Fortifying Bio-Innovation with Cyber Defense

About the Customer

The customer is a clinical-stage biotech company focused on developing targeted therapeutics for fibrotic diseases. With a commitment to scientific innovation and patient outcomes, their work spans drug discovery, pre-clinical research, clinical trials, and regulatory collaboration. As a digital-first biotech, their ecosystem includes lab data systems, cloud-hosted research environments, IP repositories, clinical trial platforms, and external research partners.

The Challenge

Biotech organizations at the forefront of innovation face some of the most targeted and sensitive cybersecurity threats. This customer needed to address:

- Safeguarding proprietary research and clinical trial data from cyber-espionage and data leakage.
- Preventing IP theft and unauthorized access to scientific documentation and molecule development data.
- Securing collaboration environments with third-party CROs (Contract Research Organizations) and external consultants.
- Ensuring compliance with HIPAA and FDA cybersecurity expectations in managing trial-related patient data.
- Enabling threat visibility across mixed environments — lab systems, SaaS research platforms, and remote access users.

Deception-Led Detection with Invinsense XDR+

Given the risk of espionage in life sciences:

- Deception credentials and honey-docs mimicking clinical protocols and compound data were deployed.
- Detected lateral movement attempts and unusual data exfiltration behavior.
- Helped accelerate threat containment before actual data compromise could occur.

Governance & Compliance with Invinsense GSOS

- Mapped internal processes to HIPAA security rules, FDA cybersecurity guidelines, and NIST controls.
- Maintained audit-ready logs for compliance with data integrity, access control, and breach response.
- Enabled automated evidence collection for annual IT and clinical audit cycles.

CTEM in Action CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 920+ digital assets, including secure file transfer systems, ELN platforms, and remote lab endpoints.
Discovery	Found 42 critical vulnerabilities across cloud storage policies and under-patched lab software.
Prioritization	Flagged 14 high-risk paths leading to IP-related folders and sensitive trial data.
Validation	Ran simulated attacks targeting researchers' machines and shared folders to test isolation and response.
Mobilization	Drove a 74% risk reduction via patching, MFA enablement, and network segmentation.

Executive Quote

"Invinsense gave us both protection and peace of mind — especially in securing our research and collaboration tools. Their layered security approach fit our biotech needs perfectly."

— Head of IT & Infrastructure, Clinical-Stage Biotech Company

Solutions Used

To proactively defend its sensitive R&D operations, the customer deployed:

- Invinsense XDR to gain unified threat detection across endpoints, research VMs, and trial systems.
- Invinsense XDR+ to add deception-based detection within molecule data vaults and trial management platforms.
- Invinsense OXDR to simulate targeted adversary behaviors and validate control gaps.
- Invinsense GSOS to centralize compliance documentation and automate security governance reporting.

Key Results

- 74% reduction in security gaps within 45 days.
- 100% visibility into research environment access and endpoint telemetry.
- 35% faster detection-to-response time, reducing risk exposure in high-stakes research operations.
- Streamlined FDA and HIPAA audit documentation, cutting preparation time by 50%.

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