OT Cybersecurity Consulting Services

OT Purple Teaming Service

Enhance Your Cyber Resilience.

Resilience requires muscle memory.

Many SCADA and OT systems were not designed with security in mind, and many lack basic security controls that you would see on common systems such as firewalls, intrusion detection and prevention and even basic encryption.

We need to keep in mind that production environments are finely tuned machines, and even small interruptions to their operation can have a profound impact on their output. Attacks against your production environment can lead not only to business interruption but also to physical injury and harm. The ability to detect an attack in an early stage is vital to ensure business continuity.

An OT Purple Teaming Service is a simulation-based training activity designed to help you practice and improve your incident detection and security alert handling capabilities.

During the exercise, participants work through a range of simulated cyber-attacks. Test cases go from very quiet "under the radar" and are gradually escalated up to a case that all alerting systems and personnel should catch.

Test your SOC's detection and response capabilities.

An OT Purple Teaming Service is a deep dive into the various attack techniques used by cyber criminals. We help you better understand your SOC's alert-handling capabilities, to identify potential areas for improvement, and increase your preparedness for responding to real-world cyber-attacks.

The service can be run as a:

Purple test, where the SOC is aware of the test and works jointly to define coverage; or

Awareness test: where the SOC is unaware of the test, which means a genuine attacker simulation is conducted (in a safe way) and one of the key elements being measured is the time-to-detect.

Phone: +45 88 13 60 30 www.csis.com

Tried and tested approach.

Simulated cyber-attacks are carried out from a PC, which can either be delivered by us or by you. The preference is a PC delivered by you and native to your network, so we can test resilience both at a network security and an endpoint security level. We will install a special virtual unit on the PC.

The PC will require connectivity to around 6 devices on your network that have been selected and assessed as non-critical.

While running the service, 12 different attack phases will be tested that the Blue Team will need to defend against. These attacks are mapped in different categories based on the ICS MITRE ATT&CK Framework.

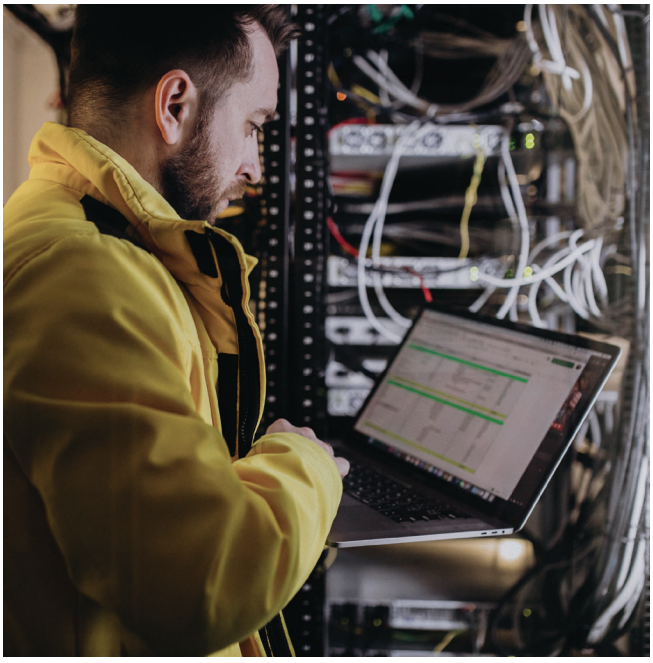
In-depth findings.
Actionable recommendations.

We will deliver a report containing all findings for all attacks, and recommendations for how to improve your cyber resilience.

You will gain real-life, actionable results based on proven ICS testing methods and techniques, to answer common questions like:

"What type of attacks will I currently not detect?"
"What parts of my tested OT environment are exposed to attackers?"
"What risk does my IT environment pose to my OT environment?"
"How can I reduce the attack surface of my OT environment?"

To ensure a full audit trail, we will deliver PCAP network file(s) from the test PC, to show what activities were performed with their associated timestamps.



CSIS is your partner for OT cybersecurity services.

20+ years of cybersecurity experience.

Roster of blue-chip customers covering IT and OT domains.

Tried and tested methodologies.

Cyber intelligence backbone.

Strategic partnership with ICS Range (https://icsrange.com).

Phone: +45 88 13 60 30 www.csis.com