PENETRATION TESTING AND RED TEAMING

Turn exploitable paths into evidence that strengthens your security posture

Reports pile up—impressive on paper, but disconnected from how real attackers move.

Attackers see clear paths to data and control. Boards see vague heatmaps they can't tie to business risk.

That means testing rarely answers the only questions that matter under pressure:

- Which paths are truly exploitable?
- Can your controls detect and contain real attacker behavior?
- How fast can you move from "we were breached" to "we can prove we acted responsibly"?

eSurelTy's penetration testing, red teaming, and purple-team validation close that gap with human-led, goal-driven exercises across network, cloud, web, mobile, and OT—backed by reports usable by both engineers and leadership.

Outcome: Evidence set that demonstrates due diligence and control effectiveness.

The risk your environment is signaling to attackers and reviewers

Typical environments expose the same fault lines:

- Internet-facing services tested lightly, with stale findings
- Flat internal networks where one foothold becomes full-domain compromise
- Web and mobile apps with business logic and API flaws that slip past "secure by design"
- Cloud tenants with misconfigured IAM, exposed storage, and orphaned services
- OT/SCADA networks where "do not touch" replaced real testing and segmentation

Attackers chain these into ransomware, data theft, and long-term access.

eSurelTy turns penetration testing and red teaming into proof points:

- How real attackers would move in your environment
- Whether detection and response hold up under pressure
- Evidence that builds justified confidence in your security posture, not just a checked box

Penetration testing and red teaming built around your risk profile

eSurelTy does not sell "one-size-fits-all" tests or AI-generated report bundles.

Every engagement starts with your risk drivers, critical systems, and operational windows—not a generic template.

Penetration Testing And Red Teaming Built Around Your Risk Profile

- External network testing - Edge infrastructure, internet-facing apps and services, exposed management interfaces.
- Internal network testing - Lateral movement, privilege escalation, data-access paths once an attacker is inside.
- Web application and API testing - Authentication and authorization flaws, business-logic abuse, injection, session weaknesses, API misuse.
- Mobile application testing - iOS and Android apps, API backends, data storage, and transport protections.
- Cloud infrastructure testing - IAM misconfigurations, insecure storage, misrouted services, attack paths between accounts and tenants.
- OT/ICS and SCADA assessments - Carefully scoped, safe-by-design testing for industrial and critical environments, focused on realistic attack paths without operational disruption.

Each engagement delivers an executive summary, detailed technical remediation report, and optional retest to confirm that high-risk issues are actually closed.

Contact Us
info@eSurelTy.com
www.eSurelTy.com

Red teaming and adversary emulation – proving detection and response

Where penetration testing focuses on specific assets, red teaming tests your entire defense:

- **Full-scope adversary emulation** - Operations mapped to known threat actor TTPs using MITRE ATT&CK–style scenarios.
- **Social engineering and phishing** - Scoped, authorized campaigns that test user behavior, workflows, and escalation, not just click rates.
- **Physical security testing** - Where contracted and legal, to validate access controls, visitor processes, and on-premise weaknesses.
- **Persistence and exfiltration simulations** - Controlled operations to see if your SOC can detect, investigate, and contain a determined adversary.

Purpose: expose the real gap between how your security program performs on a diagram and how it responds under pressure.

Purple teaming and detection validation

Purple-team engagements bring offensive and defensive teams together:

- Controlled tests to tune detections, runbooks, and playbooks in real time
- Validation of EDR/SIEM alerting, SOC workflows, and incident escalation paths
- Concrete detection engineering tasks tied to attacker behavior, not generic signatures

The outcome: fewer blind spots, fewer missed or noisy alerts, and reports that show your security operations actually work under real-world pressure.

Deliverables you can put in front of leadership and oversight bodies

You get more than a vulnerability list. You get decision-grade outputs.

- **Executive Summary:** Board-ready snapshot of risk posture, composite risk score, and the top business-critical issues in plain language.
- **Technical Remediation Report:** Reproducible findings, supporting evidence, and PoC notes (where allowed) with exact remediation steps and references for your engineering and operations teams.
- **Detection And Response Gap Report:** Mapping of missed, late, or noisy alerts; SIEM and EDR tuning guidance; recommended SOC playbook updates; clear detection engineering backlog.
- **Retest And Validation Results:** Confirmation that critical and high-risk issues have been fixed, with updated evidence you can provide to auditors, regulators, and internal risk committees.

Methodology that holds up to auditors and stakeholders

eSurelTy follows a transparent, structured methodology so your results are credible, repeatable, and defensible:

- **Scoping And Rules Of Engagement**
  - Define objectives, in-scope assets, out-of-scope systems, and business constraints
  - Agree on permitted techniques, communication protocols, and success criteria
  - Set clear safeguards for production, OT/ICS, and high-availability systems
- **Reconnaissance And Threat Modeling**
  - Passive and active discovery of assets, users, and trust relationships
  - Build realistic attack paths based on your architecture and likely threat actors
- **Vulnerability Analysis And Exploitation**
  - Move beyond scanners to validate real exploitability
  - Prioritize findings by business impact and attacker value—not just CVSS scores
- **Post-Exploitation And Lateral Movement**
  - Demonstrate what an attacker can do with access: data, persistence, privileged control
  - Stay within agreed bounds while illustrating credible worst-case scenarios
- **Reporting And Remediation Validation**
  - Deliver concise executive findings and deep technical guidance
  - Optional retest to confirm that remediation is effective and durable

Every step is documented with chain-of-custody and evidence handling practices that support audits, regulatory reviews, and internal investigations.

Why eSurelTy

- **Human-driven first** - All assessments are led by experienced human testers; automation and tooling only amplify their work. No “AI-only” penetration testing, no auto-generated noise.
- **Adversary-aware expertise** - Testers with hands-on backgrounds in offensive security, incident response, and SOC operations who understand both sides of the attack.
- **Risk- and governance-ready perspective –** Reporting designed for executives, boards, and auditors—clear documentation of due diligence, control effectiveness, and remediation progress.
- **End-to-end engagement support** - From initial scoping and asset selection through remediation validation and preparation for future audits or board updates.
- **Safe testing for sensitive environments** - Strict rules-of-engagement, production safeguards, and OT/ICS-specific precautions to protect availability and safety while still exposing real weaknesses.

Get your environment tested before your next major audit, board review, or incident—not after.
Contact eSurelTy to schedule a scoping call and align your next engagement with your risk and security objectives.

Contact Us
info@eSurelTy.com
www.eSurelTy.com