Fortifying Compliance Tech with Continuous Cyber Resilience

About the Customer

The customer is a technology firm that provides cloud-based audit and compliance automation solutions tailored for financial and superannuation firms. Their SaaS products are designed to simplify SMSF audits, financial reporting, and workflow compliance for accountants and auditors. Operating in a highly regulated space, the company integrates with multiple accounting platforms and deals with large volumes of sensitive financial data across geographies.

The Challenge

With its rapid growth and the sensitive nature of its clientele, the company faced evolving security and operational challenges:

Safeguarding financial and audit data hosted in multi-tenant cloud environments.	Ensuring secure integrations with third-party accounting platforms and data connectors	Meeting compliance expectations related to APRA, ASIC, and other regulatory frameworks.
Protecting cloud-native infrastructure from misconfigurations, credential abuse, and unauthorized access.	Managing code security risks across multiple agile dev teams and deployment pipelines.	Securing customer portals used for real-time report generation, submissions, and collaboration.

To maintain customer trust and regulatory alignment, the organization required an integrated and continuous approach to both security and compliance.

Threat Deception with XDR+

Deception was used to detect and delay threat actors:

- Created decoy superannuation audit files and admin portals to identify unauthorized access attempts.
- Launched honey user accounts and sandbox databases that signaled privilege escalation and credential stuffing efforts.
- Detection response times improved by 52% compared to earlier baselines.

Security Compliance Enablement with GSOS

GSOS helped the customer achieve:

- Continuous alignment with APRA's CPS 234 and ISO 27001 security controls.
- Streamlined evidence collection for client and auditor assessments.
- Dashboards for internal stakeholders to track control effectiveness and remediation ownership

DevSecOps Enablement

To embed security early in the software lifecycle, the DevSecOps integration included:

- Static and dynamic application testing (SAST/DAST) integrated into the CI/CD pipeline.
- Secret scanning and IaC validation for Terraform and Kubernetes configuration files.
- Container hardening across development and staging environments.
- Developer enablement programs on secure coding and threat modeling.
- Integration with Invinsense telemetry for real-time feedback loops from prod to

As a result, the organization reduced code-to-production risk and improved time-to-remediate issues before release.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified over 2,300 digital assets, including microservices, APIs, and client data endpoints.
Discovery	Found 34 critical weaknesses, primarily in exposed S3 buckets, weak IAM policies, and legacy APIs.
Prioritization	Highlighted 12 high-risk scenarios, including audit data leakage and insecure DevOps permissions.
Validation	Simulated threats like cross-account data access and token theft to validate real-world risk.
Mobilization	Closed 91% of critical vulnerabilities within 21 working days using automated and manual patching.

Solutions Used

The client deployed the full stack of the Invinsense cybersecurity platform

- Invinsense XDR to gain visibility across user sessions, data flows, endpoints, and authentication events.
- Invinsense XDR+ to embed deception mechanisms within storage systems, audit file archives, and identity stores.
- Invinsense OXDR to conduct continuous threat exposure management across their cloud and SaaS landscape.
- Invinsense GSOS to operationalize compliance mapping and evidence tracking across internal teams.
- DevSecOps Implementation to shift security left within their CI/CD pipeline and ensure secure coding practices.

Key Results

- 91% of critical issues resolved within 21 days of identification.
- 52% faster detection of advanced threats via deception assets.
- 42% reduction in security bugs introduced in staging environments post-DevSecOps rollout.
- Real-time compliance insights across multiple regional regulatory frameworks.
- Improved customer confidence and operational efficiency during audits and security reviews

Executive Quote

"Invinsense helped us evolve from reactive security to a proactive cybersecurity and compliance posture. Their DevSecOps integration alone has transformed how our developers think about risk—making secure delivery an integral part of our culture."

– CTO, Cloud-Based Audit Tech Firm

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy