



# Cyber SIEM Solutions, Cyber Attack Sandboxing & Cybersecurity Resiliency

**World-class IT & Security Solutions**

WHA partners with EPC USA to bring cutting edge IT and security solutions to members. Offering cyber SIEM solutions, managed security awareness, cyber attack sandboxing, and cybersecurity resiliency monitoring, EPC is your go-to to protect your organization from outside threats!

The Arctic Wolf logo, which includes a white silhouette of a wolf's head inside a white triangle, followed by the text "ARCTIC WOLF" in large white letters and "Cyber SIEM Solutions" in smaller white letters below it.

# ARCTIC WOLF

## Cyber SIEM Solutions

## Managed Detection & Response

Arctic Wolf® Managed Detection and Response (MDR) provides 24x7 monitoring of your networks, endpoints, and cloud environments to help you detect, respond, and recover from modern cyber attacks.

### Detect



#### Broad Visibility

Works with your existing technology stack to discover and profile assets and collect data and security event observations from multiple sources.



#### 24x7 Monitoring

Your environment is monitored for threats and risks around the clock, allowing you to focus on other important areas of your business.



#### Advanced Threats

Catch advanced threats that are missed with other approaches with a platform that analyzes more security data, and an experienced team who knows how to look for them.

### Respond



#### Managed Investigations

We investigate suspicious activity so you don't have to, making alert fatigue and time wasted on investigating false positives a thing of the past.



#### Incident Response

Every second counts. Detect and respond to critical security incidents within minutes to prevent the spread of threats.



#### Log Retention and Search

Takes the work out of managing logs, enabling you to easily conduct additional investigations, if needed.

### Recover



#### Guided Remediation

We work with you on detection, response, and remediation to validate the threat has been neutralized and verifying it hasn't returned.



#### Root Cause Analysis

Deep investigation into the root cause of incidents to promote the creation of customized rules and workflows that harden your posture.



#### Personalized Engagement

Regular meetings to review your overall security posture and find areas of improvement that are optimized for your environment.

# Managed Risk

Arctic Wolf Managed Risk enables you to discover, assess, and harden your environment against digital risks by contextualizing your attack surface coverage across your networks, endpoints, and cloud environments.

Managed prioritization and personalized protection is delivered by your Concierge Security Team<sup>®</sup>. The Concierge Security Team is a force multiplier to your existing security team. If you don't have a security team, you gain instant access to security professionals that are otherwise difficult, if not impossible to find. Your named Concierge Security Engineer works with you to prioritize vulnerabilities discovered from networks, endpoints, and cloud environments.



*"Arctic Wolf went to work the week after we signed the agreement. In just a couple of weeks, they've already identified quite a few 'opportunities' for us to bolster our environment. We are already sleeping better knowing that they are our partner."*

-Jennifer Riley, CEO  
Memorial Regional Health

- ▶ **Discover** – They start with the essential task of identifying assets in your environment and defining your attack surface across network, perimeter, host and accounts.
- ▶ **Assess** – The Concierge Security Team then contextualizes your attack surface coverage with risk policies, asset criticalities, and SLOs (service level objectives). This contextualization enables you to prepare your environment to end cyber risk. Then the Concierge Security Team assesses and provides you with the risk priorities in your environment.
- ▶ **Harden** – Finally they advise you on remediation actions to ensure you are benchmarking against configuration best practices and continually hardening your security posture.

## 24x7 Continuous Monitoring

Around-the-clock monitoring for vulnerabilities, system misconfigurations, and account takeover exposure across your endpoints, networks, and cloud environments.

## Strategic Recommendations

Your named Concierge Security engineer becomes your trusted security advisor, working with you to make recommendations that harden your security posture over time.

## Personalized Engagement

Regular meetings with your named Concierge Security engineer to review your overall security posture and find areas of improvement that are optimized for your environment.

**Reach out today to see how EPC USA and Arctic Wolf can help you improve your security posture at a reasonable cost.**

**Tom Hinchsliff**  
President, EPC USA, Inc.  
tom.hinchsliff@epcusa.net  
303.549.0556

## Managed Security Awareness

Arctic Wolf Managed Security Awareness prepares your employees to recognize and neutralize social engineering attacks and human error—helping to end cyber risk at your organization.



### Engage

Train and prepare employees to stop social engineering attacks, like phishing.



### Measure

Identify employees that fall behind and determine which threat topics require reinforcement.



### Transform

Achieve a culture of security and strengthen cyber resilience.

## Managed Security Awareness Training Addresses the Most Common Cyberthreats by Influencing Behavior and Fostering a Security Culture

### ▶ Improve Protection

Prepare employees to recognize and neutralize social engineering attacks, like phishing.

### ▶ Strengthen Resilience

Empower employees to identify cyber risks and report mistakes that could expose sensitive data.

### ▶ Achieve Compliance

Deliver security awareness training for regulatory compliance.



# Trellix

(Formally FireEye)



## Real-time Threat Prevention

The Trellix Network is designed to stop drive-by downloads and blended Web and email attacks. It also offers a defense against infections that take place outside the network. With a continuous monitoring service, they proactively hunt for threats in your environment and instantly help respond to incidents. Their products and services include a state-of-the-art virtual machine technology that responds to threats in real time.

