nextgen

Healthcare & HOSPITALS SECURITY

Critical care continuity & NIS2 compliance

Ransomware threats & disrupted critical care

nextgen
CYBERQUEST
NETALERT

Healthcare providers and hospitals are under constant cyber pressure, with patient data becoming a top target for attackers. Insider threats, weak access controls and vulnerable medical devices open the door to unauthorized access and system compromise.

Ransomware attacks can halt life-saving services, while inadequate incident response leaves institutions exposed and slow to recover. As NIS2 compliance and patient privacy regulations tighten, the need for robust protection is critical.

Cyberquest SIEM, CQ Automation, Netalert NDR, CQ Threat Intelligence and CQ AI Assistant provide the advanced defense you need to secure patient data, maintain critical care continuity and eliminate the risk of cyber failures.

We help you prevent ransomware attacks, deploy robust backup strategies, implement real-time threat detection and we can support staff on cybersecurity hygiene

Cybercriminals increasingly target hospitals with ransomware attacks, locking down critical systems and halting medical services. Without proper defenses, healthcare facilities risk operational shutdowns and potential harm to patients.

The growing impact of ransomware on critical care operations

- Medical service disruptions. Attacks can paralyze life-saving equipment and patient management systems.
- Financial strain. Hospitals may face costly ransom demands and recovery expenses.
- Compromised patient safety. Delayed or inaccessible medical records can lead to critical treatment errors.

Web
www.nextgensoftware.eu

Email
office@nextgensoftware.eu

Address
55 Clucerului Str, Bucharest, Romania

Insider threats & unauthorized access

nextgen
CYBERQUEST
NETALERT

We mitigate insider threats with strict access controls, monitor user activity and enforce role-based permissions

Hospitals and healthcare institutions face risks not only from external cyber threats but also **from insiders - employees, contractors or third-party vendors with access to sensitive systems**. Whether intentional or accidental, insider threats can lead to data breaches, system disruptions or compliance violation.

Insider threats & unauthorized access security challenges

- Unauthorized or weak access controls allow staff to view or modify confidential patient data.
- Data leaks. Employees or contractors may mishandle /steal medical records to sell them.
- Regulatory violations. Insider incidents can lead to non-compliance with NIS2 and GDPR regulation

We secure patients data & maintain critical care continuity

Healthcare organizations handle highly sensitive patient records, making them prime targets for cyberattacks. Strict adherence to NIS2 regulations is critical to protect patient privacy, maintain compliance and avoid severe penalties. Our cyber security products ensure NIS2 compliance. Encrypt patient data, help in regular security audits and enforce strict access controls.

Patient data security & NIS2 compliance fallout risks

- Data breaches. Unauthorized access to patient records violates confidentiality laws.
- NIS2 non-compliance. Failure to secure systems can result in legal action & financial penalties.
- Loss of patient trust. Data mishandling damages the institution's reputation.

Web
www.nextgensoftware.eu

Email
office@nextgensoftware.eu

Address
55 Clucerului Str, Bucharest, Romania

Medical device vulnerabilities

nextgen
CYBERQUEST
NETALERT

We secure medical devices, conduct regular security assessments and update device firmware to close vulnerabilities

Connected medical devices such as ventilators, infusion pumps and imaging equipment often lack strong security protections. If compromised, these devices can be manipulated, leading to dangerous malfunctions or data breaches.

Cyber risks linked to medical device vulnerabilities

- Device manipulation. Hackers could alter device functions, risking patient safety.
- Network entry points. Insecure devices provide an easy pathway into hospital networks.
- Data leaks. Patient information stored on devices may be stolen or exposed.

Nextgen Software provides a robust cybersecurity portfolio tailored to protect healthcare institutions from advanced threats, system disruptions and data breaches.

Cyberquest SIEM – Detects, correlates and analyzes security events in real time to ensure rapid threat identification across medical systems.

CQ Automation/ SOAR – Automates incident response workflows to reduce reaction time and human error in critical healthcare environments.

Netalert NDR – Monitors east-west network traffic to detect lateral movement and advanced threats targeting hospital infrastructure.

CQ Threat Intelligence – Enriches alerts with real-time threat data to improve detection of targeted attacks on medical devices and patient data.

CQ AI Assistant – Enhances decision-making by providing AI-driven insights and recommendations during incident triage and investigation.

Web
www.nextgensoftware.eu

Email
office@nextgensoftware.eu

Address
55 Clucerului Str, Bucharest, Romania