MANDIANT

SOLUTION BRIEF

PROACTIVE SECURITY FOR OPERATIONAL TECHNOLOGY

Operational Technology (OT) and Industrial Control Systems (ICS) have long been used in industrial environments to monitor and automate physical processes and mission-critical operations. These systems form the foundational building blocks for some of our most critical infrastructure and support essential societal functions, such as power generation, wastewater treatment, public transportation, industrial manufacturing, resource mining, oil and gas, and telecommunications.

The last decade has seen a gradual uptick in global cyber threat actor motivation for targeting special-purpose OT networks. This trend is expected to accelerate in the current decade. The rising threat profile is based on a combination of factors but primarily driven by the iterative advancement of physical automation and digital communication at multiple levels of industrial operations. The growing level of automation and connectivity has broad benefits for efficiency, reliability, and productivity; however, it also has an unintended consequence of increasing cost-benefit for OT threat actors.

The advancement in industrial automation is also coupled with the increasing use of standard communication technologies that support off-the-shelf integration between OT networks and external networks. This often translates to enterprise-level collaboration between an operator's OT network and the parent organization's IT network. The provision of remote communication paths between IT and OT means that Internet-connected IT devices can often be used as pivot points to propagate into OT networks and attempt remote compromise of previously unreachable industrial control system devices.

In this context of increasing cost-benefit for cyber threat actors and growing threat profile for OT, Mandiant recommends that governments and critical infrastructure organizations enhance their preparedness to protect industrial networks and operational technology environments from both opportunistic and motivated cyber-attacks.

Proactive Security for OT and Critical Infrastructure

Proactive security assessments, such as Red Teaming and Penetration Testing, that involve real-world simulation of adversary techniques, have proven to be invaluable methods for uncovering critical security issues and high-risk attack paths in enterprise environments. However, such assessments, if performed using traditional techniques, without considering the differences between IT and OT environments can often produce superfluous, irrelevant and unactionable results, or worse, introduce unacceptable risks to real-time operations in OT environments. The testing methodologies for proactive security assessments in OT networks need to account for the unique characteristics of industrial control system environments, with particular emphasis on real-time nature of operations and safety-critical concerns for physical processes controlled by these systems.

Proactive security assessments for OT should incorporate the following fundamental guiding principles:

