Trustwave®

Operational Technology Services

SECURE OT ENVIRONMENTS FROM PLANNING TO PROTECTION

Benefits

- Gain insights into your current state of OT security across people, processes, and technology and align your OT target state with best practices.
- Coordinate OT security priorities with business goals to baseline your security program.
- Identify exploitable vulnerabilities in IT systems that could impact OT environments for proactive risk mitigation.
- Seamlessly integrate 24×7 IT and OT monitoring to unify analytics, workflows, and visibility.
- Receive real-time monitoring and notification with Trustwave's Global Threat Operations service.
- Bridge security gaps between IT and OT environments for unified risk management.
- Access named Trustwave OT specialists to help translate SOC findings into actionable insights tailored to your environment.
- Layer detection with Trustwave SpiderLabs' unique threat intelligence and research.

Protecting both information technology (IT) and operational technology (OT) environments from evolving cyber threats requires a strategic and proactive approach. As industrial and enterprise systems become more interconnected, organizations face new security challenges that blur the lines between IT and OT. Traditional security strategies often fall short in these environments, where legacy systems, real-time processes, and safety-critical operations must be secure without disrupting production.

At the same time, IT threats such as ransomware, supply chain attacks, and insider threats increasingly pose risks to industrial control systems. Without a comprehensive security strategy that accounts for both IT and OT, organizations may struggle to detect threats early, prioritize vulnerabilities, and respond effectively to incidents.

Trustwave offers three key services to help you strengthen your OT security posture:

1. Trustwave OT Security & Architecture Design
2. Trustwave Penetration Testing an OT Environment
3. Trustwave OT Security Monitoring with Co-Managed SOC

Challenges in Bridging IT & OT

Rapid advances in technology are converging risks that have traditionally been managed in silos, particularly when it comes to integrating IT and OT. As these technologies evolve, they bring in new challenges that require a holistic approach to security:

- **Digital:** Involves aligning data systems, connectivity, and digital tools across both environments. It's critical for ensuring seamless integration and real-time access to relevant data.
- **Physical:** Barriers often arise from differing infrastructure, control systems, and access protocols. These barriers can obstruct streamlined operations and integration across IT/OT teams.
- **Health, Safety, & Environment (HSE):** Integrating IT and OT with HSE policies is critical. Risks stemming from poor integration may have severe consequences for worker safety and environment protection.

From a security perspective, OT shares many similarities with Internet of Things (IoT) technology. Each relies on connected devices and systems, often blending physical and digital realms. Both involve critical infrastructure where downtime or breaches can have significant consequences, and they frequently use legacy systems or lightweight devices with limited security features, making them susceptible to cyber threats.

Trustwave can review and test many types of infrastructure, applications, systems, and endpoints specific to your industry and vertical for OT/IoT: ICS, network devices, SCADA, vehicles, and more.

Trustwave OT Security & Architecture Design

The Trustwave OT Security & Architecture Design service provides you with a tailored roadmap that outlines prioritized activities to strengthen OT security, mature your architecture, and align with industry standards. By identifying critical gaps across people, processes, and technology, it enables you to clearly articulate initiatives and demonstrate ROI on your security investments, driving resilience and long-term value.

Trustwave adopts a four-phase approach:

1. **Information Gathering:** Understand your specific security objectives and existing OT capabilities.
2. **Threat Workshops:** Facilitate threat modelling workshops to outline threats to your OT environment.
3. **Gap Analysis:** Identify gaps between best practices and your current OT security.
4. **Roadmap Development:** Develop a prioritized roadmap tailored to your business priorities and risk tolerance.

The Trustwave OT Security & Architecture Design service is based on industry-leading frameworks such as NIST CSF and ISA/IEC 62443.

Trustwave Penetration Testing an OT Environment

Penetration testing an OT environment is essential for uncovering vulnerabilities, strengthening defenses, and ensuring the resilience of such critical systems. A successful attack on OT systems can disrupt operations, cause safety hazards, and result in significant financial loss, with OT environments often using legacy systems and specialized protocols that are more difficult to secure. The Trustwave Penetration Testing an OT Environment service identifies vulnerabilities unique to OT systems and identifies ways to protect against evolving cyber threats.

Trustwave adopts a four-phase approach:

1. **Planning & Scoping:** Define test objectives and scope to enable a controlled testing process.
2. **Reconnaissance:** Gather insights on your IT and OT environments to identify potential attack vectors.
3. **Testing & Exploitation:** Perform testing activities on in-scope systems within the OT environment.
4. **Reporting:** Identify vulnerabilities and recommendations to mature your IT-OT security posture.

Testing results are also made available in the Trustwave Fusion platform where you can download results in various formats, import results into internal systems via an API portal, and create remediation tickets with ServiceNow and Jira integration.

Trustwave OT Security Monitoring with Co-Managed SOC

As cyber threats increasingly target OT, organizations require stronger defenses to safeguard critical systems. Adding OT Security Monitoring to an existing Co-Managed SOC service provides a compelling way to expand detection coverage to OT environments, reduce risk, and enhance security investments.

Trustwave's 24×7 OT monitoring and strict rules of engagement enable OT operational integrity and safety.

Features:

- **Broad Platform Support:** A variety of SIEM-integrated OT security platforms are supported.
- **Confirmed OT Escalations:** OT alerts are investigated and escalated to a client team member for incident response.
- **Unified Security:** 24×7 IT and OT monitoring are seamlessly integrated to enable unified analytics, workflows, and visibility, where OT alerts are monitored and escalated in tandem with IT threats and context.
- **Trusted OT Advisors:** Named resources with OT experience support service outcomes by translating SOC outputs into your environment.

About Trustwave

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats.

Trustwave's comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes clients' cyber investments, and improves security resilience. Trusted by thousands of organizations worldwide, Trustwave leverages its world-class team of security consultants, threat hunters, researchers, and market-leading security operations platform to decrease the likelihood of attacks and minimize potential impact.

Trustwave is an analyst-recognized leader in managed detection and response (MDR), managed security services (MSS), cyber advisory, penetration testing, database security, and email security. The elite Trustwave SpiderLabs team provides industry-defining threat research, intelligence, and threat hunting, all of which are infused into Trustwave services and products to fortify cyber resilience in the age of inevitable cyber-attacks.

Trustwave®

www.trustwave.com