OFFENSIVE SECURITY SERVICES

Continuous. Offensive.
Measurable. Secure.

ZecurX
Break. Build. Secure.

Company Overview

ZecurX is a cutting-edge cybersecurity and technology enterprise offering a full spectrum of offensive security services, enterprise-grade solutions, and security-integrated product development. We specialize in helping organizations proactively secure their infrastructure, applications, and digital assets while enabling innovation through secure development practices.

With a strong foundation in ethical hacking and offensive security, ZecurX is built by certified professionals with international recognition. We combine hands-on penetration testing with secure software engineering and network hardening, empowering enterprises to stay ahead of evolving cyber threats.

Vision

To become a global leader in enterprise cybersecurity and secure technology innovation by integrating proactive defense, offensive security, and AI-powered solutions across digital ecosystems.

Mission

To deliver enterprise-grade cybersecurity services, secure software products, and advanced training solutions, helping businesses, institutions, and developers build and maintain trusted, attack-resilient systems.

Core Offerings

Enterprise Cybersecurity Services

- **Penetration Testing as a Service (PTaaS):** Real-time vulnerability discovery and exploitation reporting with remediation roadmap, covering web apps, APIs, networks, cloud, IoT, and Active Directory.
- **Vulnerability Assessment & Risk Auditing:** Industry-standard audits (OWASP, NIST, ISO) for risk profiling, compliance alignment, and asset protection.
- **Red Team Assessments:** Simulated adversarial attacks tailored for enterprise security stress testing and breach detection.
- **Security Operations & Threat Hunting:** Continuous monitoring, behavior-based threat detection, and response strategies for advanced persistent threats (APT).

Secure Software Development & Web Solutions

- **Web & Application Development:** Scalable, custom-built web platforms and enterprise-grade applications designed with DevSecOps integration.
- **Security-Centric Code Review & Testing:** Manual and automated code analysis to identify logical and architectural flaws before deployment.
- **Cloud Application Security:** Design and hardening of secure cloud-native applications (AWS, Azure, GCP) with CI/CD security gates.
- **Enterprise Dashboard & Portals:** Robust, role-based portals for academic institutions, internal enterprise tools, and real-time analytics.

Core Offerings

Corporate & Institutional Training Programs

- **Enterprise Cybersecurity Training (Offline + Cloud-Labs):** 160-hour AI-powered, hands-on training program for corporate teams, IT departments, and academic partners.
- **Faculty Development Programs (FDP):** Up-skilling faculty members in offensive security, red teaming, and secure programming principles.
- **Custom Workshops & Seminars:** Tailored workshops in Offensive Security, Ethical Hacking, and Awareness Programs for colleges and corporates.
- **Certification Programs:** Proprietary certifications like zxCPEH and zxCPPT with verifiable license numbers, ranked trainers, and national-level recognition.

Key Differentiators

- **Enterprise-First Approach:** We design, test, and deliver with enterprise environments in mind: scalable, secure, and compliant.
- **End-to-End Security Integration:** From code to cloud, our services embed security throughout the SDLC and deployment.
- **Original IP & Tools:** All CTFs, training modules, and utilities are 100% original and branded under ZecurX.
- **Verified Certifications:** Our students receive certifications traceable on the ZecurX platform via license ID.
- **Elite Talent Pool:** Our team includes EC-Council Certified Ethical Hackers and industry-recognized professionals.

ZecurX

Break. Build. Secure

ZecurX Red Team Assessments

Adversary Simulation. Breach Validation.
Organizational Readiness.

Executive Overview

Modern cyber threats are no longer simple malware or misconfigurations.
They are well-funded, persistent, multi-step adversaries who chain together:

- Social engineering
- Identity compromise
- Cloud pivots
- Lateral movement
- Privilege escalation
- Data exfiltration

ZecurX Red Team Assessments emulate these real-world attack paths to uncover:

- How an attacker breaks in
- How far they can go
- What your environment exposes
- Whether your security team detects or stops them

This is not a vulnerability scan.
This is real-world breach simulation without the real-world damage.

Purpose & Strategic Mission

The Reality

Organizations increasingly face sophisticated human-driven attacks:

- Ransomware groups
- Nation-state threat actors
- Supply chain breaches
- Insider threat risks

Traditional pentests reveal technical issues. Red Teaming reveals organizational exposure.

ZecurX Mission

To simulate authentic, controlled adversaries that help teams measure, mature, and strengthen their defensive posture end-to-end.

Why Legacy Security Testing Fails

What Organizations Expect	What Traditional Pentesting Lacks	What Goes Wrong
Identify true breach paths	Only surface-level vulnerabilities	Hidden kill chains remain unknown
Test detection capability	No monitoring/resilience testing	SOC blind spots
Measure response maturity	Not designed to evaluate IR teams	Delayed or ineffective response
Challenge user awareness	No phishing/social engineering	People remain untested
Gauge cloud & identity risk	Limited AD/ cloud exploitation	Attackers escalate silently

Red Teaming closes the detection–response–awareness gap.