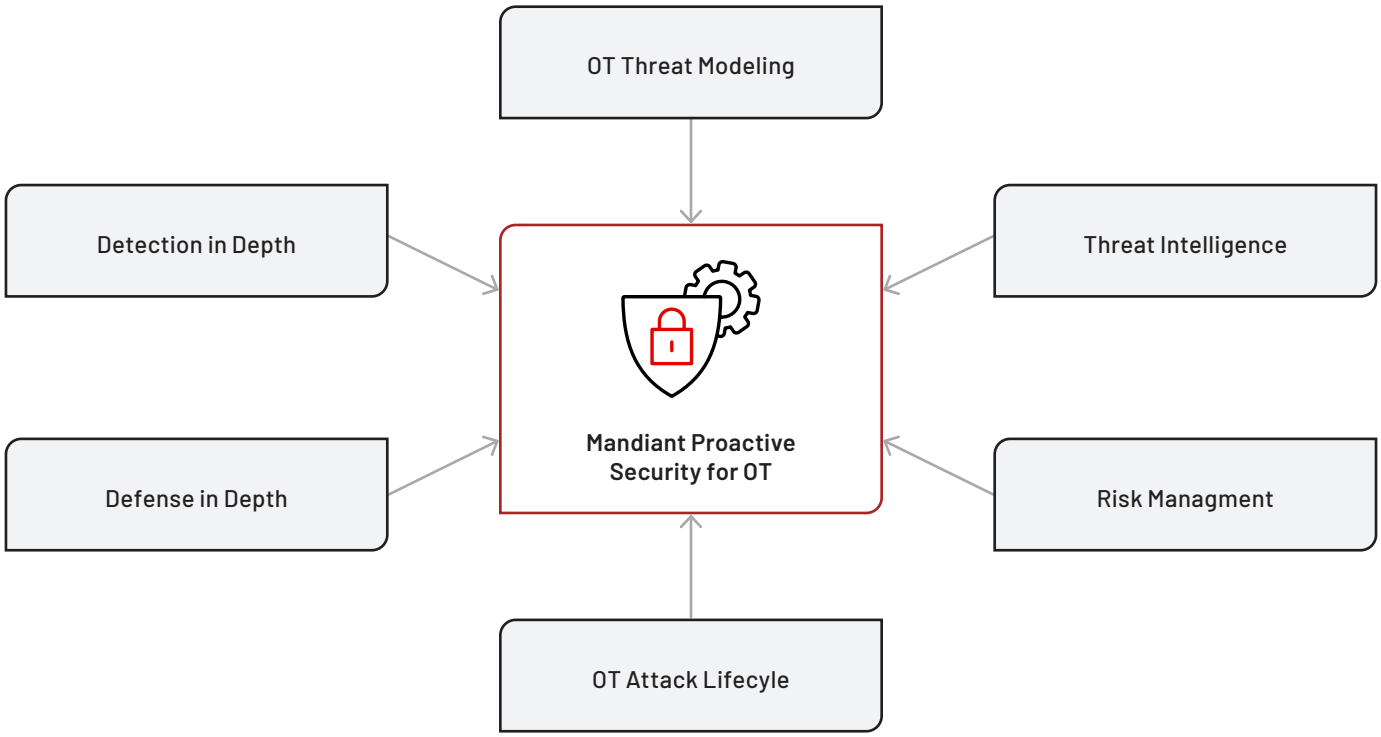

FIGURE 1. Fundamental building blocks for the Mandiant approach towards proactive security for operational technology.

OT Threat Modeling

Each OT network is acutely tailored to achieve the specific objectives of its industrial operation, and often includes a multitude of local area network segments, disparate or remote geographical sites, state dependent configuration settings, proprietary network communication protocols and special purpose embedded devices. Threat modeling can help organizations identify context-specific attack scenarios, discard irrelevant assumptions for the operating environment, establish constraints and requirements for OT specific adversarial testing and formulate a risk-prioritized plan that covers attack vectors end-to-end across the OT environment.

Threat Intelligence

Not every OT environment has the same threat profile. The size of the organization, critical infrastructure industry sector, area of operations, geopolitical landscape, threat actor motivations and evolving attacker techniques, can all play a part in defining the current threat profile of a critical infrastructure organization. In the context of proportionate prevention and response, threat intelligence forms an essential element for prioritizing of relevant proactive efforts and informed decision-making for cost-effective mitigation of cyber security risks.

Risk Management

OT networks support mission critical industrial operations and are comprised of high availability network segments with zero allowance for unintentional disruption of real-time operations. Security assessments of OT networks need to incorporate stringent risk management techniques that minimize the potential impacts to critical operations in a production environment. Testing must consider both safety-critical (engineering) and operations-critical (business) constraints within the target environment. This often involves strategic preparation, strict rules of engagement, delineation between critical and non-critical segments, partial or even full simulation in a non-production environment and customized OT-specific techniques or toolsets.

OT Attack Lifecycle

Just because an attacker can exploit a specific issue and gain unauthorized access to a critical system in OT does not mean they can cause a successful end-stage high-consequence event in the industrial environment. On the other hand, seemingly low-risk issues can often be chained together to achieve a high-gain adversarial objective, so proactive testing is not limited to identification of standalone security issues. Testing can help uncover end to end attack chains and assess impact to operations and business (without undue exaggeration or presumed mitigation). It is also important for identifying actionable mitigation efforts or alternative compensating controls that can increase the cost for attack progression and OT-specific mission completion.

