"Train how you fight, fight how you train." Limited annual penetration testing and occasional red team engagements will not help you against continuous attackers. It is time to do offense more frequently and comprehensively

Red Team-as-a-Service

For Continuous Consequence, Hazard, & Threat Protection

AIT

Applied Integrated Technologies

Isiah Jones
Cyber Engineer (ICS OT IIoT IoT)
October 2022

Red Team-as-a-Service

For Continuous Consequence, Hazard, & Threat Protection

Red team engagements and penetration tests are usually conducted once a year, or less frequently, on industrial control systems (ICS), automation systems, operational technology (OT), safety systems, embedded systems, and industrial internet of things (IIoT) systems. The problem with this is that your adversaries are moving much faster than that. They continuously survey and exploit new targets behind the scenes as organizations run their daily operations. To keep ahead of the adversary, organizations need to move to a continuous red-teaming mindset. This means focusing on potential consequences and hazards, as well as their related impacts and active threat behavior seen in the wild to emulate tactics and techniques currently being used against the same or similar targets.

Some of the benefits of continuous red teaming include:

☑ Instant emulation and testing of newly discovered tactics, techniques, and tools via attack-based threat intelligence. By observing what is happening in the wild in real-time, you can dynamically update red team activities and targets. This focuses red teaming and penetration testing on specific equipment (e.g., emulating behaviors of criminals, nation states, insiders, and other actor behavior targeting the same or similar assets, environments, or interdependencies).

☑ Regular analysis of OSINT, GEOINT, HUMINT, and SIGINT attack surfaces that adversaries use in the wild to inform and direct red team and penetration testing exploitation.

☑ Regularly testing of physical access controls through lock picking, badge cloning, drone usage at field and remote sites, USB drops and other physical exploitation tactics, tools, and techniques.

☑ Continuous targeting of new and dynamic operational shifts to consequences, hazards and their associated organizational, equipment, safety, operational, and environmental impacts.

☑ Monthly and/or quarterly attack mapping and threat modeling of dynamic production operations environments (including impacts in the supply chain, mergers, acquisitions, new building coming online into production, etcetera).

☑ Discovering new zero days in people, process, and technology through full spectrum, asymmetric, red team engagements that occur more frequently than once a year to emulate the most advanced and persistent targeted and customized attacker abilities.

☑ Frequently exercising emergency response plans, tools, run books, and more at least twice a year or quarterly while actively under attack by a continuous red team on retainer.

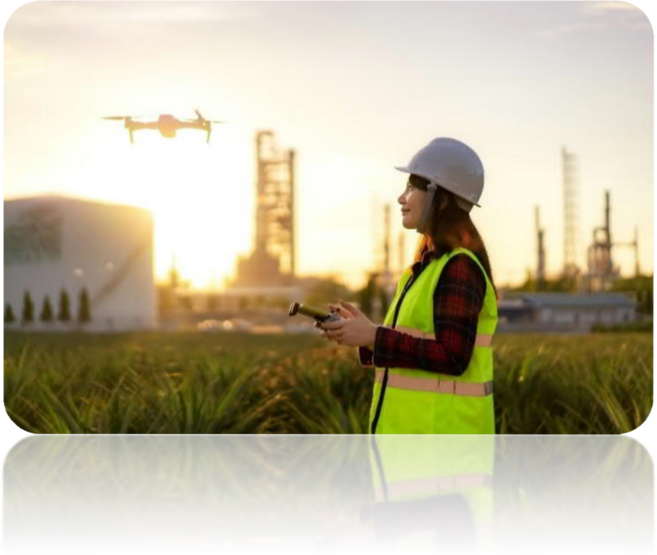
☑ Regularly validating if operations and maintenance actions in production are dynamically shifting the exploitable attack surfaces rather than relying on a once-a-year static snapshot in time.

☑ Regularly discover, map out, target, and exploit RF/wireless attack surfaces used by ICS OT Purdue level 0 and 1 field devices, IoT, and IIoT (e.g., Zigbee, zWave, LoRaWAN, cellular, unlicensed spectrum, Bluetooth, ISA100, WirelessHART, Wi-Fi, RFID, NFC, etcetera).

Many security practices, frameworks, guidelines, and standards have requirements for penetration testing and red teaming to occur

Some examples include:

- NIST SP 800-160v1 Systems Security Engineering
    - VE-2: Perform security-focused verification.
    - TR-2.7: Demonstrate that the installed system can deliver the required protection capability.
    - TR-2.8 Demonstrate that the security functions provided by the system are sustainable by the enabling systems.
    - VA-2: Perform security-focused validation.
- ISA/IEC 62443 part 3-2 – Security Risk Assessment for Systems & ISA84.00.09 Security for Safety Systems – identifying systems and components under consideration and performing detailed technical risk assessment of systems and components under consideration in scope of project phase.
- NIST Cybersecurity Framework (NIST CSF)
    - Risk Assessment (ID.RA) - ID.RA-1: Asset vulnerabilities are identified and documented.
    - Supply Chain Risk Management (ID.SC) - ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- NIST SP 800-53rev5 & 82rev2
    - CA-2 (Control Assessments).
    - CA-8 (Penetration Testing).
    - RA-3 (Risk Assessment).
    - SR-6 (Supplier Assessments and Reviews).
    - SR-10 (Inspection of Systems or Components).



AIT's security engineering professionals have global experiences providing security assessments, penetration testing, systems validation, and verification testing, and attack and threat mapping services for commercial and government customers. AIT's ICS OT security engineers are regular contributors and members of ISA/IEC 62443 and ISA84.00.09 standards committee working groups. AIT's staff also maintain current GICSP, CISSP, and other OT/IT cybersecurity certifications. To seek out continuous red team and penetration testing services please contact: otcyber@ait-i.com.