

Cyber-Security Monitoring for Utilities

Real Time Control Environment

Counterpane and Verano have partnered to offer an industry-specific Cyber-security Monitoring Service to protect systems against unauthorized access, changes, and exploits of vulnerabilities in our clients' control environment. The partnership integrates Verano's Industrial Defender® into Counterpane's Managed Security Monitoring Service, providing customers with 24x7 proactive and consistent monitoring & reporting of real-time control environments.

This solution allows for around-the-clock analysis of network and system events in real-time, providing the ultimate in security, thus reducing risk and unnecessary liability exposures, at a reduced cost. This also provides a solid foundation to customers' NERC and FERC initiatives.

Key Benefits

Safeguard Control Systems and Networks – Provide protection without sacrificing performance by utilizing Verano's Industrial Defender and Counterpane's monitoring capabilities.

Comply with Security Standards Implemented by NERC CIP through Customized Reporting and Intrusion Detection Systems.

Enable Operations to Focus on Critical Asset Availability – Counterpane receives, monitors, and takes action on logs and alerts generated from Verano's Industrial Defender (24X7X365) delivering a rapid response to emerging risks.

Enable Customers to Provide a Uniform Security Offering Across both the Corporate and Control Network:

- Ability to insert alerts from Industrial Defender into broader security monitoring posture via Counterpane Managed Security Monitoring
- Correlation of security events across critical cyber & security assets

Core Services

SECURITY EVENT MONITORING

Counterpane's Managed Security Monitoring (MSM) plus Verano's Industrial Defender (ID) provides a single plant-centric system and user interface for multiple layers of real-time cyber-security and performance monitoring. It monitors multi-vendor control systems, industrial applications, real-time networks and perimeter firewalls.

Once a potential incident is detected, MSM+ID notifies and alerts authorized personnel through phone, secure browser, email, pagers, and Internet enabled devices. For the ultimate protection, ID allows perimeter security settings to be pre-defined and rapidly adjusted according to threat level. For centralized security policy management and forensics purposes, it centralizes all security log information from existing control systems and offers comprehensive real-time and historical reporting.

PERIMETER PROTECTION

MSM+ID provide a simple means of complete protection at the real-time system network perimeter from a vast array of attacks. This comprehensive security appliance provides anti-virus filtering at the firewall level, secure remote communication through a VPN gateway, and detection and

“Security and compliance requires specialized expertise, and it makes more sense to outsource that so my staff can stay focused on the core business objectives... Counterpane can survey all the potential threats worldwide. They can provide a much wider, more current view of the threats. That’s something we can’t do as efficiently, given our current staff levels.”

*–John Lambeth, CISSP, CISA
VP Information Technology
Blackboard, Inc.*

“Because Counterpane gives us only the information we need when we need it, we can concentrate on the attacks that matter. The value of that kind of service is enormous.”

*–David MacLeod, Ph.D., CISSP
CISO
The Regence Group*

“By outsourcing monitoring and management of established security systems to managed security service providers, most enterprises can increase security while reducing operational costs, and free up internal security resources to deal with changing business needs and new threats.”

*–John Pescatore
VP Distinguished Analyst
Gartner, Inc.*

prevention of malicious attacks before they enter the network. All security events and statistics detected by MSM+ID are reported through the Industrial Defender console and Counterpane’s web portal, providing a single operator interface.

THE APPROACH AND ITS ADVANTAGES

An important advantage of Counterpane’s approach is its passive nature. The customer retains full control over what is, and is not, submitted to Counterpane’s systems for security review. Sensitive information, such as customer-identifying transaction records, can be demonstrably excluded so no risk of data leakage is present. By the same token, any message the customer explicitly wants to include in the security program can be classified to any severity level.

The key, from the security officer’s point of view, is that these capabilities are available for any device, on any part of the network. Enterprise-wide policies can be monitored and enforced via Counterpane managed security services, whether on a private specialty network, or a general-purpose corporate network, and tangible metrics of security performance and compliance are available to measure everything from incident response parameters to technology effectiveness to staff escalations.

Managed security services are valuable not just because they can detect an attack in progress, but more importantly, they contribute to an ongoing program of security improvements which ensures the customer benefits from proactive advice. This is particularly helpful in the case of zero-day exploits where a reactive posture, by definition, can’t work. The difference between a painful zero-day experience, and an inconsequential one, is how comfortably the targeted organization responds.

Managed Security Services help customers prepare for audits. Taken together, the raw data and prepared reports provide a centralized record of performance data from various security controls, and reduce the amount of time auditors must spend simply uncovering historical records.

Enterprise Security Consulting

Verano and Counterpane jointly have security consulting expertise which spans the entire range of SCADA, DCS, NERC, FERC, physical, and network security skills. Below are examples of available service types; please contact Counterpane to discuss your specific requirements.

- Network Architecture Review & Documentation
- Vulnerability Assessment Services
- Penetration Testing
- NERC Compliance Gap Analysis

Contact Us

sales@counterpane.com

US: 888-710-8175

EMEA: +31 70 5170 419

Japan: +81 80 5421 8311

1090A La Avenida
Mountain View, CA 94043

www.counterpane.com



Counterpane™
Internet Security