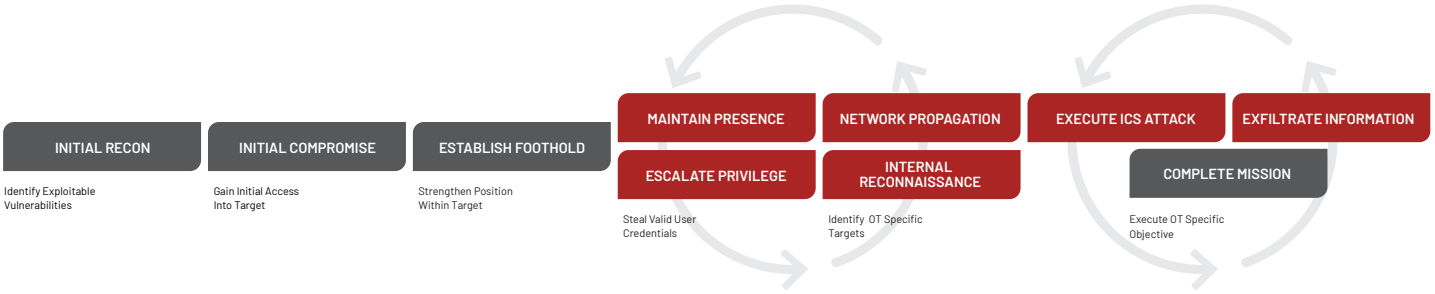

FIGURE 2. Targeted attack lifecycle for OT.

Defense in Depth

Security assessments for OT environments usually focus on network segmentation and perimeter defenses, but often neglect security weaknesses and preventive controls within the core industrial environment. Perimeter protection alone cannot defend OT networks in increasingly connected environments. Organizations must adapt to evolving attack surfaces. They must adopt an inclusive defense-in-depth approach to analyze security gaps across OT networks and integrate preventive measures across multiple levels of the control system architecture.

Detection in Depth

Security monitoring and incident response are critical to OT network security, where implementation of preventive controls or remediation of security vulnerabilities are often sidelined by competing priorities and operational requirements. Security assessments must also cover preparedness and evaluation for breach detection and incident response capabilities across OT networks.

Application across OT Environments

The Mandiant portfolio of proactive security service offerings for OT provides evidence-based technical assurance and high-value security assessments. These service offerings help customers identify both tactical actions and strategic steps for the mitigation of existing security risks and the implementation of actionable threat-specific defenses across different zones or multiple levels of end-to-end OT environments (Fig. 3).

