Managed Detection and Response (MDR) is an advanced cybersecurity service that provides 24/7 network monitoring, threat detection, and incident response capabilities to organizations of all sizes. In this comprehensive guide, we'll explore what MDR is, how it works, and why it's an essential component of a modern cybersecurity strategy.

WHAT IS MANAGED DETECTION AND RESPONSE (MDR)?

While most organizations protect their networks with antivirus software on their employee's computers and firewalls, MDR utilizes real-time threat detection and response, continuous monitoring of network activity and endpoints, proactive threat hunting and incident response, and access to advanced security technologies and expertise. Traditional Anti-virus focuses on pre-infection by preventing malware, however, blocks only 50-60% of real-world threats.

REAL-TIME THREAT DETECTION AND RESPONSE

Real-time threat detection and response is an approach to cybersecurity that involves continuously monitoring an organization's network, endpoints, and other systems for potential security threats, and taking immediate action to mitigate those threats as soon as they are detected. This approach allows organizations to quickly detect and respond to potential security incidents, reducing the risk of a successful cyber-attack by shortening dwell time. Dwell time refers to the amount of time a malicious actor has access to a compromised system before the threat is detected.

Real-time threat detection and response typically involve the use of advanced security technologies, such as intrusion detection systems (IDS), security information and event management (SIEM) systems, and machine learning algorithms. These technologies can analyze network traffic, system logs, and other data sources in real-time, looking for signs of suspicious activity that could indicate a security threat.

Once a potential threat is detected, the system can generate an alert or notification, which is then sent to the organization's security team or a third-party Managed Detection and Response (MDR) provider. The security team can then investigate the alert, determine the severity of the threat, and take immediate action to contain, remediate, or escalate the incident as needed.

Real-time threat detection and response is an essential component of a modern cybersecurity strategy, as it allows organizations to quickly detect and respond to potential security threats, minimizing the impact of any incidents that do occur. By partnering with an established MDR provider like OFFSITE, organizations gain the capabilities of a team of engineers trained to respond to modern cybersecurity threats.

CONTINUOUS MONITORING OF NETWORK ACTIVITY AND ENDPOINTS

Continuous monitoring of network activity and endpoints is a key element of any cybersecurity strategy. It involves using advanced technologies to continuously monitor an organization's network and endpoints for potential security threats, such as malware, unauthorized access, or suspicious activity.

Continuous monitoring typically involves these same security technologies, including IDS, SIEM, and EDR systems, with the same goal of uncovering security threats quickly.

Continuous monitoring also helps organizations meet regulatory compliance requirements, as many regulations require organizations to have a continuous monitoring program in place to protect sensitive data and ensure the integrity of their systems. In fact, many insurers will not provide cybersecurity insurance if these tools are not in place.

PROACTIVE THREAT HUNTING AND INCIDENT RESPONSE

Proactive threat hunting and incident response is an advanced approach to cybersecurity that involves actively searching for potential security threats before they can cause damage, and responding to incidents quickly and efficiently to minimize the impact on the organization.

Proactive threat hunting involves actively searching for potential security threats within an organization's network, endpoints, and other systems, including servers in the public cloud. This approach involves using advanced technologies, such as threat intelligence feeds, machine learning algorithms, and security analytics, to detect potential security threats that may have gone undetected by traditional security measures, such as anti-virus and malware software.

Incident response involves responding to security incidents quickly and efficiently to minimize dwell time and the impact on the organization. This approach involves having a plan in place to respond to security incidents, and having a team of skilled professionals who can quickly and effectively respond to these incidents and escalate if necessary.

By combining proactive threat hunting and incident response, organizations can detect potential security threats early and respond quickly to minimize risk and negative impact.

ACCESS TO ADVANCED SECURITY TECHNOLOGIES AND EXPERTISE

Advanced security technologies include various hardware and software solutions designed to detect and mitigate cyber-attacks, such as firewalls, intrusion detection systems, and encryption tools.

In addition to advanced security technologies, having access to cybersecurity expertise is equally important. Like any cybersecurity tool, it is only as good as the resources who are implementing, configuring, and managing it. Cybersecurity experts are critical when it comes to developing effective security strategies, policies, and responding to security incidents when they do occur. Partnering with a Managed Detection and Response (MDR) provider can provide organizations with the skills and expertise when they need to escalate a situation.

