Case Study: Securing Digital-First Insurance with Strategic Third-Party Risk Management and SIEM Playbook Automation

About the Customer

The client is a fast-growing, digital-first life insurance provider operating across multiple Asian markets. With a vision to make insurance simpler, faster, and more accessible, the company leverages technology at its core—from AI-driven customer interfaces to API-connected ecosystems. As a regulated financial entity, it operates under strict compliance mandates while also managing a large network of digital partners, service vendors, and third-party APIs that power its customer-centric insurance experience.

The Challenge

As the client scaled its digital operations, the security team faced two urgent needs:

Third-Party Risk Exposure	With dozens of third-party providers integrated into their infrastructure—from fintech partnerships to backend service providers—the company needed a cybersecurity partner who could perform comprehensive third-party risk assessments. The objective was to identify and mitigate risks originating outside their direct perimeter before they could be exploited.
Underutilized SIEM (Splunk) Investment	While the organization had invested in a robust SIEM platform (Splunk), they lacked the playbooks and structured workflows necessary to: o Automate repetitive incident response tasks o Improve consistency in response handling o Document clear escalation paths o Enable proactive threat hunting o Continuously evolve based on threat trends and incident learnings

Solutions Used

Infopercept deployed its multidisciplinary cybersecurity expertise across the following key service areas:

Third-Party Risk Assessment (TPRA)	Infopercept conducted a layered and deep-dive assessment of third-party vendors, focusing on access management, data flows, API security, compliance gaps, and potential entry points for threat actors.
Playbook Development & SIEM Optimization	Working closely with the client's internal SOC team, Infopercept mapped out existing incident response processes and pain points. Custom playbooks were authored, aligned to both business context and Splunk's capabilities, enabling automation of tasks such as log correlation, threat enrichment, and escalation protocols.
Security Process Maturity Assessment	Alongside these technical efforts, Infopercept helped benchmark the client's incident response and threat hunting capabilities, enabling process improvements and better coordination across security, IT, and compliance teams.

Executive Quote

"With Infopercept, we gained more than just a cybersecurity vendor—we gained a partner who understands both the pace of digital innovation and the risks that come with it. Their third-party risk assessments gave us visibility we never had before. And their work around SIEM playbooks turned Splunk from a passive tool into a strategic asset. We're faster, more consistent, and more proactive in our security operations today."

— Chief Information Security Officer, Leading Digital Insurance Provider

Conclusion

In a sector where trust is currency, the client's decision to strengthen its cybersecurity with Infopercept's third-party risk assessments and playbook automation has not only secured its digital backbone—but also enabled confident innovation. The results show that strategic collaboration with the right partner can deliver not just protection, but measurable operational efficiency and long-term resilience.

Outcomes Achieved

Stronger Control Over Third-Party Risk

- Assessed 35+ critical third-party vendors across 7 geographies
- Reduced vendor-related risk exposure by over 60% through remediated control gaps and security advisories
- Identified and mitigated 12 high-risk data exchange points across the API ecosystem
- Created a vendor risk scoring model that allowed the CISO's office to prioritize vendor onboarding and renewals more strategically

SIEM-Driven Incident Response Maturity

- Reviewed and enhanced 150 SIEM use cases, ensuring alignment with current threat landscape
- Authored 10 new custom playbooks, incorporating MITRE ATT&CK mappings, automated triage, and escalation logic
- Refined and updated 10 existing processes, eliminating redundancies and increasing workflow speed
- Achieved a 40% reduction in average incident response time
- Enabled 24x7 detection-to-response coverage by ensuring consistency across global teams
- Reduced manual investigation hours by over 200 hours/month through automation
- Fostered a continuous improvement loop, integrating lessons learned from over 25 prior incidents into playbook updates

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