MANDIANT

DATASHEET

PROACTIVE SECURITY FOR OPERATIONAL TECHNOLOGY

Mitigate and detect attacks on mission-critical industrial operations

BENEFITS

- Evaluate the effectiveness of your existing OT security controls against targeted and advanced cyber attacks
- Identify and mitigate security issues across end-to-end OT environments before an attacker exploits them
- Prepare your security team to monitor, detect and respond to OT-specific cyber incidents
- Use insights based on global attacker behavior to protect your complex OT and ICS environments.
- Get fact-based recommendations and comprehensive guidance that empowers you to prevent and detect real-world threats to your critical infrastructure

Operational technology (OT) and industrial control systems (ICS) support a range of national critical infrastructure such as power and utilities, oil and gas, transportation, manufacturing, resource mining and telecommunications. Protecting critical infrastructure requires rigorous security testing conducted from the perspective of advanced attackers targeting those environments.

Mandiant Proactive Security for OT combines frontline Mandiant experience in cyber security with a deep functional knowledge of ICS gained through decades of hands-on work in ICS and OT environments. Backed by world-leading Mandiant threat intelligence and unrivaled 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.

Service Overview

Proactive Security for OT is designed to help our customers identify both tactical actions and strategic steps to mitigate security risks and improve security defenses across different levels of OT environments.

Each engagement is tailored to the unique assessment requirements of the client and designed to have zero unintentional impact on critical operations in production. Mandiant consultants assess OT assets for high risk security issues, evaluate existing security controls for effectiveness and provide fact-based guidance to improve the overall security posture of the industrial environment.

TABLE 1. Offerings available through Proactive Security for OT.

Service Offering	Description
OT Red Team Security Assessment	Simulation of a real-world OT-directed attack scenario relevant to your industry or organization, without the risk of damage or impact associated with a real incident. 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.
OT Network Perimeter Penetration Testing	Use of network-based penetration testing to determine the risk of attack propagation from a low-trust peripheral network (such as corporate office, remote site or field network) to your core OT/ICS network. This assessment is performed from the perspective of an attacker that has a foothold on the peripheral network, in order to 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 Production Network Penetration Testing	Use of passive information gathering techniques and non-intrusive manual testing to identify common security vulnerabilities in your production OT network. Mandiant ICS experts work closely with your process control team to identify common security issues and potential attack paths in the production OT network, without introducing the risk of using unchecked network scanning or intrusive penetration testing tools.
OT Laboratory-Based Component Testing	In-depth (intrusive) security testing for a specific OT component in a non-production environment (such as a development area or laboratory setting). The objective of this test is to find security weaknesses, validate the existence of a vulnerability using active exploitation and determine the level of real-world risk it presents to your OT infrastructure. Examples of OT components include embedded device, operating system, software application, radio interface or communication protocol.
OT Security Monitoring Evaluation (Purple Team)	Purple teaming is a collaborative security assessment in which Mandiant experts work with your security team to simulate attacker activities that pose the most risk of OT environment compromise. This assessment uses Mandiant Advantage Security Validation to emulate threat actor TTPs seen across different phases of OT attack lifecycle and provide quantifiable evidence for the effectiveness of breach detection and security monitoring capabilities for OT.

WHY MANDIANT FOR OT

- Goal-oriented, real-world approach focused on assets critical to your business and operations
- Multi-skilled red team covering specializations for diverse processes and technologies across both IT and OT networks
- Imitations and real-world TTPs pulled from attacker groups Mandiant investigates firsthand
- Context derived from frontline experience across different industries and OT-specific threat intelligence

Learn more at **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