Anforderungen an Cyber Security in OT / IoT Umgebungen

1) Visibilität – Sichtbarkeit der gesamten OT- Infrastruktur – Asset Inventory

Kriterien	Nutzen	Kommentar
Erkennung aller Assets /IT-, IoT und OT-basierter Geräte im OT-Netzwerk ohne Auswirkungen auf den Betrieb	➔ Technologie und Prozess Konsolidierung ➔ Gemeinsames Monitoring ➔ Eliminierung von Silos ➔ Verantwortung steigern und Kosten minimieren ➔ **Zusammenführen von IT und OT** ➔ Optimiertes Assetmanagement Tipp: die schnelle Asset-Erkennung und Netzwerk Visualisierung steigern die Effizienz der Security Operation Teams	
Umfassender Support von IT, IoT und OT Protokollen		
Jederzeit aktuelles Asset Inventory mit Kommunikationsbeziehungen und Protokollen		
Identifikation von neuen Geräten (Gerätetyp, Firmwareversion, etc.) – aktiv ab Q4 2023		
Monitoring aller Fernwartezugriffe		
Optional: aktive Abfragemöglichkeit ohne Auswirkungen auf den Betrieb für Netzleit-technik, Fernwirktechnik, Steuerungen, Aktoren und Sensoren		

INDUSTRIAL AUTOMATION

Anforderungen an Cyber Security in OT / IoT Umgebungen

2) Schutz von IoT/OT-Konfigurationen

Kriterien	Nutzen	Kommentar
Identifizierung von Änderungen an speicherprogrammierbaren Steuerungen (SPS) oder Human Machine Interfaces – SPS Programm Code, Firmware, Konfigurationsänderungen	➔ Umfängliches Protokoll der ICS-Aktivitäten	
Monitoring und Anzeige von IoT und OT Prozessvariablen		

Anforderungen an Cyber Security in OT / IoT Umgebungen

3) Schwachstellenanalyse und Risikomanagement

Kriterien	Nutzen	Kommentar
Identifizierung von spezifischen IT, IoT und OT Schwachstellen der Produktionsanlagen	➔ Workflow für die **schnelle Erkennung von Anomalien** für das bestehende Security Operations Team ➔ Erweiterte Einblicke für das Risikomanagement, ohne zusätzliche Ressourcen aufbauen zu müssen ➔ Verhaltensbasierte Anomalie-Erkennung zur einfachen und kontinuierlichen Bedrohungserkennung für eine umfassende Risikoüberwachung	
Erkennung von Anomalien und Manipulation im Netzwerkverkehr		

INDUSTRIAL AUTOMATION

Anforderungen an Cyber Security in OT / IoT Umgebungen

4) Gefährdungserkennung inkl. Alarmierung

Kriterien	Nutzen	Kommentar
Supervised Machine Learning zur Alarmierung bei Veränderungen der Bedrohungslage	➔ Schnelle Erkennung von Cyberangriffen und proaktive Schadensminimierung ➔ Steigert Robustheit gegen Cyberangriffe ➔ Sofortschutz gegen Ransomware ➔ Stärkt operative Leistungsfähigkeit und Zuverlässigkeit ➔ Verbessert Verfügbarkeit des Unternehmens /der Organisation	
Kontinuierliche Identifikation der Ausnutzung möglichen Angriffsvektoren		
Echtzeit-Warnung zu verdächtigen Aktivitäten und Gefährdungen in OT-Netzwerken (Malware, Fehlverhalten, Komplexidität,..)		

INDUSTRIAL AUTOMATION

Anforderungen an Cyber Security in OT / IoT Umgebungen

5) Audit und Compliance

Kriterien	Nutzen	Kommentar
Nicht veränderbare Audit Logs	➔ Einhaltung der nationalen und betrieblichen Anforderungen an die Cybersicherheit ➔ Kriterien zum Nachweis und Messung des kontinuierlichen Verbesserungsprozesses des ISMS	
Unterstützung der Umsetzung von internationalen Standards wie IEC 62443, Critical Security Controls, ISO 27000 Serie		
Monitoring und Überwachung von Zonen und Conduits nach IEC 62443		
Unterstützung bei der Umsetzung der NIS Verordnung		

