ACCURA
Industrial & Information
Cybersecurity

OT Security Operation Center

Accura sets up a Cyber Defense Center (CDC), also known as Security Operations Center (SOC), in your company and manages its continuous operation: quickly up and running, using tried and tested principles and based on cutting-edge technology that understands industrial environments

PROACTIVE INDUSTRIAL CYBERSECURITY MONITORING

Industrial networks connect the virtual with the physical world and thus represent critical goals. OT environments often consist of older and sensitive systems that are not adequately protected with security solutions. By networking IT and OT systems, there are new gateways for attackers from inside and outside.

Accura helps companies protecting both IT and OT systems without interfering with work processes. OT Security Monitoring enables complete transparency of network traffic. This enables a better understanding and deeper insight into the underlying processes and leads to more security overall.

	KEY OT SOC FEATURES & SERVICES
✓	• Analysis of OT privilege command behavior (integrity alerts) • Behavior analysis threat detection (zero days) • Signature-based threat detection (known threats) • Real-time visualization of devices and their connections based on Purdue Model
✓	• Continuous and passive scanning of the devices • Automatic attack vector calculation to OT network • On-demand safe active query monitoring of industrial devices • Detecting and extracting information from various industry protocols
✓	• Passive vulnerability management (PLC, RTU, IED, DCS etc.) • OT honeypot to catch attackers • Automatic notification of security-related incidents • Detailed visualization of devices and collected knowledge

BENEFITS OF OT SOC

- **Enhanced Security Monitoring:** Real-time monitoring of OT environments allows for the early detection of threats, helping to prevent costly downtime and maintain operational integrity.
- **Threat Intelligence Integration:** An OT SOC leverages both IT and OT threat intelligence, providing insights into unique threats targeting industrial systems, such as ransomware tailored for OT environments.

- **Continuous Vulnerability Management:** OT SOC manages vulnerabilities by detecting and mitigating risks, where legacy systems may be vulnerable to cyberattacks.
- **Reduced Operational Downtime:** By preemptively addressing issues and promptly responding to threats, an OT SOC minimizes unexpected downtime and maximizes uptime for critical OT systems.

- **Regulatory Compliance:** Many industries are required to follow strict regulatory standards (e.g., NIS2, IEC 62443)