FORTRA®

Manufacturing Sector

Red Teaming to Safeguard Intellectual Property & Operational Technology

Background

A high-tech manufacturing firm commissions a red team engagement to proactively test its readiness against targeted attacks. The firm is active in industrial automation and advanced components, and relies on proprietary designs, digital manufacturing workflows, and legacy OT systems. It understands its vulnerability to compromises aimed at IP theft and production disruption, and it wants to test its ability to detect, investigate, and respond in real-time.

Phase 1: Initial Access Operations

The Red Team begins by gathering necessary intelligence on the manufacturer's employees, internal systems, vendors, and third-party ecosystems. This includes the software supply chain, physical supply chain, retailers, and SCADA systems.

- **Reconnaissance:** They discover a public-facing vulnerability in a newly internet-connected SCADA system.

- **Spear Phishing:** An AI-crafted email is sent to the Manager of Manufacturing requesting an immediate update, seemingly from the Head of Operations. The update details are contained in a (malicious) downloadable document. Using **Outflank Security Tooling's (OST's)** PE Payload Generator and Office Intrusion Pack, they create a payload that will detonate upon the attachment opening.

- **Web Drive-By Attack:** The Red Team also injects malicious code, embedded in product descriptions, into the company's customer-facing website.

Phase 2: Lateral Movement & Privilege Escalation

After gaining initial access to the manufacturing company's systems, Red Teamers move laterally to compromise additional systems and escalate privileges.

- **Credential Harvesting:** Hashed credentials are extracted from compromised databases using OST's Credential Pack.

- **Lateral Movement:** Leveraging OST's Lateral Pack, they move swiftly across internal architecture and through the network to access sensitive intellectual property and stored trade secrets.

- **Privilege Escalation:** By exploiting an overlooked vulnerability in a vendor API, Red Teamers escalate to admin privileges and position themselves to gain access to even more data.

Phase 3: Maintaining Persistence & Evasion

To maximize damage and data exfiltration, the Red Team employs a range of techniques to maintain persistence in the system.

- **Quiet Transmission:** Communication with their **Cobalt Strike** C2 server is maintained and hidden via a custom C2 channel leveraging the internal communication tools the target company uses.

- **Asynchronous Communication:** Red Teams avoid detection by asynchronous communication, a style that allows commands to be placed in a queue and executed when Cobalt Strike Beacon checks in. This low-and-slow technique puts key communications off the radar for increased stealth..

- **Remote Access Trojans (RATs):** They use RATs to establish a backdoor through which they can maintain extensive control over the system and continue to modify files, steal vendor lists, exfiltrate sensitive IP files, and more.
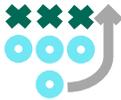
Phase 4: Simulated Attack Scenarios

The Red Team simulates a real-world attack against its manufacturing target.

- **Data Exfiltration:** They capture, encrypt, and even exfiltrate sensitive files containing patents, trade secrets, and other forms of intellectual property vital to manufacturing competitiveness.

- **Operational Disruption:** Red Teams simulate an attack on the manufacturer's SCADA systems and bring to light how unmitigated weaknesses could lead to production halts, workflow errors, and loss of revenue.

- **Supply Chain Compromise:** They demonstrate how weak partner access controls could initiate a supply chain attack that could deliver harmful malware from

a less-protected partner to their own internal systems.

Phase 5: Red Team Engagement & Blue Team Training

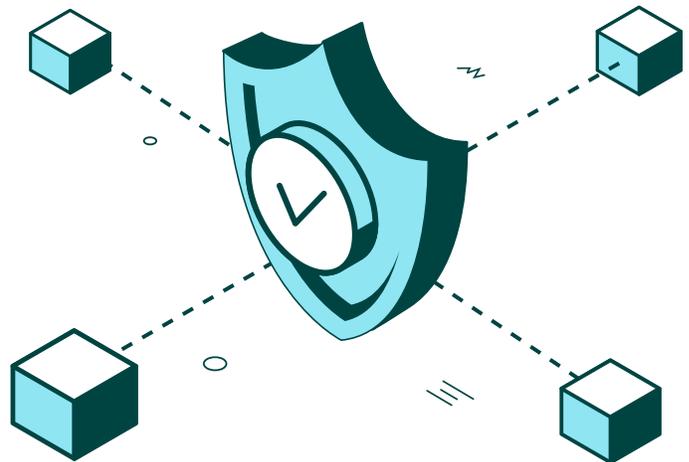As offensive Red Teams and defensive Blue Teams collaborate, a **Purple Team** mindset is developed.

- **Shared Sessions:** The Red Team openly shares its attack methodologies in real-time as the Blue Team looks on to gain context, insight, and experience. .

- **Extensive Logging:** Each adversarial tactic and response is documented so teams can learn from them post-engagement.

- **Purple Team Exercises:** Using the Red Team's findings as a basis, the Blue Team improves its defensive techniques.

- **Incident Response Drill:** With the red team engagement as a foundation, Blue Teams practice containing and responding to simulated threats in real-time.

Outcome & Lessons Learned

When done correctly, offensive security engagements can provide manufacturers with insights available in no other way (other than a real-world attack). Using Red Teaming, these invaluable lessons can be gleaned safely.

- **Identified Weaknesses:** Red Teams expose gaps in endpoint security, access controls, user social engineering awareness, patch management, permissions, and network segmentation.
- **Security Improvements:** The manufacturer deploys any or all of the following: multi-factor authentication (MFA) across all access points, a secure patch management system, a **security awareness training (SAT)** program, improved advanced malware detection capabilities, and enhanced monitoring or security upgrades for SCADA systems.
- **Enhanced Cyber Preparedness:** Ongoing and regular red team engagements are scheduled as the manufacturer invests in long-term, enhanced cyber preparedness.

Advanced Red Team Tools

Without the advanced offensive security techniques made available by Cobalt Strike and Outflank Security Tooling, most teams would be hard pressed to recreate full-scale simulated attacks at the size and sophistication of those found in the real world. Each solution functions as a standalone platform, but together, the synergy provided by industry-leading red teaming software and a standard-setting advanced red teaming toolkit is unmatched.

Don't let your Blue Teams meet today's attackers unprepared. Invest in the industry's best red teaming solutions from Fortra.

FORTRA

Fortra.com