BUSINESS MODEL: BREAKING POINT IDENTIFICATION WITH MITIGATION GUIDANCE

OVERVIEW

Breaking Point identification with mitigation guidance as a Service enables enterprises to test and validate the resilience, scalability, and security of their IT and OT infrastructure against realistic and sector-specific cyber threat scenarios. Powered by an indigenous hybrid **Cyber Range**, organizations gain actionable insights into their cyber readiness posture.

The service is delivered through three tiers — **Bronze, Silver, and Gold** — enabling organizations to align testing with their criticality, compliance requirements, and risk appetite.

CLIENT FITMENT EVALUATION CRITERIA

Zettawise uses a structured evaluation framework to determine whether a client organization best fits the **Bronze, Silver, or Gold** service model. The following parameters are assessed:

1. **Organizational Maturity**
   - Assessment of governance structures, cybersecurity program maturity, and existing risk management processes.
2. **Organizational Culture**
   - Evaluation of leadership commitment, cybersecurity awareness across staff, and integration of security into daily business processes.
   - Identifies if the culture supports proactive resilience or is reactive to incidents.
3. **Business Model Complexity**
   - Analyzes business operations, regulatory obligations, and dependency on IT/OT systems.
4. **Knowledge, Skill, and Ability (KSA) of the Technology Workforce**
   - Measures the competence of internal IT, OT, and cybersecurity teams.
5. **Regulatory and Compliance Requirements** *(Additional Parameter)*
   - Evaluation of applicable mandates (ISO 27001, IEC 62443, NIST CSF, RBI, SEBI, NCIIPC, GDPR, etc.).
6. **Risk Appetite and Tolerance** *(Additional Parameter)*
   - Determination of how much risk the organization is willing to accept versus mitigate.
   - Low risk tolerance drives the need for higher-tier services.
7. **Incident History and Threat Exposure** *(Additional Parameter)*
   - Review of past security breaches, attempted attacks, and exposure to sector-specific threats.

SERVICE SEGMENTS

BRONZE LEVEL

Assess resilience of enterprise IT systems, identify fault thresholds, using Cyber Range and suggest actionable mitigations.

Coverage Parameters:

- **Sitewise Network Simulation**: Emulation of customer network architecture, identifying bottlenecks and testing segmentation effectiveness. Creation of the exact replica of the Client Information Communication and Technology network shall be done only after exact license / firmware is provided by the client. In case such licenses are not available, the available near match version shall be used to create the simulation environment.
- **Core Devices Testing**: Evaluation of routers, switches, firewalls, and load balancers for performance, Load/Stress Testing and DDoS resilience.
- **Enterprise Application Traffic Simulation**: Generating web, email, Enterprise traffic under normal and stress conditions; detecting application-layer vulnerabilities.
- **Hybrid Infrastructure Simulation**: Replicating traffic flows across on-premise and cloud setups to detect misconfigurations, architectural deficiencies and validating OEM FAT reports/ published data sheets.
- **Attack Vectors Application**: Simulating phishing, brute-force, and basic ransomware to test IDS/IPS, host devices (up to 5 critical servers only, up to 20 randomly selected endpoints), firewall effectiveness.
- **Malware Propagation Test**: Simulating spread of sector-specific malware; measuring EDR/XDR effectiveness.

Sample Output Reports:

- Resilience Scorecard
- Attack Vector Impact Report
- Executive Summary Dashboard

SILVER LEVEL

Enhanced coverage with **advanced adversarial simulation and proactive risk assessment** for organizations with moderate to high security requirements.

Coverage Parameters:

- **Advanced Threat Emulation**: Simulates multi-stage Advanced Persistent Threats (APTs), ransomware campaigns, and kill chain attacks to assess maturity across the attack lifecycle.
- **Cloud & Multi-Cloud Traffic Simulation**: Tests workloads in SaaS, IaaS, and PaaS environments to detect misconfigurations and improper access controls.
- **Encrypted Traffic Testing (SSL/TLS, IPSec)**: Validates IDS/IPS and firewall capabilities for traffic carried over secure channels.
- **Insider Threat Simulation**: Mimics credential theft, privilege escalation, and lateral movement scenarios to test detection and response.
- **Incident Response Stress Testing**: Evaluates SOC and IR teams under live simulated attacks, measuring detection speed and containment effectiveness.
- **Comprehensive Attack Surface Mapping**: Identifies vulnerabilities across endpoints, IoT, shadow IT, and network perimeters.
- **Zero-Day Attack Simulation**: Uses threat libraries to mimic exploits before patches are available.

