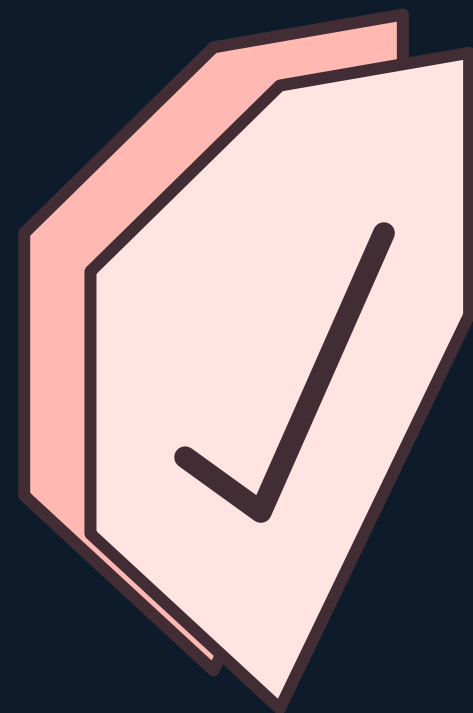




OT - CYBERSECURITY

Was ist initiationOTC?

Operational Technology Cybersecurity: Eine transparente Firewall, die Ihre Produktionsnetze schützt und sichtbar macht, ohne die Anlagen umzubauen.





PROBLEM

Viele Zugänge. Wenig **Kontrolle**.

Offene Kommunikation

Viele Steuerungen sprechen im Klartext. Befehle lassen sich mit wenig Aufwand mitlesen oder verändern.

Zugänge ohne Grenzen

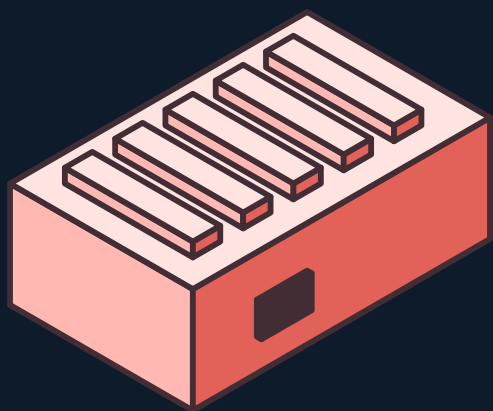
Fernwartung, Notebooks und Netzübergänge sind häufige Einfallstore, oft ohne feine Freigaben.

Schäden zu spät sichtbar

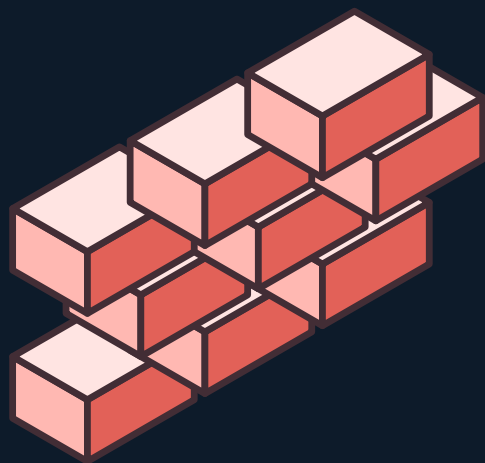
Wer das OT-Netz nicht sieht, merkt Angriffe spät. Die Folgen: Stillstand, Ausschuss, Know-how-Verlust.

IN EINEM SATZ

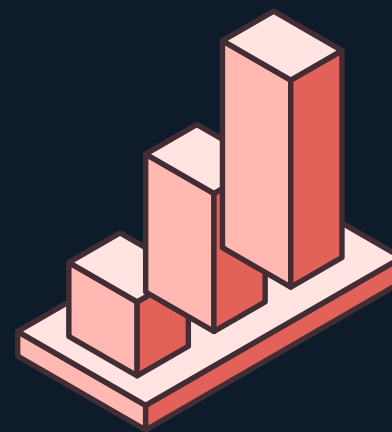
initiationOTC sichert Ihre
Produktionsnetze ab:
transparent, ohne Umbau der
Anlagen und **in einem Produkt**.



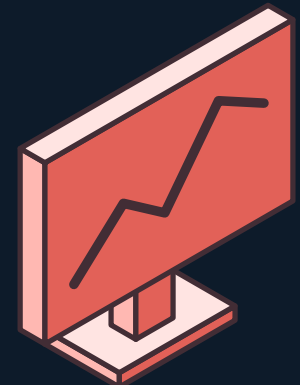
Edge



Security Layer



Analyse



Dashboard



SO FUNKTIONIERT ES

Vier Schritte vom **Risiko** zur Kontrolle.

01 Verbinden

Bindet Maschinen, Steuerungen und Netze an, transparent und ohne Umbau der Anlagen.

02 Absichern

Der Security Layer teilt das Netz in Zonen und lässt nur freigegebene Kommunikation zu (IEC 62443).

03 Schützen und analysieren

Die transparente Firewall prüft den Datenverkehr, erkennt Auffälliges und protokolliert Zugriffe, auch aus der Fernwartung.

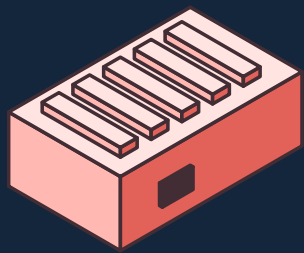
04 Bereitstellen

Liefert Dashboards, Berichte und Alarme für Betrieb, IT und Geschäftsführung.



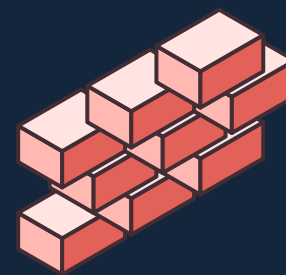
DIE LÖSUNG

Schutz und Sicht, **eine** Lösung.



Anbindung

Verbindet Maschinen, Steuerungen und Anlagen, ohne sie umzubauen.



Security Layer

Transparente Firewall: erlaubt nur Freigegebenes, schottet nicht patchbare Systeme als sichere Inseln ab.



Analyse

Erkennt ungewöhnliche Verbindungen und Befehle und protokolliert die Kommunikation nachvollziehbar.



Bereitstellung

Dashboards, Berichte und Alarme für Betrieb, IT und Geschäftsführung.



GEFRAGT BIS 2027

Vier Anwendungen, die **gefragt** sind.

01

NIS2-Nachweise in der OT

JETZT

Segmentierung, Zugriffskontrolle und Protokolle als Grundlage für Nachweise.

02

Fernwartung absichern

JETZT

Zugriffe von Dienstleistern freigeben, begrenzen und protokollieren.

03

Sicht ins OT-Netz

JETZT

Erkennen, was im Produktionsnetz kommuniziert, und Auffälliges melden.

04

CRA und Maschinenverordnung

2027

Vernetzte Maschinen auf die EU-Vorgaben ab 2027 vorbereiten.



SCHUTZ IN SCHICHTEN

Eine Maßnahme reicht nicht. Mehrere Schichten schon.

Das BSI empfiehlt Defense in Depth: mehrere Schutzschichten, die sich gegenseitig ergänzen. initiationOTC unterstützt diese Empfehlung im OT-Netz mit Segmentierung, kontrollierter Fernwartung und Überwachung.

Erst sehen. Dann schützen.



ALS NÄCHSTES

Lernen Sie initiationOTC **aus der Nähe** kennen.

In den nächsten Beiträgen zeigen wir jeden Schritt an
Beispielen.



Jetzt scannen

und mehr über initiationOTC erfahren.

initiationware.com