IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Cisco

Businesses that seek to defend their valuable data from theft or destruction need to recognize that a strong detection and response capability is an absolute requirement.

Managed Detection and Response: A Better Way to Defend Against the Cyberpredator

July 2020

Written by: Craig Robinson, Program Director, Security Services

AT A GLANCE

KEY STATS

A 2019 study showed the average time to detect a security breach is 206 days, or 6.8 months, while the average time to contain a breach is 73 days, or 2.4 months.

KEY TAKEAWAY

Given that it takes *months* to detect and contain breaches, the tools and technologies used to keep bad guys out need a major upgrade.

Introduction

The 50th anniversary of the first computer worm will be recognized in 2021. While that early effort at disrupting computers did nothing other than display the message "I'm the creeper: catch me if you can" on computer terminals, the more recent attacks that are launched and often find success in their sinister missions are much more dangerous.

In recent years, chief information security officers (CISOs) have been doing everything that they can to elevate their cybersecurity programs to defend the institutions that they are charged with protecting. Attacks that seek to bring down networks and websites, destroy data, steal intellectual property, or install ransomware have seen CISOs respond with point product after point product to try and stem their losses. Even adding newer cybersecurity services to provide higher uptime and advanced capabilities has not done enough to significantly prevent these attacks from landing on their intended target.

The various metrics that measure how quickly firms can detect, contain, and recover from these attacks are not seeing any significant improvement. A 2019 study by IBM Security and the Ponemon Institute showed the average time to detect a security breach is 206 days, or 6.8 months, while the average time to contain a breach is 73 days, or 2.4 months. When the time it takes to detect and contain breaches can be measured in months, it can be safely surmised that the tools and technologies that are being used to keep the bad guys out are in need of a major upgrade.

As a result of the global pandemic, perhaps the one attack method that scares CISOs and boards of directors the most is the usage of leakware amid the new challenges of an increasingly remote workforce. This new tactic involves the planting of ransomware, but with a sinister twist; instead of holding the keys to unencrypting the data that they encrypt, cyberattackers threaten to leak the data in batches until their monetary requirements are met. It becomes increasingly frustrating to security operations centers (SOCs) to see so many of their recent improvements in their overall security posture rendered ineffective by this new, evil tactic.

On top of all the concerns that security teams must deal with, the arrival of the COVID-19 pandemic in early 2020 gave birth to a slew of new concerns. The expansion of the risk surface with the usage of residential networks and personal computing devices, along with the rush to the cloud to enable the new reality of work-from-home environments, has given cybercriminals new opportunities to cause mayhem.

Recognition of the need for a robust defense to protect a vastly expanded risk surface in the cloud, on edge devices, and in on-premises locations while building up the capability to identify, contain, and remove malware that finds its mark has led to the creation of new managed security service (MSS) capabilities appropriately named managed detection and response (MDR).

Definitions

MDR is a subset of managed security services that combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity life-cycle capabilities for an organization. Service providers can deploy MDR services utilizing a mixture of a client's existing capabilities along with cybersecurity partner–supplied tools or services and private intellectual property. MDR services are supplied by a provider's well-trained cybersecurity staff in a 24 x 7 x 365 remote SOC.

IDC recognizes the following as a minimum set of MDR capabilities:

- Utilization of endpoint protection capabilities as embodied in endpoint detection and response (EDR) with its heavy focus on protecting and detecting the endpoint. Alternatively, an extended detection and response (XDR) system that has access to "X" telemetry data such as the network, cloud, or messaging systems can be used in place of an EDR system.
- Integration of threat intelligence feeds to provide timely information into the MDR service. Multiple intelligence feeds from sources such as endpoints, dark web intelligence forums, open source and commercial service feeds, and vertically focused threat intelligence feeds are all critical. Having insight into not only what systems are being targeted but also who is doing the targeting allows for a better understanding of the tactics, techniques, and procedures (TTPs) that are vital in moving cybersecurity from a reactive stance to a proactive stance.
- Regular usage of human-led threat hunting based on risk analysis or integrated threat intelligence feeds, in addition to threats that are unearthed by indicators of compromise (IOCs) that are revealed as part of the regular MSS capabilities. The processes and playbooks that are created in the human-led threat hunting activities should also be included in the equally important automated threat hunting activity that occurs.
- Remote incident response (IR) services that can contain and remove incidents or breaches. IDC believes that the core part of the MDR service must go beyond providing guidance and recommendations by providing a component that can automate the response for the customer and, if necessary, provide an IR service (at an additional charge) for the more serious breaches that require a coordinated response, remediation, and forensic capability.
- Web-based consoles and dashboards that allow for the monitoring, updating, and reporting of all IOCs and/or tickets that are created from the service.
- The intellectual property that goes into the finished product represents the combined intellectual capital of the data scientists, cybersecurity practitioners, network engineers, threat hunters, governance and compliance experts, and engineers who provide all of the code that pulls together all of these systems into a deliverable service.

