Team kann Prozessabhängigkeiten und sichere Betriebszustände beurteilen, während Security die Bedrohung untersucht und mögliche Containment-Massnahmen vorschlägt.

Dieselben Informationen können die interne Dokumentation, Incident Reviews und regulatorische Reporting-Prozesse unterstützen. Sie liefern möglicherweise Nachweise über überwachte Kommunikation, erkannte Veränderungen und Investigation Timelines. Sie erstellen jedoch weder automatisch einen compliance-fähigen Audit Report noch stellen sie die Compliance einer Organisation sicher. Governance Teams bleiben dafür verantwortlich, die Nachweise zu interpretieren, den Anforderungen zuzuordnen und die notwendigen Meldungen zu erstellen.

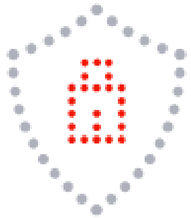
Worauf Sie achten sollten

- Konsistente Timeline und gemeinsamer Kontext für OT, Security und externe Service Provider
- Rollengerechter Zugriff auf die Informationen, die für Beurteilung und Eskalation erforderlich sind
- Integration in etablierte Incident- und Case-Management-Prozesse
- Historische Informationen für Reviews, Beweissicherung und Reporting Workflows
- Klare Grenzen zwischen Detection Support, operativen Entscheidungen und Compliance-Verantwortung

EVALUATIONSFRAGE

Stärkt die Lösung unseren Response-Prozess und belässt operative sowie sicherheitsrelevante Entscheidungen bei den dafür verantwortlichen Personen?

6. DEPLOYMENT, SOUVERÄNITÄT UND SKALIERUNG TESTEN



OT-Architekturen sind selten einheitlich. Ein zentraler Produktionsstandort verfügt möglicherweise über umfangreiche Telemetrie, während entfernte Standorte mit begrenzter Bandbreite, älterer Infrastruktur oder strikter Isolation arbeiten. Die Evaluation muss das Deployment-Modell deshalb an den schwierigsten Teilen der Umgebung prüfen, nicht nur am einfachsten Pilotstandort.

Verteilte Collectors oder Gateways können Daten nahe an der Quelle parsen, normalisieren und zwischenspeichern. Nur die für die zentrale Analyse benötigten Informationen werden weitergeleitet. Das reduziert die Bandbreite und vereinfacht die Anbindung entfernter Umgebungen. Bei Anforderungen an Souveränität oder Isolation sollten On-Premises-, Self-Hosted- und Air-Gapped-Optionen geprüft werden, ebenso Updates, Support und Datenverwahrung in jedem Modell.

Ein schrittweises Deployment ist meist sinnvoller als ein Big-Bang-Programm. Der Start in einem kritischen oder unzureichend verstandenen Segment ermöglicht es, Datenqualität zu prüfen, Kommunikationsabhängigkeiten zu erkennen und Erfolgskriterien zu verfeinern. Gleichzeitig sollte das Pilotprojekt zeigen, dass Sicherheitsarchitektur und Betriebsmodell über mehrere Standorte skalieren können, ohne Infrastruktur und Wartungsaufwand zu vervielfachen.

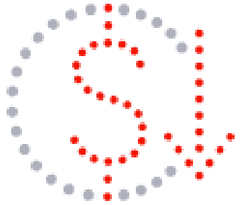
Worauf Sie achten sollten

- On-Premises-, Self-Hosted- und Air-Gapped-Deployment, wo erforderlich
- Verteilte Datenerfassung mit lokalem Parsing, Normalisierung und Buffering
- Kontrolle darüber, welche Daten an jedem Standort weitergeleitet, verarbeitet und gespeichert werden
- Schrittweiser Rollout mit minimalen Netzwerkänderungen und geringem Produktionsrisiko
- Transparente Anforderungen an Sensoren, Collectors, Bandbreite, Compute, Storage und Administration

EVALUATIONSFRAGE

Bleibt das Design sicher, verwaltbar und wirtschaftlich, wenn es vom Pilot auf verteilte und isolierte Umgebungen ausgeweitet wird?

