MANDIANT®

DATA SHEET

Offensive Security for Operational Technology

Mitigate and detect attacks on mission-critical industrial operations

BENEFITS

- Evaluate the effectiveness of your existing OT security controls against real-world cyber attacks
- Identify and mitigate security issues across complex OT environments before an attacker exploits them
- Prepare your security team to monitor, detect and respond to OT-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

Cyber threat actors continue to evolve their attacks to bypass protections for operational technology (OT) and industrial control systems (ICS). Protecting critical infrastructure requires rigorous security testing conducted from the perspective of advanced attackers targeting those environments.

Mandiant Offensive Security for OT combines frontline Mandiant experience in cyber security with a deep functional knowledge of control systems gained through decades of hands-on work in ICS and OT settings. Armed with world-leading Mandiant threat intelligence and unrivaled knowledge of attacker behaviors, our OT experts conduct advanced security testing and help you effectively mitigate, detect and contain threats across end-to-end industrial networks.

Service Overview

Mandiant Offensive 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 layers of an OT or ICS environment.

Each engagement is tailored to the unique assessment requirements of each client and ensures zero operational impact to high availability network segments. Mandiant consultants assess critical OT assets for high risk security issues, evaluate existing security controls for effectiveness and provide guidance to improve the overall security posture of the industrial environment.

Table 1. Offerings available through Offensive Security for OT.

Service Offering	Description
OT Scenario Based Attack Simulation (Red Team)	Simulation of an OT-specific attack scenario relevant to your industry or organization (typically originating from the Internet), without the risk of damage or impact associated with a real incident. Mandiant consultants mimic attacker activities and TTPs observed in the real world to determine security risk to OT, identify gaps in preventive and defensive controls and assess your security team's ability to respond to an attack targeted towards your OT environment.
OT Network Segment Penetration Testing	Use of a targeted penetration test to determine the risk of attack propagation from a low-trust peripheral network (such as an office, corporate 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 Manual 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 a production OT network, without introducing the risk of using active network scanning or intrusive penetration testing tools.
OT Component/ Embedded Device Security Testing	Comprehensive security testing for a specific OT component in a non-production environment (such as a development area or laboratory setting) to find complex security weaknesses, validate the existence of a vulnerability using active exploitation and determine the level of 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)	Collaborative assessment in which Mandiant experts work with your security team to simulate controlled attack scenarios and assess breach detection capabilities across each phase of a targeted OT attack lifecycle. This assessment uses Mandiant Security Validation to emulate threat actor TTPs that pose the most risk to OT environments and provides quantifiable evidence on the effectiveness of breach detection and response capabilities across different layers of the OT environment.

WHY MANDIANT SOLUTIONS FOR OT

- Security specialists with over 100 years of combined experience across OT and ICS environments
- 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

To learn more about Mandiant Solutions, visit **www.FireEye.com/mandiant**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®