MSS is the around-the-clock remote administration and/or monitoring of IT security functions delivered by remote personnel at SOCs operated by a third party. Activities such as patch management, managed endpoint/antivirus, managed firewall/unified threat management (UTM), and managed security information and event management (SIEM) are performed on cloud and/or managed on-premises devices.

Threat hunting is the process of searching for malware or attackers on a network, whether in the cloud, on the edge, or in an on-premises location. Threat hunting is carried out by highly skilled professionals utilizing advanced tools and technologies, such as threat intelligence, machine learning, and behavioral analysis, to aid in the detection and eradication of the threat. There are two distinct types of threat hunting:

- Targeted threat hunting is when hunts occur around the high-value assets of an organization.
- Proactive threat hunting is driven by analysis based on an indicator of compromise or an indicator of attack (IOA) as a result of an alert, event, or intelligence source or around a hypothetical analysis of the tactics, techniques, and procedures of a likely adversary and then performing a hunt around a likely area of compromise. Managed services providers utilize IOC/IOA to develop a hypothesis and initiate searches for those indicators across all related customers.

Benefits: Offering a Complete Program

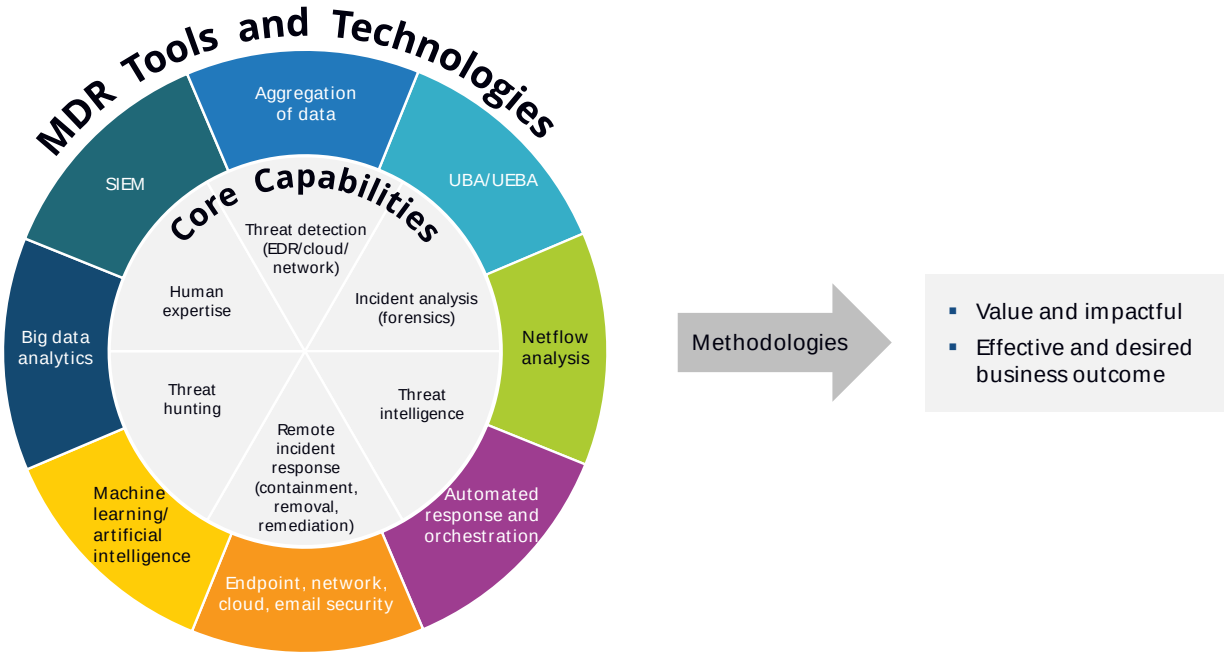
Prior to the introduction of MDR services, the tactics, strategies, and service capabilities that were used to defend against cyberattacks went through a couple of phases. Initial strategies focused on perimeter-based defenses. Firewalls, intrusion detection systems, and endpoint protection products were the focus of these early efforts to keep attackers out of the network.

As attacks continued to hit their intended marks, new services and capabilities were introduced to try and detect attacks. Recognition that classic endpoint protection systems, with their heavy reliance on blocking attacks based on hashed malware signatures, were insufficient to handle the "zero day" attacks led to the evolution of EDR as a mainstay of endpoint protection. SIEM systems were introduced, threat intelligence services with the capability of proactively detecting incoming attacks, and endpoint detection and response systems were deployed.