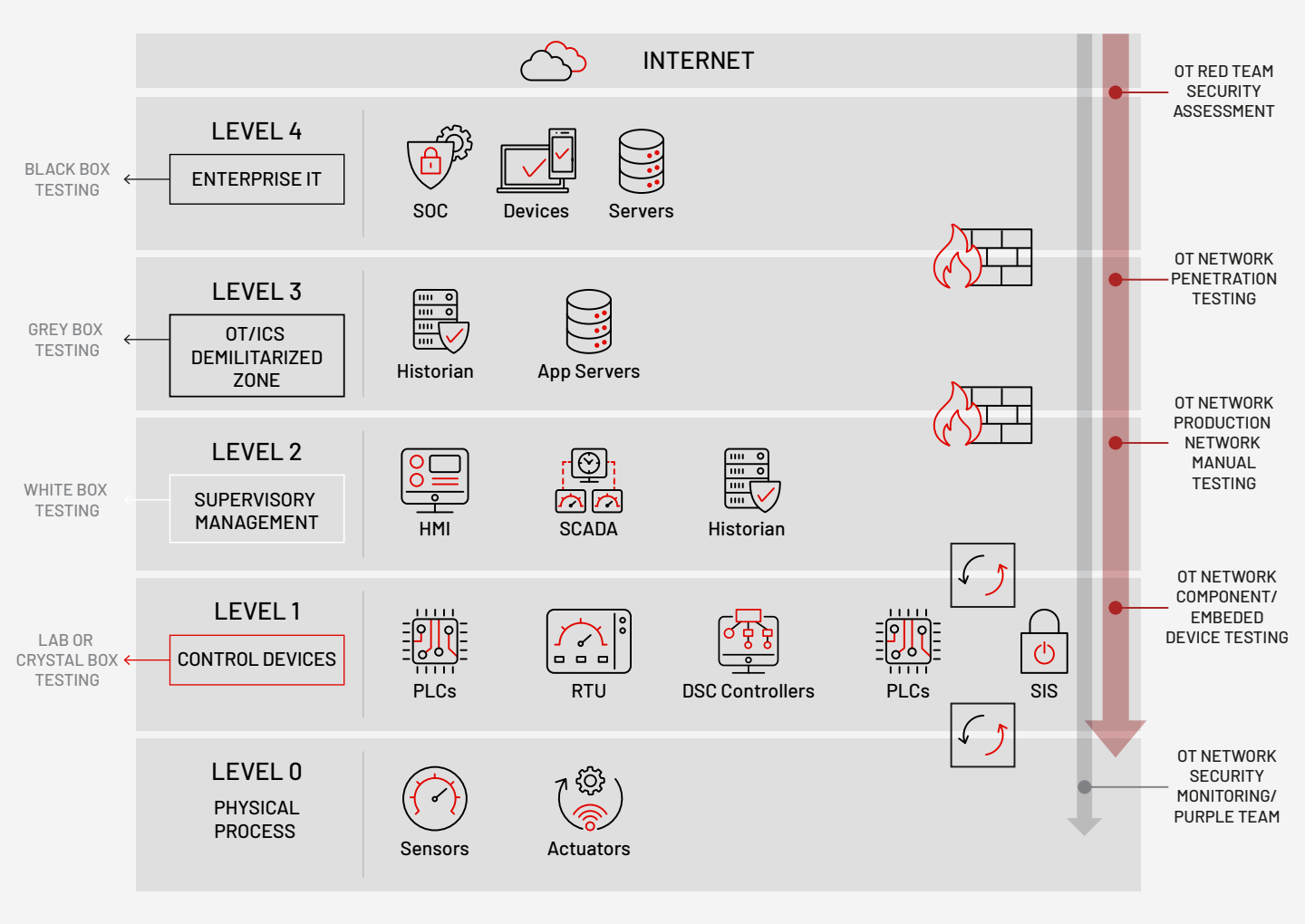

FIGURE 3. How Mandiant proactive security service offerings map to OT environments.

TABLE 1. Industry application of Mandiant proactive security service offerings.

Power & Utilities	Transportation	Manufacturing, Oil & Gas	Telecommunications
• **Red Team Security Assessment** for remote access and forced shutdown of an electric smart meter in a distributed smart grid environment. • **Network Perimeter Penetration Testing** from an insecure field service device at a substation to the core network for an energy and distribution management system. • **Production Network Manual Testing** for SCADA network at a wastewater treatment plant. • **Embedded Device Security Testing** for remote terminal unit (RTU), smart meter, smart inverter, remote sensors and field network cellular gateway devices.	• **Red Team Security Assessment** for remote access and ransomware attack on human machine interface (HMI) workstations at an operations control center for communication-based train control system (CBTC). • **Network Perimeter Penetration Testing** from a wayside communication network to back-office network for an automatic train supervision system. • **Production Network Manual Testing** in an OT environment for a driverless train control system • **Embedded Device Security Testing** for on-board vehicle control system, remote telematics gateway, rail signaling equipment and HMI Software.	• **Red Team Security Assessment** for unauthorized manipulation of configuration files on process controls and product validation stations in an industrial manufacturing environment. • **Network Perimeter Penetration Testing** from corporate network at a central office to process control network at a remote manufacturing plant. • **Production Network Manual Testing** for SCADA systems at a resource mining and processing plant. • **Embedded Device Security Testing** for safety instrumentation systems (SIS), programmable logic controller (PLC) and ICS communication protocols used in manufacturing environments.	• **Red Team Security Assessment** for interception of call data records, voice calls, SMS and user plane communications on a 4G/5G cellular network. • **Network Perimeter Penetration Testing** from RAN/backhaul network to 5GP/EPC core network. • **Production Network Manual Testing** for systems and devices in 4G/5G core network and network management system. • **Embedded Device Security Testing** for backhaul equipment , distributed base station, telecommunication software and signaling protocols (UDP, TCP, SCTP, etc).

