REVOLUTIONARY SECURITY

LiveFire® Advanced Threat Emulation

Comprehensive Adversarial Threat Emulation and Defensive Posture Mapping

The Challenge

With the increase in frequency and sophistication of cyber attacks, companies are making significant investments in cyber security capabilities. However, even with the increased investment, companies continue to see their peers who have made similar investments becoming the next victim of cyber attacks. Navigating the technology market continues to be increasingly challenging with thousands of established vendors and even more emerging solutions.

Companies are faced with the challenge of determining if they have the right capabilities in place across people, process and technology. This includes determining if gaps exist not only in the information security ecosystem, but also across the broader IT infrastructure. If you want certainty about your cyber security capabilities, LiveFire® Advanced Threat Emulation (A.T.E.) will determine if your enterprise is defensible against all levels of cyber attacks and:

- ✓ Develop a comprehensive threat map allowing the prioritization of risks and mitigations;
- ✓ Evaluate defensive depth to determine resilience against multiple divergent adversarial TTPs simultaneously; and
- ✓ Discover the macroscopic view of your enterprise defenses and how an adversary might see your systems.

Why Revolutionary Security?

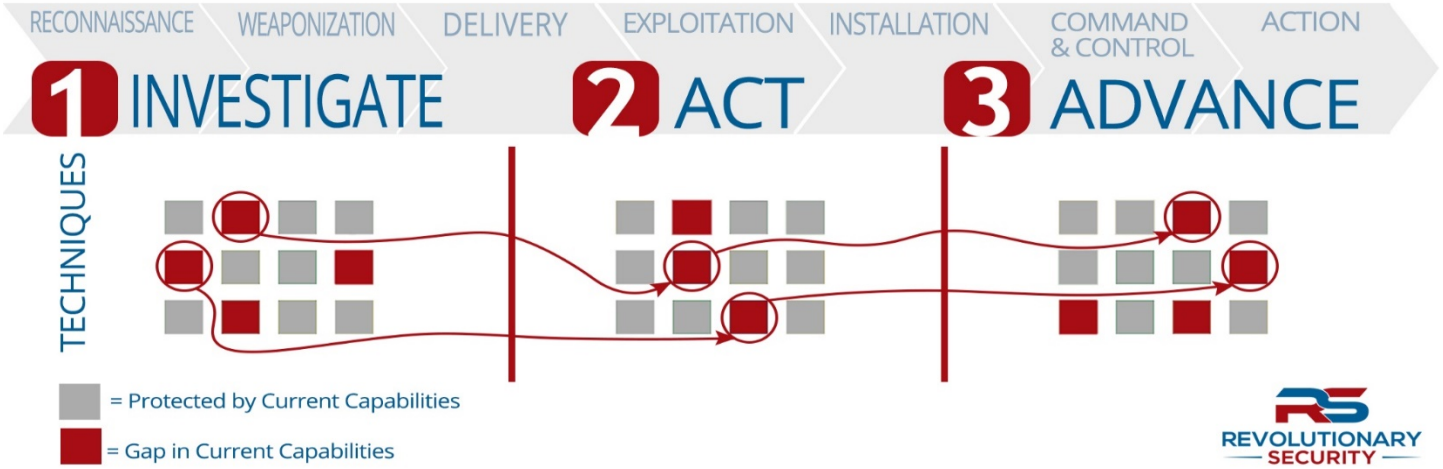
- ✓ ***Our People*** – Our enterprise security testers have extensive cross-domain experience. We honed our skills defending high-stakes, heavily-attacked networks.
- ✓ ***Our Services*** – Comprehensive and informed by real world adversarial tactics, techniques, and procedures (TTP's), Revolutionary Security's LiveFire® goes well beyond industry best practice to set a new standard in advanced threat emulation.
- ✓ ***Our Experience*** – We have a proven track record of securing critical infrastructure spanning Oil & Gas, Utilities, Financial Services, Health & Life Sciences, Chemical, Technology & Communications, Manufacturing, Transportation, Law, and other industries.

LiveFire® Advanced Threat Emulation

Revolutionary Security's experts excel in helping organizations advance their cyber security capabilities by leveraging their knowledge and expertise garnered from successfully defending enterprises against advanced cyber attacks. By using our LiveFire® Advanced Threat Emulation (A.T.E.) testing services, we address a company's need to understand its specific attack surface, defend against advanced cyber threats, and adjust to evolving organizational priorities.

LiveFire® is an industry-leading cyber security testing method for testing multi-vector cyber threats to an enterprise across the various phases of an adversary's lifecycle. Building on the core DNA from Lockheed Martin's Cyber Kill Chain® and Mitre's ATT&CK™ frameworks, the approach utilizes discrete test cases to identify defensive gaps across people, process, and technology. These testing results identify and prioritize security projects and remediation activities for enterprise risk mitigation which the Revolutionary Security's cyber security experts craft into a comprehensive and relevant view of your enterprise defensive posture and capabilities and identify gaps in controls.

Unlike a traditional penetration test which attempts several paths to identify vulnerabilities in a targeted system, LiveFire® executes hundreds of discrete test cases that combine to create thousands of permutations of how an attacker might compromise your environment. In addition to testing the effectiveness of the technical controls, LiveFire® measures the response of the enterprise security team to various attacks. The testing culminates in a report that identifies which attacks were stopped, which were detected and responded to, and which elicited no response.



How We Do It

- ✓ Next generation defensive and offensive testing approach that goes beyond traditional pen testing
- ✓ Simulated adversary tactics through discrete test cases attributable to real-world adversarial TTPs that combine to create thousands of permutations of how an attacker might compromise the environment
- ✓ Detailed explanation of identified vulnerabilities with remediation recommendation priority that include relative defensive value, cost, effort, and time required to implement

What to Expect

- ✓ A thorough analysis of cyber threats and attack vectors based on actual adversary TTPs
- ✓ More than a subjective assessment and pen test by measuring both effectiveness of the technical controls and response of the enterprise security team to various attacks
- ✓ A comprehensive test of cross-domain enterprise defensive capabilities to determine a ground truth view of enterprise defenses
- ✓ A rigorous heat-map that spotlights hot-spots enabling organizations to focus on risk and defensive countermeasures in those areas
- ✓ Identification of gaps in detection and response which are prioritized with recommendations to address the gaps to create an actionable roadmap to improve the organization's defensive posture

About Revolutionary Security

Revolutionary Security is an experienced and talented team of cyber security professionals whose mission is to provide our clients with the knowledge and expertise to defend their enterprises against cyber threats. Our cyber security consulting and advisory services focus on helping our clients evolve their capabilities across the entire spectrum of people, process, and technology. Revolutionary Security was established by a team whose expertise comes from Defense and Intelligence Community experience and over a decade of tailoring solutions to protect Fortune 500 / Global 1000 companies from all cyber threats.

Stephen Snyder
Director
stephen.snyder@revsec.com
+1.615.332.2671