White Paper

Operational Technology Security: Our Approach

What is OT security?

OT (Operational Technology) Security involves safeguarding the control and monitoring systems used in critical infrastructure and industrial processes. Originally isolated, OT systems have now integrated with external IT networks and Industrial Internet of Things (IIoT), exposing them to new threats.

Understanding OT security in critical infrastructure

OT systems are designed to control and monitor physical processes, such as manufacturing operations, power generation, and transportation. These systems are traditionally isolated from any external network. However, the integration of OT systems with IT networks and the rise of Industrial Internet of Things (IIoT) exposes them to new threats. Often the bulwark of IT security is having in-support devices and an effective patch management strategy. This can be a challenge for OT as they often include legacy systems with limited security features, a longer system lifetime, and the security context of the network demands high levels of assurance before patches are deployed. This is in spite of the potential for physical consequences if compromised.

The convergence challenge

The convergence of OT and IT systems requires organisations to bridge the gap between the traditionally separate disciplines of IT and OT security which requires a holistic approach to security, where both domains are leveraged appropriately to protect critical infrastructure and data. This convergence emphasises the importance of collaboration, communication, and knowledge-sharing between IT and OT teams to effectively address security challenges – something which is historically challenging.

The impact of IT-OT integration

Irrespective of the domain (OT or IT) organisations must establish their security programme on a foundation of comprehensive risk assessment and a solid understanding of vulnerabilities and threats. With OT/IT integration, organisations must additionally risk assess the conduit between the two systems, the Industrial De-Militarised Zone (DMZ). This includes evaluating physical security, network architecture, access controls, and system configurations as well as performing vulnerability scans and penetration tests to help identify weaknesses and allow for proactive remediation. This is further supported by having robust access controls and network segmentation to isolate critical assets which can in turn limit the impact of security breaches and contain potential threats and help prevent unauthorised access to critical systems and sensitive data.

Foundations of an OT security program

Continuous monitoring of both OT and IT environments is essential for early detection and response to security incidents. Implementing security information and event management (SIEM) solutions, intrusion detection systems (IDS), and security analytics enable organisations to detect anomalies, identify potential threats, and respond swiftly to mitigate risks. Appropriate processes for patch management and software updates to address the known vulnerabilities in both OT and IT systems must be considered.

Vulnerabilities that affect OT systems – especially on assets with external connectivity must be validated then considered for remediation and a process followed to determine the appropriate response to the vulnerability; immediate or delayed remediation, compensating controls, or temporary acceptance. Where the risk of a vulnerability is high, and the decision is anything other than immediate remediation, a plan must be established for when a patch should be deployed with metrics maintained against these plans.

Building a security-aware culture

Building a security-aware culture is also crucial for ensuring the effectiveness of security measures and this could be done by implementing comprehensive training programs to employees, covering best practices, security protocols, and potential threats. This will provide them with a sense of responsibility and accountability among staff members and reduce the risk of human error.

Adhering to industry-specific standards

Compliance with industry-specific regulations and standards is essential to ensure the security and integrity of OT and IT systems. Organisations must understand and adhere to relevant security frameworks, such as regulations for the industry under NIS-R, NCSC CAF, the NIST Cybersecurity Framework or industry-specific standards like IEC 62443 for industrial control systems.

The benefits and challenges of convergence

The convergence of OT and IT has brought about significant benefits for industries but has also introduced new security challenges. Effective OT and IT security is crucial to safeguard CNI, sensitive data, and other industrial processes from emerging threats. By adopting a unified approach to security, organisations can bridge the gap between OT and IT teams, fostering collaboration, and sharing expertise. With robust risk assessments, access controls, security monitoring, employee training, and compliance measures, organisations can effectively remediate this risk to acceptable levels.

Our approach to OT security

Our approach to this is simple, we assess, protect, and help you to manage your critical infrastructure safely and securely. We'll work together to create a solid foundation, capable of taking the weight of an ever-evolving technological landscape.

Fujitsu's OT Security services encompass three essential elements:

1. OT assessment and asset discovery

This analyses your existing networks, identifying gaps in compliance and standards, establishing your risk profile, and baselining your networked digital assets.

2. OT network transformation

Applies priority remediations to protect your OT networks.

3. OT managed monitoring service

Provides 24/7 service identifying anomalous behaviours across OT environments.

Each of three complementary services can be ordered and delivered independently based on your maturity and security requirements.

Since 2011 we have been helping clients secure CNI and have been actively supporting OT/IT integration since 2019.

The differences between IT and OT are not only in technology, but also in people, training, organisation, and culture. The convergence of OT and IT has brought about tremendous benefits for industries but has also introduced new security challenges. Effective OT and IT security is crucial to safeguard critical infrastructure, sensitive data, and operational processes from emerging threats. By adopting a unified approach to security, organisations can bridge the gap between OT and IT teams, fostering collaboration and robust risk assessments, access controls, compliance, and security monitoring.

Checklist: things to look for in an OT/IT security partner

When looking for a security partner, consider including the following requirements when contacting suppliers or issuing invitations to tender:

- Verifiable use cases of performing discovery activities including OT asset discovery and security assessment
- Personnel with demonstrable domain experience able to understand your environment, regulatory framework, and unique security context of your environment
- Proven experience in deploying key mitigations for OT environments including but not limited to:
    - Secure remote access
    - Devoted Identity Access Management for OT environment
    - Segmentation of OT networks
    - Boundary protection for the OT network
    - OT Security Governance review
    - Implementation of IDS for OT environments

About Fujitsu

Our Purpose is to make the world more sustainable by building trust in society through innovation.

To fulfill the Fujitsu Group Purpose, we will enhance our ability to stay in tune with global society, while continuing to make agile changes, and creating value. We offer a broad range of products, services and solutions, and have approximately 130,000 employees supporting customers from over 50 countries and regions.

To find out more about Our Approach to OT Security, please email askfujitsu@fujitsu.com and/or +44 (0) 1235 79 7711 and quote 4218.

Contact

Fujitsu
The Lantern
75 Hampstead Road
London
NW1 2PL