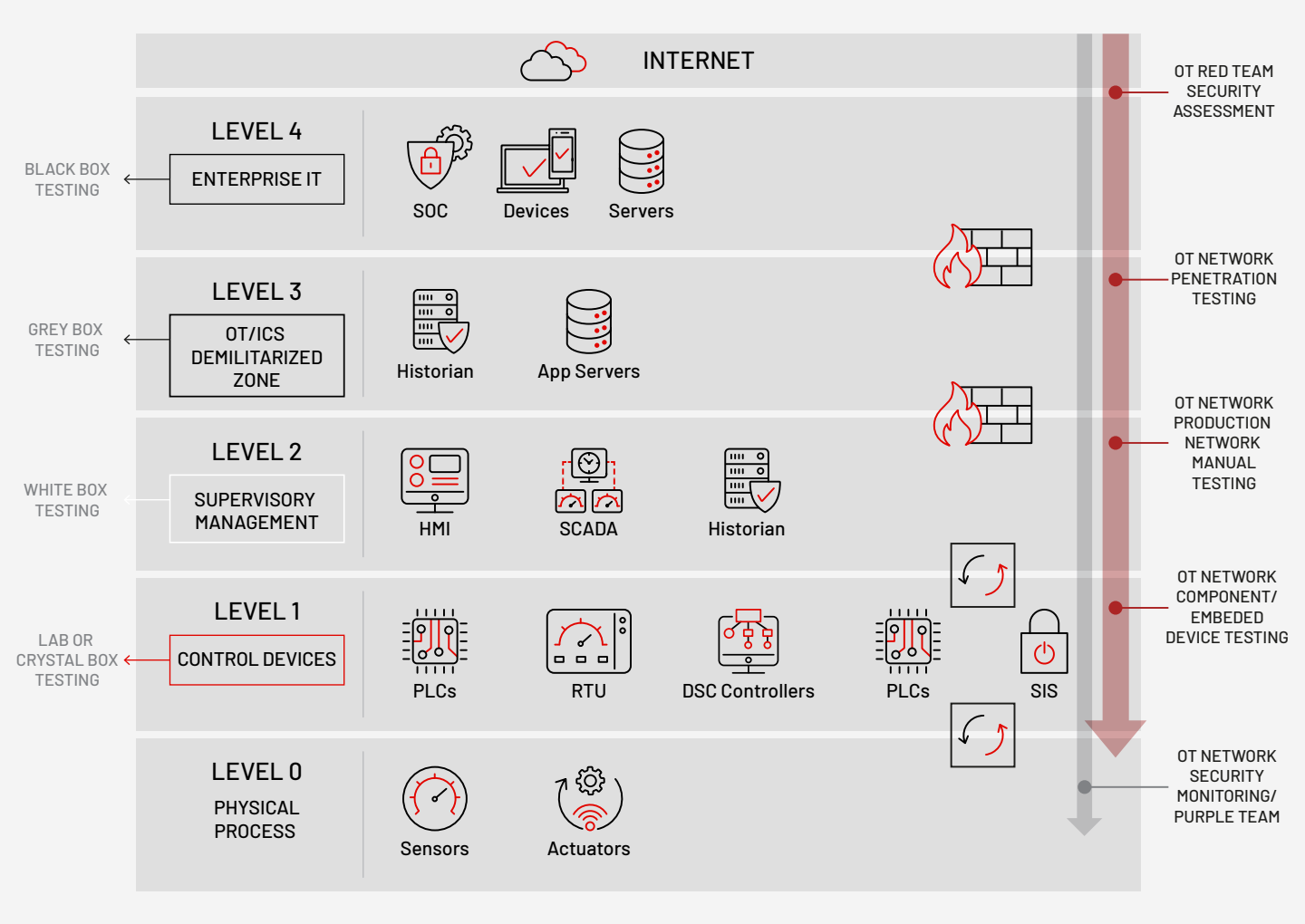

FIGURE 3. How Mandiant proactive security service offerings map to OT environments.