## The Trellix Network

- ▶ Deploys in-line (block/monitor mode) or out-of-band (TCP reset mode/monitor mode) and enables security analysis for IPv6 traffic
- ▶ Analyzes all suspicious web objects
- ▶ Integrates with the Trellix Threat Prevention Platform to stop blended spear-phishing attacks
- ▶ Distributes threat intelligence locally and globally through the Trellix Dynamic Threat Intelligence Cloud
- ▶ Supports remote third-party AAA network service access in addition to local authentication
- ▶ Provides role-based access control and audit logging
- ▶ Consolidates signature-based and signature-less technologies with the IPS add-on license to Trellix Network to automatically reduce false alerts and drive down operational spend

According to Inc. Magazine, Trellix is, "...the go-to company whenever there's a huge data breach by hackers, for its expertise in forensic sleuthing deep into compromised computer networks. In recent years, JP Morgan Chase, Sony Pictures, and the health insurer Anthem have all turned to Trellix, the Milpitas, California company, for help."

**Reach out today to see how EPC USA and Trellix can help you prevent cyber attacks.**

**Tom Hinchsliff**  
President, EPC USA, Inc.  
tom.hinchsliff@epcusa.net  
303.549.0556



## SecurityScorecard

Take your Cybersecurity  
Capabilities to New  
Heights with Services  
from SecurityScorecard

A focus on expert-led continuous improvement, actionable insights, and tailored strategies positions SecurityScorecard as a trusted partner in achieving and maintaining a robust cybersecurity posture.

### Predictive Capabilities

SecurityScorecard offers critical data points through its proprietary factors analysis. Risk factors range from Network Security to Application Security. Each factor is predictive. For example, companies with a C, D, or F rating are up to five times more likely to experience a data breach or face compliance penalties than those with an A or B rating. Good grades make a difference.

### Improve Your Ability to Meet HIPAA & Other Compliance Challenges

In order to facilitate an effective security and compliance program, organizations must continually monitor their cybersecurity posture and that of any third party. SecurityScorecard enables organizations to meet or exceed regulation mandates regarding continuous monitoring while simplifying the compliance process.

### Powerful Threat Reconnaissance

SecurityScorecard's unmatched threat intelligence capabilities and attribution engine combine to deliver actionable cybersecurity intelligence that enables the reduction of exploitable vulnerabilities. Threat reconnaissance answers the questions: what assets are at risk, and what entity do they belong to?



By leveraging SecurityScorecard's proprietary collection capabilities and utilizing commercial and open source threat intelligence feeds, you can now identify vulnerable assets in your ecosystem to proactively eliminate weaknesses and defeat threats.

## Complete Visibility into Third-party Risk

- ▶ Continuously monitor the cybersecurity health of your vendors
- ▶ Identify the security profile of your vendors and business partners
- ▶ Leverage the breadth of data across 10 risk factor groups
- ▶ Clearly understand your cybersecurity posture
- ▶ Send and manage security questionnaires to your vendors and automatically validate them against industry best practices and compliance frameworks



**SecurityScorecard is easy to implement and immediately usable. Reach out today to see how EPC USA and SecurityScorecard can help you minimize your risk.**





Don't have the budget or staff for an in-house SIEM?  
**We can help!**

Safeguarding patient health information and protecting hospital infrastructure is a huge burden for our rural members to manage. And, don't forget the compliance component. Through a relationship with EPC USA and Arctic Wolf, WHA members no longer need to carry this burden alone.

Arctic Wolf also offers Managed Security Awareness which prepares your employees to recognize and neutralize social engineering attacks and human error—helping to end cyber risk at your organization.



Online security that is **easy to implement** and **cost effective.**

We are well aware that cybercriminals use the web to target your facility and your community. The increasing digitization of patient health records and under-funding of network security are putting healthcare organizations at risk.

Western Healthcare Alliance (WHA) is dedicated to ensuring you are protected and saving money. To help members minimize risk, WHA has partnered with EPC USA and Trellix, experts who have front line experience analyzing environments for everyday threats and battling breaches that might otherwise make headlines.



Instantly **monitor the cybersecurity health** of your vendors and other partners.

While the overall security profile of the healthcare industry has improved over the last few years, we're still not without threats. To effectively combat risk, you must have continuous visibility into your ecosystem's cybersecurity posture. Through Western Healthcare Alliance's (WHA) relationship with EPC and SecurityScorecard you have help to manage these threats.

SecurityScorecard provides the most accurate rating of security risk for any organization worldwide. The platform uses non-intrusive proprietary data collection methods and trusted commercial and open-source threat feeds to quantitatively evaluate the cybersecurity posture of more than one million enterprises globally.



**Reach out today to see how the EPC USA suite of products can help you minimize your cyber security risks.**

**Tom Hinchsliff**  
President, EPC USA, Inc.  
[tom.hinchsliff@epcusa.net](mailto:tom.hinchsliff@epcusa.net)  
303.549.0556