Your Operational Technology. Protected.

Continuous Industrial Network Cybersecurity
Risk Assessment & Security Monitoring
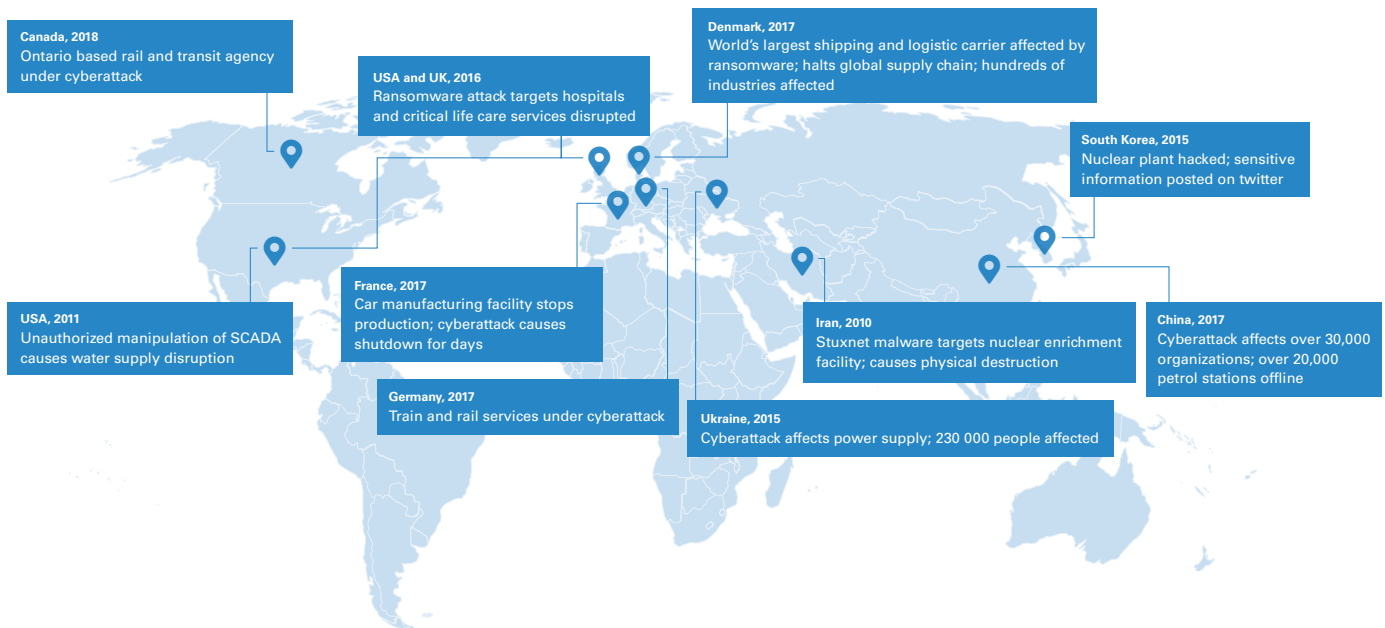
TÜVRheinland®
Precisely Right.

Did you know that cyberattacks are on the rise in OT and Industrial Control Networks?

The trend for digitization and systems interconnectivity has left many OT engineering and operating personnel ill-prepared to deal with cybersecurity incidents. This is aggra-vated by the increased frequency and sophistication of attacks on OT systems.

Canada, 2018
Ontario based rail and transit agency under cyberattack

USA and UK, 2016
Ransomware attack targets hospitals and critical life care services disrupted

Denmark, 2017
World's largest shipping and logistic carrier affected by ransomware; halts global supply chain; hundreds of industries affected

South Korea, 2015
Nuclear plant hacked; sensitive information posted on twitter

USA, 2011
Unauthorized manipulation of SCADA causes water supply disruption

France, 2017
Car manufacturing facility stops production; cyberattack causes shutdown for days

Iran, 2010
Stuxnet malware targets nuclear enrichment facility; causes physical destruction

China, 2017
Cyberattack affects over 30,000 organizations; over 20,000 petrol stations offline

Germany, 2017
Train and rail services under cyberattack

Ukraine, 2015
Cyberattack affects power supply; 230 000 people affected

Graphic shows notable global OT and Industrial Security Incidents.

Why are attacks so successful in OT and Industrial Control Networks?

- Standard IT security risk models do not support the special requirements of OT and Industrial Control Systems (ICS).
- IT and engineering staff are often not equipped with technology to detect cyberattack attempts on their OT and associated systems.
- Traditional IT security tools, approaches and skill-sets were not designed for complex OT solutions.

- Well-publicized reports have shown how sophisticated malware and threat actors can disrupt safety critical industrial operations. These reports have raised concerns about cybersecurity vulnerabilities across all types of industries.
- Industrial systems can no longer rely on air gaps to provide a secure environment as these are often undermined by the use of USB sticks, WiFi connections and other technologies.

Why assess your Industrial and Operational Technology Risk?

Severe Impact on Society
Organizations operating industrial facilities have an accountability to monitor, detect and mitigate cybersecurity attacks in order to maintain the integrity and availability of plants which may otherwise have a severe impact on society.