Power and Utilities

- Red Team Security Assessment for remote access and unauthorized shutdown of targeted electric smart meters in a distributed smart grid environment.
- Network Perimeter Penetration Testing from a remote terminal unit at an electric substation to the core network for an energy and distribution management system.
- Production Network Penetration Testing for SCADA network at a wastewater treatment plant.
- Laboratory Based Component Testing for power control system, remote terminal unit (RTU), smart meter, smart inverter, remote sensors and field network gateway devices.

Transportation

- Red Team Security Assessment for remote access and ransomware attack on HMI workstations at an operations control center for communication-based train control system (CBTC).
- Network Perimeter Penetration testing from a wayside communication network to back-office network for an automatic train supervision system.
- Production Network Penetration Testing in an OT environment for a driverless train control system.
- Laboratory Based Component Testing for on-board vehicle control system, remote telematics gateway, signaling equipment and HMI software.

Manufacturing, O&G

- Red Team Security Assessment for remote access and unauthorized manipulation of configuration files on process control stations in an industrial manufacturing environment.
- Network Perimeter Penetration Testing from corporate network at a central office to process control network at a remote manufacturing plant.
- Production Network Penetration Testing for SCADA systems at a resource mining and processing plant.
- Laboratory Based Component Testing for safety instrumentation systems (SIS), programmable logic controllers (PLC) and distributed control systems (DCS).

Telecommunications

- Red Team Security Assessment for remote compromise of call data records (CDR) and interception of voice calls, SMS and user plane communications in a 4G/5G cellular environment.
- Network Perimeter Penetration Testing from RAN/backhaul network to core Telco network (EPC/5GC).
- Production Network Penetration Testing for systems and devices in 4G/5G core network and network management system (NMS).
- Laboratory Based Component Testing for backhaul network devices , distributed base station, cellular network nodes and telecommunications signaling protocols.

FIGURE 4. Example case studies for Mandiant proactive security service offerings for OT.

OT Red Team Security Assessment

Red Team Security Assessment for OT involves the simulation of a real-world OT-directed attack scenario. This assessment is performed within the confines of strict rules of engagement and pre-approved attacker objectives. The goal is to assess the effectiveness of the organization to proactively detect and respond to advanced attackers, while simultaneously testing the preventive and defensive controls around different levels of OT environment. Mandiant consultants mimic advanced persistent threat actors with OT-specific objectives. This gives the customer real-world experience defending and responding to the most advanced industry specific attacks without the potential damage or impact associated with a real incident.

Purpose

- Determine risk to OT by assessing the capability of existing security controls and incident response procedures to protect OT in a targeted multi- phase attack scenario
- Raise awareness of OT specific risk using a real-world attack simulation, without the damage or impact associated with a real incident

Differentiators

- Objective-oriented and industry specific, focusing on high-risk attack scenarios against assets critical to business and industrial operations
- Imitations and real-world tactics, techniques and procedures (TTPs) pulled from attacker groups investigated by Mandiant
- Custom-built command-and-control (C2) infrastructure and tooling
- Multi-skilled red team covering expert knowledge and real-world experience across a diverse set of technologies and industries
- ICS specialists with extensive experience of working in OT and industrial control system environments

Mandiant Approach

- De-chained (phase by phase checkpoint based) execution across different levels of OT networks
- Define and agree upon rules of engagement and requirements across each phase of the exercise
- Emulation of real-world C2 traffic that is representative of targeted attack lifecycle and MITRE ATT&CK Framework
- Latest attacker techniques designed to evade detection and gain remote access to target OT network
- Step-by-step walk through for client security team across each phase of the attack simulation

BENEFIT

- Test your security team's ability to respond to an attack targeted towards OT, without the occurrence of a real incident
- Identify gaps in existing security controls across different levels of an OT network
- Enhance detection and response processes for advanced persistent threat attack vectors
- Prepare your security team to defend against an OT-specific attack scenario
- Know whether your critical operations are at risk and get fact-based recommendations for improving security posture of end-to-end OT environments

OT Network Perimeter Penetration Testing

OT Network Perimeter Penetration Testing allows critical infrastructure organizations to validate perimeter security controls for OT and evaluate the risk of attack propagation from a low-trust peripheral network (such as office network, remote site, field network or radio network) to a high-trust OT DMZ or OT core network. Mandiant typically begins this assessment by connecting to an initial foothold on the peripheral network and attempting to breach the protected perimeter for the target OT network. Testing in this assessment is aimed at the identification of attack paths and gaps in network segmentation controls, while active exploitation of OT components is restricted to prior approval and close coordination with relevant stakeholders.