7. OPERATIVEN MEHRWERT STATT NUR LIZENZKOSTEN VERGLEICHEN



Die tatsächlichen Kosten eines OT-Security-Ansatzes gehen über die Software hinaus. Zusätzliche Sensoren, Appliances, Storage, Integrationen, Standortbesuche, Wartungsfenster und Spezialisten können die Kosten über drei Jahre dominieren. Auch Verzögerungen sind relevant: Ein ambitioniertes Design reduziert keine Risiken, solange es in der Planung bleibt.

Ein fairer Vergleich berücksichtigt, wie viel vorhandene Telemetrie und Infrastruktur wiederverwendet werden kann, wie schnell das erste Segment nützliche Informationen liefert und welchen Aufwand die Erweiterung verursacht. Ebenso wichtig ist, ob die Lösung den Wert bereits gekaufter Tools erhöht, indem sie deren Output mit breiterem Netzwerkkontext und etablierten Workflows verbindet.

Aussagen über eine schnelle Abdeckung oder Kostensenkung brauchen eine klare Grundlage. Fragen Sie, was als sichtbares Asset oder Segment zählt, welche Datenquellen vorausgesetzt werden und welche Teile des Rollouts nicht in der Schätzung enthalten sind. Ein limitiertes, messbares Pilotprojekt liefert bessere Nachweise als ein generischer Benchmark.

Was während der Evaluation gemessen werden sollte

- Zeit vom Datenzugriff bis zu einer nutzbaren Sicht auf Assets und Kommunikation
- Anzahl bisher unbekannter Assets, Pfade oder Ausnahmen in der Segmentierung
- Aufwand für die Untersuchung eines ausgewählten OT-Alerts oder einer Anomalie
- Zusätzliche Infrastruktur, Wartung und Spezialkenntnisse für Pilotprojekt und Rollout
- Gesamtkosten über drei Jahre, einschliesslich Datenerfassung, Compute, Storage, Integration und Betrieb

EVALUATIONSFRAGE

Liefert der Ansatz früh genug messbaren operativen Mehrwert, um nachfolgende Investitionen fundiert zu steuern?

EINE EVALUATION, DIE DIE REALE UMGEBUNG ABBILDET

Ein sinnvoller Proof of Concept (PoC) testet eine Architektur und ein Betriebsmodell, nicht nur eine vorbereitete Demo. Der Scope sollte begrenzt genug sein, um den PoC abzuschliessen, aber repräsentativ genug, um reale Einschränkungen sichtbar zu machen.

01 Wählen Sie ein oder zwei kritische Segmente mit bekannten Herausforderungen bei Sichtbarkeit, Segmentierung oder Untersuchungen.

02 Erfassen Sie die vorhandene Telemetrie, Sensoren und Security-Plattformen in diesem Scope.

03 Definieren Sie Erfolgskriterien für Asset Visibility, Communication Mapping, die Validierung der Segmentierung und Investigation Workflows.

04 Dokumentieren Sie vor der Datenanbindung alle Einschränkungen bezüglich Deployment, Souveränität, Bandbreite und operativer Änderungen.

05 Vergleichen Sie die beobachteten Assets und Verbindungen mit Inventaren, Netzwerkdiagrammen und vorgesehenen Policies.

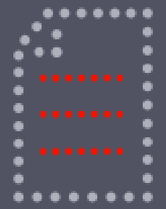
06 Testen Sie eine Ausnahme in der Segmentierung und eine End-to-End-Untersuchung gemeinsam mit OT- und Security-Verantwortlichen.

07 Messen Sie Infrastrukturbedarf, operativen Aufwand und Time to Value. Modellieren Sie anschliessend die Erweiterung auf weitere Standorte.