INDUSTRIAL AUTOMATION

Anforderungen an Cyber Security in OT / IoT Umgebungen

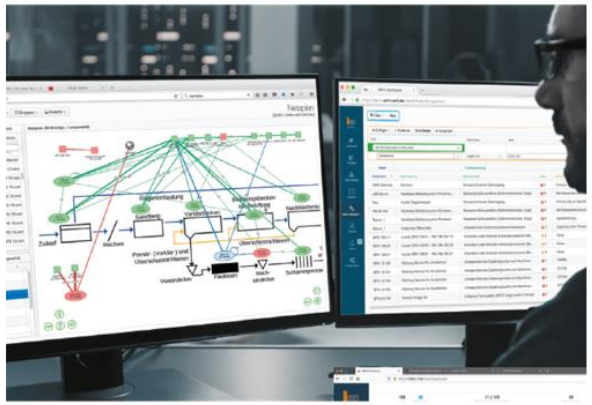
6)

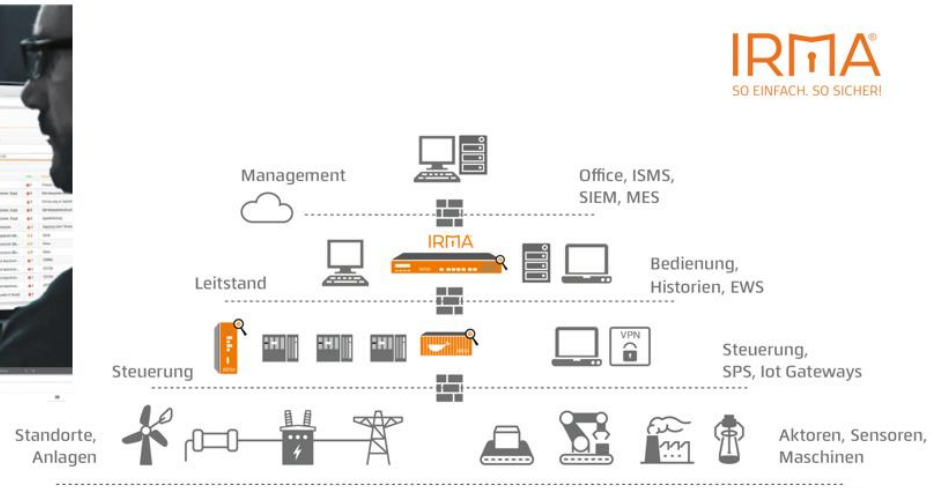
Kriterien	Nutzen	Kommentar
Standardkonforme Analysen und Reports	➔ Warnungen, Dashboards und Berichte, die Sicherheitsmaßnahmen beschleunigen und das OT- und IoT-Risikomanagement erheblich verbessern ➔ Nahtlose Integration in SOC/IT-Tools und Workflows, einschließlich automatischer Reaktion auf blockierte Angriffe, bei Integration mit kompatiblen Firewalls und Endpunktsicherheitsprodukten ➔ Globale Skalierbarkeit zum Schutz von 1000enden von Standorten	
Skalierbare Lösungsmodelle für ON Premisses Anforderungen		
Skalierbare Lösungen für SaaS Anforderungen		
Sofortige Integration mit weiteren Sicherheitssystem wie SIEM, SOC, Syslog, Active Directory / LDAP, Remote Access sowie dem OT-Leitstand		

Ihre Vorteile durch eine Zusammenarbeit mit uns:

Das Industrial Automation Team mit IT-, IoT und OT-Security Know-How ermöglicht:

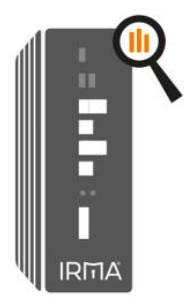
- eine einfache Inbetriebnahme
- minutenschnelle Ergebnisse
- unterstützt Sie beim Know-How-Transfer und direktem Support beim Aufbau Ihres IoT/OT-Security Operation Teams





SecurITy made in Germany

INDUSTRIAL AUTOMATION



INDUSTRIAL AUTOMATION