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

Security Operations & Threat Hunting

Continuous Monitoring. Proactive Hunting.
Intelligent Defense.

Executive Overview

Cybersecurity today is no longer about blocking known threats — it's about identifying **unknown, emerging, and behavior-driven attacks** before they cause impact.
Modern attackers bypass signatures, evade detection, exploit identity systems, and operate quietly inside networks for months.

ZecurX Security Operations & Threat Hunting combines:

- Continuous monitoring
- Behavior-based analytics
- AI-driven anomaly detection
- Real-time log correlation
- Threat intelligence
- Proactive hunt missions

This creates a defense system that is **predictive, not reactive.**

Purpose & Strategic Mission

The Detection Gap

- 80% of breaches are discovered months later.
- 60% of attacks originate from compromised identities.
- Traditional SIEM-only setups miss lateral movement and insider threats.

ZecurX Mission

To deliver advanced detection capabilities that identify malicious behavior across endpoints, cloud, identities, and networks — **before attackers achieve their objectives.**

Our goal:

Turn raw data into actionable detection.

Turn alerts into decisions.

Turn threats into prevention.

Key Benefits

Detect APTs, Insider Threats & Anomalies
Go beyond signature detection with:
- Behavioral fingerprints
- Dwell-time reduction
- User/entity behavior analytics (UEBA)
- Identity threat detection

AI & Log Analytics
AI-enhanced models detect:
- Impossible travel
- Rare logon sources
- Privilege escalation attempts
- Cloud configuration drift

Seamless SIEM/SOAR Integration
Supports platforms such as:
- Microsoft Sentinel
- Splunk
- IBM QRadar
- Elastic SIEM
- Palo Alto Cortex XSOAR

Monthly Threat Intelligence Reports
You receive:
- Industry-specific threat trends
- Observed attack patterns
- MITRE technique evolution
- Emerging malware indicators
- Zero-day alerts

Where Traditional Monitoring Fails

What Organizations Need	Why Legacy Monitoring Fails	Resulting Gaps
Behavior detection	Signature-based alerts only	Missed APTs & insider threats
Rapid triage	High alert fatigue	Slow response
Visibility across cloud & endpoints	Fragmented logs	Blind spots
Proactive threat hunting	Not included	Unknown threats persist
Threat intelligence	Static feeds	No contextual correlation
Incident readiness	No playbooks or modeling	Slow IR activation

ZecurX addresses these detection and response challenges holistically.

What ZecurX Security Operations & Threat Hunting Is

A unified security operations service that provides:

- Monthly threat intelligence briefings
- Continuous monitoring across all assets
- Incident simulation & response planning
- SIEM/SOAR integration for automated triage
- Threat hunting missions based on MITRE ATT&CK
- AI-enhanced detection of anomalies and suspicious behavior

This is not a log management service. It is a proactive threat detection ecosystem.

Threat Hunting Lifecycle

1. Hypothesis Creation

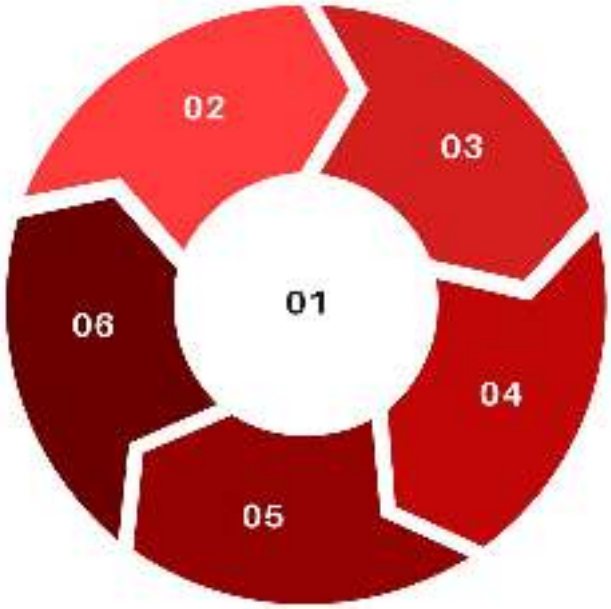
Based on intel, alerts, attacker patterns.

