Safeguarding Pharmaceutical Innovation Through Proactive Cybersecurity

About the Customer

The customer is one of the oldest and most respected pharmaceutical manufacturers in the region, with a global footprint spanning formulations, APIs, and research-driven healthcare solutions. With manufacturing units, R&D centers, and operations across more than 75 countries, the company has embraced digital transformation in supply chain, quality control, and clinical data management—making cybersecurity a critical pillar of business continuity and regulatory compliance.

The Challenge

Operating in a highly regulated and IP-sensitive environment, the customer faced growing cyber risks across its value chain:

- Protecting proprietary formulations and clinical research data from IP theft and espionage.
- Securing OT and IT convergence, especially in manufacturing plants using legacy systems and SCADA.
- Ensuring compliance with international pharma regulations such as FDA 21 CFR Part 11, EU GMP Annex 11, and GxP.
- Preventing targeted phishing and business email compromise (BEC) aimed at executive leadership and procurement teams.
- Improving visibility and response times across a globally distributed network of R&D, production, and logistics systems.

The organization needed a continuous threat management strategy to secure digital operations without disrupting regulatory workflows.

Deception-Led Detection with Invinsense XDR+

Deception was crucial in identifying stealthy threats targeting sensitive assets:

- Deployed decoy drug trial databases and fake SCADA terminals to lure attackers.
- Detected unauthorized credential access attempts during after-hours sessions.
- Reduced false positives and improved MTTD by 38% in the R&D and manufacturing environments.

Governance & Compliance with Invinsense GSOS

With pharma regulations at the core, GSOS helped streamline:

- GxP alignment through automated controls and audit-ready logs for lab and plant systems.
- FDA 21 CFR Part 11 compliance with access controls and digital signature protections.
- Global cybersecurity reporting tied to operational risk dashboards for senior leadership.

This enabled the customer to unify security practices across production, research, and compliance.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Mapped 1800+ digital assets, including IoT-enabled plant systems, laboratory servers, and SAP-based ERP.
Discovery	Uncovered 48 critical vulnerabilities, including exposed R&D credentials and outdated firmware in PLCs.
Prioritization	Identified 22 exploitable attack paths targeting IP repositories and batch control systems.
Validation	Simulated lateral movement from compromised IoT devices to ERP and formula management systems.
Mobilization	Closed 92% of critical gaps within 40 days through coordinated remediation and patching cycles.

Executive Quote

""Invinsense empowered us to take control of our digital security while ensuring zero disruption to our research and manufacturing processes. Their proactive model gave us visibility, agility, and compliance in one integrated platform."

— Chief Digital & Compliance Officer, Leading Global Pharma Company

Solutions Used

The customer partnered with Infopercept and deployed the full Invinsense platform stack:

- Invinsense XDR for centralized threat detection across endpoints, research networks, and cloud workloads.
- Invinsense XDR+ to deploy deception technologies across OT, R&D, and plant environments.
- Invinsense OXDR for attack surface management, red teaming, and adversary simulation.
- Invinsense GSOS to align cybersecurity governance with pharma compliance frameworks and quality protocols.

Key Results

- 92% of critical vulnerabilities remediated in 40 days across IT and OT networks.
- 38% improvement in threat detection speed, particularly in sensitive R&D environments.
- Reduced compliance audit effort by 25%, due to policy mapping and centralized reporting.
- Strengthened IP protection across drug research pipelines and clinical operations.

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