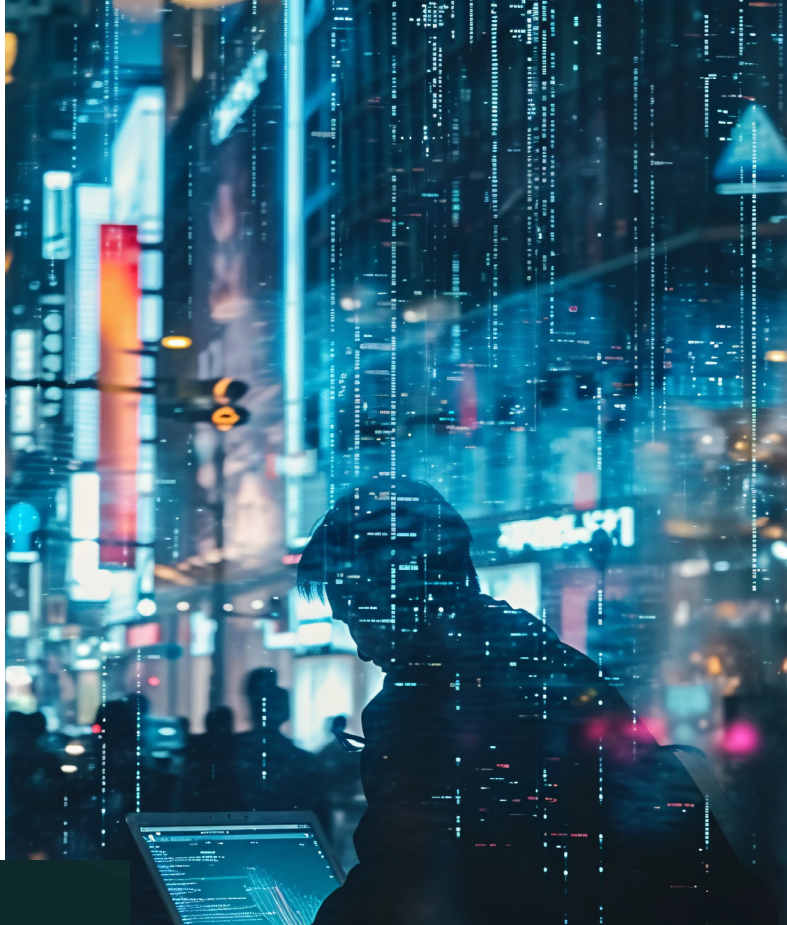




Red Team Attack Simulation

Cybercriminals constantly evolve their attack tactics and digital attributes in order to bypass the latest security controls and exploit vulnerabilities in systems, network configurations and cloud environments while bypassing endpoint protection solutions. In this challenging threat environment, you need a partner that can help you manage your risk.

In Tevora's Red Team Attack Simulations, we conduct a covert attack on your organization to test the effectiveness of security controls against a sophisticated stealth adversary. The exercise provides a real-world view of your security posture from the attacker's perspective, which allows you to "strike first" to find and fix your security weaknesses before an attacker exploits them.



Tevora's Red Team Attack Simulation Process

Reconnaissance

- Perform discovery efforts including:
 - Open source intelligent gathering
 - Network enumeration and service footprinting
- Conduct stealthy exploitation by mapping and targeting externally facing assets and vulnerable systems
- Conduct phishing, vishing, and physical social engineering assessments to test human and physical security controls

Assessment

- Emulate known attack patterns and vectors
- Map and exploit externally facing assets
- Conduct thorough information gathering and public record analysis
- Identify known vulnerabilities
- Develop and execute exploits
- Simulate sophisticated threat activity by deploying tailored malware to move laterally and gain elevated access without triggering security controls
- Conduct social engineering campaigns against target employees

Report

- Conduct a collaborative debrief session
- Provide a detailed findings report with recommended remediation
- Retest with validation
- Deliver a comprehensive report to the executive team that outlines key findings, attacker activity, and a timeline of events throughout the assessment
- Create an executive summary of findings for management

Red Team Attack Testing Scenarios:

Every Tevora Red Team Attack Simulation is customized to your organization's environment to ensure an effective, thorough and disruption-free assessment.

Black box testing

The Tevora Red Team is provided with little or no information of the internal structure or design of the environment being tested. Attack vectors are discovered through comprehensive reconnaissance that includes open source intelligence gathering. The knowledge-level of an unaffiliated attacker is simulated.

White box testing (a.k.a. Purple Teaming)

Tevora's Red Team collaborates with your Blue Team to design a custom test for your environment and identify blind spots or misconfigurations within the defensive security tools. Attack vectors are discovered through the same efforts as in our black box testing. Testing focused on identifying real-world attack scenarios while working with the blue team to confirm attack visibility and response capabilities.

Go forward. We've got your back.

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's organizations, people, and assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments, so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges, so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership, and—year after year—apply our cumulative learnings to continually strengthen the company's digital defenses.

ACHIEVED ACCREDITATIONS



ACHIEVED ASSESSOR



AI SECURITY STRATEGY

Artificial Intelligence has prompted a new landscape of compliance frameworks, threat vectors, and security tools. We make it our job to understand and pioneer the security programs that account for—and take advantage of—all that AI brings to the table.

COMPLIANCE

The assessment is only the first step of your compliance journey. We'll help you understand your path to achieving and maintaining continuous compliance against the security and privacy frameworks you need to do business.

THREAT MANAGEMENT & RESPONSE

Whether proactive or in case of emergency, Tevora has your back in the face of threat actors. We offer comprehensive and targeted penetration testing, social engineering, and other tactics to find gaps before others can exploit them.

SECURITY INFRASTRUCTURE

Tevora takes a vendor-agnostic stance to help companies find the best fit software solutions for their security needs. And with knowledge of hundreds of solutions vendors across dozens of categories, we'll help you find your fit.

RISK & STRATEGIC SERVICES

Address risks before they become an issue. Proactive and comprehensive exercise to find and address weaknesses in your security program through Enterprise Risk Management, Third Party Risk Management, Business Continuity and Disaster Recovery exercises, and more.

RESOURCE AUGMENTATION

The complex and specialized work required by cybersecurity and compliance programs sometimes require a focused, expert resource. Tevora can supplement your internal team with flexible Governance, Risk & Compliance (GRC) support, expert DevSecOps support, or even executive-level CISO assistance.