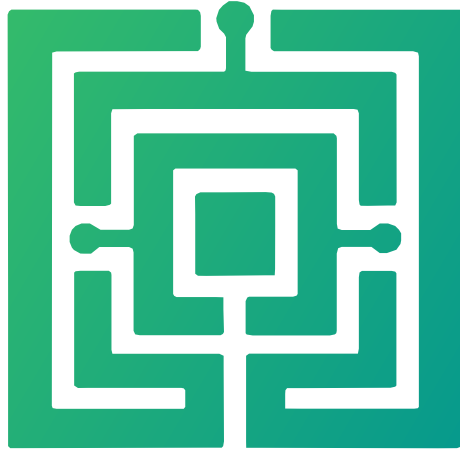


TECHNOLOGY · CYBER DEFENSE · TRADING



TORAIZON

Cybersecurity & SOC Brochure

Offensive, defensive and managed security — in detail

www.toraizon.com.sa

CYBERSECURITY • MANAGED SOC

Security that is run and proven

Security that is built, run and proven by one team.

01

Cybersecurity

Offense and defense under one roof. VAPT, red teaming, compliance audits, identity, cloud security and incident response — everything that stands between your business and a breach.

- ◆ Vulnerability Assessment & Penetration Testing
- ◆ Red Team & Adversary Simulation
- ◆ Security Audits & Compliance
- ◆ Endpoint Detection & Response (EDR/XDR)
- ◆ Identity & Access Management (IAM)
- ◆ Cloud Security & CSPM
- ◆ Application & API Security
- ◆ Data Loss Prevention (DLP) & Encryption
- ◆ Incident Response & Digital Forensics
- ◆ Security Awareness Training & Phishing Simulation

02

Managed SOC

Round-the-clock threat monitoring powered entirely by our proprietary security stack. No third-party tools. Total control. Maximum intelligence. Average threat-to-triage: 4.2 minutes.

- ◆ 24/7 Managed Detection & Response (MDR)
- ◆ SIEM Deployment & Management
- ◆ Threat Hunting & Threat Intelligence
- ◆ Managed EDR/XDR Operations
- ◆ Log Management & Correlation
- ◆ Security Orchestration, Automation & Response (SOAR)
- ◆ Managed Firewall & IPS/IDS
- ◆ Vulnerability Management Programme
- ◆ Incident Escalation & Response Playbooks
- ◆ Monthly Security Posture Reporting

Frameworks We Align To — COMPLIANCE READY

NCA ECC

ISO 27001

SOC 2

PCI-DSS

HIPAA

GDPR

NIST CSF

SAMA CSF

CYBERSECURITY

CYBER SECURITY

Offense and defense under one roof. VAPT, red teaming, compliance audits, identity, cloud security and incident response — everything that stands between your business and a breach.

01

Vulnerability Assessment & Penetration Testing

Web, network, cloud and mobile pentests that find the holes before attackers do.

02

Red Team & Adversary Simulation

Full-scope adversarial simulations testing people, process and technology together.

03

Security Audits & Compliance

Gap analysis and certification support for ISO 27001, SOC 2, PCI-DSS, NCA ECC and more.

04

Endpoint Detection & Response (EDR/XDR)

Real-time endpoint visibility and automated containment against modern malware.

05

Identity & Access Management (IAM)

Least-privilege access, MFA and identity governance across every application.

06

Cloud Security & CSPM

Continuous posture management across AWS, Azure, GCP and hybrid environments.

07

Application & API Security

Secure SDLC, code review and API hardening baked into your development pipeline.

08

Data Loss Prevention (DLP) & Encryption

Policy-driven controls that stop sensitive data leaving your environment.

09

Incident Response & Digital Forensics

Rapid containment, root-cause investigation and chain-of-custody evidence handling.

10

Security Awareness Training & Phishing Simulation

Ongoing staff training and simulated phishing campaigns that measurably cut risk.

Engagement Process — SCOPE TO REMEDIATION

01

Scope

Define target systems, rules of engagement and compliance objectives.

02

Test

Manual and automated testing against the agreed scope.

03

Validate

Every finding manually verified to eliminate false positives.

