TECHGUARD LABS FOUNDATION

IT / SaaS / Product Tech

Israel-India DevShield · Coimbatore, Tamil Nadu

~43,600 / week

Cyber Incidents in India

Cybersecurity events rose from 10.29 lakh in 2022 to 22.68 lakh in 2024, scaling digital risk for software-driven firms. (Press Information Bureau, Gov of India)

6 hours

Incident Reporting Window

CERT-In directions require body corporates and service providers to report cyber incidents within a strict 6-hour timeframe.

180 days

Log Retention Period

Service providers and intermediaries in India are mandated to securely maintain data logs for a rolling period of 180 days.

TECHGUARD DEVSHIELD

DevSecOps Pipeline Controls

Threat-led review of your software delivery pipeline. We focus on where attackers can poison builds, steal secrets or push insecure code into production.

✓ **Deliverables:**
Pipeline risk register; Secrets /dependency exposure review · Secure build control matrix · Prioritized remediation roadmap

Secure SDLC Governance

We assess whether security is truly embedded into the product lifecycle - from design and threat modeling to code review, testing, approvals and release governance.

✓ **Deliverables:**
Secure SDLC maturity assessment · Release gate criteria · Control ownership model · Security-by-design improvement plan

Cloud Posture Management Operating Model

We evaluate your cloud control plane and operating model across IAM, storage, networking, encryption, logging, workload exposure and security monitoring. This is designed to reduce misconfiguration risk without slowing engineering teams.

✓ **Deliverables:**
Cloud posture findings report · IAM / exposure review · Logging and detective-control map · CSPM operating model roadmap

Tenant Isolation & Customer Data Boundary Reviews

For SaaS and multi-tenant platforms, we test the controls that separate customers from each other — logical segmentation, authorization boundaries, support-access controls and data handling paths.

✓ **Deliverables:**
Tenant-boundary assessment · Cross-tenant risk scenarios · Authorization / access review · Data-boundary remediation plan

SOC Integration for Product Telemetry & Detection Engineering

We connect product reality to security monitoring — product logs, audit trails, admin actions, auth events, API abuse, release events and cloud telemetry. The aim is to help your SOC detect product abuse, insider misuse and attacker movement earlier.

✓ **Deliverables:**
Product telemetry onboarding plan · Detection use-case catalog · Alert tuning recommendations · Incident investigation playbooks

Quick Self-Check

☐ Do you know every internet-facing API, admin console, cloud asset, code repository and package registry in your product stack?

☐ Can you prove that every production release passed code scanning, dependency checks, secrets detection, and defined release gates?

☐ Are your cloud identities, service accounts, CI/CD roles and support-access paths least-privileged, monitored and time-bound?

☐ Have you tested tenant isolation and customer data boundaries deeply enough to prove one tenant cannot see, extract or influence another tenant's data?

☐ Does your SOC ingest product telemetry, audit logs, admin actions, authentication events and API abuse indicators — or are product attacks largely invisible?

"No" = your product may already have a security gap

TechGuard DevShield

- **DevSecOps pipeline controls (SAST /DAST / Secrets / Dependencies)**
- **Secure SDLC governance and release gate criteria**
- **Cloud Posture Management Operating Model (CSPM-style)**
- **Tenant isolation & customer data boundary reviews**
- **SOC integration for product telemetry and Detection Engineering**

What Happens Without Protection — Real India Cases

Infosys McCamish | Apr 2024

Infosys disclosed that its subsidiary Infosys McCamish Systems experienced a cybersecurity incident in November 2023. In its April 2024 update, Infosys stated that information of up to approximately 6.5 million individuals was subject to unauthorized access and exfiltration, including items such as contact details, identification numbers, usernames/passwords, financial/account data, salary data and personal medical information.

Entry: Compromised third-party processing environment / customer data exfiltration.

WazirX | Jul 2024

WazirX stated that on 18 July 2024 it suffered a cyber attack on one of its multisig wallets, resulting in theft of digital assets exceeding $230 million. The affected wallet was managed using third-party digital asset custody and wallet infrastructure, and the company reported the incident to CERT-In and other authorities.

Entry: Product-logic / signing-control compromise amplified by third-party dependency risk.

Make your IT services harder to breach - and easier to trust

techguardlabs.com · info@techguardlabs.com · Coimbatore, Tamil Nadu | Israel

Ariel University (Israel) | ERA IT Consulting & Audit | SNR Sons Charitable Trust | SREC | Promitei Ltd