



EXECUTIVE INSIGHTS: WHY ADVERSARIAL EMULATION IS THE CYBERSECURITY TEST YOU NEED

Digital Defence Ltd.

Robert W. Beggs, CISSP
01 July 2025 v1.0

Phone: 519.771.8808 | Web: <https://www.digitaldefence.ca>

EXECUTIVE SUMMARY

In today's hyperconnected world, the cyber threat landscape is evolving faster than most organizations can keep up. High-impact ransomware attacks, supply chain compromises, and sophisticated nation-state campaigns have shifted cybersecurity from a technical issue to a strategic business imperative. Yet, many organizations still rely on outdated assumptions about their defenses—until it's too late.

Adversarial emulation is a next-generation approach to testing security preparedness by simulating the tactics, techniques, and procedures (TTPs) of real-world threat actors. Unlike traditional penetration testing or vulnerability scans, adversarial emulation is tailored to mimic specific threats an organization is most likely to face—giving leadership a clear picture of how their defenses perform under realistic attack conditions.

This type of testing goes beyond checking boxes for compliance. It empowers executives to:

- Assess realistic risk exposure by demonstrating how your systems hold up against the exact tactics used by today's top threats (hackers, ransomware).
- Reduce the cost of a data breach. Proactive testing, including adversarial emulation, saw **cost reductions** of up to \$2.2 million per breach.
- Evaluate the speed and effectiveness of detection and response capabilities and identify the measures needed to detect, contain, and respond to attacks. MITRE-based adversarial emulation can **improve incident response**, reducing detection and response times by 30-50%. Identifying exploitable attack paths reduces remediation workload by 20-40%.
- Validate the existing security spending and prioritize security investments with confidence. Using adversarial emulation to identify misconfigured tools or eliminate redundant systems can enable 10 – 25% **optimization in security budgets**.
- Demonstrate resilience to boards, regulators, and customers and negotiate for enhanced insurance terms or premium reductions.

Using frameworks like MITRE ATT&CK, adversarial emulation translates technical security exercises into business-relevant insights. By seeing their environment through the eyes of an attacker, organizations gain actionable intelligence to close gaps before adversaries can exploit them.

THE THREAT LANDSCAPE

In today's business climate, cybersecurity isn't just an IT issue, it's a matter of operational continuity, reputational integrity, and board-level accountability. Executives are facing a threat landscape where attacks are faster, stealthier, and more targeted than ever before.

Organizations are contending with adversaries who operate like businesses themselves: leveraging R&D, automation, and global networks to industrialize cybercrime. These groups use multi-stage attacks, living-off-the-land techniques, and social engineering tactics to bypass traditional defenses. They aren't "hacking in"—they're logging in, pivoting silently, and exfiltrating critical data without detection.

Yet despite this sophistication, many enterprises still rely on outdated methods to validate their defenses.

Vulnerability scans flag known issues—but only those mapped to existing CVEs. They don't account for configuration drift, chained exploits, or how those vulnerabilities might be used in the real world.

Penetration tests are typically limited in scope, often conducted annually or to satisfy compliance requirements. Their outputs are tactical, not strategic—more about identifying "low-hanging fruit" than evaluating how an attacker would accomplish their goals across your specific environment.

Audits and risk assessments check whether controls exist—not whether they can withstand a motivated, evasive threat actor. A box might be ticked, but the question remains: can it stop an attack?

This is a dangerous gap—especially as companies accelerate cloud adoption, support hybrid workforces, and integrate with sprawling third-party ecosystems. The attack surface is changing faster than controls can adapt, and traditional testing methods are blind to the most important factor: how adversaries operate.

What executives need isn't another 80-page report listing theoretical weaknesses. They need clarity on their real-world exposure: How would today's ransomware operator move through our network? Would our detection controls alert in time? How quickly would our team respond?

Adversarial emulation answers these questions head-on. By simulating the exact behaviors of threat actors relevant to your industry and infrastructure, it tests your defenses against the attacks that matter most—today, not six months ago.

This approach shifts cybersecurity from reactive to proactive. It moves leadership from assumption to assurance. And it reframes security not as a cost center, but as a strategic capability—essential for navigating risk in a digital-first world.

