FUJITSU

Industrial Security

Fujitsu's Cyber Security Services for Operational Technology provide a secure network for manufacturing customers, continuously monitoring and protecting their business critical digital assets.

The Business Challenge

Operational Technology (OT) equipment, sites and related processes are critical to the safe and reliable delivery of manufacturers' core products and services. Be it in discrete or process manufacturing, all producers and suppliers are obliged to maintain reliable and high-quality services for their customers, with uninterrupted operations. In addition, they must provide for safety and well-being of their workers, and the communities within which they operate.

Today, operations equipment is networked in many new ways to provide connectivity to data, in order to increase overall equipment efficiency (OEE) and customer value. With the business benefits of digitization comes the need to ensure the security of OT. Cyber security is fundamental to successful digitization and a critical requirement for digital supply chains.

Cyber security in manufacturing is a new quality characteristic that manages the threats to the control of equipment and production processes. If this is not addressed, the threat can impact production targets, causing damage to machines, workers or even whole communities, and cause loss of intellectual property. These threats may come from external actors, malicious insiders or via suppliers.

Addressing the need for cyber security under the imperatives of reliable and compliant operations is challenging. Guidelines such as the ISA/IEC 62443 set of standards, describe the requirements on the operators, integrators and component suppliers of physical processes. The big challenge is turning theory into practice.

Brown-field landscapes need to be carefully assessed as the design and implementation of the connectivity network must be capable of evolving to support new demands. As these elements come into place, continuous security monitoring of core internal assets and processes must be established, and a new level of collaboration created between cyber security and operational technology experts. An additional challenge for many production environments is a lack of systematic visibility of their digital assets. This visibility is required to secure the assets and to exploit the value of their data.

Fujitsu OT Cyber Security Services comprises three elements

OT Assessment - baseline the opportunity for technological and organizational transformation, and compliance. Discover your networked digital assets

OT Network Transformation – design and build secure, segmented, connectivity within and between sites

OT Managed Monitoring Services – constantly monitoring the IT assets and traffic that control OT equipment, maintaining an interface to the customer's operational control center

Our Approach

Fujitsu's approach is: Connect, Protect and Manage Digital Assets. Ensuring secure digital operations is not a one-off challenge. We work in collaboration with customers to create a solid foundation for the continuous evolution of OT and its associated cyber security. The three complementary security services described can be ordered and delivered individually.

Fujitsu's OT Cyber Security Offerings

OT Assessment
Baseline the existing environment from the cyber security perspectives of people, processes and technology. Make recommendations backed by a development roadmap, reflecting technical, and if necessary, organizational aspects and associated compliance requirements. The assessment may involve offline data analysis, online passive asset discovery, and interviews with operations experts, based on factory documentation or a proof-of-value trial phase, isolated from live production. Depending on the scope and environment of the assessment, Fujitsu may collaborate with other specialist partners to deliver this service. The output of the passive asset discovery can be fed into a Configuration Management Database (CMDB) to support further digitalization steps.

OT Network Transformation
Based on the development roadmap, we shall analyze in depth the existing connectivity within sites and, if appropriate, between sites. While making the best possible use of previous investments (e.g. firewalls), we recommend and implement a segmented network architecture that reflects the Purdue model, the functional demands and the risk profiles across the network. Tested and cost-effective techniques such as SD-WAN are used for connectivity between sites and the enterprise network, while attention is paid to the secure use of wireless intra-site communication. Side-door access to the network by maintenance partners is considered. The zones and conduits approach of IEC 62443-3-2 underlies the architecture. We work closely with the customer's OT field team and their specialist OT partners to minimize the risk of disruption to critical processes during the transformation.

OT Managed Monitoring
The OT Monitoring Service is provided from Fujitsu's Security Operating Centers (SOCs). Incoming information from the customer's OT is monitored and analyzed. Actionable insights are reported to the customer's operations management team, helping to prevent, detect, mitigate and recover from cyber incidents in the OT estate. In the initial setup phase, Fujitsu works with the customer's security operations team to establish the working model and data exchange with the Fujitsu SOC, and to connect the OT environment to the Fujitsu SOC. We jointly establish what normal cyber behavior of the OT environment is, and rehearse communication between the Fujitsu and customer teams. We then continuously monitor the cyber health of the IT equipment that is controlling OT (e.g. the SCADA systems) and monitor the traffic on the OT network for anomalies. In the operational phase, monitoring and reporting are carried out according to agreed procedures. The service will detect new assets added to the network, optionally allowing continuous updates to the CMDB.
On a regular basis, we shall jointly undertake a review of performance, effectiveness, and customer satisfaction.

Outcomes and benefits

OT Assessment
The customer understands the current state of their OT from a cyber-security perspective and is provided with recommendations and a proposed development roadmap, reflecting their risk profile and compliance priorities. A POV trial provides deep insight to the requirements of the customer's specific environment. Assessment results cover people, process, and technology aspects as appropriate. The service provides CMDB input to support the broader digitalization of the environment.

OT Network Transformation
The OT network is fit for purpose and provides both the security and the flexibility required to innovate operational processes. The implementation facilitates OT Monitoring.

OT Monitoring
Customers receive regular reports and analysis of their OT cyber security posture as monitored. Events and incidents recorded at the service desk are classified, ticketed and triaged, according to priority, and then referred to the nominated customer interface. This allows timely decision-making for the appropriate actions to be taken by the customer. Fujitsu will provide initial incident investigation support as part of this service. Further service options such as Vulnerability Management and Privileged Access Management can be agreed.

Why work with Fujitsu?

Fujitsu has its own Security Operating Centers, Security Consultancy Practice and implementation capability that bring experience and expertise to all its engagements.
We have:
- Experience in the manufacturing and utilities sectors, in NIS-D compliance, NCSC CAF, IEC 62443 and other sector-specific standards
- Extensive experience protecting and securing data with proven credentials in ISO27001 and ISO22301
- Experience of data processing principles and have been helping customers for many years
- A proven track record providing strategic guidance and practical solutions on data processing and regulatory compliance
- A strong brand, market presence and a reputation for providing high quality services to our customers
- A passion to work collaboratively

What next?

Call Fujitsu now to ask about our OT Cyber Security Services for Manufacturing. We can help you to deliver safe and reliable services while you and your customers reap the benefits of digitalization.