Lower Concerns
Business executives are concerned about how cybersecurity issues can impact their business.

Legal Requirement
There is a regulatory or legal requirement to understand cybersecurity risk if you operate in a safety critical or hazardous industry.

Comply with Standards
Leading cybersecurity standards for industrial control systems such as NIST Cybersecurity Framework (CSF) and IEC 62443 emphasize that plant operators are to have monitoring solutions for their OT networks.

Protected Investments
Investors and shareholders need reassuring that systems are robust and capable of managing likely cybersecurity issues and that new investments will be protected.

Protected Customer Data
Customers are demanding that their intellectual property and process information is protected on your OT network.

Safety and Industrial Cybersecurity

You can't have a safe plant if it is not secure.
A plant that is safe from technical failure due to a rigorous functional safety design and implementation could still be compromised by a cyberattack. Control systems may be appropriately designed and implemented from a safety perspective -- but if the industrial network is not secured using suitable security measures systems it could be tampered with.

Learn more about www.tuv.com/en/ot

How are Industrial and Operational Technology Cybersecurity Risks Assessed?

Our team will engage with you in an effective way to help you understand how mature your OT cybersecurity posture is. Engagements are adaptable using either IEC 62443 or NIST CSF industry standards depending on what is best for your situation, also NERC CIP could be cited.

An assessment can be completed in a relatively short period of time, allowing for quick feedback to the business. This allows the business to start remedial steps as soon as possible. Our experts take a collaborative workshop approach enabling findings to be discussed in a friendly, informed way with internal teams to maximize the learning opportunity and ensure that key parts of the business and operations are engaged in the process.

During the engagement the team will work with you to install the SecurityMatters SilentDefense™ passive network monitoring and situational awareness platform to provide visibility across your industrial control systems, Distributed Controls Systems (DCS) and SCADA networks. This will provide the team with detailed information on your OT network assets, build a network map and monitor for any ongoing ICS specific threat indicators from a library of 1300+ protocol checks, vulnerabilities and behavioral checks.

If threats are found the SilentDefense™ Threat Hunting Framework provides a comprehensive search tool as well as continuous full traffic recording for for efficient threat analysis and remediation.

Our Partner:

SECURITY MATTERS

For more information on SecurityMatters, please visit
www.secmatters.com

SILENTDEFENSE COMMAND CENTER AND MONITORING SENSORS CAN BE PROVIDED IN DIFFERENT CONFIGURATIONS:

- During the assessment process the Command Center and one Monitoring Sensor will be provided, either physically or virtually, in a bundled configuration.

- For deployments in production environments, the Command Center can be installed on a rack server or VMware ESXi hypervisors. Monitoring Sensors are installed on dedicated hardware.

How it works

Once configured as part of the Continuous Industrial Network Cybersecurity Risk Assessment (CINCRA) the monitoring solution will do the following:

1 Start packet and protocol analysis; detect assets and map communications of your control networks.

2 Present a visual map based on the IEC 62443 model.

3 Present real-time information about the hardware (serial, interfaces, etc.) and associated vulnerabilities.

4 Detect and alert unauthorized communication or access attempts in real time.

5 Provide customizable dashboards for technical, IT and management staff.

Risk assessment based on a flexible technology stack

Can be integrated with Industrial and Operational Technology across all sectors using legacy or modern equipment and protocol.

Has the capability to support non IP devices and protocols. (As per support)

Is totally passive, so that it never interferes or interacts with the industrial process. The solution passively listens to network traffic and control signals using a proprietary analysis engine enabling it to identify the OT equipment and network configuration to create a baseline. This passive network listening can be achieved in segmented and non-segmented networks using a network tap or via port mirroring.

Has a small learning curve and can start generating value for plant operators, security staff and executive management during the risk assessment process. It can provide valuable insights into vulnerabilities, security issues, operational issues and areas of concern.

Is powered by an ICS-CERT and vendor signature-based threat feed which can provide real time threat analysis.

# Supported Vendors and Protocols

SUPPORTED ICS VENDORS

ABB, Allen-Bradley/ Rockwell, Beckhoff, Emerson, General Electrics, Honeywell, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa*

SUPPORTED INDUSTRIAL AND IT PROTOCOLS

Aspentech Cim/IO, Beckhoff ADS, CEI 79-5/2-3, DNP3, EtherNet/IP - CIP, Foundation Fieldbus, Honeywell, ICCP, IEC-60870-5-104, IEC-61850 (MMS, GOOSE, SMV), Modbus/TCP, MMS, OPC, PI-Connect, Profinet, Siemens S7 BitTorrent, DCE-RCP, DHCP, DNS, Dropbox, eDonkey (eMule), FTP, FTPS, HTTP, HTTPS, IMAP, IMAPS, ISO-TSAP/COTP, Kerberos, KMS, LDAP, LDAPS, MS SQL Server, MySQL, NetBIOS, NTP, POP3, Remote Desktop, SSH, SMB, SMTP, SNMP (full parsing of MIBS), STP, Syslog, Telnet, VNC

Legacy or product vendors or protocols not in the list above can be supported using rich context language capabilities in the solution and may need customization.

