Protecting Patient-Centric Care: How a Leading Healthcare Group Strengthened Ransomware Defense and Optimized Cybersecurity Operations with Infopercept

About the Customer

The customer is one of India's largest multi-specialty healthcare groups, operating a network of advanced hospitals and diagnostic centers. Known for its adoption of cutting-edge medical and digital technologies, the group has made significant investments in electronic health records (EHR), patient portals, cloud-based systems, and connected medical devices—making cybersecurity essential to patient safety and operational continuity.

The Challenge

As the healthcare provider expanded its digital footprint, it faced growing challenges in managing cyber risks:

A diverse stack of cybersecurity tools—EDR, SIEM, email security, and vulnerability scanners—was underutilized due to misconfigurations or lack of optimization.	Ransomware attacks were an increasing concern, with multiple ransomware-like events triggering emergency containment.
The in-house IT and security teams needed external support to perform deep-dive threat hunting, forensic analysis, and post-incident reporting.	Leadership demanded faster response and better visibility into security performance and incident impact.

The healthcare group needed a trusted cybersecurity services partner who could ensure their security investments were functioning effectively, and who could respond quickly and decisively during critical incidents.

Infopercept's Role

Infopercept was engaged to provide a combination of proactive cybersecurity operations and on-demand ransomware response services, including:

Implementation, configuration, and optimization of existing cybersecurity tools	Continuous support and maintenance of critical security infrastructure
Incident response services including threat hunting, red teaming, and forensic analysis	Executive-level incident reporting for ransomware events and other major threats

Tools and Technologies Supported by Infopercept

Infopercept's cybersecurity services covered a broad ecosystem of tools:

- SIEM (e.g., IBM QRadar, Splunk) for real-time log analysis and alerting.
- EDR/XDR (e.g., SentinelOne, Microsoft Defender for Endpoint) for endpoint monitoring and response.
- Email Security Gateways for phishing and malware prevention.
- Firewalls and IPS/IDS platforms including Fortinet and Palo Alto.
- Vulnerability Scanning Tools integrated with patching workflows.
- Backup & Recovery Systems evaluated for ransomware readiness and tested during response.

Ransomware Response Services

Over the course of the engagement, the healthcare provider experienced multiple ransomware-like security incidents. Infopercept played a key role in containment, impact minimization, and root cause investigation.

Key Response Actions Included:

Live Threat Hunting	• Investigated abnormal endpoint and network activity. • Isolated potentially infected systems within minutes of detection.
Red Team Simulations	• Assessed lateral movement possibilities after incidents. • Simulated attacker behavior to strengthen internal defense.
Forensic Investigations	• Collected memory, disk, and network artifacts post-incident. • Reconstructed the kill chain and identified patient zero.
Executive Reporting	• Delivered detailed incident analysis reports within 72 hours, outlining: ➢ Attack vector ➢ Spread potential ➢ Affected assets ➢ Recommended remediations

Outcomes Results

Metric	Before Infopercept	After Infopercept
Security Tool Utilization	~40% effective	88–90% optimized usage
Ransomware Containment Time	18–36 hours	< 4 hours average
Forensic Report Delivery Time	Ad hoc or delayed	Within 72 hours of incident
Ransomware Impact Scope	Multiple servers affected	Contained to single endpoint in recent cases
Prevented Incidents via Threat Hunting	Not tracked	5 early-stage attacks disrupted
Executive Awareness & Visibility	Manual updates	Structured post-incident summaries

Business Impact

Ensured 24/7 availability of core clinical systems such as EHR and diagnostic platforms even during threat events.	Significantly improved the effectiveness of existing security investments through tuning and managed support.
Reduced potential business downtime and reputational risk by shortening response time and containing spread.	Empowered leadership with faster decision-making through structured and timely incident reporting.

Executive Quote

"In healthcare, cybersecurity is patient safety. With Infopercept's expert support, we've transformed our defense posture—not just by reacting faster, but by making our entire security ecosystem smarter and more resilient."

— Chief Information Officer, Leading Healthcare Group

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