Table 1: Comparison of Security Tests

Testing Type	Benefits	Limitations
Vulnerability Scanning	Rapid identification of known issues. Scalable. Useful for compliance reporting.	Only detects known vulnerabilities. High rate of false-positive results. Lacks context or proof of exploitability.
Penetration Testing	Actively exploits vulnerabilities. Demonstrates real-world impact. Focused, goal-oriented testing.	Point in time test, may be limited in scope. May lack threat-actor realism. Can miss multi-step attack paths.
Adversarial Emulation	Simulates real attacker behavior. Validates controls and responses. Aligned with threat intelligence (MITRE ATT&CK framework). Provides strategic and business-relevant insights.	Requires planning and experienced operators. Can reveal uncomfortable truths!

Adversarial emulation is best delivered as part of a formal and comprehensive testing program.

WHAT IS ADVERSARIAL EMULATION

Adversarial emulation is a strategic security testing method that mimics the tactics, techniques, and procedures (TTPs) of real-world threat actors. Instead of asking “what vulnerabilities exist?” it asks a more urgent question: if attackers targeted us using the same approach they’ve used elsewhere, what would they achieve—and how fast?

This methodology goes beyond scanning tools or one-off penetration tests. It provides a controlled, intelligence-led simulation of a cyberattack—mirroring the behavior of threat groups relevant to your industry, technology stack, or geography. These may include ransomware operators like LockBit, espionage groups such as APT29, or actors exploiting third-party software in supply chain attacks.

By emulating these adversaries, organizations learn how attacks unfold in their own environment, from initial breach to lateral movement, privilege escalation, and data exfiltration. These tests are not theoretical. They’re designed to answer critical business questions like:

- Would we detect this type of attack?
- How long would it take for our response teams to act?
- What systems, data, or operations are at risk?

Adversarial emulation draws upon frameworks like MITRE ATT&CK—a globally recognized knowledge base of threat behaviors used by attackers across the world. This framework provides a structured way to align emulation activities with known attacker playbooks, making outcomes more relevant, repeatable, and measurable.

The ultimate value lies not just in identifying vulnerabilities—but in revealing the path an attacker could take to achieve a business-impacting objective. This includes testing detection controls (e.g., EDR, SIEM), validating incident response processes, and pinpointing where escalation or containment breaks down.

Done well, adversarial emulation is a collaborative effort. It brings together red team operators (who emulate the attacker), blue teams (who defend), and security leaders (who interpret findings and drive action). Often, these exercises also include “purple teaming,” where offensive and defensive units work in lockstep to learn and improve in real time.

CASE STUDY: SECURING A HEALTHCARE PROVIDER



A regional hospital serving a large metropolitan area requested an adversarial emulation engagement to evaluate how effectively it could detect and respond to a modern ransomware-style attack—without compromising patient care or compliance obligations. With a hybrid cloud infrastructure and reliance on electronic health records (EHR), imaging systems, and remote telehealth services, hospital executives wanted a clear picture of how real adversaries could impact clinical operations.

Hospitals average \$1.9 million in daily downtime losses, with recovery times often exceeding 17 days.

Simulation Scenario

Digital Defence testers created a custom scenario for the hospital. The objective was to simulate encryption of patient records and scheduling systems, coupled with mock exfiltration to mimic a double-extortion ransomware model.

- Initial Access: Simulated spear-phishing campaign against a finance team member with access to vendor portals and payroll systems.
- Persistence & Escalation: Use of credential theft to gain domain-level access.
- Lateral Movement: Pivot from business systems into EHR and radiology servers using PowerShell remoting and token impersonation.



Key Findings

- **Failed Detections:** The third-party responsible for monitoring endpoint security logged some elements of the simulated attack but failed to provide any alerts to the hospital while the attack was in progress.
- **Vulnerable Staff Workstations:** Several endpoints lacked recent patches and relied on outdated antivirus, offering easy entry points for the emulated attacker.
- **Unsegmented Critical Systems:** EHR, radiology, and email servers were reachable on the same flat network as administrative systems—enabling rapid lateral movement.
- **Backup Risks:** Backup systems were online and accessible during the simulation. Had the encryption been real, recovery would have been compromised.

The emulation revealed that a ransomware event could delay emergency care, force surgical rescheduling, and threaten regulatory compliance—risks that far exceed a “technical incident.” As a result, leadership prioritized cybersecurity readiness alongside patient safety in strategic planning. The network was segmented to protect critical systems, a vulnerability management program was put in place, and the backup program was re-engineered. Finally, the third party responsible for endpoint monitoring was changed and the new provider was validated by a repeated adversarial emulation test.