Purpose

- Determine the risk of attack propagation from a low trust peripheral network (such as IT network, field network or remote site) to a core OT network
- Test and enhance network segmentation controls that protect core OT network from targeted attacks originating in peripheral and remote interconnect networks

Differentiators

- Track record of successful penetration tests for OT networks across every major critical infrastructure industry sector
- Evidence backed assessment—not a "check the box" exercise
- Imitations and real-world TTPs pulled from attacker groups investigated by Mandiant
- ICS specialists with extensive experience of working in OT and industrial control system environments

Mandiant Approach

- Penetration testing from the perspective of an attacker that has an initial foothold on the peripheral network with the stated objective to gain remote access to a core OT network
- Identify security vulnerabilities on interconnect nodes
- Evaluate communication paths between peripheral networks and OT networks
- OT-specific exploitation performed under authorization and close coordination with appropriate stakeholders from client organization

BENEFIT

- Discover weaknesses in network segmentation controls that can allow perimeter breach of a high-trust core OT network.
- Identify security vulnerabilities on systems and applications in peripheral network that have an interconnect communication path to a service or node in an OT network.
- Improved capability to set compensating controls and network monitoring for ICS attacks originating from external networks

OT Production Network Penetration Testing

Traditional methods for uncovering common security vulnerabilities (such as network wide scanning and black box active testing) can introduce unacceptable risks to continuous operation of mission critical nodes in OT environments. Vulnerability assessment in production networks must use risk-conscious techniques for information gathering and service enumeration. Mandiant uses a combination of passive information gathering techniques and non-intrusive manual testing for the identification of common security issues on production nodes in OT network. Mandiant OT experts work with the process control team to model end-stage attack paths that can allow an attacker to compromise nodes at the control system level or cause high-consequence events attributable to real-world attackers targeting physical processes controlled by OT networks.

Purpose

- Discover common security vulnerabilities in a running production OT network, without introducing the risk of using intrusive active network scanning or penetration testing tools
- Identify attack paths within the core OT network that can allow an attacker to compromise control of critical process control systems.

Differentiators

- Consultants who speak the language of OT and work directly with the engineers responsible for OT to adapt cyber security best practices that are suitable for your specific ICS environment
- Motivated by security best practices to help secure OT systems
- Context derived from frontline threat and machine intelligence
- ICS specialists with extensive experience of working in OT and industrial control system environments

Mandiant Approach

- Use of safe passive information gathering and service enumeration techniques
- Use of open source and custom-built tools for pre-approved non-intrusive safe checks
- Stakeholder approval and four-way stops for all active testing in production OT network
- Tabletop assessment to identify attack paths that can allow an attacker to compromise critical nodes at level 2 and below and achieve end goals attributable to real-world attackers targeting OT networks

BENEFIT

- Identify common security vulnerabilities on systems and devices in a production OT network
- Uncover hardening opportunities to be addressed by system, software, or application vendor
- Discover high risk components that merit further testing in a non-production lab environment
- Connect the outcomes (attack paths) produced in a corollary red team or penetration test exercise to OT specific end goals (physical impact or manipulation of industrial control process)

OT Laboratory-Based Component Testing

Threat modeling and attack simulation can often highlight the need for more intrusive testing of specific OT components or embedded systems. Examples of OT components can include a PLC, RTU, HMI application, ICS protocol or purpose-built embedded system in the operational environment. Mandiant recommends performing in-depth testing in a laboratory or non-production environment to avoid operational impact or cascading problems in the production environment. Mandiant uses a combination of open-source and custom developed software and hardware tools to identify security issues in the target component, validate the exploitability of an issue, determine the level of risk it presents to safety, operations or business and identify mitigating or compensating controls that can be used to reduce the risk of a high-consequence event in the OT environment.

