MANDIANT

SOLUTION BRIEF

STRENGTHEN SECURITY FOR MISSION CRITICAL OT AND ICS

BENEFITS

With Mandiant, you can activate your OT and ICS cyber defenses:

- Evaluate the effectiveness of your existing OT and ICS security controls against real-world cyber attacks.
- Identify and mitigate security issues across complex OT and ICS environments before an attacker exploits them.
- Prepare your security team to monitor, detect and respond to OT and ICS specific cyber incidents, without risking dangerous impacts.
- Use insights based on global attacker behavior to protect your critical OT and ICS environments.
- Get fact-based advice and comprehensive guidance that empowers you to prevent and detect real-world threats to your critical infrastructure.

To prevent operational disruption from cyber threats, organizations need to extend their cyber defense from IT to operational technology (OT) and industrial control systems (ICS) security. Protecting critical infrastructure requires understanding of relevant cyber threats, rigorous security testing and threat detection and response across the entire enterprise. All organizations across industries and verticals face similar risk with the convergence of IT and OT environments.

TABLE 1. Industry Concerns.

 Manufacturing	 Utilities	 Transportation
• Secure growing set of interconnected IT and OT and ICS environments • Help ensure intellectual property across manufacturing plants and supply chains globally	• Help ensure systems availability at all phases of production and distribution • Identify critical threats upstream, midstream and downstream to protect operations and the connected supply chain • Maintain consistent security across global span of production and distribution	• Reduce risks introduced by IT-OT convergence and digital transformation while limited effects of environmental drift • Maintain compliance and ensure controls are effective • Better understand risk posture to maintain operational efficiency and safety

There has been a rapid growth of OT vulnerabilities since 2010, the year Stuxnet was disclosed. Most vulnerabilities Mandiant tracks in this space appeared after 2010, and an upward trend in their growth is expected.

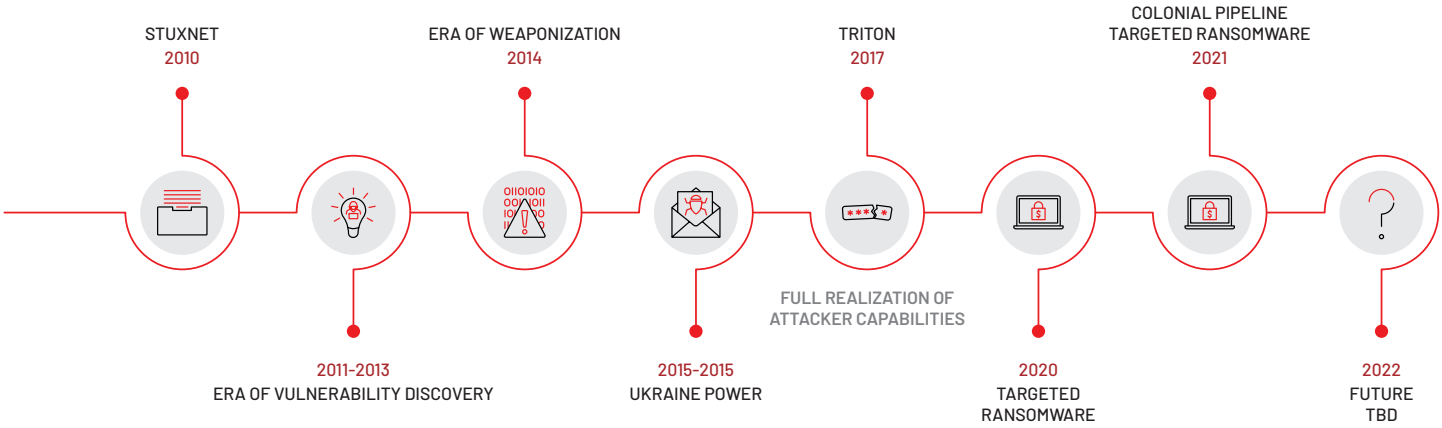

FIGURE 1. All known ICS attacks in the past 10+ years employed basic TTPs, followed the standard attacker lifecycle and used Windows/Linux malware.

How Mandiant Helps Address This Challenge

Mandiant delivers a specialized set of services and SaaS offerings to mitigate the risks to operational technology with the convergence of IT and OT environments. We help you protect those systems through our threat intelligence teams, Managed Defense experts, consultants and training.