04

Report

Executive summary plus technical remediation guidance.

05

Retest

Free retest to confirm every fix closes the gap.

Our compliance engineers map every control to evidence — so your next audit is a formality, not a fire drill.

24/7 OPERATIONS

SECURITY OPERATIONS CENTRE

Round-the-clock threat monitoring powered entirely by our proprietary security stack. No third-party tools. Total control. Maximum intelligence. Average threat-to-triage: 4.2 minutes.

01

24/7 Managed Detection & Response (MDR)

Continuous, human-supervised monitoring and response across your entire estate.

02

SIEM Deployment & Management

Centralised log correlation and alerting tuned to your environment.

03

Threat Hunting & Threat Intelligence

Proactive, hypothesis-driven hunts fed by commercial and dark-web intel feeds.

04

Managed EDR/XDR Operations

Full lifecycle management of endpoint and extended detection tooling.

05

Log Management & Correlation

Normalised, retained logs across endpoints, network, identity and cloud.

06

Security Orchestration, Automation & Response (SOAR)

Playbook-driven automation that resolves routine alerts in seconds.

07

Managed Firewall & IPS/IDS

Rule tuning, patching and 24/7 monitoring of perimeter defenses.

08

Vulnerability Management Programme

Continuous scanning, prioritisation and remediation tracking.

09

Incident Escalation & Response Playbooks

Pre-built, rehearsed playbooks that cut response time when it matters.

10

Monthly Security Posture Reporting

Executive-ready reporting on risk trends, incidents and control coverage.

Detection Lifecycle — FROM SIGNAL TO RESPONSE

01

Collect

Endpoint, network, identity, cloud, and application telemetry — normalized and enriched.

02

Detect

ML models, behavioural rules, and IOC matching across the unified data fabric.

03

Triage

Tier-1 analysts validate alerts; SOAR auto-resolves the routine ones.

04

Respond

Containment, isolation, evidence capture — playbook-driven, human-supervised.

05

Hunt & Improve

Post-incident hunts; rules tuned; playbooks updated; lessons fed back into detection.

Toraizon Stack — OUR PROPRIETARY SUITE

Every tool in our SOC is built and owned by Toraizon. No vendor licensing bottlenecks. No telemetry leaving your environment without permission.

TZ-EDR Endpoint Detection & Response	TZ-XDR Extended Detection & Response	TZ-MDR Managed Detection & Response	TZ-DLP Data Loss Prevention
TZ-RMM Remote Monitoring & Mgmt	TZ-SIEM Security Info & Event Mgmt	TZ-SOAR Orchestration & Automation	TZ-NDR Network Detection & Response

Engagement Tiers — CHOOSE YOUR POSTURE

From co-managed to fully outsourced — we scale with your team.

CORE Essentials For growing organizations that need professional-grade monitoring without an in-house SOC. ◆ 24/7 endpoint & network monitoring ◆ SIEM with 90-day retention ◆ Monthly threat report ◆ Email + ticket support ◆ Standard incident playbooks	ELITE Most balanced Full-spectrum detection-and-response with proactive threat hunting and a named analyst pod. ◆ Everything in Core ◆ Threat hunting + MITRE alignment ◆ SOAR automation playbooks ◆ 365-day retention ◆ Dedicated analyst pod ◆ <4hr critical SLA	SOVEREIGN On-prem / regulated Air-gapped, jurisdiction-locked SOC for government, defence, BFSI, and regulated industries. ◆ Everything in Elite ◆ On-prem / air-gapped option ◆ Data sovereignty controls ◆ Cleared analysts (NDA-bound) ◆ Custom retention & jurisdiction ◆ <1hr critical SLA option
--	--	---

TECHNOLOGY • CYBER DEFENSE • TRADING

Let's talk

Request a proposal, a demo or a quotation — we respond within 48 hours.

WhatsApp / Tel +91 98951 99521

Email info@toraizon.net

Trading enquiries infotrade@toraizon.com.sa

Web www.toraizon.com.sa

Address Building 6845, Al Sulay District, Riyadh, Kingdom of Saudi Arabia