Security Services

1. Network Security & Infrastructure Hardening

We secure enterprise network infrastructures against **Advanced Persistent Threats (APT)** and sophisticated cyber attacks using globally recognized security frameworks (**CIS, NIST, ISO 27001, MITRE ATT&CK**) combined with proprietary automation tools for rapid, repeatable, and verifiable hardening. Our approach ensures maximum resilience while maintaining operational efficiency.

By implementing this package, your organization will:

- Significantly reduce the risk of cyber intrusions and ransomware attacks
- Achieve compliance with leading international security standards (CIS, NIST, ISO 27001)
- Gain full visibility over network security posture through continuous monitoring
- Ensure rapid detection and response to any security incident
- Build long-term resilience against both external hackers and insider threats
- Protect critical data, maintain operational continuity, and safeguard brand reputation

---

Service Tiers

Tier 1 – Foundational Security Hardening

- Full infrastructure security assessment against **CIS Controls v8** and **NIST SP 800-53**
- Secure baseline configuration of **Layer 2 & Layer 3** devices (Cisco, Mikrotik, Juniper)
- Firewall configuration review, rule optimization, and **attack surface minimization**
- Windows Server & Active Directory **Group Policy Object (GPO)** hardening
- Administrative privilege restriction & credential hygiene enforcement
- Automated baseline deployment using **Ansible, Python, and Infrastructure-as-Code (IaC)**
- Logging & audit policy configuration to ensure forensic readiness

---

Tier 2 – Advanced Network Defense

- All Foundational features
- Virtualization platform hardening (**VMware vSphere, Hyper-V, Proxmox**)
- Advanced network segmentation & **Zero Trust Architecture** deployment

- Network Access Control (NAC) enforcement with device posture checks
- Continuous network monitoring using **SIEM/SOC** with custom correlation rules
- Automated vulnerability scanning integrated with **real-time threat intelligence feeds**
- Configuration compliance verification against CIS, NIST, and **ISO 27001 Annex A controls**
- Secure configuration of remote access (VPN, SSL, IPsec) with MFA enforcement

---

Tier 3 – Offensive Security & Assurance

- All Advanced features
- Proprietary **white-box, black-box** covering internal & external attack vectors
- **Red Team simulations** aligned with MITRE ATT&CK framework for realistic adversary emulation
- Social engineering & phishing resilience testing for staff awareness measurement
- Exploitation reporting with **risk-prioritized remediation roadmap**
- Automated **post-remediation validation** to ensure all vulnerabilities are closed
- Executive-level **Security Posture & Compliance Report** for board-level decision-making
- Optional integration with **Continuous Security Validation** platforms

---

2. Web & Application Security

We safeguard mission-critical web and application assets through **automated compliance validation, continuous vulnerability management, and advanced attack simulations**. Our methodology aligns with **CIS Benchmarks, NIST SP 800-53, OWASP Top 10, OWASP API Top 10, and ISO/IEC 27034**, integrating proprietary testing tools and automation frameworks to ensure long-term resilience.

By implementing this package, your organization will:

- Drastically reduce the likelihood of website or application breaches
- Eliminate common vulnerabilities such as SQL Injection, XSS, CSRF, and API abuse
- Protect customer data and meet compliance requirements (PCI-DSS, GDPR, ISO 27034)
- Maintain continuous security even during development cycles through DevSecOps integration
- Gain 24/7 visibility into web threats with instant response capabilities
- Safeguard brand reputation, customer trust, and operational continuity

---

Service Tiers

Tier 1 – Secure Hosting & Server Baseline

- Full hardening of **Linux-based hosting** environments (SSH, kernel security, file permissions, service lockdown...)
- Secure web server configuration (Apache, Nginx, IIS) based on **CIS & NIST guidelines**
- Automated **malware, rootkit, and integrity monitoring** with anomaly detection
- DNS security hardening & anti-DNS hijacking measures, TLS 1.3 enforcement, HSTS, and perfect forward secrecy configuration
- Server resource isolation & sandboxing for hosted applications

---

Tier 2 – Application-Level Protection

- All **Secure Hosting** features
- Comprehensive **OWASP Top 10** & **OWASP API Security Top 10** vulnerability testing
- Proprietary **application-layer penetration testing** (logic flaws, business logic abuse, chained vulnerabilities)
- Web Application Firewall (**WAF**) deployment, tuning, and custom rule writing
- Continuous automated vulnerability scanning with **threat intelligence integration**
- Secure session management & authentication hardening (MFA, token-based auth)
- API gateway security enforcement and abuse prevention

Tier 3 – Full Lifecycle Application Security Management

- All **Application-Level Protection** features
- Continuous **DevSecOps** integration with CI/CD pipelines (SAST, DAST, IAST)
- Real-time security event correlation with **SIEM/SOC** integration
- 24/7 **application-level threat monitoring** and incident response coverage
- Automated **security patch management** for CMS, frameworks, and libraries
- Secure code review & static/dynamic analysis for in-house development
- Deployment of **Runtime Application Self-Protection (RASP)** for real-time attack mitigation
- Periodic **bug bounty program management** for proactive vulnerability discovery

---

3. Information Security Management & Compliance (ISMS)

We help organizations design, implement, and maintain an **Information Security Management System (ISMS)** aligned with **ISO/IEC 27001:2022**, **NIST Cybersecurity Framework (CSF)**, and other regulatory frameworks such as **GDPR, PCI-DSS, and UAE NESA standards.** Our approach combines governance, risk management, and compliance (GRC) best practices with automation tools for continuous readiness and audit success.