ADVERSARIAL EMULATION - THE STRATEGIC BUSINESS BENEFITS

Adversarial emulation isn't a technical experiment—it's a business enabler. It transforms cybersecurity from a reactive expense into a proactive strategy that drives resilience, readiness, and confidence at the highest levels of leadership.

For executives, the question isn't if an attack will happen—it's when and how prepared we'll be. Adversarial emulation offers a way to answer that question with data, not assumptions.

1. Risk Visibility That Matters to the C-Suite

Adversarial emulation produces business-relevant insights. It reveals how a real-world adversary could disrupt critical operations, compromise sensitive data, or erode customer trust. This level of visibility helps leaders contextualize cyber threats in the language of business risk, operations, and brand exposure.

2. Validation of Cybersecurity Investments

With increasing pressure on cybersecurity budgets, executives need assurance that their investments are delivering measurable protection. Adversarial emulation validates the performance of existing controls—from endpoint detection and SIEM tools to segmentation policies and incident response plans. It shows what's working and where further investment is needed.

3. Faster, More Confident Decision-Making

By demonstrating how current defenses perform against specific threats, adversarial emulation helps prioritize action. It arms leadership with clear evidence to support technology upgrades, staffing changes, or new processes. It enables faster, data-driven decisions—not reactive ones created during a crisis.

4. Demonstrable Resilience to Stakeholders

Boards, insurers, regulators, and customers increasingly demand proof that organizations are managing cyber risk effectively. Adversarial emulation provides that proof. It shows a proactive stance toward threat preparedness and an executive commitment to resilience—essential for protecting brand equity and maintaining stakeholder trust.

5. Continuous Program Maturity

Resilience isn't built in a day. But adversarial emulation enables measurable progress. It helps organizations benchmark their capabilities over time and chart a path from basic detection to advanced response and containment. Through repeated exercises, organizations develop muscle memory, close detection gaps, and refine escalation playbooks.

6. Cross-Functional Engagement

Cybersecurity isn't just an IT issue—it's an organizational challenge. These engagements bring together IT, risk, compliance, legal, communications, and executive leadership to align on goals, understand risk holistically, and practice coordinated response. That cross-functional unity is essential when facing real-world threats.

7. Strategic Advantage in an Uncertain World

In a rapidly evolving digital economy, resilience is a competitive differentiator. Organizations that can detect, contain, and recover from attacks swiftly are better positioned to navigate uncertainty, comply with regulatory mandates, and outpace less-prepared competitors. Adversarial emulation turns readiness into a business strength.

From budget justification and board reporting to response readiness and strategic alignment, adversarial emulation delivers value far beyond the security team. It gives executives the confidence that comes from knowing—not guessing—how their organization would perform under fire.

THE DIGITAL DEFENCE SOLUTION

Since 2003, Digital Defence has provided elite security testing, including adversarial emulation testing. Adversarial Emulation is a proactive, intelligence-led security assessment that simulates the tactics, techniques, and procedures (TTPs) of real-world threat actors targeting your industry. Unlike traditional testing methods, our emulation engagements replicate the step-by-step behavior of known adversaries—ransomware crews, nation-state actors, insider threats—within your environment to uncover gaps in detection, response, and containment.

A typical engagement includes:

- A customized threat intelligence–driven scenario specific to your sector and adversary risk profile.
- An attack simulation from initial access to privilege escalation and data exfiltration using the tactics, techniques, and procedures (TTPs) of a real attacker or advanced persistent threat.
- Alignment with the MITRE ATT&CK framework for standardized, measurable testing.
- Full collaboration between our offensive experts and your defensive staff (a “purple team” test). Known entry points, escalation paths, and attack times ensure your organization can evaluate the effectiveness of EDR/XDR, SIEM, logging, and alerting infrastructure.
- Technical- and executive-level debriefs, including technical findings and prioritized remediation roadmap.
- Assistance with remediation and retesting.

Contact info@digitaldefence.ca for assistance in planning your adversarial emulation testing.

**The time to test your defenses is before someone else does.
A well-executed simulation today could prevent a crisis tomorrow.**