cyber security services

Managed Detection and Response (MDR)

Maintaining the level of technology and talent required to address our ever-evolving threat landscape can be challenging, but Cyber Security Services provides organizations with comprehensive solutions. At Cyber Security Services, our complete strategy includes 24x7x365 Managed Detection and Response (MDR) as well as Extended Detection and Response (XDR) for a solution that's notably unique within our marketplace. Seal vulnerabilities proactively and minimize the chance of attack without ever having to invest in added technology or personnel.

With our defense in-depth approach, you gain numerous layers of security to address:

- **Endpoint Security Threats**
- **Unmanaged Device Threats**
- **Perimeter Network Threats**
- **Cloud Applications and Cloud Threats**

We can customize monitoring and response procedures to suit your organization and environment. This includes tailored response measures for endpoint isolation and threat blocking, options for monitoring device types outside of EDR and endpoint security agents—even options to block attacks using existing network equipment and security investments.

CROWDSTRIKE

Our approach to MDR at the endpoint begins with CrowdStrike Falcon.

As a CrowdStrike strategic SOC/MSSP partner, we provide you with the assurance that your company's MDR solution is backed by the world's leading breach prevention software designed to stop attacks in progress. And the CrowdStrike Falcon Next-Gen Antivirus and EDR solution is included within our standard MDR service offering.

A powerful 24x7x365 threat hunting and prevention service, MDR For the Endpoint by Cyber Security Services is coupled with industry leading breach prevention from CrowdStrike Falcon. Backed by CrowdStrike's unparalleled threat intelligence and Indicators of Attack (IOA), our certified analysts provide you with real-time response to expedite investigations and quickly isolate malicious endpoints.

Gain powerful around-the-clock threat hunting support to address even the most undetectable and sophisticated attacks. Our incident responders can isolate endpoints and provide managed remediation services to restore your systems back to their pre-attack state. This comprehensive service includes a dedicated CrowdStrike tenant for each client with co-managed features.

We manage risk from unmanaged devices without agents.

At Cyber Security Services, we enhance the endpoint MDR service by detecting and responding to threats on devices unable to receive a sensor or security agent. Our 100 percent US-based Security Operations Center bridges the security gap introduced by unmanaged devices on your network.

MDR gives clients the option to detect and block threats that come in from BYOD, IoT, and OT devices along with unmanaged workstations, medical and manufacturing devices, and other device types that cannot be monitored with an EDR agent. Our fully managed SIEM solution comes complete with notifications and response procedures. Employing our state-of-the-art SIEM, we monitor your existing infrastructure and security investments without ever requiring additional network hardware or overhead.

Prevent attacks at the perimeter.

Our MDR capabilities extend to the perimeter of your network and beyond with added 24x7x365 monitoring support. In addition to this, we can add your existing technology investments under the same umbrella, such as perimeter firewalls, intrusion prevention systems (IPS), email security appliances, and web application firewalls (WAF). Let our SIEM solution ingest traffic from hundreds of device types to be correlated and reviewed by our SOC.

cyber security services

We provide response services beyond the managed endpoint.

As part of our MDR service, you can opt to have our responders block threats on your firewalls, switches, and security appliances with preapproved procedures. Response procedures can also address threats both inside and outside of your network. Whether employing your perimeter firewall to block an external attack from a nation state or using an internal switch to block a malicious IoT device where it connects, we deliver the right solution to respond to infrastructure threats around the clock. This tailored response procedure sets us apart from comparable service providers in the MDR and XDR space.

While most MDR providers stay within managed endpoints, we offer a comprehensive security monitoring and response strategy to secure your entire network.

Our MDR services include:

- 24x7x365 Monitoring and Threat Detection Services
- CrowdStrike Falcon Sensors for Endpoints
  - Machine-Based Learning
  - Artificial Intelligence
  - Indicators of Attack (IOA)
- Preapproved Procedures for Endpoint Response with Falcon Including Endpoint Containment and Isolation
- A Dedicated CrowdStrike Tenant for Your Organization
  - Co-Managed Solution
  - Endpoints Review
  - Endpoints Report
  - As-Needed Response
- Options for Vendor Agnostic Log Monitoring and Threat Detection Including CSS Managed SIEM
- Options for Vendor-Agnostic Blocking Procedures Using Client Infrastructure Based on Preapproved Procedures with Strategy and Architecture Discussions on Process
- SOC Monitoring of Hundreds of Device Types and Manufacturers
- Flexible Escalation Services (Email, Phone, Text, and Slack)
- Threat Hunting Included as Standard Service
- Optional Remediation of Incidents on Endpoints
- Custom Signature and Threat Detection Services for Security Events Based on CrowdStrike Custom Policies
- Support Ticket Reviews/Monitoring and Management Using CrowdStrike Support Management by Cyber Security Services
- No Additional Hardware Required

Since 2014, we've provided expert counsel and security solutions to clients across a broad range of industries nationwide—from start-ups to Fortune 100 companies. We bring the intelligence and proven experience required to ensure 24x7x365 monitoring support, to effectively analyze and evaluate security risk, and to mitigate incidents before they affect your bottom line.

Drop us a line at **sales@cybersecurityservices.com** or call **800-390-1053** to schedule an initial service consultation.

Cyber Security Services
752 N. State Street No. 172
Westerville, Ohio 43082

www.cybersecurityservices.com