



CTECH Consulting Group Inc.

Comprehensive Cybersecurity Monitoring and Compliance for Healthcare Organizations

DETECT

Detect hidden threats on your network like malware, dangerous website traffic, and malicious user activity before they result in an infection or data breach.

RESPOND

Alerts can be routed directly to your support team to immediately respond and stop cybersecurity threats.

COMPLY

For healthcare organizations, continuous monitoring of your security logs is required by HIPAA-HITECH compliance regulations. Our service meets these regulations as well as GLBA, PCI-DSS, COBIT, ISO, NIST, and others for ongoing monitoring and daily reviews.



Cybersecurity threats in healthcare can put patient safety at risk, shut off access to records, and take down medical devices. Recent incidents have shown that healthcare organizations, whether small private practices or large provider networks, are under constant attack from hackers, phishers, and other cyber criminals and the impact can be enormous. If infected by ransomware, you may be forced to pay tens of thousands of dollars to get your data back. The average cost for healthcare organizations per record lost or stolen in a breach is \$380, and 65% of patients say they would steer away from companies whose records have been compromised.

However, most organizations lack the technology or personnel to even detect these emerging cybersecurity threats. Studies show the average time between a data breach and discovery is 205 days – that's over 7 months! Simply implementing security tools such as firewalls or anti-virus isn't enough.

- Healthcare organizations experience more than twice the number of attacks on average as compared to organizations in all other business segments.
- Electronic health records (EHR) are far more valuable than financial data, EHRs can sell for \$50 in the black market, compared to just \$1 for a stolen social security number or credit card number.
- 88% of ransomware attacks are directed at the healthcare sector.

This is even more true for healthcare organizations that fall under HITECH, HIPAA, and MU regulations. Compliance is absolutely critical to avoid fines or worse consequences.

Today's threats and compliance guidelines require healthcare organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation.

Our comprehensive cybersecurity monitoring and compliance solution solves this need by providing continuous monitoring of your entire network to detect and respond to hidden cybersecurity threats.





CTECH Consulting Group Inc. Comprehensive Cybersecurity Monitoring

Customized, Feature Rich Solution

WHAT WE MONITOR

Firewalls
IDS/IPS Devices
Servers
Routers
Switches
WAPs
Office 365
AWS/Azure/Google Cloud

EASY DEPLOYMENT

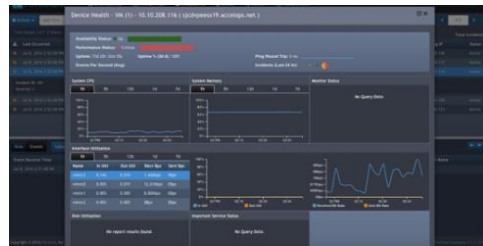
No hardware or software to purchase. Most customers can be deployed in 1 day, and we'll manage everything for you.

OPTIONAL ADD-ONS

Remediation Support
Device Management
Patch Management
Endpoint Protection
DNS Protection
Vulnerability Scanning
and Much More

For more information on any of our products or services please contact us at:

4034571478



- Cloud-Based Cybersecurity Monitoring Platform
- In-Depth Behavioral and Anomalous Activity Monitoring
- Customized Cybersecurity Detection Rules
- Ongoing Rule Tuning and False Positive Reduction
- Detailed Notifications Including Remediation Guidance
- Integrated Global Threat Intelligence Feeds
- Automated Notifications, 24x7x365
- Daily Reviews and Oversight by SOC Analysts
- Incident Investigation and Compliance Assistance
- Tier 3 Incident Response Escalation Support
- Event Log Consolidation and Management
- Network, Virtualization, and Application Intelligence
- Configuration Change Management
- Over 2,500 Pre-Built Compliance and Standards Reports
- Custom Report Creation and Scheduling
- Comprehensive Device Support
- Audit / Exam Support

Important Benefits for You

- Enterprise-grade cybersecurity monitoring for low monthly cost
- Immediate detection of hidden threats and malicious behavior
- Significant reduction of risk from a hack or data breach
- Optional remediation services from our support team
- Regulatory compliance with log monitoring and daily reviews

COMMON THREATS THAT WE DETECT

Hacker Reconnaissance
Brute Force Attacks
Compromised Credentials
Policy Violations
Configuration Errors
Malicious Website Traffic
Device Vulnerabilities
Statistical Anomalies
Foreign Country Attacks
Suspicious User Behavior
Unusual File Transfers



CTECH Consulting Group Inc.
Station M Box 231,
Calgary, Calgary, T2P 2H6
<https://www.ctechgroup.net>