2. Data Collection & Correlation

Log analytics + AI + anomaly scoring.

3. Pattern Discovery

Identify hidden attacker movements.



4. Investigation

Deep dive into root cause and impact.

5. Response Recommendation

Isolation, containment, hardening steps.

6. Validation & Reporting

Measure detection coverage & gaps.

Hunting is continuous — attackers don't wait.

Threat Hunting Lifecycle

Advanced Telemetry Correlation

All events are enriched with:

- Threat intelligence
- MITRE ATT&CK mapping
- Geo-IP analysis
- AI anomaly scoring

Incident Readiness Modeling

Simulated scenarios to test:

- IR team readiness
- SOC response time
- Detection quality
- Escalation accuracy

Daily/Weekly/Monthly Analysis

- SOC summary reports
- Alert pattern changes
- Observed threat vectors
- Operational improvements

Core Capabilities

1. Behavior-Based Detection	• Uncover malicious intent through: • Abnormal login patterns • Unusual lateral movement • Rare process executions • Identity misuse indicators
2. Continuous Monitoring	24/7 correlation of: • Logs • Events • Identity telemetry • Network traffic • EDR signals • Cloud audit logs
3. Proactive Threat Hunting	Regular hunt missions targeting: • APT techniques • Zero-day behavior patterns • Insider activity • Credential misuse • Cloud privilege escalations
4. SIEM/SOAR Integration	Automated workflows for: • Alert enrichment • Blocking malicious IPs • Account isolation • Case creation • Automated triage

Security Operations Coverage Areas

01

Identity & Access Monitoring

- Privilege misuse
- MFA bypass attempts
- Token theft signals

02

Cloud Monitoring

- Malicious process execution
- Lateral movement indicators
- Persistence mechanisms

03

Endpoint & Server Monitoring

- IAM role escalation
- Public exposure alerts
- Cloud drift detection

04

Network Monitoring

- C2 channel detection
- Beaconing activity
- DNS tunneling

05

Application & API Monitoring

- Anomalous requests
- Access pattern deviations

A complete visibility ecosystem.

Multi-Industry Use Cases

Industry	Threat Hunting Focus Areas
Banking & FinTech	Fraud pattern detection, insider misuse, identity anomalies
Healthcare	PHI access misuse, ransomware detection, medical system monitoring
SaaS & Tech	Cloud escalation paths, identity compromise, supply chain signals
Retail & E-commerce	Payment system anomalies, bot detection patterns
Manufacturing	OT network anomalies, ICS threat detection
Government	APT detection, espionage behavior analytics

Where threats evolve daily — ZecurX brings continuous defensive intelligence.

Why Enterprises Choose ZecurX

Value Dimension	Traditional SOC	ZecurX SOC + Threat Hunting
Detection method	Signature-based	Behavioral + AI
Visibility	Limited	Full identity, cloud, endpoint coverage
Threat hunting	Not included	Continuous hunt missions
Response	Manual	Automated SOAR playbooks
Threat intelligence	Generic feeds	Monthly tailored reports
Maturity evolution	Stagnant	Continuous improvement roadmap

ZecurX delivers **intelligent detection, not noisy alerts.**

Final Call to Action

Modern threats are adaptive.
Your security operations must be smarter, faster, and more proactive.

See threats earlier.
Respond intelligently.
Stay ahead of adversaries.

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

Activate ZecurX Security Operations & Threat Hunting today.

ZecurX — Intelligence-driven cybersecurity for the modern enterprise.

Contact us:

ZecurX

Yelahanka, Bengaluru-560064

Website: www.zecurx.com

Phone: 7488813601

Email: official@zecurx.com

Instagram: @zecurx