Is an MDR the Right Solution for Your Organization?

360-DEGREE VISIBILITY INTO SECURITY AND PROACTIVE DETECTION OF CYBER THREATS

Managed Detection and Response (MDR) is an outsourced cybersecurity management service that provides organizations with 360-degree visibility into security and proactive detection of cyber threats. MDR then neutralizes those threats once discovered. MDR is a combination of technology and human expertise working in concert to ensure your network protection.

What Does the MDR Service Do for an Organization?

Solve the HR Challenge

MDR solves a critical problem that affects more and more companies: the lack of trained and experienced cybersecurity professionals on the IT team. While training and building specialized security teams capable of hunting down threats on a full-time basis may be feasible for large organizations that can afford it, most companies will find it a real challenge given their limited resources. This is particularly true for SMBs who are often targeted by cyberattacks specifically because their defenses are assumed to be less sophisticated.

Even organizations that are willing to spend the time and money may have difficulty finding appropriate personnel. The skills required to recognize signals related to a cyberattack are scarce, even among computer security specialists.

Flatten the Learning Curve

Companies also struggle to master and manage the variety of security tools and the unique knowledge needed to make them work. As a result, organizations find themselves with a series of security tools that are inadequately configured to meet their security needs. StreamScan has developed its own artificial intelligence technology to maximize detection rates for its clients.

Eliminate Alert Overload

Another often overlooked problem is the volume of alerts generated by security software that security and IT teams have to cope with. Many of these alerts can't be easily identified as malicious, and so they have to be researched and verified on a case-by-case basis. Security teams also need to correlate these threats to discover whether seemingly insignificant indicators add up as part of a larger attack. This is called Alert Overload in the industry, and it can overwhelm and cripple small security teams.

An MDR solution addresses this problem by detecting threats and analyzing all the factors and indicators involved in an alert. MDRs also typically provide recommendations and changes to organizations based on an analysis of security events. One of the most essential skills that security professionals need is the ability to contextualize and analyze compromise indicators to better position the organization against future attacks. Security technologies may have the ability to block threats, but digging deeper into the how, why, and what of incidents requires a human touch.

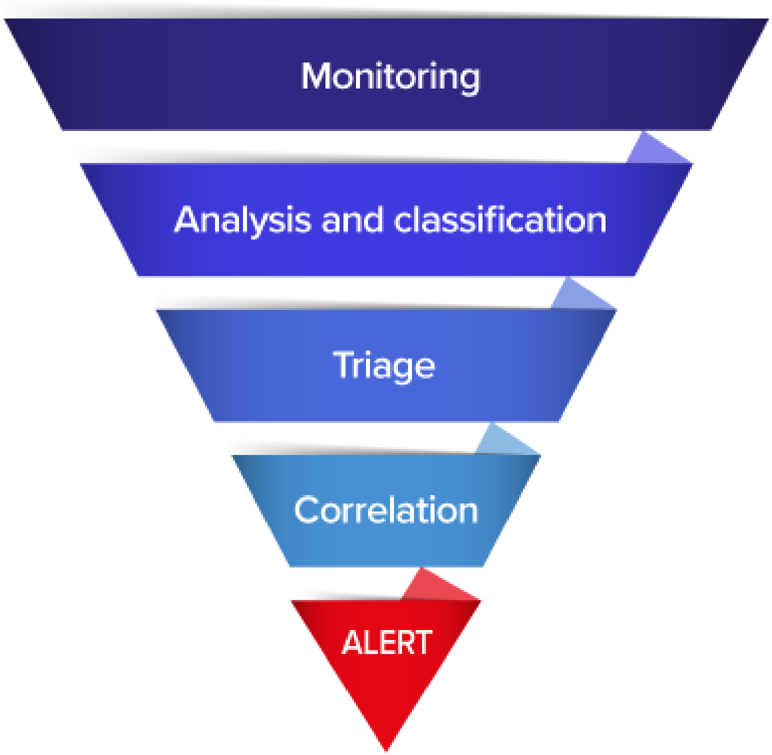
Address the Skills Gap

MDRs are designed to address the cybersecurity skills gap within organizations. They provide organizations with access to the more advanced analytical skills needed for complex threats that an in-house IT team cannot fully address. Ideally, it does so at a lower cost than what the company would have to spend to build its own dedicated security team.

How Does the Streamscan MDR Service Work?

Our StreamScan MDR team operates 24/7 and acts as an extension of your internal IT team, ensuring that your network is secure at all times. This team is made up of experienced cybersecurity pros whose expertise covers cyberattack management, intrusion detection/prevention, incident response, malware reversing, forensics and evidence collection, etc.

Our MDR team covers the full detection and response funnel:



MONITORING: 30%

The StreamScan team remotely and continuously monitors security signals, alerts, and events generated by CDS technology and security tools that make up your security stack. The slightest suspicious behavior detected by our innovative Cyberthreat Detection System (CDS) and your other security tools are isolated and investigated by our analysts.

ANALYSIS & CLASSIFICATION: 30%

As true threat hunters, our analysts investigate identified suspicious cases to confirm whether or not there is a security issue. The objective is to deal with suspicious cases upstream before they become a problem. The analysis classifies signals into two categories: true threats and false positives.

TRIAGE: 10%

Following the first analysis (i.e., true threat vs. false positive), an incident ticket is created in StreamScan's CDS to initiate a thorough investigation of the problem cases, which are then classified according to their level of severity and impact (LOW, MEDIUM, HIGH, or CRITICAL). Response is automatic for HIGH and CRITICAL cases.

CORRELATION: 20%

When the StreamScan team is faced with a complex case, it analyzes the collected attack signals, cross-referencing all available data, and conducts further research where needed. In some cases, we reverse-engineer malicious code or reproduce the attack scenario to understand all of its parameters. This allows us to anticipate the hacker's next move and protect against it.

ALERT AND TICKET: 10%

We notify our customers and propose an in-depth, precise, and concrete intervention plan to resolve threats quickly and efficiently. We notify by phone or email, depending on the level of severity.

We understand that our clients' IT teams are very busy, and we provide all the information necessary to take action without requiring them to do additional research. For example, we go so far as to provide the link where IT teams need to download the patch for an identified vulnerability.

Note: In addition to the activities carried out by our MDR team, the CDS has functionalities allowing it to block certain types of cyberattacks automatically. It also has email and SMS notification functions. The combination of our CDS and our MDR teams' human expertise offers proactive cybersecurity management adapted to the reality of today's cyberattacks.

Periodic Reports

We provide a monthly network monitoring report to summarize the security activities observed on your network, the response actions taken, and our recommendations for security enhancements. This report is used to improve your security continuously.

Cloud and Internal Networks Are Covered

Our MDR service covers your internal network and your systems and applications in the Cloud (e.g., Microsoft 365). The objective is to have 360-degree visibility of your network and manage its security in one place.

Our CDS technology can be installed in the Cloud or any other virtual environment (Virtual Appliance) or as a Physical Appliance.

MDR Provides Protection and Exceptional Value

As you will have noticed, our MDR solution combines technology and people for efficient management of your security. While giving you access to several people with different profiles, our MDR service costs a fraction of what you would pay to deploy one or more security technologies and manage them daily.