www.ibs.com.cy

SECURING CRITICAL INFRASTRUCTURE WITH FORTINET.

The convergence of operational technology (OT) and information technology (IT) has brought significant advancements to industries, but it has also introduced new security challenges. Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are particularly vulnerable to cyber threats from hackers involved in terrorism, cyber warfare, and espionage. Attacks on critical infrastructures like power plants, factories, and transportation systems can have severe consequences for national security, financial stability, and even human lives.

Fortinet has been at the forefront of protecting OT environments in critical infrastructure sectors for over a decade. Their approach involves integrating security measures into complex infrastructures through the Fortinet Security Fabric. This comprehensive solution enables organizations to efficiently protect their OT environments while ensuring compliance with regulations.

The Fortinet Security Fabric for OT Environments relies on multifactor authentication, network segmentation, and micro-segmentation to establish layered security. Quarantine and sandboxing prevent threats before they can cause harm. Continuous analysis of behaviors and intelligence gathering provide insights into known and unknown threats, facilitating proactive mitigation. Central security tools assist with logging, reporting, and analytics, ensuring comprehensive oversight of activities across the system.

Fortinet's ICS/SCADA solution seamlessly integrates OT security with best-of-breed threat protection for corporate IT environments, spanning from the data center to the cloud and network perimeter. This holistic approach offers visibility, control, and automated threat detection within the OT environment. It reduces complexity and operating expenses compared to siloed solutions, ensuring efficient management.

Fortinet provides tailored security solutions for different zones within an industrial environment. The Industrial Zone, where production occurs, is protected by FortiSwitch, FortiAP, FortiPresence, and FortiCamera. Site Operations, the control hub, benefits from FortiGate next-generation firewall appliances, ensuring secure data exchange between OT and IT systems. The Industrial Demilitarized Zone (IDMZ) securely connects networks with different security requirements, employing authentication, business segmentation, sandboxing, and deception detection. The Enterprise Zone, at the corporate level, relies on

Fortinet products to secure crucial business systems and data. The Internet/WAN Zone delivers secure access to cloud-based services and employs strong authentication and VPN tunnels.

Fortinet's comprehensive suite of products and solutions provides the necessary security measures to safeguard critical infrastructures. By implementing the Fortinet Security Fabric and leveraging its capabilities across different zones, organizations can proactively protect their OT environments, mitigate risks, and ensure the continuity and reliability of their operations.

The Fortinet ICS/SCADA Solution Includes:

- Next-Generation Firewall
- Wireless LAN (WLAN)
- Ethernet Switching
- Inline Sandbox Service
- Identity and Access Management
- Central Management
- Analytics, Reporting & Response
- SIEM

In conclusion, Fortinet's expertise in OT security and their integrated approach through the Fortinet Security Fabric offer efficient and effective protection for critical infrastructure. By implementing multifactor authentication, network segmentation, continuous threat analysis, and other security measures, Fortinet enables organizations to safeguard their OT environments and ensure the security, resilience, and sustainability of their operations in today's interconnected world. IBSCY Ltd, as a certified partner of Fortinet in Cyprus, offers fast and professional IT solutions in Cyprus and abroad.

Source