TÜV Rheinland support across the OT Network
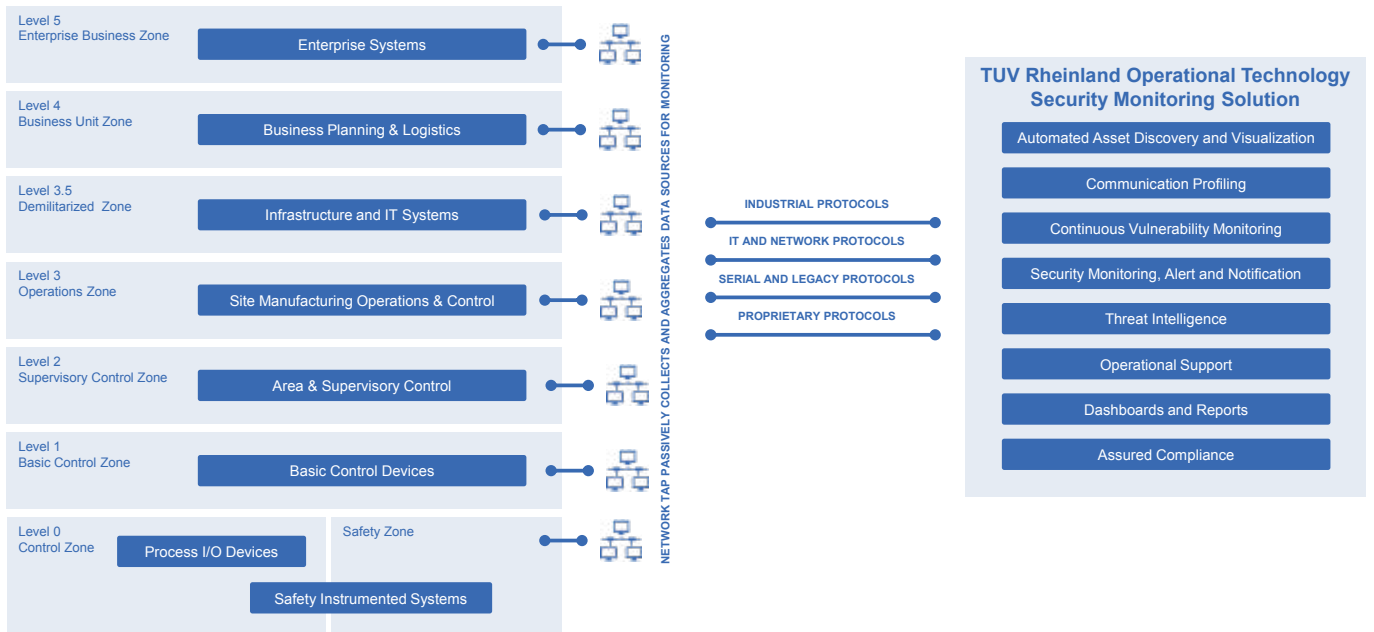
Our approach for risk assessments

CINCRA have been undertaken across many installations worldwide in sectors including oil and gas, energy generation and distribution, rail and road transportation, manufacturing and infrastructure. The TÜV Rheinland approach to risk assessments combines an advanced and mature OT process, an equipment and network monitoring and threat intelligence platform, along with an insightful and informative consultative process. Once the assessment has been completed TÜV Rheinland can, if required, work with your teams to implement any additional cybersecurity measures to address any issues that were found, thereby providing an end-to-end solution to the complexities of OT cybersecurity risk.

COLLABORATIVE WORKING

TÜV Rheinland will work collaboratively with your internal team to ensure the solution addresses their concerns.

IDENTIFY ASSETS

The solution is able to identify assets, and based on TÜV methodology, these assets can be prioritized based on criticality for risk assessment.

IDENTIFY THREATS

Our solution has a catalog of over 600 threats that encompasses the majority of the threat landscape. Coupled with information gained from the risk assessment process clients can focus their resources on vulnerabilities that need the most attention.

IDENTIFY VULNERABILITIES

The solution has an integrated feed from vendors, national and international agencies and leading commercial providers. Without probing or scanning a sensitive or legacy industrial network the solution can help clients identify the vulnerabilities in hardware (IT, OT) , software, applications, industrial processes, architecture, configuration, and protocols.

RISK ASSESSMENT AND MANAGEMENT

TÜV Rheinland has developed a risk assessment and management approach which can be used with qualitative or quantitative data to conduct risk assessment for Industrial and OT facilities. The method is precise and quick with the use of accelerators, such as threat detection solutions. Further, our model supports clients by updating risk profiles when new vulnerabilities or threats emerge within their Industrial or OT environments.

1 Establish Context	2 Risk Identification	3 Risk Analysis	4 Risk Evaluation	5 Risk Treatment

TÜV Rheinland
ICT & Business Solutions
otsecurity@tuv.com

www.tuv.com/en/ot

TÜVRheinland®
Precisely Right.