Purpose

- Discover security issues and exploitable vulnerabilities in a specific high-risk component in the OT network (embedded device, operating system, software application or communication protocol)
- Perform comprehensive assessment and validation (including intrusive testing and exploit demonstration) that is often not possible in a running production OT environment.

Differentiators

- Multi-skilled red team with proven track record of testing special purpose embedded systems, firmware, software, network protocols and ICS field devices
- Evidence-backed assessment with particular focus on exploitability, impact to OT and risk.
- In-house capabilities for reverse engineering, protocol fuzzing and other techniques
- ICS specialists with extensive experience of working in OT and industrial control system environments

Mandiant Approach

- Dependent on the type of component in-scope for the assessment
- Understand the threat model for the component's typical deployment scenario in OT network
- Use of a combination of hardware and software tools to conduct a comprehensive assessment
- Exploit development to demonstrate the impact of high-risk issues
- Provide recommendations for short-term fixes and long-term improvement.

BENEFIT

- Identify security vulnerabilities in the OT component, validate practical exploitation of known issues, and determine the level of risk each issue presents to your OT infrastructure
- Identify security issues, controls and behaviors that need to be addressed by the device vendor or application developer
- Reduce the risk of compromise of a critical component and identify compensating controls that can be utilized at both network level and device level

OT Security Monitoring Evaluation (Purple Team)

During a purple team assessment, Mandiant consultants work with the client organization's security team to identify gaps in active and passive monitoring controls and enhance breach detection indicators for attacker activities that pose the most risk for compromise. This assessment uses Mandiant Advantage Threat Intelligence and Mandiant Advantage Security Validation to simulate threat actor TTPs across different phases of OT attack lifecycle. Each exercise is designed to assess and optimize monitoring controls for current and evolving attack vectors across industrial networks. The assessment allows the client security team to provide quantifiable evidence of response effectiveness with respect to cyber security incidents and targeted attacks on OT infrastructure.

Purpose

- Evaluate and enhance security monitoring and breach detection capabilities for existing and emerging threats against OT environment and industrial operations
- Test and tune technical defenses to improve breach detection capabilities across the OT environment without introducing additional risk to critical operations.

Differentiators

- Consultants who speak the language of OT and work directly with the engineers responsible for OT to adapt cyber security best practices that are suitable for your specific ICS environment.
- Use of Mandiant Advantage Security Validation to quantify security effectiveness
- Imitations and real-world TTPs pulled from attacker groups Mandiant investigates first-hand
- ICS specialists with extensive experience of working in OT and industrial control system environments

Mandiant Approach

- Use Threat Intelligence and Mandiant Security Validation to simulate attacker TTPs for the most relevant and realistic attack scenarios for your organization
- TTPs mapped against targeted attack lifecycle and MITRE AT&CK Framework
- Mandiant consultants closely collaborate with your security operations team at each phase of the exercise
- If an action is not detected, help the client's team to optimize existing monitoring controls to improve detection for that action

BENEFIT

- Identify high-risk gaps in your active and passive monitoring controls
- Scoreboard before and after exercise to quantify immediate improvements to your monitoring, detection, and response capabilities
- Short-term improvements and long-term recommendations
- Improve your organization's ability to respond to attacker techniques that pose the most risk to your industry or sector.

Conclusion

Mandiant draws on extensive experience in providing security services to global organizations, which includes the delivery of world-leading incident response, threat intelligence, technical assurance, managed defense and frontline research, to deliver end-to-end proactive security service offerings for critical infrastructure and OT environments.

OT specialists work with customer teams from multiple departments across client organizations, including control engineering, network engineering, information technology, process automation, operations and maintenance, to develop a comprehensive understanding of the OT environment, build a detailed assessment plan for proactive security testing and adopt an OT-specific risk-conscious approach to deliver high-value outcomes throughout the engagement.

For more information, please visit **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