By implementing this package, your organization will:

- Achieve and maintain **international security certifications** (ISO/IEC 27001, NIST CSF)
- Prove compliance to regulators, partners, and clients, enhancing trust and credibility
- Reduce operational, legal, and reputational risks associated with data breaches
- Ensure continuous readiness for audits with minimal disruption to operations
- Establish a security-aware culture across all levels of the organization
- Strengthen resilience against both cyber and physical security threats

Service Tiers

Tier 1 – ISMS Gap Analysis & Foundation

- Compliance readiness assessment against **ISO 27001, NIST CSF, GDPR, PCI-DSS, UAE NESA**
- Information asset inventory, classification, and ownership assignment
- Initial **risk assessment** and threat landscape mapping
- Development of core information security policies, standards, and procedures
- Security awareness & compliance training for staff and management
- Basic incident response policy & escalation procedures
- Executive gap analysis report with prioritized roadmap

Tier 2 – ISMS Full Implementation

- All **Foundation** features
- Comprehensive **ISMS documentation** (Statement of Applicability, Risk Treatment Plan, Security Manual)
- Implementation of **Annex A controls** from ISO/IEC 27001:2022
- Detailed **risk treatment plan** with mitigation strategies and control deployment
- Business Continuity & Disaster Recovery (BC/DR) planning aligned with **ISO 22301**
- Internal compliance audits, pre-certification assessments, and readiness checks
- Supplier/vendor security assessment and third-party risk management
- Integration of key metrics and KPIs for continuous improvement

Tier 3 – ISMS Managed Service

- All **Full Implementation** features
- Continuous compliance monitoring with automated control verification tools
- Quarterly or annual **internal audits** and full management reviews
- Incident Response integration with SOC for real-time detection & reporting
- Automated compliance reporting dashboards for executives & auditors
- Annual ISMS re-certification support and evidence preparation
- Periodic policy and procedure updates aligned with evolving regulations
- Continuous improvement cycle with threat intelligence integration

4. Specialized Cybersecurity Consulting

Our specialized consulting services provide **high-impact, tailored cybersecurity solutions** for organizations requiring advanced expertise, strategic planning, and hands-on execution. Leveraging globally recognized frameworks such as **MITRE ATT&CK, NIST SP 800 series, CIS Benchmarks, ISO/IEC 27035 (Incident Management), and Zero Trust Architecture**, we deliver advisory and operational support for complex, large-scale, and high-risk environments.

By engaging our specialized consulting services, your organization will:

- Gain tailored, expert-driven solutions to address your unique security challenges
- Enhance resilience against sophisticated cyber threats and targeted attacks
- Rapidly detect, respond to, and recover from complex security incidents
- Ensure cloud environments meet the highest security benchmarks
- Build a proactive defense posture through ongoing threat hunting and adversary simulations
- Align long-term security strategy with evolving business and regulatory requirements

Service Tiers

Tier 1 – Strategic Advisory & Assessment

- Advanced **threat landscape assessment** tailored to your industry and geography
- Review and design of **security architecture** aligned with business objectives
- Cloud security posture review (AWS, Azure, GCP) against **CIS Benchmarks**
- High-level **Zero Trust adoption roadmap**

- Threat Intelligence (TI) integration planning with industry-specific feeds
- Gap analysis for current Incident Response (IR) capabilities against **NIST SP 800-61**

Tier 2 – Advanced Security Operations Enablement

- All **Strategic Advisory** features
- Implementation of **Zero Trust** principles (identity, device, network, application layers)
- Deployment of Threat Intelligence platforms & integration with SOC/SIEM
- Advanced Incident Response playbooks & automation workflows
- Proactive **threat hunting** using hypothesis-driven and behavior-based techniques
- Red/Blue Team exercises for incident preparedness and defense validation
- Forensic readiness planning, evidence handling, and chain-of-custody processes

---

Tier 3 – Comprehensive Cyber Resilience Program

- All **Advanced Security Operations** features
- Full **Purple Team engagements** for continuous improvement of defense capabilities
- Cloud-native security implementation with automated remediation pipelines
- Full-spectrum Incident Response & **Digital Forensics** investigations (malware, insider threats, APT campaigns)
- 24/7 crisis response retainer service for major cyber incidents
- Continuous adversary emulation using **MITRE ATT&CK** and **custom threat scenarios**
- Executive-level cyber risk advisory with quarterly board briefings and threat forecasts