Anomaly Detection

Gain full spectrum OT and IoT visibility, continuous security monitoring, and real-time risk insights

Solution overview

The increase in digitalization initiatives and the expansion of remote operations have made it challenging for once isolated operational technology (OT) organizations to maintain a current OT asset inventory and identify anomalous behavior on the network.

Schneider Electric's Anomaly Detection solution continuously monitors your network for anomalous activity and alerts you when an event or potential risk arises.

The Anomaly Detection Solution protects against cybersecurity threats by implementing security controls, including:

- Automated OT asset inventory to understand what is within the network
- An up-to-date network diagram on-demand with guidance on network segmentation
- Threat and anomaly detection capabilities that produce timely alerts
- Contextualizing and assigning risk scores to optimize response efforts
- Analytics and reporting capability at the site- or multi-site level

These functions are provided in one console to support you in maintaining your security posture.

Key benefits

- Provides visibility into OT and internet of things (IoT) networks by automating the asset inventory process
- Detects and notifies of anomalies, known/emerging threats, and zero-day attacks through 24/7 continuous threat and vulnerability monitoring
- Focuses response team efforts to address relevant events by providing a risk ranking methodology that prioritizes and provides operational and security context of potential threats
- Simplifies and cost-effectively scales technology to fit organizational needs (i.e., multi-site deployment)
- Easy access to OT data through dashboards and customizable reports

se.com/cybersecurity-services

Life Is On | Schneider Electric

How it works

The Anomaly Detection solution works in the following phases:

- **Phase 1 - Learning Phase** – The solution learns the network under normal conditions and then creates a system baseline to compare all future network activity.
- **Phase 2 - Detect mode** – The solution runs continuously in the background and automatically determines any events outside the expected parameters identified in the Learning Phase.
- **Phase 3 - Alerting** – An alert is created in real-time when potentially malicious activity is identified. Contextualized event and risk information enables teams to investigate and respond accordingly.
- **Continuous monitoring and asset inventory** – The solution runs continuously and passively in the background to provide visibility to all network assets, have an up-to-date architecture drawing, verify software/firmware versions, and understand the threats relevant to their environment. This is the foundation for an effective anomaly detection solution.

Key capabilities

Industrial visibility and asset management

Effective industrial cybersecurity starts with knowing what to secure. Schneider Electric leverages the industry's broadest and deepest industrial protocol coverage to provide comprehensive industrial and asset visibility, resulting in a highly detailed, centralized inventory of all OT, IoT, and industrial internet of things (IIoT) assets, processes, and connections.

The Schneider Electric solution can collect information in multiple areas to support identifying and managing risks.

- **Asset inventory** – This encompasses all OT, IoT, and IIoT assets on an industrial network, as well as extensive attributes about each asset, including model number, firewall version, card slot, serial number, components and more. The inventory also identifies missing patches and can identify vulnerabilities.
- **Network visibility** – This includes all industrial network sessions along with their bandwidth, actions taken, changes made, connectivity paths, and other details relevant to industrial network sessions.
- **Operational process visibility** – This includes tracking all industrial operations, the code section, and tag values of all processes involving OT, IoT, or IIoT assets, and any abnormal changes to these assets' process values that could indicate threats to process integrity.

Anomaly and Threat Detection

Schneider Electric's Anomaly Detection solution automatically profiles assets, communications, and processes in identified industrial networks, generates a behavioral baseline, and alerts users in real-time to anomalies and emerging threats.

- **OT threat intelligence** – Intelligence that is updated in real-time to identify cybersecurity and process reliability threats.
- **Contextualization of risks** – A single metric enabling security teams to quickly weed out false positives and prioritize alerts for triage and mitigation.
- **Automated guidance for identified alerts** – Groups related events of the same incident into a single alert, providing a view of the chain of events and a root-cause analysis enabling your team to be more efficient and effective during the triage and mitigation stage.

Vulnerability management

Anomaly Detection provides visibility of identified asset vulnerabilities, including insecure protocols, configurations, standard security practices tracked by Schneider Electric, and the lasted common vulnerabilities and exposures (CVE) data from the National Vulnerability Database.

- **Detailed alerts** – Provide key information on alerts to support security and operations staff.
- **Risk-based prioritization** – Vulnerabilities/alerts are automatically scored based on their impact and likelihood on each OT environment, enabling your team to be more efficient and effective.
- **Risk simulator** – Models out how changes to a device type could impact the overall risk score.
- **Custom configuration of enterprise risk score** – Tailor the risk scoring metrics to fit your organization based on prioritizing the importance of various assets in your OT environment.

Why partner with Schneider Electric?

Experts in cybersecurity for OT

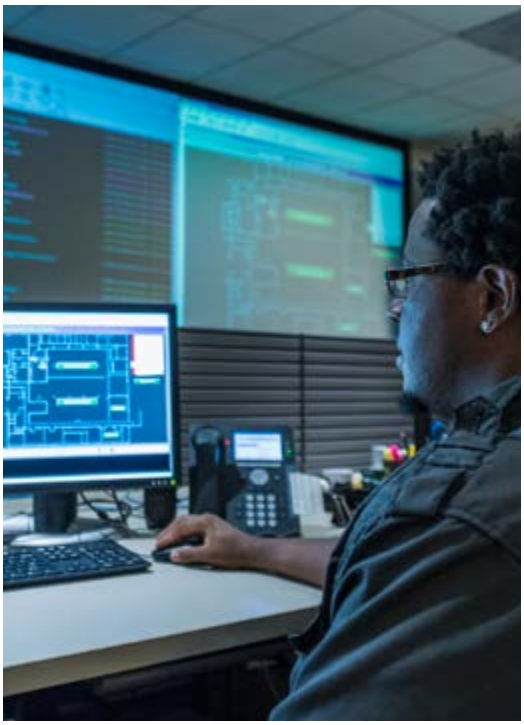
Schneider Electric is committed to providing solutions that support your need for cybersecurity protection across any industry. We have decades of experience in OT and have been pioneering connectivity through our EcoStruxure™ Platform. This digital backbone connects our best-in-class technology solutions with the latest IT technology to leverage the true potential of the IoT.

- We have a global reach with locally certified cyber experts dedicated to ensuring cybersecurity is embedded at all levels of our solutions, from plant to plug.
- As system providers, we are committed to partnering with customers to continually adapt and meet the evolving needs of your industrial network.
- We provide vendor-agnostic services to help you assess risk, implement cyber-specific solutions, and maintain long-term defenses.
- Our software can work with various manufacturers' platforms; even if your entire system is a multi-manufacturer, we can still deliver our expert cyber services.
- Schneider Electric brings you secure, flexible monitoring and visibility of your OT and IoT networks.

5,200

Monthly cyber attacks on IoT devices

– Source: Cyber Magazine



Experienced, capable, and globally available

Schneider Electric's global team of cybersecurity experts understands the unique needs and challenges of OT systems and technologies.

- Our focus is on finding solutions that fit your unique requirements, regardless of the systems you use.
- Our experts will work with you to understand your requirements and help implement and customize the right level of security to meet your specific needs.
- We work with leading cybersecurity product experts to bring the right solution to your operation to ensure that your people, processes, and technologies are protected.

Our services allow you to focus on what you do best while ensuring your entire network's safety.

Contact us

Learn more about **Anomaly Detection** and our range of solutions that support your cybersecurity protection needs across all business types and industries.

se.com/cybersecurity-services

Life Is On Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

• 998-22243000_GMA