TLC TECH
WE SPEAK HUMAN

Managed Detection and Response *(MDR)*

Managed Detection and Response *(MDR)* is a comprehensive service that includes 24/7 threat monitoring, threat hunting, and detection response. We leverage a combination of hand-picked and vetted technologies deployed at the host using advanced analytics, threat intelligence, and human expertise to deliver sophisticated and thorough incident investigation and response.

Why Do You Need MDR?

Roughly 50% of cyberattacks target small businesses, and 60% of those attacked go out of business within six months. That's why you can't rely on basic, limited cybersecurity.

To protect yourself and your business you need Advanced Endpoint Security backed by 24/7/365 security

MDR Contains

- **RAPID RESPONSE:** The average breach lasts an average of over 200 days before detection. In this time *(nearly 9 months!)* the average criminal can do whatever they want with you or your clients' information, presenting a massive risk to your company.
- **ACTIVELY MONITORING THREATS 24/7:** The bad guys don't work "normal business hours"—that's why we monitor and search for threats year-round, nights, and weekends with Security Analysts who know what to look for
- **PROTECTION FROM MODERN THREATS:** Hackers are now more advanced than ever before. New malware and ransomware variants are designed to get past traditional solutions of long ago
- **ARTIFICIAL INTELLIGENCE:** We use today's AI technology to keep you protected from today's modern threats

Powered by:

BlackBerry Infocyte® STELLAR CYBER®

How Does MDR Work?

Anomaly-Based Detection

Utilizing heuristics, statistical analysis, and machine learning, ARR highlights atypical events or features of an artifact/file which aids in the detection of advanced and zero-day threats.

- Real-time Process and Script Monitoring
- Continuous Live Memory Analysis
- Powershell and other "Living-off-the-Land" adversary techniques
- Abuse of legitimate administrative tools
- Lateral movement
- User Account Misuse

Behavior-Based Detection

The behavioral analytics engine identifies suspicious behaviors of legitimate processes and events and maps them to known attacker tactics, techniques, and procedures *(TTPs)* as described in the MITRE ATT&CK framework *(A curated knowledge base and model for cyber advesary behavior)*.

We concentrate defenses against the Top 20 most commonly observed ATT&CK techniques that are also achievable to monitor. These allow us to be more effective and catch adversaries' actions more often.

Forensic State Analysis

The agent has the ability to collect and analyze live forensic data from your endpoints, including from both volatile and non-volatile memory. This capability enables proactive inspection of thousands of hosts for current and historical compromise as well as aiding in the root cause identification of detected attacks.

- Active Processes & Scripts
- Triage of Live Volatile Memory
- Registry and Autoruns *(Run Keys, Startup Folders, Link Files, Schtasks/Cron, etc.)*
- Execution Artifacts *(shimcache, amcache, prefetch)*
- OS Subversion *(API hooks, disabled controls)*
- Local Event Log Triage
- Privileged Accounts
- Installed Applications & Vulnerabilities
- Active Host Connections & Listeners

Continuous Endpoint Monitoring, Response, And Forensics

ARR's advanced threat hunting and monitoring add another layer of security-focused on identifying key behaviors observed during and following an attack. In addition, automated forensic analysis enables our analysts to proactively verify the integrity of endpoints or quickly determine the root cause once a breach is found. MDR simplifies and accelerates the identification, investigation, and response to sophisticated cyber attacks.

Harness Advanced Cybersecurity

MDR gives you both the capability to better defend your business, as well as the expert support that you need to manage it. It's a robust cybersecurity service that allows you to be confident in the way your business is defended.

Talk to the TLC Tech team to discover how MDR will enhance your cybersecurity.

TLC TECH
WE SPEAK HUMAN

Powered by:

BlackBerry Infocyte® STELLAR CYBER®