Securing a Multi-Sector Enterprise: How a Regional Conglomerate Strengthened Detection, Resilience, and App Security with Infopercept

About the Customer

The customer is a diversified conglomerate operating across food manufacturing, retail, logistics, and healthcare sectors in the Middle East. With operations spanning more than 30 companies and thousands of employees, the group has embraced digital transformation to streamline operations, scale services, and ensure supply chain continuity. This rapid digitization, however, introduced complex cybersecurity challenges—from managing diverse applications to securing cross-border operations.

The Challenge

With a growing IT footprint and increasing exposure to regional and global threats, the customer faced a number of pressing cybersecurity challenges:

- Existing SIEM infrastructure lacked proper use cases and alert tuning, leading to noise and missed incidents
- Limited in-house capacity for developing and updating detection playbooks
- Applications across various business units were not consistently tested for vulnerabilities
- Forensic expertise was needed during critical incidents but not available internally
- Compliance requirements and business continuity expectations required stronger security posture across the environment.

The client needed a cybersecurity partner capable of improving both operational security and incident response readiness—without the overhead of managing a full internal security team.

SIEM Optimization & Use Case Engineering

Infopercept helped the customer transform their SIEM from a compliance checkbox into an active detection platform:

- Migrated and optimized existing SIEM (based on IBM QRadar) with custom parsing rules and log normalization.
- Developed 65+ custom use cases based on MITRE ATT&CK mapping, tailored to business-specific threats.
- Reduced false positives by 42% within the first quarter through iterative tuning.
- Built modular playbooks for identity misuse, suspicious file movements, cloud anomalies, and insider threats.
- Integrated alerts with email and ticketing systems to streamline SOC workflows.

Vulnerability & Application Security Services

Infopercept conducted regular VAPT and AppSec testing for web, mobile, and internal applications across business units:

- Scanned and manually tested 20+ applications in retail, logistics, HRMS, and finance modules.
- Identified and reported over:
  - 140 vulnerabilities, including 9 critical (e.g., Insecure Direct Object References, SQLi)
  - 22 insecure authentication or session management issues
- Delivered dev-ready remediation guidance and revalidation testing within 10 working days.
- Shared executive summaries for leadership with CVSS-based risk scoring and business impact notes.

On-Demand Forensics & Incident Response

Infopercept provided expert-led forensic support during suspicious activities and policy violations, including:

- Disk and memory imaging for compromised servers.
- Analysis of suspicious email-based payloads and lateral movement patterns.
- Identification of misused privileged credentials and unauthorized access events.
- Delivered comprehensive forensic reports within 72 hours of request, including IOC listings and containment steps.

Infopercept's Role

Infopercept was engaged as a strategic cybersecurity services partner, delivering:

- SIEM implementation, optimization, and ongoing use case development
- Custom detection playbooks and alert tuning
- Regular vulnerability assessments and application penetration testing (VAPT & AppSec)
- Need-based digital forensics and incident advisory
- Quarterly security health assessments and executive reporting

Executive Quote

"Infopercept has helped us go from reactive to resilient. Their team has been instrumental in not just optimizing our SIEM, but also making security measurable and actionable for our leadership. Whether it's a suspected incident or regular application testing, they're always on-point, fast, and effective."

— Group IT Manager, Regional Multi-Sector Enterprise

Quantifiable Results

Metric	Before Infopercept	After Infopercept
SIEM Alert Accuracy	~50% signal-to-noise	88% accuracy post tuning
Detection Use Cases	10+ generic rules	65+ tailored use cases
AppSec Vulnerabilities Found	Point-in-time scans only	Continuous assessment; 9 critical flaws neutralized
Mean Time to Forensic Report	External delays	72-hour turnaround with detailed IOCs
SOC Response Time	Manual triage	Alert + playbook integration reduced triage time by 40%
Executive Visibility	Ad hoc updates	Structured quarterly summaries with business risk insights

Business Impact

- Strengthened the detection and response capability across multiple subsidiaries and countries.
- Reduced exposure to business logic vulnerabilities through regular application testing and developer coaching.
- Established a forensics-on-demand model, ensuring that the customer had access to expert-level analysis whenever needed—without investing in a full-time incident response team.
- Enhanced leadership awareness of cyber risks and priorities via risk-aligned reporting and dashboards.

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.

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