While these were all welcome advances, the flood of false positive tickets that these systems produce left understaffed security teams frustrated and demoralized. The perpetual shortage of cybersecurity professionals has led to a proliferation of incomplete or misconfigured security solutions. Frustrated C-suite executives and boards of directors complain that even though cybersecurity budgets increase, attackers still are often able to break through the patchwork of disparate systems to find their mark.

The arrival of MDR services has rectified many of the aforementioned issues and others. Arguably the best thing that has occurred has been the recognition that a robust cybersecurity program is not a binary choice of focusing on a perimeter-based defense or on a capability of detecting and responding to cyberattacks (see Figure 1). CISOs along with the C-suite and boards of directors are coming around to the notion that having a managed system that can protect, detect, and respond to launched attacks, in a timely manner, is not a luxury but a necessity.

FIGURE 1: ***An Effective Managed Detection and Response Service***



Source: IDC, 2020

If there is a silver lining to COVID-19, it would be the push for organizations to speed up their digital transformations.

The move to the cloud that digital transformation pushed has also led to an expansion of the risk surface that must be defended. Properly scoped MDR services can correlate the rich data that comes from these new surfaces, such as the public and private cloud, email, and edge devices, to detect and defend against cyberattacks.

The prioritized list of IOCs that require investigation allows cybersecurity professionals to focus their valuable time on the IOCs that require a human element. When focusing on the higher-priority IOCs, the advanced playbooks that MDR services deploy to their clients allow for a quicker containment and response capability than the manual processes that MSS and other point products rely on. Having a practiced playbook response to any compromise is crucial in preventing breaches from becoming headline-producing news items.

Key Trends

IDC launched a survey in 2020 asking IT and cybersecurity leaders in the United States about the most important features they wanted in an MDR service. Not surprisingly, two of the top three requests were tied to the keyword "integration." Integration of threat intelligence, the second most requested feature, is a recognition of the key role that threat intelligence plays in key areas of a full-featured cybersecurity program.

Having "over the horizon" visibility into attacks that are yet to be launched gives the good guys defending the turf of their respective organizations an opportunity to take proactive measures. Being able to identify what key cloud or on-premises systems are potentially vulnerable and need patching or other network measures taken to protect them is critical. A robust threat intelligence system that feeds and is fed information around the tactics, techniques, and procedures of cybercriminals allows MDR services to know when and how to respond to any attacks that have broken through the perimeter.

Having seasoned professionals behind the proverbial wheel of these integrated threat intelligence services is invaluable. After a threat has been contained and removed, the automated threat hunting that is launched to look for other incursions is augmented by these seasoned security professionals and their intimate knowledge of their clients' systems.

Considering Cisco

The recent rollout of Cisco's partner-sold MDR service continues a legacy of excellence by providing a robust MSS offering that is powered by a strong suite of security solutions. Cisco's transformation from being a trusted network partner to being the provider that can secure the networks that Cisco and its channel partners are so familiar with provides CISOs with a strong partner that can help them elevate their cybersecurity posture. Customers benefit from working with a channel partner that is backed by Cisco's security and network capabilities because they retain the local channel partner that can focus on the unique challenges their clients are facing in these rapidly changing times.

Cisco's leveraging of the Talos threat intelligence, combined with automated response capabilities, speeds up the time it takes to respond to threats.

The backbone of Cisco's security offerings is the research, threat intelligence, and thought leadership that the company's Talos organization provides. Perhaps one of the biggest needs for organizations that are looking to mature their cybersecurity platform is the ability to move toward a proactive security posture. Having a robust threat intelligence team that can access the telemetry across a diverse set of worldwide clients, and then proactively have the capability to act on a customer's behalf, is revolutionary for a firm's cybersecurity posture. Cisco's MDR service has access to this rich intelligence, and can bring to bear a set of automated playbooks, to rapidly apply the defensive measures that clients need to ward off the advanced attack methods that are in play today. Cisco's leveraging of the Talos threat intelligence, combined with automated response capabilities, speeds up the time it takes to respond to threats.

