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 → Gemeinsames Monitoring → Eliminierung von Silos → Verantwortung steigern und Kosten minimieren → **Zusammenführen von IT und OT** → Optimiertes Asset Management **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.	
	Umfassender Support von IT-, IoT- und OT-Protokollen		
	Interaktives automatisiert erstelltes Asset Inventory mit Assets, Kommunikationsbeziehungen und Protokollen		
	Identifikation von neuen Geräten (Gerätetyp, Firmware-Version etc.)		
	Monitoring aller Fernwartezugriffe		
	Optional: aktive Abfragemöglichkeiten ohne Auswirkungen auf den Betrieb für Windows, Unix Hosts bzw. Netzwerkgeräte		
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 → Integrierte Cyber Threat Detection kombiniert verhaltensbasierte Anomalie-Erkennung, signaturbasierte Bedrohungserkennung und Asset Intelligence für eine umfassende Risikoüberwachung	
	Erkennung von Anomalien und Manipulation im Netzwerkverkehr		
Advanced Cyber Threat Detection – Bedrohungserkennung inkl. Alarmierung			
	Nutzung der laufend aktualisierten Sicherheitsdatenbanken	→ Schnelle Erkennung von Cyberangriffen und proaktive Schadensminimierung → Steigert Robustheit gegen Cyberangriffe → Bei Integration eines Firewall-Systems aktive Blockfunktion → **Sofortschutz gegen Ransomware**	
	Proaktive Schwachstellen- und Risikoerkennung und Identifizierung von MITRE Attack Angriffsvektoren		
	Echtzeit-Warnungen zu verdächtigen Aktivitäten und Bedrohungen in OT-Netzwerken (z.B. Malware Detection)		

Blechturmgasse 11 | A-1050 Wien | Telefon: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Audit und Compliance			
	Nicht veränderbare Audit-Logs	→ Einhaltung der nationalen und betrieblichen Anforderungen an die Cybersicherheit	
	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		
	Monitoring über Überwachung von Zonen und Conduitsnach IEC 62443		
	Unterstützung der Umsetzung der NIS(2)-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 → **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 Tausenden von Standorten → Flexibilität beim Einsatz mit physischen, virtuellen, Container-und tragbaren Appliances vor Ort sowie SaaS- und Cloud-Deployment	
	Anpassbare Analysen und Reports		
	Skalierbare Lösungsmodelle für On-Premises-Anforderungen		
	Skalierbare Lösungsmodelle für SaaS-Anforderungen		

Ihre Vorteile durch Nozomi Networks MSSP- und Platinum Partner IKARUS Security Software:

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

www.IKARUSsecurity.com/industrial-cyber-security