Ein gutes Ergebnis ist eine bessere Investitionsentscheidung

Die Evaluation sollte zeigen, wo breite Sichtbarkeit aus Metadaten ausreicht, wo gezielte DPI oder ein anderer Control notwendig bleibt und wie sich die kombinierte Architektur ohne eine neue Ebene operativer Belastung erweitern lässt.

KOMPAKTE CHECKLISTE ZUR EVALUATION VON OT SECURITY



Nutzen Sie diese Checkliste für den Vergleich ergänzender Ansätze in Anbietergesprächen sowie während eines Proof of Concept. Dokumentieren Sie, ob ein Kriterium vollständig, teilweise oder nicht unterstützt wird oder in Ihrer Umgebung noch validiert werden muss.

Architektur und Sichtbarkeit	
Ergänzt bestehende OT-IDS-, DPI-, Firewall- und SIEM-Investitionen, statt deren Ablösung vorauszusetzen.	☐
Nutzt vorhandene Flow-, Log-, Netzwerk- und OT-Telemetrie über herstellerunabhängige Integrationen.	☐
Arbeitet passiv, ohne Agents, Active Scanning, Packet Decryption oder Traffic Injection.	☐
Erkennt kommunizierende Assets, Abhängigkeiten, Remote-Pfade und zonenübergreifende Aktivität.	☐
Zeigt transparent, wo Metadaten ausreichen und wo gezielte DPI oder eine weitere Datenquelle benötigt wird.	☐

KOMPAKTE CHECKLISTE ZUR EVALUATION VON OT SECURITY

Segmentierung und Operations	
Vergleicht beobachtete Kommunikation mit vorgesehenen Zonen, Conduits oder genehmigten Mustern.	☐
Erkennt neue Pfade, verbotene Protokolle und Abweichungen in der Segmentierung über die Zeit.	☐
Korreliert Netzwerkverhalten mit Alerts und Kontext bestehender OT-Tools.	☐
Liefert erklärbare Detections und Investigation Timelines, die OT und SOC gemeinsam nutzen können.	☐
Integriert sich in bestehende SIEM-, SOC-, MSSP- und Incident Workflows.	☐

Deployment und langfristiger Mehrwert	
Unterstützt On-Premises-, Self-Hosted- und Air-Gapped-Umgebungen, wo erforderlich.	☐
Ermöglicht verteilte Datenerfassung, lokales Buffering und Kontrolle über weitergeleitete Daten.	☐
Unterstützt einen schrittweisen Rollout ohne umfassende Netzwerkänderungen oder zusätzliche Sensoren an jedem Standort.	☐
Stellt historische Informationen für interne Nachweise und regulatorische Reporting-Prozesse bereit.	☐
Macht Infrastrukturbedarf, Betriebsaufwand und Gesamtkosten über drei Jahre transparent.	☐

FÜNF FRAGEN AN JEDEN ANBIETER

01 Was ergänzt Ihre Lösung in unserer bestehenden Architektur und von welchen Tools oder Controls hängt sie weiterhin ab?

02 Wie viel nützliche Sichtbarkeit erhalten wir aus bereits vorhandener Telemetrie?

03 Können Sie zeigen, wo sich unsere dokumentierte Segmentierung von der tatsächlichen Kommunikation unterscheidet?

04 Kann unser SOC einen OT-Event untersuchen, ohne den Kontext aus mehreren Systemen manuell zu rekonstruieren?

05 Welche Infrastruktur und welcher Betriebsaufwand sind erforderlich, um den Ansatz auf alle relevanten Standorte auszuweiten?

NÄCHSTER SCHRITT: OT ARCHITECTURE ASSESSMENT

Erfassen Sie vorhandene Datenquellen, Sichtbarkeitslücken und Einschränkungen beim Deployment, bevor Sie einen Pilot auswählen.
Das Ergebnis sollte eine praxisnahe Zielarchitektur sein, die bestehende Investitionen dort nutzt, wo sie Mehrwert liefern, und neue Datenerfassung nur dort ergänzt, wo sie nachweislich benötigt wird.

exeon

exeon.com