Why Legacy Security Testing Fails

What Organizations Expect	What Traditional Pentesting Lacks	What Goes Wrong
Identify true breach paths	Only surface-level vulnerabilities	Hidden kill chains remain unknown
Test detection capability	No monitoring/resilience testing	SOC blind spots
Measure response maturity	Not designed to evaluate IR teams	Delayed or ineffective response
Challenge user awareness	No phishing/social engineering	People remain untested
Gauge cloud & identity risk	Limited AD/ cloud exploitation	Attackers escalate silently

Red Teaming closes the detection–response–awareness gap.

Key Benefits

Real-World Adversarial Emulation
Simulates actual threat actors (FIN7, APT29, ransomware groups) with mapped MITRE ATT&CK techniques.

Internal Threat Hunting Triggers
The assessment activates internal SOC/hunting workflows, revealing:

- Missed detections
- False negative patterns
- Slow triage gaps • Alert fatigue points

Breach Impact Visualization
Shows exactly:

- What attackers could access
- What systems were vulnerable
- What data could be stolen
- How close a real breach could occur

Customized TTPs (MITRE ATT&CK-Aligned)
Scenarios crafted for:

- Cloud environments
- AD-heavy infrastructures
- Hybrid networks
- Remote workforce
- Industry-specific threats (FinTech, Healthcare, SaaS)

What ZecurX Red Team Assessments Are

ZecurX delivers **multi-vector, multi-phase adversarial simulations** designed to evaluate:

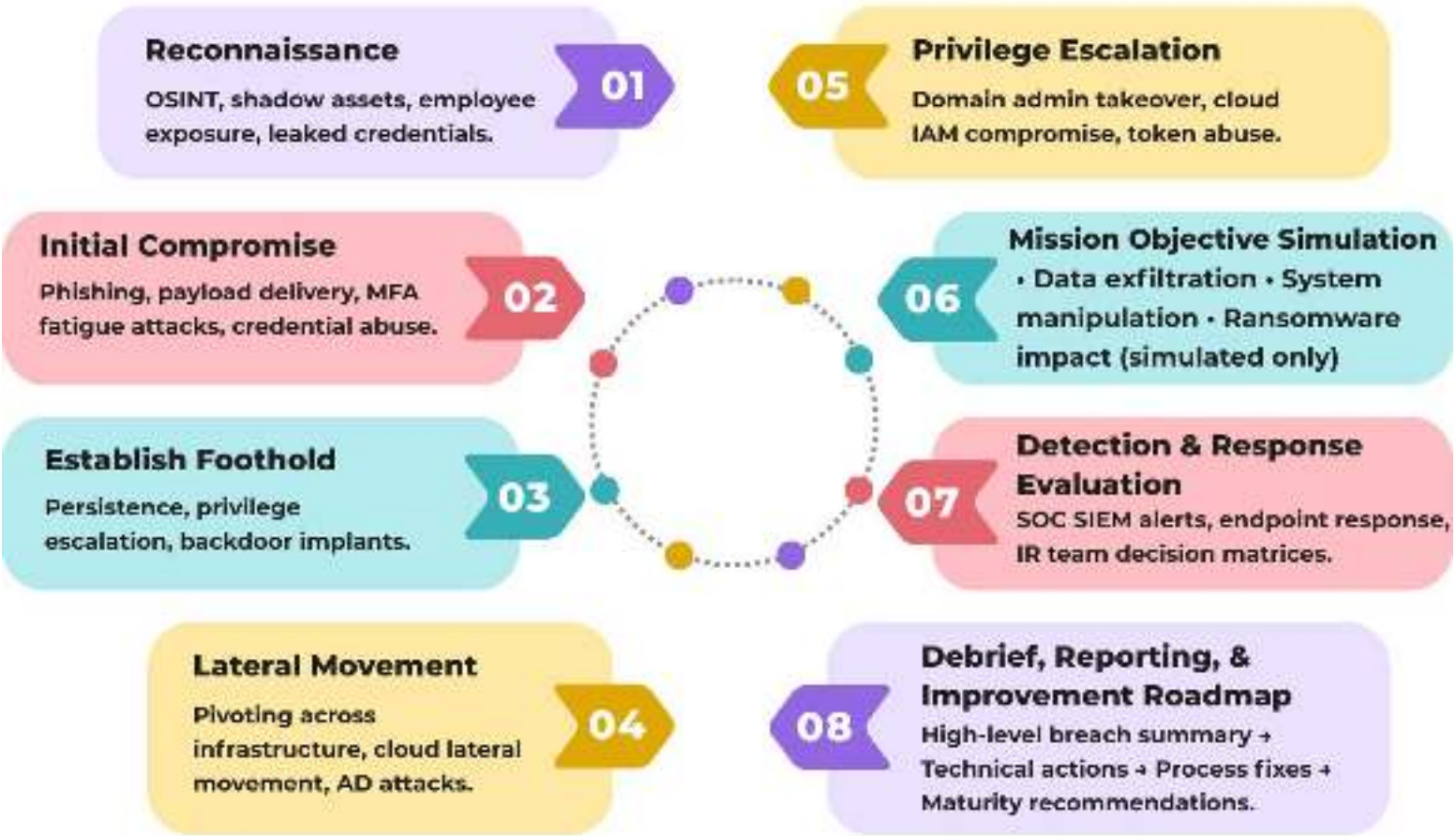
- People (awareness, fallibility, decision-making)
- Processes (IR workflows, escalation readiness)
- Technology (SIEM, EDR, identity security, cloud posture)

Adversarial Emulation + Breach Validation + Organizational Maturity

This enables organizations to see **how a real attacker would operate** within their environment — safely and ethically.

