

Anforderungen an Cyber-Security in OT- / IoT-Umgebungen

Kriterien	Nutzen	Kommentar
Visibilität – Sichtbarkeit der gesamten OT-Infrastruktur – Asset Inventory		
Erkennung aller Assets (IT-, IoT- und OT-basierte Geräte) im OT-Netzwerk ohne Auswirkung auf den Betrieb	→ Technologie- und Prozess-Konsolidierung	
Umfassender Support von IT, IoT und OT Protokollen	→ gemeinsames Monitoring → Eliminierung von Silos	
Interaktives automatisiert erstelltes Asset Inventory mit Assets, Kommunikationsbeziehungen und Protokollen	→ Verantwortung steigern und Kosten minimieren	
Identifikation von neuen Geräten (Gerätetyp, Firmware-Version etc.)	→ Zusammenführen von IT und OT → optimiertes Asset Management	
Monitoring aller Fernwartezugriffe		
Optional: Aktive Abfragemöglichkeiten ohne Auswirkungen auf den Betrieb für Windows, Unix Hosts bzw. Netzwerkgeräte		Nozomi-User sehen den Kundennutzen innerhalb von wenigen Minuten nach der Implementierung. Die schnelle Asset-Erkennung und Netzwerk-Visualisierung steigern das Bewusstsein der Security Operations Teams.
Schutz von IoT/OT-Konfigurationen		
Identifizierung von Änderungen an Speicherprogrammierbaren Steuerungen (SPS) oder Human Machine Interfaces – SPS Programm Code, Firmware, Konfigurationsänderungen	→ Vollständiges Protokoll der ICS-Aktivitäten	
Monitoring und Analyse für IoT- und OT-Prozessvariablen		
Schwachstellenanalyse und Risikomanagement		
Identifizierung von spezifischen IT-, IoT- und OT-Schwachstellen	→ erweiterte Einblicke für das Risikomanagement, ohne zusätzliche Ressourcen aufbauen zu müssen → Workflow für die schnelle Erkennung von Anomalien für das bestehende Security Operations Teams	
Erkennung von Anomalien und Manipulation im Netzwerkverkehr	→ integrierte Cyber Threat Detection kombiniert verhaltensbasierte Anomalie-Erkennung, signaturbasierte Bedrohungserkennung und Asset Intelligence für eine umfassende Risikoüberwachung	
Advanced Cyber Threat Detection – Bedrohungserkennung inkl. Alarmierung		
Nutzung der laufend aktualisierten Sicherheitsdatenbanken	→ schnelle Erkennung von Cyberangriffen und proaktive Schadensminimierung	
Proaktive Schwachstellen- und Risikoerkennung und Identifizierung von MITRE Attack Angriffsvektoren	→ steigert Robustheit gegen Cyberangriffe → bei Integration eines Firewall-Systems aktive Blockfunktion	
Echtzeit-Warnungen zu verdächtigen Aktivitäten und Bedrohungen in OT-Netzwerken (z.B. Malware Detection)	→ Sofortschutz gegen Ransomware	

Audit und Compliance		
Nicht veränderbare Audit Logs		
Vollumfängliche Timemachine (Snapshot-Funktion) inkl. Versionsvergleichsprüfung		
Unterstützung der Umsetzung von internationalen Standards wie IEC 62443, CIS Critical Security Controls, ISO 2700 Serie inkl. 27001, Mitre ICS Attack Framework	→ Einhaltung der nationalen und betrieblichen Anforderungen an die Cybersicherheit	
Monitoring über Überwachung von Zonen und Conduits nach IEC 62443		
Unterstützung der Umsetzung der NIS Verordnung		
Integration in die Enterprise Architektur und Unterstützung von Security Operations Teams		
Sofortige Integration mit führenden Sicherheitspartnern, Active Directory, SIEM, Syslog, REST API, Datenexporten	→ Warnungen, Dashboards und Berichte, die Sicherheitsmaßnahmen beschleunigen und das OT- und IoT-Risikomanagement erheblich verbessern	
Anpassbare Analysen und Reports	→ Nahtlose Integration in SOC/IT-Tools und -Workflows, einschließlich automatischer Reaktion auf blockierte Angriffe bei Integration mit kompatiblen Firewalls und Endpunktsicherheitsprodukten	
Skalierbare Lösungsmodelle für On-Premises-Anforderungen	→ Globale Skalierbarkeit zum Schutz von Tausenden von Standorten	
Skalierbare Lösungsmodelle für SaaS-Anforderungen	→ Flexibilität beim Einsatz mit physischen, virtuellen, Container- und tragbaren Appliances vor Ort sowie SaaS- und Cloud-Deployment	

Ihre Vorteile durch die Zusammenarbeit mit Nozomi Networks Platinum Partner IKARUS Security Software:

Das **interdisziplinäre Expertenteam** mit IT-, OT- und IoT-Security Know-how ermöglicht eine **einfache Inbetriebnahme** und **minutenschnelle Ergebnisse** und unterstützt Sie mit **Know-how-Transfer** und **direktem Support** beim Aufbau Ihres **IT/IoT/OT Security Operations Teams**.

