



CTECH Consulting Group Inc.

Comprehensive Cybersecurity Monitoring and Compliance for Financial Institutions

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



- The financial services industry tops the charts as the most targeted industry with the highest volume of security incidents and the third highest volume of cyber-attacks.
- Financial services firms are hit by cybersecurity incidents a staggering 300 times more frequently than businesses in other industries.
- Data breaches damage financial institutions' profits, reputation, customer experience, and can result in regulatory actions.

Cybersecurity threats are on the rise and only getting more dangerous for financial institutions. It seems every day there's a new headline about another data breach. And it's no longer only large financial organizations that must be concerned. Recent incidents have shown that small and medium-size institutions are also highly vulnerable to today's threats, 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 financial organizations per record lost or stolen in a breach is \$336, many financial institutions may not survive such an event.

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.

This is even more true for financial institutions that fall under GLBA, Sarbanes-Oxley, FFIEC, or NCUA regulations. For those firms, compliance is absolutely critical to avoid fines or worse consequences.

Today's threats and compliance guidelines require financial institutions 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

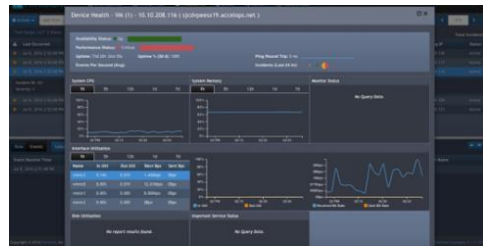
No hardware or software to purchase. Most customers can be deployed in 1 day, and we'll manage everything for you.

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>