virsec®

Services Overview

Virsec Security Risk Advisory and Assessment Service for ICS/IT/OT Environments

Key Features

- Identify IT/OT security issues before they are exploited
- Reinforce security in critical vulnerable areas
- Maintain the integrity of business-critical services
- Avoid application downtime

Systems Covered

- **ICS:** Industrial Controls Systems
- **SCADA:** Supervisory Controls & Data Acquisition
- **MES:** Manufacturing Execution Systems
- **PLC:** Programmable Logic Controller
- **HMI:** Human Management Interface
- **Hist:** Historian System
- **EW:** Electronic Warefare traditional staffing

Identify vulnerabilities across the critical system stack to prevent breaches

IT/OT systems are exposed more than ever to a variety of threats and are vulnerable to both internal and external attackers. Recent attacks—Triton, Stuxnet, HaveX, BlackEnergy and Industroyer—used advanced hijacking techniques that weaponize at runtime, increasing pressure to harden systems to ensure uptime and safety.

Critical infrastructure systems are increasingly targeted by highly skilled attackers often representing organized syndicates or nation-states. These criminals exploit known and unknown vulnerabilities in unconventional ways—using zero-day attacks and fileless techniques that can persist over months before detection.

Leveraging memory exploits and advanced threats that weaponize at runtime (WRTs), criminals easily bypass conventional security to breach systems, hijack controls and disrupt services.
Most professional assessments and security solutions focus only on identifying specific signatures or patterns commonly at the network level. Unfortunately such solutions lack visibility into critical applications, WRTs and other threats that manipulate trusted tools and code functions to jeopardize services.

Operations and security teams are challenged to understand and immediately patch system vulnerabilities in order to stop advanced attacks at the outset.

Virsec Security Risk Advisory and Assessments helps organizations understand the effectiveness and completeness of critical IT/OT infrastructure security—from the network through the entire composite application system and through to memory. These services provide clear and actionable insight into security strengths and weaknesses throughout your ICS/SCADA environment.

Why choose Virsec for your assessment?

Virsec investigates the full IT/ICS/SCADA infrastructure and security posture to uncover the most critical vulnerabilities. We take an in-depth look at system design and programming, workflows and day-to-day processes and procedures.

Our professional services team enables organizations to determine current infrastructure resilience to attacks such as Stuxnet, Black Energy, Industroyer/Crash Override, as well as sophisticated injection attacks and rogue processes increasingly targeting isolated ICS networks.

Experts closely examine current security policies, procedures, controls and defenses, and conduct uncommon testing. Adherence to NIST, PTES and other security best practices are gauged. Customers receive a detailed report of key findings, areas of concerns and critical gaps in security, with advice on potential remediation strategies.

What to expect

Virsec measures ICS/IT/OT resilience from comprehensive assessment that covers the application infrastructure including compiled and interpreted code, file systems, resources, data input analysis and the supporting network under the stress of complex attacks.

Virsec delivers deep security insight with actionable recommendations for remediation to help your organization strengthen security and minimize risk.

Virsec also enables operations and security teams to make smarter decisions about securing environmental controls, manufacturing systems and critical services, even legacy systems, and potential new investments that improve upon risk management.

Proven methods

Virsec IT/OT risk assessment is based on a proven methodology that includes:

Information gathering
Investigation of system design and programming, workflows and day-to-day processes and procedures

Security assessment
Examination of current security policies, procedures, controls and defenses against commons exploits, WRTs, and evasive uncommon attacks

Technical testing
Assessment of the application to uncover security vulnerabilities and weaknesses

Deliverables
Detailed report summarizing key findings, areas of concerns and critical gaps in security infrastructure with insights on compliance with NIST, PTES and other security best practices, as well as specific actionable remediation strategies.

virsec®

Ask your Virsec rep about Virsec Security Risk Advisory and Assessment Service

Benefits

- Identifies IT/OT security issues before they are exploited
- Increases knowledge and awareness of targeted exploit techniques
- Reveals risks and recommends potential remediation
- Provides suggestions for zero-trust security modeling
- Helps prevent application downtime and ensure operational integrity
- Supports efforts to maintain regulatory and industry compliance

Value Delivered

- Reliable and consistent ICS/SCADA security expertise
- In-region representatives provide dedicated support
- End-to-end and full stack system focus
- Specialized skills and tools for in-depth analysis
- Accurate knowledge of the resilience level for IT/OT systems
- Actionable recommendations to immediately improve security
- Significant cost savings when compared to traditional staffing