Trustwave®

OT Security Maturity Diagnostic by Trustwave

AN ASSESSMENT AND ADVISORY SERVICE COVERING STRATEGY, RISK, AND SECURITY MATURITY

Industrial automation and control systems (IACS) used in manufacturing and process automation are increasingly integrated with internal and external company networks. In addition, the continuously evolving convergence of IT/OT increases data transfer between systems and networks, increasing at the same time the susceptibility to cybersecurity risks. Trustwave realizes the constraints in many OT environments and that standard IT security models and frameworks do not fully support these special requirements. Our team will help you baseline your OT cybersecurity posture and roadmap your maturity strategy.

OT Diagnostics to Meet Your Needs

The OT Maturity Diagnostic is technology-agnostic and provides an assessment and advice regardless of whether the organization has decided on an OT security platform. Delivered by Trustwave's experienced cyber advisory team, the maturity diagnostic is based on NIST CSF, and informed by ISA/IEC 62443, and provides a holistic assessment of people, process, and technology as they relate to the OT cybersecurity program goals and requirements of your organization. It helps organizations define their cybersecurity risk posture regarding their OT environment, develop a vision of the desired target state aligned with business objectives and requirements, and outline a strategic maturity roadmap as a prescriptive plan for optimization and continuous improvement.

Trustwave's OT subject matter experts understand that control systems vary greatly from traditional IT infrastructure and have unique requirements and threat landscapes. Our approach to providing security assurance services is tailored to your organization, environment, and level of integration with traditional IT infrastructure to ensure that we're delivering what you need that is also in-line with your risk profile.

How we do it

Trustwave understands that all projects with our clients are important and require appropriate planning and alignment. Therefore, Trustwave follows a clear, consistent, and distinct set of project activities to enable effective and efficient delivery.

An assessment can be undertaken in a relatively short period of time to allow quick feedback to the business regarding risks and recommendations. Our experts take a collaborative workshop approach, enabling findings and recommendations to be discussed in a friendly, informed way with internal teams to maximize learning opportunities and ensure that key parts of the business and operations are engaged in the process.

The final report is tailored to your needs and will leverage established industry maturity operational baselines, identify strengths and opportunities to scale the program while optimizing the value to the business, and develop recommendations that mitigate risk by closing critical gaps and prioritizing areas for improvement.

Benefits

- Gain insight into your current state of OT security across people, process, and technology.
- Align your cyber programs' target state to best practices and established standards.
- Align security and business requirements to baseline the cybersecurity program.
- Identify top risks to generate "quick wins" to help decision-makers mature the organization efficiently & effectively.
- Quick feedback to the business to support wider initiatives, business alignment, and visibility into risks.

What Makes Us Different

Adopting a mature Defense-in-Depth approach to industrial automation and control systems (IACS) is crucial. With advances in technical capabilities and resources of malicious actors and the convergence of OT/IT, it is no longer practical to rely on security through obscurity or air-gapped networks to protect your infrastructure.

Trustwave's OT Security Maturity Diagnostic service offering is based on NIST CSF and ISA/IEC 62443 (Cyber Security Controls for Automated and Control System Environments) and provides an in-depth, holistic assessment of people, process, and technology as they relate to your organization and industry.

Trustwave provides consultancy services to help you to bolster your resilience to threats to your OT environment. Our specialized delivery team has broad experience across the functional domains as well as emerging areas of cybersecurity. In addition, team members have extensive cybersecurity knowledge and experience solving complex security, data, and infrastructure challenges and can articulate issues at the technical and board levels.

Assessment Report

The final report is tailored to your needs with findings and recommendations organized per the enterprise cybersecurity functional risk domains of identify, protect, detect, respond, and recover. This provides a comprehensive, consistent view of your organization's OT cyber risk profile, that includes required activities and desired outcomes, and enhances integration and alignment with broader enterprise risk management processes.

The report is comprised of the following three sections.

Executive Review

This section is intended for executive management and provides a high-level overview and synthesis of report findings and recommendations and allows quick identification of strengths and opportunities.

Gap Analysis and Assessment Details

This section presents the detailed findings and observations regarding the gaps between your current and desired states of maturity. The details help define foundational capabilities and document operational cybersecurity challenges. Operational domain analysis across people, process, and technology, which support the enterprise cybersecurity functional risk categories, provides a more prescriptive plan to empower the organization. Operational analysis includes the following domains:

- Governance & Policy
- Risk Management
- Asset Management
- Identity & Access Management
- Awareness & Training
- Processes & Playbooks
- Monitoring & Detection
- Continuity, Contingency, & Recovery Planning
- Technology & Architecture
- Metrics & Reporting

Roadmap

This section shows you how to get from where you are to where you want to be, in a defined timeframe. The roadmap will help you identify and articulate the vision for advancing the maturity of your OT security program, create actionable steps for achievement, and provide a narrative to obtain stakeholder engagement and define requirements.

Trustwave®

www.trustwave.com