Defend Against Cyberattacks 24x7x365

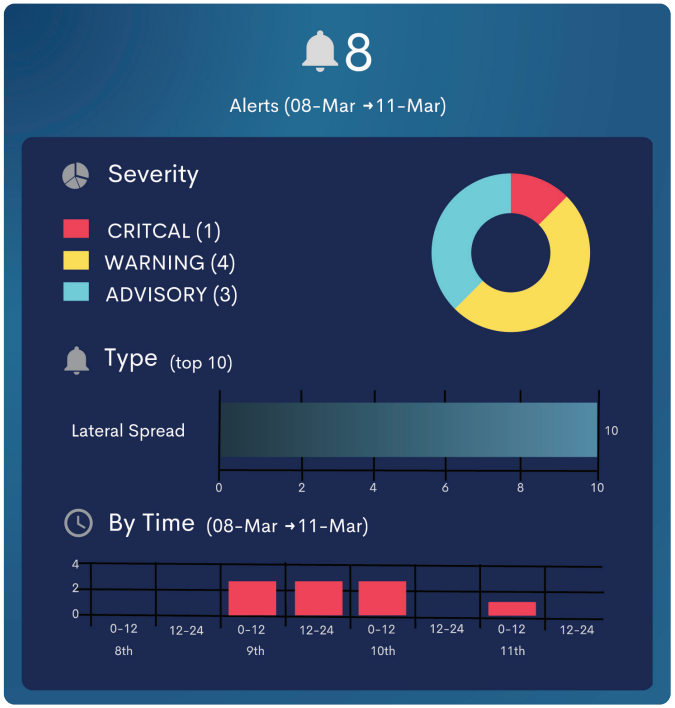
# Managed Detection & Response

## Protect Against the Latest Cyber Threats

Rapid detection and response are critical to avoiding operational downtime, revenue loss, and damage to your business reputation. Our **Managed Detection and Response (MDR)** service monitors your network and devices 24x7x365, with a focus on catching breaches and responding to contain them within minutes.

## Real-Time Threat Hunting, Detection, and Response

We catch cyber threats before they can spread with real-time threat hunting, detection, and response. With our advanced combination of network visualization, insider threat monitoring, anti-malware, traffic analysis, and endpoint security, we keep you safe around-the-clock.




## 24x7x365 Security Operations Center (SOC)

Basic perimeter protection and legacy antivirus are no longer sufficient to detect and stop cyberattacks. Organizations need artificial intelligence, automation, and experienced security analysts in a 24x7x365 SOC to stop cyber attacks as they unfold. M.A. Polce's MDR service is that solution.

**Core Service:**

Advanced Threat Monitoring & Detection
Zero Trust Managed Application Control
Rapid Response & Isolation
Expert Guidance
Detailed Reports
Dashboard Visibility
M365 & Google Cloud Protection

M.A. Polce
IT & CYBERSECURITY

Defend Against Cyberattacks 24x7x365

# Managed Detection & Response

## Additional Services

**Endpoint Detection & Response (EDR) -** An integrated endpoint security solution that combines real-time continuous monitoring and the collection of endpoint data with rules-based automated response and analysis capabilities.

**Email Security -** Analyzes email communications to prevent unauthorized access, malicious payloads, phishing, and more. Email security is essential, given that email remains the number one threat vector.

**DNS Security -** Stops attacks that are riding on otherwise legitimate user requests for your servers, services, and websites. It provides category-based website blocking and other essential security functions.

**Multifactor Authentication (MFA) -** A multistep authentication method by which your users must successfully present two or more credentials to verify their identity and gain access to websites or applications.

**Syslog and Device Event Logging -** Identify critical network devices from which to capture syslog information to have important data available in the event of a security incident, audit, or other situation.

**File Integrity Monitoring -** Capture meaningful data from your server infrastructure to use whenever you need to see if unauthorized access or file changes have been made.

**Let's Connect**

www.mapolce.com

315-338-0388

M.A. Polce

IT & CYBERSECURITY