Long View

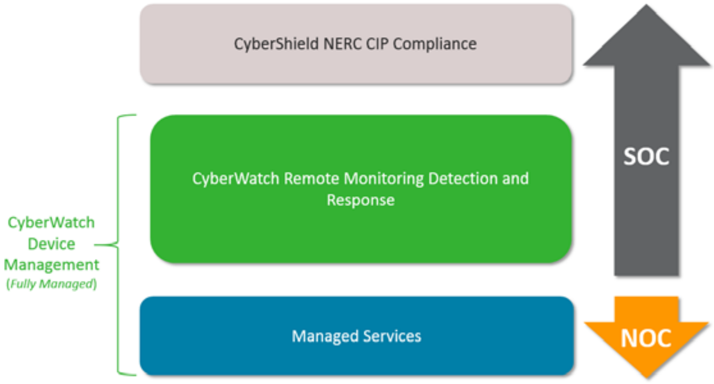
CyberWatch Managed Security Services

We have entered the era of targeted cyber-attacks. The question is not "if" your company has been breached, or even "when." It has already happened. The real questions are: is your organization aware of it, and are you capable of detecting and responding to future threats?

An effective Security Operations Center (SOC) can form the heart of an organization's operational defense against advanced cyber-attacks. However, many organizations struggle to implement their SOC ambitions. When developed in-house, SOC challenges include identifying suitably skilled resources to provide 24x7 coverage and leveraging the most effective technologies for advanced threat detection and reporting metrics.

CyberWatch Managed Security Services

Remote Monitoring Detection and Response


CyberShield NERC CIP Compliance
CyberWatch Remote Monitoring Detection and Response
Managed Services
CyberWatch Device Management (Fully Managed)
SOC
NOC

CyberWatch Managed Security Services is a 24x7x365 fully- or semi-automatic service to remotely monitor, detect, respond and neutralize cyber threats, enhanced by our NERC CIP aligned Security Operations Center (SOC). It is built on a next generation security intelligence and analytics platform powered by LogRhythm. The main objective of the CyberWatch service is to deliver the right information, at the right time, with the appropriate context, to minimize the amount of time it takes to detect (Mean time to Detect (MTTD)) and respond (Mean Time to Respond (MTTR)) to damaging cyber threats. The service is provided to our client's OT/IT Infrastructure environment via data collection technology deployed as an appliance or as a software agent.

Utilizing the latest in threat management and incident response services, CyberWatch will arm our security operation analysts with the ability to proactively identify vulnerabilities for repair and quickly react to detected abnormal behavior.

Security incidents will quickly be identified and alerted for faster isolation and repair through:

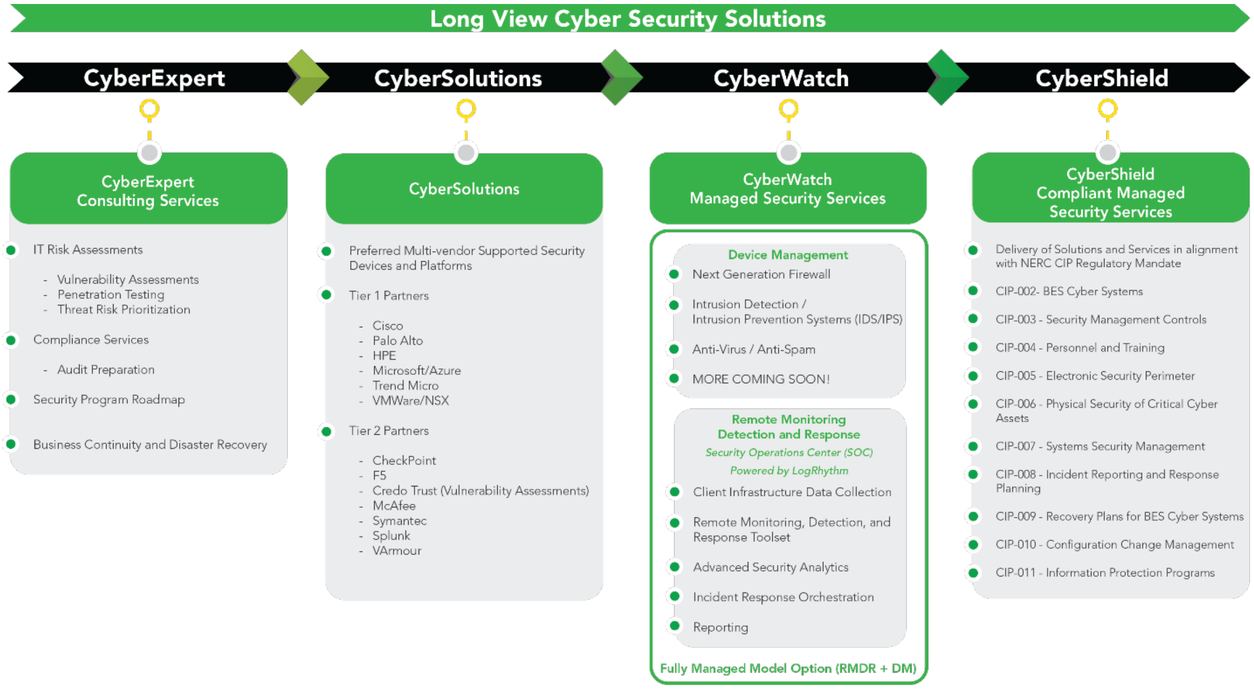
- **Client infrastructure Data Collection:** Gathers real time data collection within the client's infrastructure covering Security, System, Audit and Application logs as well as data flows. The service is available in two (2) options:
  1. *Hardware-based (appliance deployed into the client environment).*
  2. *Software-based (agent deployed into the client environment).*

