SpiderOak

SERVICES

ACTRA: Advanced Cyber Threat & Resilience Assessments

Tactical edge systems face advanced adversaries who exploit misconfigurations, trust assumptions, and architectural system weaknesses – not just known vulnerabilities.

Advanced Cyber Threat & Resilience Assessments (ACTRA) is SpiderOak's threat-driven vulnerability assessment service tailored for the software and components powering mission-critical platforms at the tactical edge.

From ground infrastructure (IT and OT systems) to UAVs and space vehicles (Embedded Systems) or specialized payload systems hosted on varying system platforms. ACTRA goes beyond surface scans to uncover exploitable vectors, insecure component boundaries, and system-level exposures that threaten operational continuity in highly contested, DDIL environments. SpiderOak's threat-informed assessment methodology and mission-aware remediation guidance strengthens your platform's cyber resilience against real-world compromise.

Scan to Get Started

What ACTRA Delivers

- **Mission-Aligned Threat Modeling:** Technical assessments are scoped and executed based on intended system's operational context, platform role, and threat actors
- **Threat-Informed Technical Evaluation:** Combining red and blue team methods with static and dynamic testing to identify realistic cyber-attack vectors and exploitation chains
- **Architecture & Configuration Review:** Analyze system designs, enforcement layers, and access controls for weaknesses in segmentation, authentication, or privilege management
- **Attack Vector to Risk Mapping:** Identify and trace system flaws, such as misconfigurations, insecure interfaces, or vulnerable components, which create exploitable paths to mission-compromising outcomes, including data loss, system disruption, or degraded performance
- **Actionable Remediation & Hardening Guidance:** Findings are prioritized based on mission relevance and accompanied by tailored mitigation recommendations

Why ACTRA

While many tactical systems are built to compliance under detailed specifications with cyber security engineering in mind, adversaries abroad through skilled teams or nation-states consistently evolve their conventional and non-conventional methods, tactics, techniques, or procedures (TTPs) to achieve their short and long-term objectives of compromising systems. ACTRA goes beyond compliance scanning to discover weaknesses that matter in real-world operations and environments. Whether operating ground stations, airborne platforms, or space vehicles, SpiderOak helps focus on what is exploitable, not just what is detectable.

Who SpiderOak Supports

SpiderOak's ACTRA service offering supports commercial and defense aerospace programs, companies, and operators who are:

- Fielding or sustaining tactical platforms, control systems, or autonomous mission assets
- Managing sensitive, exposed systems, sub-systems, and critical components operating in contested or denied environments
- Preparing for secure delivery, red/blue team evaluation results or corrective actions in real time
- Pursuing Approval to Operate (ATO) package artifacts submission (i.e., Body of Evidence [BOE]) to responsible mission organizations

Key Benefits

- Surfaces realistic, mission-impacting vulnerabilities and adversary attack vectors
- Scores and prioritizes findings that consider operational threat models
- Enhances system security posture with actionable, mission-aligned mitigation recommendations
- Accelerates secure deployment and strengthens ATO-readiness
- Avoid costly rework by catching critical security issues earlier in the lifecycle

Compliance & Framework Alignment

ACTRA is a real-world cyber threat and vulnerability assessment, not a standalone compliance audit – its findings help teams:

- Support mission-based frameworks like MRTC and MRAP-C by connecting technical findings to ideal operational outcomes to better strengthen an enterprise or enhance tactically deployed assets
- Take a layered security approach to thoroughly identify and mitigate vulnerabilities that undermine key security controls or critical components (e.g., NIST 800-53, 800-171)
- Strengthen Secure-by-Design posture through adversary-informed validation
- Harden configurations and expose system-level weaknesses ahead of an ATO or red team informed events
- Align with evolving CISA, DoD, and IC guidance on operational cyber resilience

Get Started with ACTRA

Achieving cyber resilience is not about scanning or assessing through authoritative checklists (i.e., DoD STIGs). It is about understanding how a system can be compromised and fixing weaknesses before adversaries exploit its vulnerabilities in real time and how a system will potentially respond during actual exploitation. ACTRA brings mission-aligned threat knowledge, vulnerability research, and tailored remediation to the tactical edge. Adversaries go beyond compliance to compromise systems – act one step ahead with SpiderOak's ACTRA.

Scan to Get Started

The ACTRA Process

While the ACTRA process follows a proven structure, each engagement is tailored to align with your target environment, mission context, and threat landscape. The phases below represent an adaptable framework designed to generate mission-relevant insights and support informed security decisions aligned with your assessment goals.

1 Assessment Planning

Define the assessment scope, align stakeholders, and establish understanding of mission context, system architecture, and critical components.

2 Threat Modeling

Identify adversary objectives and map realistic tactics and attack paths by analyzing system architecture, access vectors, trust boundaries, and mission risk factors.

3 Threat-driven Assessment

Execute focused penetration testing and evaluation across physical, software, and network interfaces using real-world adversary techniques, such as those outlined in the MITRE ATT&CK framework.

4 Exploitation Analysis

Analyze and trace how adversaries gain access, move laterally, and establish persistence to assess full system exposure and mission impact.

5 Risk Prioritization

Translate technical findings into mission-relevant risks, supported by impact scoring and visualized attack chains.

6 Hardening & Validation

Recommend actionable mitigations and confirm their effectiveness through focused re-testing and validation.

7 Strategic Wrap-Up

Deliver stakeholder-focused summary of assessment findings, demonstrated impacts, and overall system security posture to support risk-informed decision-making and future security planning.