MODERN CYBERSECURITY FOR THE HEALTHCARE SECTOR

CYBERSECURITY ENSURES PATIENT SAFETY

Healthcare institutions are at the front lines when society is experiencing turmoil. This makes their cyber threat landscape especially vulnerable to developments in current events.

This has been made increasingly evident by the COVID-19 pandemic. The pandemic sparked the interest of cybercriminals and nation-states alike to target the healthcare sector. These threat actors are taking advantage of the situation to compromise the confidentiality, integrity and availability of patient data and critical healthcare IT systems through extortion, disinformation and espionage campaigns. The healthcare sector also regularly has to deal with data leaks due to malware infections, phishing, human error and web application vulnerabilities.

Cybersecurity has become a baseline to ensure patient safety and secure patient data. For the sector to continue to be at the front line, its threat intelligence, detection and response capabilities need to keep pace to ensure cyber threats won't impede the critical tasks this sector provides to society.

ARGUS – A COMPLETE MANAGED DETECTION AND RESPONSE SOLUTION FOR THE HEALTHCARE SECTOR

mnemonic has been a trusted partner of the healthcare industry for close to two decades. Spanning the medical supply chain, suppliers, public and private institutions, regional health authorities and medical retail, mnemonic's team of specialists provide the advanced security services needed to protect this vital industry.

Powering our 24/7 Security Operations Center is Argus - our purpose-built threat analytics and response platform that enables our security analysts to monitor, detect and respond to cyber threats as they occur.

Detect and respond to threats: Ensure attacks are detected before they cause long-term harm. Argus' industry leading 98% alert accuracy reduces false positives and noise, so you can allocate your resources for when it really matters.

Secure non-traditional environments: Proven threat detection for connected IoT and medical devices that sit outside traditional IT security programs.

Keep track of vulnerable resources: Continuous monitoring for vulnerable systems, services, and assets enables your team to remediate vulnerabilities before they become a threat.

Better navigate the threat landscape: Stay prepared with up-to-date threat intelligence, contextualised reports and detailed recommended response actions.

Ensure maximal uptime: Know that if you need us, our Incident Response Team have the capacity and competence to manage complex security breaches 24/7 and help you restore normal operations as quickly as possible.

Minimise technology refresh: Argus is technology agnostic, and adapts to your organisation's current security stack and environment to maximise the return of your investments.

info@mnemonic.io
mnemonic.io

Oslo • Stavanger • Stockholm • The Hague • London • Palo Alto

mnemonic
Securing your business.