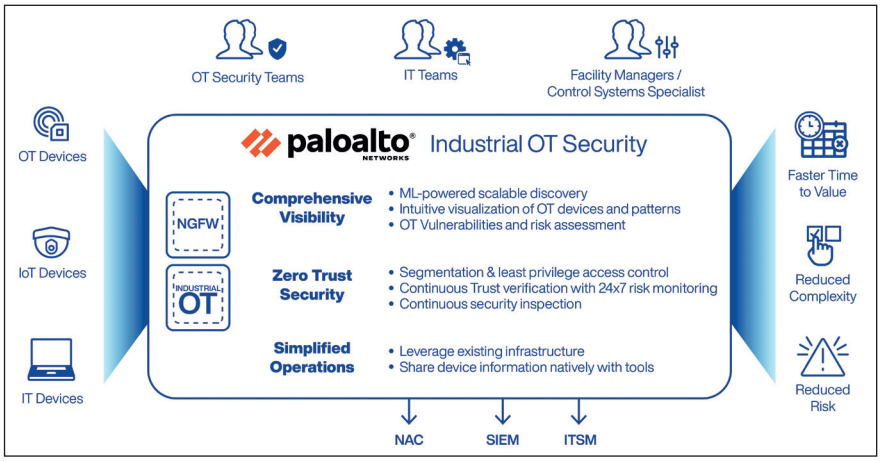
Advertorial

Industrial Security mit Palo Alto Networks

Bisher isolierte oder abgekoppelte Systeme in Industrie und Fertigung benötigen immer öfter interne und/oder externe Konnektivität zum Firmennetzwerk und zum Internet. Dabei sind Lösungen gefragt, die eine «logische» Trennung der OT-Netzwerke unterstützen und eine sichere Kommunikation mit externen Diensten ermöglichen. Echtzeitdaten zur Überwachung und Steuerung in OT-Netzwerken erfordern Echtzeit-Streaming von (Sicherheits-)Telemetriedaten. Palo Alto Networks bietet eine sichere Telemetriedaten-Streaming-Architektur, bestehend aus Segmentierungs-Firewalls (Layer-7-Firewall), Telemetrie-Gateway und einem in der Schweiz stehenden Cloud-Datenspeicher (Data Lake).



Umfassende Sichtbarkeit

Durch fortlaufende Erkennung und Bewertung aller angeschlossenen cyberphysischen Systeme wird eine umfassende Sichtbarkeit gewährleistet. Industrial OT Security kombiniert dabei maschinelles Lernen (ML) mit App- und Device-ID-Technologie sowie crowdgesourcten Telemetriedaten, um schnell ein Profil aller OT-, IT- und IoT-Geräte und -Anlagen zu erstellen. Dazu gehören kritische OT-Geräte wie Distributed Control Systems (DCS), Industrial Control Systems (ICS), Human-Machine Interfaces (HMI), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Supervisory Control and Data Acquisition (SCADA) Systems, Historians und Jump Server. Auch gängige IoT-Geräte wie Sicherheitskameras, Drucker und HLK-Systeme werden dabei erkannt und geschützt. Die KI/ML-basierte Technologie erkennt die Geräte passiv und klassifiziert diese anhand von mehr als achtzig einzigartigen Attributen.

Segmentierung und Zugriffskontrolle mit geringsten Rechten

Industrial OT Security ermöglicht die Trennung der OT-Netzwerke von der Unternehmens-IT und vom Internet und sichert OT-Anlagen mit Zoning- und feinkörnigen Segmentierungsrichtlinien auf der Grundlage von OT-Anlagen, Protokollen und Risikokontext. Diese Funktionen verhindern, dass sich infizierte oder infiltrierte Systeme auf weitere Anlagebereiche ausdehnen respektive diese stören.

Dabei bietet die Lösung automatisierte Empfehlungen für Zugriffsrichtlinien mit den geringsten Privilegien (Least-Privilege Access), die auf kontextbezogenen Informationen und Verhaltensprofilen basieren. Darüber hinaus machen automatisierte Sicherheitsrichtlinien die fehleranfällige und zeitaufwendige manuelle Richtlinienerstellung überflüssig. Mit den Layer-7-Firewalls von Palo Alto Networks lassen sich diese Richtlinien mithilfe von Device-ID leicht durchsetzen. Alternativ können sie durch die Integration in eine auf Network Access Control (NAC) basierende Lösung durchgesetzt werden.

Kontinuierliche Sicherheitsüberprüfung

Industrial OT Security verhindert Zero-Day-Angriffe durch Inline-Deep-Learning, das Erkennen von Anomalien im Anlageverhalten und die kontinuierliche Bewertung von ICS-Prozessen, um die Prozessintegrität und Sicherheit der cyberphysischen Systeme zu gewährleisten. Ergänzt durch fortschrittliche Bedrohungsabwehr (ATP), können bekannte und unbekannte Attacken in kritischen OT-Anlagen und Prozessen erfolgreich erkannt und abgewehrt werden.

Palo Alto Networks Industrial OT Security: Die Highlights

- Sichtbarkeit der OT-Ressourcen, Einblicke in Risiken und Verhalten
- Fortschrittliche Erkennung und Abwehr von Bedrohungen in abgekoppelten OT-Netzwerken
- Geräte- und App-ID-gesteuerte Richtlinienempfehlungen und -durchsetzung für die Mikrosegmentierung von OT-Netzwerken mit geringsten Rechten
- Gehärtete Telemetrie-Gateways zur Sicherung von Datenströmen aus OT-Netzwerken
- Sichere und verschlüsselte Übertragung von Telemetriedaten aus OT-Netzwerken in die Cloud über eine ausgehende mTLS-Verbindung

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch,
www.boll.ch