Cisco's MDR service doesn't utilize just the robust Talos intelligence in its offering. Other key components of the company's integrated cloud security architecture are seamlessly integrated into its platform, which allows for a more standardized offering. Clients don't have to worry about supporting legacy security software that does not provide the following capabilities that Cisco's platform offers:

- **Cisco Stealthwatch Cloud** is designed to provide the network visibility so crucial in today's cloud-centric architecture and work-from-home reality. Combining the threat intelligence from Talos with the behavioral modeling that Stealthwatch Cloud has with its baseline monitoring allows deviations from normal behavior to be detected and appropriate action to be taken on remote endpoints regardless of where they are located. Data exfiltration, a major concern of organizations with a highly distributed workforce like there is in the COVID-19 era, can be detected by peaks in network bandwidth, and appropriate action can then be taken.
- **Cisco AMP for Endpoints** provides the endpoint protection platform (EPP) and advanced endpoint detection and response capabilities to block known threats utilizing machine learning, file reputation, and other advanced techniques. In responding to suspected attacks, the endpoint isolation and containment features help prevent incidents from turning into headline-producing breaches.
- **Cisco Umbrella** is a proactive service that provides the visibility across all devices, ports, and cloud services to detect, protect, and block suspicious activity from entering the network. For example, phishing attacks with COVID-19 themed messages that have proliferated during the pandemic are blocked. Risky domains, as identified in conjunction with the threat intelligence capabilities of Talos, have their traffic tagged for deeper inspections. Meanwhile, roaming users also gain from the protection when they are off the corporate or organizational network.
- **Cisco Threat Grid** provides the sandbox and malware analysis that is crucial for determining what malware is doing or attempting to do. Uncovering the capabilities by forensically analyzing the malware provides critical intelligence to more rapidly contain an attack that has successfully landed. Uncovering the tactics, techniques, and capabilities of the cybercriminal allows for proper responses such as targeted patching, DNS blocking, and threat hunting similar artifacts for other relevant clients of Cisco's MDR service.

As previously noted, MDR has detection and response components to support the full life-cycle service. The response piece is an important component because some service providers fail to finish the loop and just advise their clients of attacks that have broken through and found their destination. Cisco's MDR service provides a battle-hardened response capability to respond to the cybercriminal. The automated playbooks used to respond to attackers are a key core component of the MDR service. Minutes, and with some attacks even seconds, can be the difference between engaging an attack that has just landed versus an attack where the attacker is able to make lateral movements and start to engage in evil tactics. Having refined, practiced playbooks at the ready to use to quickly contain and remove the malware is extremely important.

Another key component of MDR services is having an emergency IR capability to tackle true breaches that require advanced response, forensics, and remediation capabilities. Cisco once again differentiates itself with an optional 40-hour Talos IR capability that can be included in its offering to provide peace of mind for those times when a full-scale IR capability needs to be put into play to triage, investigate, contain, and remediate a potential breach incident. The ability to properly respond to and clean up serious incidents is important because any misstep can slow down a response or lead to increased fines for not following the prescribed actions necessary for the associated country or industry-specific regulatory body.

Challenges

Cisco's MDR benefits from its roots in other parts of the Cisco security platform. Integrating the MDR service into the recent SecureX platform, with its single-pane-of-glass concept and Duo-powered single sign-on, should be a very high priority for Cisco to consider as it competes against a growing set of managed security service providers and other security providers that are trying to provide their own offerings.

In addition, expanding the language capabilities beyond English will be critical to accelerating the rollout of the service beyond its initial U.S. deployment.

Conclusion

The increasing number of cybersecurity service companies that are offering their own MDR services is a testimony to the recognition that cyberattacks are becoming advanced enough that prior attempts to prevent and respond in a timely manner have fallen short. Utilization of disparate, disconnected systems from a growing number of cybersecurity solution providers is not making organizations any safer, nor has it been speeding up key metrics that measure how quickly organizations are detecting and responding to attacks.

IDC recognizes that security service providers that have a prescriptive approach to responding to attacks on behalf of their clients will emerge as leaders in the increasingly competitive pool of providers that are offering MDR services. Having a recognized security leader such as Cisco as a security service partner is a game changer for organizations that are seeking to take their cybersecurity programs to a higher maturity level.

About the Analyst

Craig Robinson, *Program Director, Security Services*

Craig Robinson is a Program Director within IDC's Security Services research practice, focusing on professional security services, consulting, and integration. Coverage areas include IoT security, blockchain services, and managed detection and response services.

MESSAGE FROM THE SPONSOR

Cisco Managed Detection and Response service

Today, organizations are experiencing a higher risk of breach than ever before. The inability to recruit and retain security expertise exacerbates the problem of keeping pace with current threats and a rapidly expanding attack surface.

Minimizing the impact of a breach is largely a function of reducing the mean time to detection. Without a focused detection capability providing visibility, breaches can go undetected for months. Cisco Managed Detection and Response (MDR) protects your most critical assets and shields your organization from the high costs of a security breach by reducing mean time to detect and contain threats, from months to hours. We combine an elite team of security experts leveraging threat intelligence, defined investigation, and automated response playbooks supported by Cisco Talos threat research to deliver relevant, meaningful prioritized response actions.

To learn how Cisco MDR can advance your security operations capabilities, visit: ***www.cisco.com/go/mdr***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com