TEVORA™

SECURITY Solutions

Attack Simulation Services

Cybercriminals are constantly evolving their tools and tactics to identify vulnerabilities in your systems that can be exploited to deploy ransomware and other malicious software. Tevora's Attack Simulation Services can help identify these vulnerabilities and shore up your defenses before a potentially devastating attack occurs.

Attack Simulation Tests

Our Attack Simulation Services use a set of benign scripts that simulate the tactics, techniques, and procedures used by major advanced persistent threat (APT) groups and past attack campaigns, to test your defenses against a broad spectrum of external attacks.

Tevora will work with you to deploy and execute the simulated APT attacks in your environment. These automated tests run on Windows, macOS, and Linux operating systems and simulate an external attacker attempting to identify and exploit vulnerabilities in your network and systems. Tests are mapped to the MITRE ATT&CK™ framework, which defines categories and tactics for each of the common methodologies attackers use. This gives your team a highly actionable way to test your defenses against a comprehensive range of common attack scenarios.

Test Results

The attack simulation test results will let you know how well your defenses worked against attacks in each of the 12 MITRE ATT&CK™ categories. For each category, the results will tell you which attacks were:

- Detected
- Alerted on
- Blocked or prevented
- Visible in logs or other defensive telemetry

The results also include a heat map that identifies weak points in your environment for each MITRE ATT&CK™ category.

Tevora Attack Simulation Methodology

Adversary Tactics & Techniques

- Map tests to MITRE ATT&CK™ framework for coverage of all common attack scenarios.
- Use benign scripts to test and simulate a broad spectrum of attacks.
- Identify Indicators of Compromise (IoCs) and test organization's ability to detect and respond.

Tevora's Execution Engine

- Deploy Tevora's automated test execution engine with easy-to-use graphical interface.
- Use execution engine to run all attack simulation tests and generate test results and logging automatically.

Analysis & Evaluation

- Conduct manual and automated analysis to identify areas that need improvement to defend against real-world adversaries.
- Identify cases where simulated attacks were not detected.
- Make changes to ensure detection of all attack simulations and re-run tests to confirm that the changes work.

Resource Recommendations

- Make recommendations on further equipping staff and systems environments to be fully prepared for real-world external attacks.

TEVORA™

Strengthening Your Defenses

Tevora's execution engine enables tests to be run quickly, which lets you spend most of your time reviewing test results, gaining a deeper understanding of your environment and controls, identifying and resolving any identified vulnerabilities, and re-running the tests to confirm that vulnerabilities have been remediated.

After you've addressed vulnerabilities identified by the simulated attack tests, you can expand the scope of your testing to address specific attack tactics that you know to be relevant based on threat intelligence, baseline, or recommendations from other sources.

Let Tevora be a trusted partner

to help you protect your valuable systems, data, and reputation in this environment of increasingly frequent and sophisticated cyberattacks. Contact us by phone at (833) 292-1609 or email us at sales@tevora.com.

Go forward. We've got your back.

We live in a digital world, and your customers trust you to keep their information safe. We make it our responsibility to equip you with the information, tools, and guidance you need to stay out of the headlines and get back to business.

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

ISO 27001 LEAD AUDITOR

ISO 27018:2014

AICPA SOC

HITRUST Authorized CSF Assessor

ACCREDITED

bsi. ISO/IEC 27001 Information Security Management

FedRAMP

PCI Security Standards Council PCI FORENSIC INVESTIGATOR

Tevora offers a full range of services designed to anticipate and meet the changing needs of your enterprise

Compliance

We assess, audit, and certify compliance across a comprehensive portfolio of cybersecurity standards.

Enterprise Risk Management

We speak the language of cyber risk and translate it into business impact - giving you rich data to make meaningful decisions.

Data Privacy

We help you craft strategies and plans that work; allowing you to meet the growing demands of domestic and international privacy regulations.

Security Solutions

We help you plan, implement, and integrate cybersecurity products that reduce your risk profile: on-prem, mobile, and in the cloud.

Threat Management

We test your systems, processes, and security with a world class team of certified hackers and security researchers.

Incident Response

We are a team of first responders, threat hunters, and incident containment specialists working with the latest tools and techniques; ready to serve when your business needs it most.