Korcomptenz

Cybersecurity Advisory and Managed Services for Healthcare

Protecting Patient Data and Ensuring Compliance in a Digital World

In an era where healthcare organizations are increasingly reliant on digital systems, the need for robust cybersecurity has never been greater. Cyberattacks targeting healthcare providers are on the rise, threatening patient data, operational continuity, and regulatory compliance.

Our Cybersecurity Advisory and Managed Services are designed to help healthcare organizations safeguard sensitive information, mitigate risks, and maintain trust in an evolving threat landscape.

The Cybersecurity Challenge in Healthcare

Why Healthcare is Vulnerable

- Healthcare organizations manage vast amounts of sensitive patient data, making them a prime target for cybercriminals.
- The proliferation of connected medical devices, telemedicine platforms, and cloud-based systems has expanded the attack surface.
- Regulatory requirements like HIPAA and GDPR add complexity to data protection efforts.

Common Threats to Healthcare Organizations

- **Ransomware Attacks:** Encrypting critical systems and demanding payment for access.
- **Data Breaches:** Unauthorized access to patient records, insurance details, and payment information.
- **Phishing and Social Engineering:** Exploiting employees to gain access to sensitive systems.
- **IoT Vulnerabilities:** Exploiting insecure medical devices and connected equipment.
- **Insider Threats:** Accidental or intentional misuse of data by employees or contractors.

Korcomptenz End-to-End Cybersecurity Services for Healthcare

Protect your entire healthcare technology ecosystem from every threat. We cover the entire security lifecycle, from identifying risks to managing them securely. Our services span from roadmaps and architecture to penetration testing, security controls, and managed security services. We offer a comprehensive range of solutions tailored for healthcare, including:

- **Endpoint Protection:** Secure medical devices, workstations, and mobile devices used by healthcare professionals.
- **Network and Email Protection:** Protect sensitive patient data transmitted across networks and email systems.
- **Cloud Security Layers:** Ensure the security of cloud-based Electronic Health Records (EHR) and other healthcare applications.
- **Email Archiving and Backups:** Safeguard critical patient data and ensure compliance with healthcare regulations.
- **Identity and Access Management:** Control access to sensitive healthcare systems and data.
- **Monitoring and Logging:** Continuously monitor for threats and maintain logs for compliance and forensic analysis.
- **Cybersecurity Testing:** Regularly test your systems for vulnerabilities.
- **Zero Trust Network Access:** Implement a zero-trust architecture to secure access to healthcare systems.

Korcomptenz NOC and SOC Center

Continuous Monitoring

We offer 24/7 monitoring through our NOC and SOC, ensuring proactive detection and response to security threats and operational issues.

Security Event Correlation

We integrate security events from IDS, firewalls, endpoints, and threat intelligence, enabling the detection of complex threats and prioritizing response efforts.

Performance Optimization

Our NOC & SOC teams monitor system performance and availability, proactively identifying bottlenecks, latency issues, and disruptions to optimize performance and ensure uptime.

Advanced Threat Detection

We use advanced threat detection technologies to monitor suspicious traffic, unauthorized access, malware, and other compromise indicators in real-time.

Compliance Monitoring

We ensure compliance with regulatory requirements, industry standards, and internal policies through continuous monitoring and reporting, covering data protection, security best practices, and industry-specific frameworks.

What We Offer

Cyber Advisory Services

> Evaluate your current security posture and controls to identify gaps and areas for improvement. > Develop a robust security plan, outlining the tools, technologies, and processes needed for successful implementation. > Strategize and deploy an enhanced security strategy that minimizes disruption to daily operations. > Provide expert training to increase security awareness and strengthen your team's capabilities.

Managed Security Services

> Provide 24/7 monitoring of your network, cloud environment, and endpoints to detect advanced threats and deliver real-time alerts. > Collect data and security event insights from various sources for comprehensive visibility. > Quickly identify and respond to security incidents, neutralizing threats through root cause analysis. > Investigate and enhance your security posture to prevent future incidents.

Cyber Incident Response

> Quickly contain the breach and secure your environment to prevent further access by threat actors. > Conduct a thorough investigation to identify the root cause and scope of the breach. > Implement improvements to strengthen defenses and prevent future attacks. > Swiftly restore data and applications to their pre-incident state.

What We Assure

Real-time Threat Intelligence

Endpoint Protection

Incident Response Capabilities

Endpoint Detection and Response

Advanced Threat Protection

Data Loss Prevention

Spam and Virus Filtering

Zero Trust Architecture

Micro-Segmentation

Identity-based Access

Secure Access to Applications

Special Offer: Close Security Gaps with a Security Advisory Assessment

Why It Matters:

As threats evolve and IT landscapes change, traditional networks struggle to protect valuable assets. With increasing demand for mobile access, web applications, and hybrid environments, new security risks emerge constantly. Regular security reviews are key to maintaining strong protection and compliance.

What You Can Expect:

Our Security Advisory Assessment identifies security gaps and provides a strategic roadmap to address them. It ensures compliance, aligns with best practices, and strengthens your security as your business grows. The roadmap helps you plan the budget and resources needed to mitigate risks.

Tailored to Your Needs:

We customize the assessment based on your focus areas and desired level of detail. Whether you need a broad overview or a deep dive, our baseline assessment covers people, processes, and technology. We also offer specialized evaluations for multicloud, OT security, firewalls, and more.

Our Approach:

We evaluate security risks from every angle—starting with vision, risk appetite, policies, assets, and technical controls. Our recommendations are based on standard frameworks like SABSA, ISO 27000, NIST, and CIS.

Through workshops and architecture reviews, we:

> Identify internal and external security influences
> Define your current security posture
> Determine risks and recommend solutions

We then map your current and target maturity levels on our Information Security Dashboard and Security Architecture Reference Model.

Ready to strengthen your cybersecurity posture?

Contact us today to learn how our tailored solutions can protect your organization and ensure the safety of your patients' data.