- **Remote Monitoring, Detection, and Response Toolset:** Powered by LogRhythm, 7 x 24 centralized collection, processing and analysis of events generated by monitored client infrastructure. The results are presented within a secure, client-facing web portal where authorized client and Long View personnel can view, analyze, and respond to alerts;
- **Advanced Security Analytics:** Customer infrastructure data is combined and analyzed with external threat intelligence to produce a prioritized set of alerts based on client and external information;
- **Incident Response Orchestration:** Security Incident Response Orchestration built upon a "Smart Response Automation Framework" that supports several execution options to automate or semi automate manual remediation processes reducing Mean Time To Repair (MTTR). All activities are tracked as part of the case history, providing real-time status and a tamper-proof audit trail. Threats are proactively identified, prioritized based on organizational risk and rapidly investigated within the Security Intelligence Platform; and,
- **Reporting:** Incident recap and trend analysis. Contextual awareness of client business and IT environments communicated on a predetermined frequency aligned to your needs.

CyberWatch Remote Monitoring Detection and Response Features

Features	
Multi-Tenant Data Architecture (Tenant Data Encryption, Data isolation) in support of CIP-011-2-Information Protection	✓
Core Security Intelligence Platform house within Physical Security Perimeter, implemented in alignment to CIP-006-5, NIST 800-53 High-Impact Systems (Controls: PE-2, PE-3, PE-4, PE-5)	✓
24x7x365 fully - or semi-automatic remote monitor, detect, respond and neutralize cyber threat services, which include: • Flexible Data Collection Technology that supports a variety of devices and formats, including custom log sources	✓
• Machine and Forensic Analytics with Precision Search	✓
• Threat Intelligence (Open and Commercial Threat sources)	✓
• Actionable Intelligence whereby MTTD and MTTR are actionable within minutes or seconds	✓
Security Monitoring with fully integrated Case Management for collecting, distributing and analyzing data tied to specific events and incidents	✓
Security Incident Response Orchestration built upon a "Smart Response Automation Framework" that supports several action execution options to cuts down reliance on manual processes thereby reducing MTTR response times	✓
Client Dashboard (Web Portal) to view real-time threat level, alarms, or open a case	✓
Standard Log Retention - 90 days online, two (2) years offline (CIP-008-5 R2.3)	
File Integrity Monitoring - Alert on malware-related registry changes, improper access of confidential files, and theft of sensitive data	*Fee Applies*
Network Monitoring - Detect protocol misuse attempting to hide malicious activities	*Fee Applies*

Threats continue to evolve; your SOC must too. Long View's Managed SOC is designed to wrap experienced people and efficient processes around leading technologies to provide a business-focused SOC that will evolve with your organization's needs and the changing threat landscape.



Long View Cyber Security Solutions

CyberExpert

CyberExpert Consulting Services

- IT Risk Assessments
  - Vulnerability Assessments
  - Penetration Testing
  - Threat Risk Prioritization
- Compliance Services
  - Audit Preparation
- Security Program Roadmap
- Business Continuity and Disaster Recovery

CyberSolutions

CyberSolutions

- Preferred Multi-vendor Supported Security Devices and Platforms
- Tier 1 Partners
  - Cisco
  - Palo Alto
  - HPE
  - Microsoft/Azure
  - Trend Micro
  - VMWare/NSX
- Tier 2 Partners
  - CheckPoint
  - F5
  - Credo Trust (Vulnerability Assessments)
  - McAfee
  - Symantec
  - Splunk
  - VArmour

CyberWatch

CyberWatch Managed Security Services

Device Management

- Next Generation Firewall
- Intrusion Detection / Intrusion Prevention Systems (IDS/IPS)
- Anti-Virus / Anti-Spam
- MORE COMING SOON!

Remote Monitoring Detection and Response

Security Operations Center (SOC)

Powered by LogRhythm

- Client Infrastructure Data Collection
- Remote Monitoring, Detection, and Response Toolset
- Advanced Security Analytics
- Incident Response Orchestration
- Reporting

Fully Managed Model Option (RMDR + DM)

CyberShield

CyberShield Compliant Managed Security Services

- Delivery of Solutions and Services in alignment with NERC CIP Regulatory Mandate
- CIP-002- BES Cyber Systems
- CIP-003 - Security Management Controls
- CIP-004 - Personnel and Training
- CIP-005 - Electronic Security Perimeter
- CIP-006 - Physical Security of Critical Cyber Assets
- CIP-007 - Systems Security Management
- CIP-008 - Incident Reporting and Response Planning
- CIP-009 - Recovery Plans for BES Cyber Systems
- CIP-010 - Configuration Change Management
- CIP-011 - Information Protection Programs

Have questions? Interested in learning more?

Contact a Long View sales representative at 1.866.515.6900 or info@longviewsystems.com.

Talk to us | longviewsystems.com | info@longviewsystems.com | 1.866.515.6900