By partnering with an MDR provider, organizations can benefit from the latest in cybersecurity technology and knowledge, without the need to invest in expensive hardware and software solutions or hire dedicated cybersecurity professionals. This approach allows organizations to focus on their core business activities while ensuring that their networks and systems are protected against potential cyber threats.

HOW DOES MANAGED DETECTION AND RESPONSE (MDR) WORK?

MDR utilizes Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) to provide a service. That service is managed by a 3rd party, as the “M” in MDR suggests.

EDR and XDR technologies work by collecting and analyzing data from various sources, such as endpoints, network devices, and cloud applications, to create a cohesive security operations system. It uses advanced analytics and machine learning to detect anomalies and potential threats and provides real-time alerts and recommendations to security teams. These tools also provide incident response services, such as containment, investigation, and remediation.

Endpoints, such as desktops, laptops, and mobile devices, are common entry points for cyber-attacks. By collecting and analyzing data from endpoints, organizations can detect potential security threats, such as malware infections or unauthorized access attempts. Endpoint detection and response (EDR) tools are often used to collect and analyze endpoint data, providing organizations with real-time visibility into potential security threats.

Network devices, such as routers, switches, and firewalls, are another important source of data. By collecting and analyzing data from network devices, organizations can detect potential security threats, such as network intrusions or suspicious traffic patterns. Intrusion detection and prevention systems (IDS/IPS) are often used to collect and analyze network data, providing organizations with real-time alerts and recommendations for mitigating potential security threats.

Cloud services, such as cloud storage or cloud-based applications, are becoming increasingly popular among organizations. By collecting and analyzing data from cloud services, organizations can detect potential security threats, such as unauthorized access or data breaches. Cloud security solutions, such as cloud access security brokers (CASBs), are often used to collect and analyze data from cloud services, providing organizations with real-time visibility and control over their cloud-based systems and data.

USING ADVANCED ANALYTICS AND MACHINE LEARNING

Using advanced analytics and machine learning technologies can analyze large volumes of data in real time, looking for patterns and anomalies that may indicate a potential security threat.

Using various statistical and mathematical techniques, they analyze data, such as log files, network traffic, and user behavior. This approach can help identify potential security threats by detecting unusual activity patterns, such as unusual login times or unusual data transfers.

Machine learning is a type of artificial intelligence (AI) that can automatically detect patterns and anomalies in data. By training machine learning algorithms on large datasets, organizations can teach these algorithms to identify potential security threats, such as malware infections or suspicious network activity.

Combining advanced analytics and machine learning can provide organizations with a powerful tool for detecting potential security threats in real time. By analyzing large volumes of data and identifying unusual patterns and behaviors, these technologies can help detect potential security threats early, enabling organizations to take immediate action to protect their sensitive data and systems.

PROVIDING REAL-TIME ALERTS AND RECOMMENDATIONS

Real-time alerts typically involve sending notifications to security teams when potential security threats are detected, such as suspicious network activity or malware infections. These alerts can be sent via email, SMS, or through a security dashboard, providing security teams with real-time knowledge of potential security threats.

In addition to real-time alerts, these technologies can also provide for mitigating potential security threats. For example, a SIEM system may recommend that a security team isolate an infected device from the network or update software to patch a vulnerability that has been exploited.

INCIDENT RESPONSE SERVICES: CONTAINMENT, INVESTIGATION, AND REMEDIATION

When a security incident occurs, it is critical to have a plan in place to contain the incident, investigate the cause, and remediate the damage as quickly as possible.

Containment involves isolating the affected systems and data to prevent the incident from spreading further. This approach can help prevent additional damage and protect other systems and data from potential security threats.

Investigation involves determining the cause and extent of the incident, including identifying the type of attack and the data or systems that were affected. This approach can help organizations understand how the incident occurred and develop strategies to prevent similar incidents in the future.

Remediation involves taking steps to restore affected systems and data to their original state and implementing measures to prevent similar incidents from occurring in the future. This approach may involve installing software updates, patching vulnerabilities, or reconfiguring security systems.

By providing incident response services, organizations can respond quickly to security incidents, minimizing their impact. This approach can help prevent data breaches, intellectual property theft, and other serious consequences of cyber-attacks.