Red Team Assessment Methodology (Full Kill Chain)

ZecurX follows an intelligence-driven attack lifecycle:



Complete Offensive Testing Lifecycle

Stage	What ZecurX Delivers	Enterprise Impact
Reconnaissance	OSINT, attack surface mapping	Early discovery of unknown risks
Enumeration	Port, service, identity enumeration	Foundation for real exploitation
Exploitation	Manual exploit chains + automation	Proof of real business risk
Privilege Escalation	Lateral, vertical privilege gain	Visibility into breach blast radius
Impact Simulation	Data access, takeover scenarios	True risk prioritization
Reporting & PoC	Videos, screenshots, attack paths	Developer clarity
Remediation Support	Fix validation & consulting	Faster patch cycles
Continuous Retest	Automated & on-demand	Ongoing security assurance

Security is not an event — it is a continuous cycle.

Detection & Response Maturity Evaluation

Red Team Assessments highlight your real security posture:

Detection Questions Answered:

- Did your EDR detect malicious behavior?
- Did SIEM raise relevant alerts?
- Were logs complete or missing critical telemetry?

Response Questions Answered:

- Did IR teams respond on time?
- Was escalation appropriate?
- Were containment procedures followed correctly?

Outputs include:

- False negatives map
- Alert correlation gaps
- Logging deficiencies
- SOC performance score
- IR playbook effectiveness grade

Intelligence & Reporting Layer

Attack Path Map

Visualized chain from initial access to domain control and data exfiltration.

Breach Timeline

Minute-by-minute attacker activity and defender response.

Executive Summary

Business risk overview: financial impact, brand exposure, compliance risk.

Technical Report

TTP mapping, exploit PoCs, detection gaps, required controls.

Remediation Roadmap

Prioritized fixes across people, process, technology, and architecture.

Assessment Components

1. Social Engineering Campaigns	• Spear phishing • Vishing • MFA fatigue attacks • QR code phishing • Credential harvesting portals
2. Network Attack Simulation	• Internal pivoting • Weak segmentation exploitation • Hidden asset discovery
3. Active Directory & Identity Attacks	• Kerberoasting • Pass-the-Hash • Token manipulation • Golden ticket simulation
4. Cloud Intrusions (AWS/Azure/GCP)	• IAM misconfig exploitation • Over-permissioned roles • Cross-tenant traversal (where applicable)
5. Endpoint & EDR Evasion	Test your agent's ability to: • Detect malicious activity • Block payload execution • Prevent credential theft • Stop lateral movement

Multi-Industry Red Team Use Cases

Industry	Red Team Focus Areas
Banking	Fraud systems, SWIFT workflows, privileged banking apps
Healthcare	EMR access, PHI leakage, ransomware simulation
IT & SaaS	Multi-tenant breakout attempts, CI/CD attack chains
Government	Identity abuse, data exfiltration simulations
Manufacturing	OT/ICS environment compromise
E-commerce	Payment flows, API abuse, customer data targeting

Where protection failures are unacceptable — ZecurX reveals them first.

Why Enterprises Choose ZecurX

Value Dimension	Traditional Pentest	ZecurX Red Team Assessment
Threat realism	Limited	High (APT-inspired TTPs)
Detection evaluation	No	Complete SOC simulation
Response evaluation	No	Full IR testing
Impact analysis	Low	Actionable breach-level insight
Reporting	Snapshot	Live timeline + attack map
User awareness	Minimal	Full social engineering suite
Cloud & identity testing	Basic	Multi-layered exploitation

ZecurX offers **true adversarial perspective**, not just vulnerability discovery.

Final Call to Action

A breach is not a matter of “if” — but “when.” Red Teaming prepares you for both.

ZecurX — Real Attacks. Real Insights. Real Readiness.

Our Partners & Pages

GURUDEV ENGICON
PRIVATE LIMITED

Gurudev Engicon Pvt. Ltd.

HONEY HERBAL BEAUTY PARLOUR

Honey Herbal Beauty Parlour

My Garden Space

My Garden Space

& many more available on our website ZecurX

Book your ZecurX Red Team Assessment

Understand your real exposure. Strengthen your defenses. Stay ahead of adversaries.

Contact us:

ZecurX

Yelahanka, Bengaluru-560064

Website: www.zecurx.com

Phone: 7488813601

Email: official@zecurx.com

Instagram: @zecurx