- **Incident Recovery Responses Effectiveness**: Evaluates the efficiency and timeliness of organizational recovery measures post-attack, including data restoration, service resumption, and adherence to RTO/RPO benchmarks.

Sample Output Reports:

- Advanced Threat Simulation Report
- SOC Response Readiness Matrix
- Cloud Security Resilience Report
- Insider Threat Propagation Map
- Network Resilience Heatmap

GOLD LEVEL

A **premium, continuous assurance model** for mission-critical and highly regulated organizations.

Coverage Parameters:

- **Continuous Attack Simulation**: Quarterly campaigns to ensure constant readiness.
- **Complete Digital Twin Deployment**: Replica of IT and OT environments for safe, realistic attack testing.
- **Customized Threat Intelligence Integration**: Aligns testing with live global and sector-specific threat feeds.
- **Business Continuity & DR Validation Under Simultaneous Attack/Failure Scenarios**: Combines cyberattacks with infrastructure failures like outages to test compound crisis readiness.
- **AI/ML-Based Anomaly Detection Validation**: Introduces subtle anomalies in traffic to test AI/ML-driven systems for false positives/negatives and adaptive learning.
- **Supply Chain Resilience Testing (3rd-Party/Vendors)**: Evaluates resilience of vendor-provided platforms, APIs, and third-party integrations against compromise.
- **Regulatory & Compliance Alignment Tests**: Ensures readiness against ISO 27001, IEC 62443, NIST CSF, RBI, SEBI, NCIIPC frameworks.
- **Executive & Board-Level Reporting**: Business-friendly reporting with ROI, risk forecasts, and resilience heatmaps.
- **Red Team – Blue Team Exercises**: Blends offensive and defensive exercises for real-time resilience assessment.
- **Sectoral Malware Campaign Testing**: Tailored simulations for industry-specific threats (ICS ransomware, banking trojans, healthcare IoT attacks).
- **Core Device Firmware Vulnerabilities**: Conducts in-depth analysis of firmware versions and configurations of critical network devices (routers, switches, firewalls, industrial controllers), identifying exploitable flaws and recommending patching or configuration hardening.

Sample Output Reports:

- Digital Twin Threat Impact Dashboard
- Regulatory Compliance Scorecard
- Business Continuity Stress Test Report
- Executive Cyber Risk Heat Map
- Annual Resilience Trend Report
- AI/ML Detection Effectiveness Report
- Supply Chain Resilience Dashboard

COMPARATIVE SERVICE LEVEL TABLE

Service Component	Bronze	Silver	Gold
Sitewise Network Simulation	✅	✅	✅
Core Devices Testing (Physical/Emulated)	✅	✅	✅
Enterprise Application Traffic Simulation	✅	✅	✅
Hybrid Infrastructure Simulation	✅	✅	✅
Attack Vectors for Resilience Testing	✅	✅	✅
Malware Propagation Test (Sector Use Cases)	✅	✅	✅
Advanced Threat Emulation (APT, Ransomware, Kill Chain)	❌	✅	✅
Cloud & Multi-Cloud Traffic Simulation	❌	✅	✅
Encrypted Traffic Testing (SSL/TLS, IPSec)	❌	✅	✅
Insider Threat Simulation	❌	✅	✅
Incident Response Stress Testing	❌	✅	✅
Comprehensive Attack Surface Mapping	❌	✅	✅
Zero-Day Attack Simulation	❌	✅	✅
Incident Recovery Responses Effectiveness	❌	✅	✅
Continuous Attack Simulation	❌	❌	✅
Digital Twin Deployment	❌	❌	✅
Customized Threat Intelligence Integration	❌	❌	✅
BCP/DR Validation Under Simultaneous Attack/Failure	❌	❌	✅
AI/ML-Based Anomaly Detection Validation	❌	❌	✅
Supply Chain Attack Simulation	❌	❌	✅
Regulatory & Compliance Alignment	❌	❌	✅
Executive & Board-Level Reporting	❌	❌	✅
Red Team – Blue Team Exercises	❌	❌	✅
Customized Sectoral Malware Campaigns	❌	❌	✅
Core Device Firmware Vulnerabilities	❌	❌	✅