Partnering with a Managed Detection and Response (MDR) provider can provide organizations with access to incident response services, as well as a team of skilled cybersecurity professionals who can respond to incidents quickly and effectively. MDR providers can provide organizations with these capabilities 24/7/365, when internal resources may not be available such as on weekends, holidays, and after normal business hours.

WHY IS MANAGED DETECTION AND RESPONSE (MDR) IMPORTANT?

MDR is important because modern cyber threats are becoming increasingly sophisticated and difficult to detect with traditional security measures. Many cyber-attacks today involve advanced tactics, such as social engineering, fileless malware, and zero-day exploits, that can easily evade traditional security measures.

In addition to providing advanced threat detection and response capabilities, MDR is important because it allows employees to focus on other tasks, while ensuring that their business is protected against potential cyber threats. MDR providers handle the day-to-day management and monitoring of an organization's security systems, freeing up internal resources to focus on other critical business functions. By partnering with a trusted MDR provider, organizations can gain the peace of mind they need to focus on their core business activities and achieve their strategic objectives.

IMPORTANT CONSIDERATIONS WHEN CHOOSING A CYBERSECURITY SOLUTION

There are a number of considerations to keep in mind when choosing the solution that is right for you. First, a variety of system and service functionality is available when it comes to MDR, so careful consideration should be given to the tools chosen. It's key to know the core function of the tools and their true scope. Secondly, integration capabilities must be considered. Integration: You've likely invested in some security tools already. Your MDR solution should be able to integrate with the endpoints that your organization has, the applications that you use, and your way of working.

Before choosing a solution, you must consider the setup and management of your cybersecurity technologies. Do you have the internal resources to configure, integrate and manage the solution?

Do you have resources to monitor and respond outside of normal business hours, on weekends and holidays? A 3rd party managed MDR solution is key in instances where internal resources are lacking.

Do you have business processes in place? It is rarely the technology to blame for the large data breaches that make news headlines. In almost every major cyber event, the root cause turns out to be a failure of the business process. When implementing a new solution, it is imperative that policies and processes be documented, for example determining escalation paths when issues are detected. OFFSITE recommends having white-board sessions with your CIO, COO, CCO, CFO, attorneys, insurance specialists, and MDR provider(s).

Lastly, it is important to consider that there is no silver bullet to achieving cybersecurity, and no technology will alleviate all cyber-risk. It is critical to have robust business processes in place in order to reduce the risk of a cyberattack. By implementing strong policies and protocols and investing in employee cybersecurity training and resources, companies can greatly decrease this risk.

OFFSITE'S APPROACH TO MDR

- Industry-leading Managed SIEM tools with detect & respond service.
- AI processing detects suspicious behavior, discovers cyber events, and provides steps to remediate
- Programmed, automated, orchestrated response
- Set 3 types of irresistible traps for bad actors within your environment.
- Receive weekly executive reports from the OFFSITE security team
- 30-minute weekly CISSP meetings to address findings, discuss steps to remediate
- 24/7 alerting, supported by our local engineering team
- OFFSITE engineers are available to complete steps to remediate on a T&M basis, as needed

WHY OFFSITE?

OFFSITE's key differentiators for MDR solutions include:

- 24/7/365 monitoring and response
- Local engineers trained in a variety of industry leading MDR solutions
- Customizable solutions, from fully managed to comanaged and everything in between
- Audit & Due diligence support
- Experienced security analysts oversee your environment without adding full-time staff and resources

OFFSITE redefines the data center experience with its high-performing environment for managing data operations. We operate safe and secure facilities, with powerful infrastructure, industry-leading technology, strategic processes, comprehensive services, and data solutions

expertise. Since 2001, OFFSITE has provided clients with managed IT services, protection against cyberattacks, private cloud services, IaaS, custom colocation services, business continuity services, network operations center (NOC) and security operations center (SOC) services, and hosted and managed solutions. OFFSITE's spacious facilities and customized services enable businesses to solve their IT challenges and discover new opportunities.

READY TO TAKE YOUR CYBERSECURITY STRATEGY TO THE NEXT LEVEL?

OFFSITE has a team of engineers working around the clock to provide support to our clients. If you'd like guidance from OFFSITE's Security Operations Center, we are available to help develop a managed solution to protect your organization's data. Contact us today to learn more about our Managed Detection and Response (MDR) services and how we can help protect your organization from cyber threats. **To get in touch, email info@off-site.com or call (262) 564-6500.**