Strengthening the Digital Backbone of a Global Automation Platform

About the Customer

The customer is a global provider of cloud-native intelligent automation solutions that help enterprises automate complex business processes using a combination of RPA, AI, and analytics. Their platform powers automation for organizations across finance, healthcare, telecom, and retail, and is designed to scale in fast-paced, multi-tenant cloud environments. With continuous delivery cycles, sensitive data pipelines, and integration-heavy workflows, security is both a foundational expectation and a strategic differentiator.

The Challenge

As a fast-scaling automation company, the customer faced multiple security challenges stemming from their highly distributed, API-driven architecture and DevOps-centric culture.

- Securing automation orchestration servers and bot credentials from unauthorized access or misuse.
- Preventing API abuse and data leakage in customer-facing modules that integrate with third-party enterprise tools.
- Managing vulnerabilities in containerized microservices deployed across cloud regions.
- Embedding security in DevSecOps pipelines, without slowing down continuous innovation cycles.
- Achieving global compliance with SOC 2, ISO 27001, and GDPR while managing internal GRC obligations.

Given the speed of innovation and the breadth of their integrations, the customer needed an adaptive cybersecurity solution that offered real-time visibility, continuous threat exposure management, and built-in compliance governance.

Deception as Defense with XDR+

To counter sophisticated attacks and insider threats:

- Deployed decoy bots and dummy admin panels to trap lateral movement attempts.
- Detected 4 credential harvesting incidents within the first 60 days.
- Reduced mean time to detect suspicious behavior by 74%.

DevSecOps Integration with Infopercept

Security was embedded directly into development cycles:

- Automated vulnerability scanning for every container image during CI/CD builds.
- Created custom logic to enforce secrets management and least-privilege access in staging and production.
- Enabled 37% faster remediation of code-level security gaps without delaying releases.

Compliance Enablement with GSOS

- Mapped 150+ controls across SOC 2, ISO 27001, and GDPR.
- Automated evidence collection for audit preparation, reducing manual GRC work by 48%.
- Achieved zero critical compliance findings in client-facing audits.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Discovered over 750 assets including bots, APIs, and orchestration services.
Discovery	Flagged 43 vulnerable containers, 19 misconfigured access points, and 13 exposed secrets.
Prioritization	Identified 51 critical exposures that could lead to unauthorized data access.
Validation	Simulated 12 breach paths to validate the real-world impact of discovered vulnerabilities.
Mobilization	Closed 89% of critical exposures within two weeks via automated and manual patching.

Executive Quote

"With Invinsense, our automation platform is as secure as it is intelligent. Their continuous threat exposure management, combined with seamless DevSecOps integration, has fundamentally improved the way we deliver and protect innovation."

– Head of Platform Security, Global Automation Company

Solutions Used

The customer implemented the Invinsense platform to take a multi-layered approach to security:

- Invinsense XDR unified threat detection across cloud workloads, APIs, automation agents, and orchestration tools.
- Invinsense XDR+ deployed deception controls to proactively detect credential misuse and insider threat behavior.
- Invinsense OXDR enabled continuous mapping and validation of exposed assets across environments.
- Invinsense GSOS helped streamline compliance for SOC 2 and ISO frameworks through automated control mapping.
- Infopercept's DevSecOps engineering support helped integrate security into CI/CD pipelines for real-time remediation.

Key Results

- 66% reduction in attack surface across automation infrastructure.
- 4.7x faster response to threats across API and bot layers.
- 12 attack paths neutralized before exploitation.
- 37% improvement in release-time risk management via DevSecOps integration.
- 48% GRC workload reduction through Invinsense GSOS automation.
- Zero critical compliance gaps during multiple third-party audits.

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