TEVORA™

Purple Teaming

Purple Teaming is a collaborative exercise that brings together the offensive expertise of Red Teams and the defensive insight of Blue Teams into a single engagement. Unlike traditional penetration tests that focus solely on identifying exploitable weaknesses, a Purple Team exercise goes deeper, validating not just where vulnerabilities exist, but how well your organization can detect, respond, and adapt in real time.

The value is twofold: immediate improvements to security controls and long-term maturity gains for the SOC.

By aligning simulated attacks with collaborative defensive monitoring, Purple Teaming uncovers gaps that would otherwise remain hidden: blind spots in logging, ineffective detection rules, or delays in incident response workflows.

Tevora's Purple Teaming Process

Breach Post-Exploitation Simulation

Purple teaming typically starts from an "assumed compromise" perspective, often with the attacker starting with access to an employee workstation and user-level credentials.

Testing is an iterative collaborative process typically covering:

- Payload Delivery and EDR Bypass
- Network Reconnaissance
- Lateral Movement
- Targeted Asset Compromise
- Data discovery & Staging
- Defensive validation

Communication

- Daily standing meeting
- Ad-hoc working sessions
- Iterative testing and detection feedback

Reporting

- Executive Summary
- Findings overview
- Technical Details

Remediation Validation

- Following remediation of discovered vulnerabilities, Tevora will perform remediation validation testing. The report will be updated to reflect remediation actions.

Why Purple Teaming Delivers:

Stronger Defenses
Validates that your tools and teams can stop real-world threats

Faster Response
Reduces detection and response times to minimize impact

Smarter Investments
Maximizes ROI from existing security tools and processes

Greater Confidence
Provides assurance to leadership, auditors, and the board

Lasting Resilience
Builds a mature, adaptive security posture for evolving threats

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

ISO 27001 Lead Auditor · ISO 27017 Certified · ACCREDITED CERT #5062.01 · CREST PEN TEST

ACHIEVED ASSESSOR

PCI Security Standards Council — PCI DSS QSA, PCI PA-DSS QSA, 3DS ASSESSOR · AICPA SOC · ISO Audit · HITRUST Authorized CSF Assessor · FedRAMP · TRUSTED PARTNER NETWORK · GovRAMP

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.