EVIDEN

Red Team Services

an atos business

Eviden Red Team services show you how an attacker would infiltrate your network and what you must do to reduce your risk from a real-world incident.

Will You Be Able to Stop a Real-World Attack?

Most organizations can only answer this question after it's too late. They do everything possible to improve their defenses, harden their perimeter, and deploy a wealth of detection and response capabilities. Still, they don't know if it will work until an attacker strikes and real-world business harm is on the line.

CISOs widely recognize the Eviden Red Team as a team that can reveal critical insights and enhances business resilience by resolving complex issues.

Eviden Red Team Services

Our Red Team performs simulated cyberattacks using ethical hacking techniques and tools to showcase how a potential attacker may infiltrate your network. We assist in assessing the proficiency of your blue teams and your organization's defense mechanisms against an attack. We help identify any vulnerabilities that could lead to a breach and provide the necessary remediation guidance. Eviden Red Team Services can simulate any cyberattack — from social engineering to ransomware.

With Eviden Red Team services, you get:

- **A Real-World View of Your Security:** Discover your security posture's failure points and learn if you're ready to stop an attack - before you suffer one.
- **Practical Security Roadmap:** Identify the exact path an attacker would take to achieve their goals and rapidly address the specific vulnerabilities they would target.
- **Risk-Free Front-Line Experience:** Give your internal security teams a chance to practice stopping a real-world attack without real-world risk.
- **Increased Compliance:** Comply with security regulations, such as PCI DSS and HIPAA. Our services can help you demonstrate that you are taking steps to comply with these required regulations.

A Full Range of Red Team Services

Our Red Team services include simulated attacks in a combination of the following approaches:

Black Box:

Our teams think like attackers with no prior knowledge of the target system. We simulate a real-world attack to identify vulnerabilities that can be missed in other tests.

Grey Box:

We will do the same with some knowledge of your organization's internal workings - e.g., what an attacker might know if they acquire elevated user privileges.

Physical Engagement

We will conduct a simulated attack that includes attempts to access your physical premises as part of the attack pattern.

What's Included in Every Engagement

Our Red Team experts will simulate a real-world attack against your organization, targeting the areas you are most concerned about through a custom-made incident:

Step 0: Definition

First, we will work with your leaders to define the attack target you want to test your defenses against and what malicious objective you want us to work towards.

Step 1: Perform Reconnaissance

We will analyze your networks, systems, employees, processes and physical facilities to find the blind spots and vulnerabilities a threat actor would use to launch a successful attack.

Step 2: Prepare the Attack

We will establish tools, systems, content, and infrastructure to launch a successful attack that exploits the vulnerabilities we found in Step 1.

Step 3: Begin the Attack

We will follow our plan to breach your network, move laterally within it, and develop a strong enough foothold to compromise your systems, employees, and data.

Step 4: Compromise Your Org

Next, we will advance our attack and move to complete whatever malicious objectives we agreed upon, all while hiding from or combating your internal or external 3rd party blue teams.

Step 5: Post-Mortem

After we complete our simulated attack, we will prepare a report for both your business and technology leaders outlining our exercise results and what to do next.

Step 6: Hardening (Optional)

If requested, we can deploy our cybersecurity experts to address any security gaps identified during our exercise through a complete range of managed services.

Why Eviden, a proven, reliable partner in your cyber defense

Eviden is the largest managed security provider in the world and has decades of frontline experience resolving complex, high-impact cybersecurity incidents. We deliver our Red Teaming services through hundreds of certified ethical hackers, in-house security researchers, and specialized business vertical experts.

By partnering with Eviden, you gain:

Human Expertise Leverage our hundreds of battle-tested frontline operators and consultants.

Flexible Engagements Design the Red Team engagements that best meet your unique security needs.

Detailed Post-Mortems Receive an in-depth report on the results of our engagement and what we learned.

Blended Attacks Test your security's human, technological, process and physical elements in one attack.

Up-to-Date TTPs Experience today's most complex and challenging attack patterns - without risk.

Vertical-Specific Knowledge Deploy solutions designed for the unique needs of each industry and org structure.

Unified Security Remediate the results of your Red Team exercise with our fully managed services.

Global and Local Coverage Tap into our worldwide ecosystem of Global CERT with "boots on the ground" support for most regions.

Bring Eviden Red Team Services to Your Organization

With Eviden Red Team services, you will:

- Learn how your structural defenses and security teams will perform when under a real-world attack
- Identify the weak spots in your defenses - before attackers find them and exploit them first
- Eliminate the vulnerabilities that attackers will most likely exploit and reduce your fundamental security risk
- Give your security team hands-on experience fighting back an attack without the risk of suffering real-world harm

Reach out today to partner with Eviden.

Connect with us

eviden.com

ECT-230626-AR-BR-Eviden-Red-Team-Services-en-v1