We identify both strategic steps and tactical actions to mitigate security risks and improve security defenses across different layers of OT and ICS environments.

Leverage Threat Intelligence

Mandiant Advantage Threat Intelligence Fusion

Takes cyber threat intelligence to the next level. Combine all the benefits of our Security Operations, Digital Threat Monitoring and Vulnerability subscriptions with a deeper understanding of cyber threat trends. This subscription includes cyber physical system threats, via tens of thousands of uniquely crafted financial intelligence reports.

Detect and Respond to Threats

Managed Defense for OT

Technology alone does not fully protect against a determined attacker or accidental misuse. Finding IT talent with OT expertise or OT talent with advanced cyber response experience to secure OT assets can be a daunting task. You need a trusted partner with services specifically tailored for OT and ICS environments to monitor your network around the clock with a pro-active, analyst-driven approach leveraging the latest threat intelligence cultivated from experience.

Incident Response Services and Retainer

Activate the best-in-business response experts to complete in-depth attack analysis, perform crisis management over the complete ransomware attack lifecycle, and help recover business operations after a breach. Establish an IR Retainer to have Mandiant incident response experts on standby with a competitive service level agreement (SLA) option that enables faster and more effective response to cyber incidents.

Assess and Test your OT/ICS Environment

Industrial Control Systems (ICS) Healthcheck

The ICS Healthcheck helps your organization assess its cyber security posture without the operational risk associated with software-based agents, network scanning and other aggressive and invasive assessment techniques.

Embedded Device Assessment

Embedded Device Assessments highlight the strengths and weaknesses of a specific device as well as your team's development process. This assessment addresses specific security aspects of the device based on the current state of its lifecycle, expected use and existing security hardening measures. Mandiant experts work with you to identify and accomplish mutually agreed upon security objectives.

OT Red Team Security Assessment

Mandiant consultants mimic attacker activities and tactics, techniques and procedures (TTPs) to achieve pre-approved objectives, determine risk of compromise of OT, identify gaps in preventive and defensive controls and assess your security team's ability to detect or respond to an attack targeted towards the OT environment without the risk of damage or impact associated with a real incident.

OT Network Perimeter Penetration Testing

Use of network-based penetration testing assesses the risk of attack propagation from a low-trust peripheral network to your core OT and ICS networks. Discover gaps in network segmentation controls and identify remote attack paths that can allow the attacker to breach the protected perimeter for your OT network.

OT Security Monitoring Evaluation (Purple Team)

This collaborative security assessment includes Mandiant experts working with your security team and uses Mandiant Security Validation to emulate threat actor tactics, techniques and procedures (TTPs) that pose the most risk to OT environments, simulate controlled attack scenarios, assess breach detection capabilities across each phase of a targeted OT attack lifecycle. The assessment can provide quantifiable evidence on the effectiveness of breach detection and response capabilities across different layers of the OT environment.

Evaluate your security program

Cyber Security Program Assessment

The Mandiant Cyber Security Program Assessment provides an independent maturity assessment of your organization's ICS/OT security program across four core critical areas: security governance, ICS security architecture, cyber defense and security risk management. After an in-depth, collaborative analysis of your existing program, we provide best practice recommendations to improve your security posture based on your specific risk profile and level of security maturity.

Educate Your Team with Mandiant Academy

Fundamentals of Industrial Control Systems (ICS) Security

Become familiar with OT and ICS security concepts, secure architecture, threat models, security standards and best practices. The course includes discussions around today's security trends and the current threat landscape.

Digital Forensics and Incident Response for Programmable Logic Controllers (PLCs)

Attacks against ICS are on the rise. To effectively respond to this emerging threat, organizations must be aware of the challenges that come along with performing digital forensics and incident response (DFIR) for ICS. In this course, ICS security personnel learn to identify and understand threats targeting ICS devices that use embedded operating systems.

Conclusion

Mandiant offers frontline experience in cybersecurity with a deep functional knowledge of industrial control systems gained through decades of hands-on work in ICS and OT environments. Backed by Mandiant Advantage Threat Intelligence and expansive knowledge of attacker behaviors, our OT experts conduct advanced security testing to help industrial organizations improve mitigation and detection capabilities across end-to-end OT networks.

Learn more at **https://www.mandiant.com/solutions/operational-technology**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT