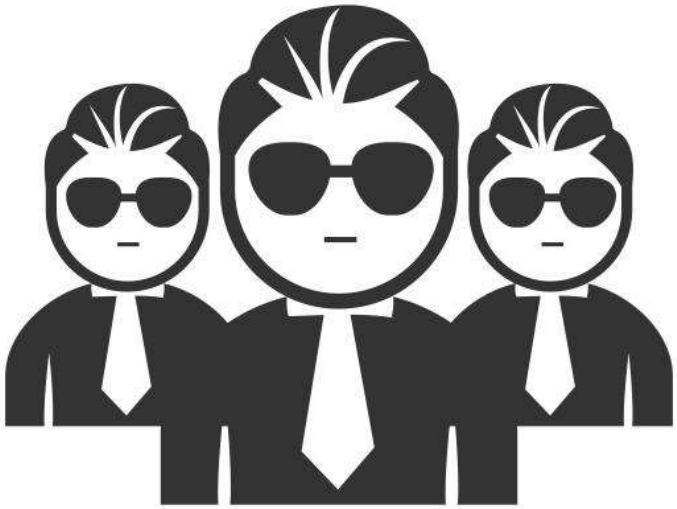

ControlScan Managed Detection and Response [Built on Our Powerful SIEM Platform, *Cyphon*]

Why ControlScan MDR?

ControlScan performs **Managed Detection and Response (MDR)** for organizations that don't have the internal bandwidth to keep a vigilant watch over the security events in their IT environment. We employ the right people and the right processes to efficiently supplement your organization's cybersecurity management efforts.

Our team identifies intrusions **as they are happening**, so you can extract them from your environment before any damage is done by:

- Defining, implementing and updating security rules
- Running targeted threat hunting sequences to trace anomalies
- Examining alerts to separate true concerns from false positives
- Addressing and appropriately escalating threats in real-time

What sets us apart?

ControlScan MDR includes monitoring for syslog devices such as Network Devices, POS Systems, etc. But those devices are not counted as an endpoint with licensing. Those systems are **integrated** into logging during the onboarding process.

Many MDR providers dictate that their response to be a notification to the customer that an event has occurred, with no active further investigation or hands-on remediation of the threat and affected systems. **ControlScan** provides **hands-on true "response".** Our analysts perform **extensive investigation and correlation** of any event on the customer network and **performing the necessary actions in real time** to ensure the customer environment remains protected.

Our Cyphon platform will hash known bad viruses and can monitor any new threat.

What is included with ControlScan MDR?

As part of our MDR service, we collect, aggregate and normalize your organization's log data from servers, endpoints, applications and security devices for compliance and infrastructure management. Our expert security analysts monitor and analyze your log events, **freeing up your IT resources to focus on growing your business**.

The ControlScan **Security Operations Center (SOC)** captures and compiles data from both physical and digital sources to develop a level of decision support not possible in a standard monitoring environment. This process combines our people, processes, and technology to analyze and act on robust data sets - allowing us to see the **whole picture** of an enterprise. We keep your business optimized and running no matter what challenges arise.

Our SOC runs **24x7** and is staffed by **highly trained** SecOps personnel. Located in **Hunt Valley, MD**, the SOC is a secure facility featuring video surveillance, biometric access control, redundant fiber-optic Internet connectivity, and battery and diesel redundant power.

What is included with ControlScan MDR? *(continued)*

24x7 Managed Detection and Response of threats and attacks against your systems and networks.

ControlScan provides a **fully managed solution** incorporating:

- Log Collection and Correlation
- Monitoring and identification of anomalies and security threats in your organization.
- Cloud Application Monitoring for Office 365, Gmail, on-premise Microsoft Exchange
- ControlScan provided Next Gen Endpoint Protection
- File Integrity Monitoring with 3 or 12 months of retention (MDR and MDR+)
- Interactive web-based dashboards
- Cloud Productivity Tool Connectors (Office 365 or Google GSuite)
- Command and Control Traffic; Identify source/ block and quarantine quickly
    - Defend against spray password attacks
    - Disable Account Access Attempts
    - Defend Network Probing
    - Identify Rogue Machines

Replaces traditional Log Collection (SIEM) and Endpoint (Anti-Virus/Anti-Malware) solutions.

Installation

ControlScan MDR provides a consolidated installer that is **easy to use and deploy**, with only four clicks to completion on average. The installer also **supports centralized deployment** through any existing software management systems in place (SCCM, Active Directory, etc.)

PCI Fulfillment

MDR can assist in completing sections of **PCI requirements**:

- Requirement 3: Protect stored cardholder data
- Requirement 5: Use and regularly update anti-virus software
- Requirement 10: Track and monitor all access to network resources and cardholder data

Questions?

Contact me today.

Joe Gaeta
Territory Account Executive
Direct: 678-694-0687
Mobile: 404-435-7376
jgaeta@controlscan.com