IDC ANALYZE THE FUTURE

IDC ANALYST CONNECTION

Sponsored by: Secureworks

In today's always-on, hyperconnected business world, the cybersecurity provided by managed detection and response services has become increasingly important.

Making the Most of Managed Detection and Response

August 2019

Questions posed by: Secureworks

Answers by: Martha Vazquez, Senior Research Analyst, Infrastructure Services

Q. What exactly is managed detection and response?

A. IDC defines managed detection and response (MDR) as a continuous and proactive security and threat monitoring, detection, incident analysis, and response service that correlates specific threat intelligence and telemetry collected from the client's environment. MDR utilizes vendor-supplied technologies that work in a coordinated fashion with all aspects of the solution, such as endpoint detection and response (EDR), as well as network and threat intelligence to facilitate effective outcomes. MDR services monitor activity and apply advanced analytics on endpoints, user activity, the application layer, and at the network perimeter, as well as traffic moving laterally within an enterprise network. MDR monitoring — especially application and user supervision — can also be extended into cloud environments.

The core technologies and tools used in MDR services include advanced detection and analytics techniques such as machine learning, behavior analytics, big data analytics, NetFlow analysis, deception and threat intelligence, and ongoing threat hunting to identify known and unknown threats. Other key components in MDR services are automation, orchestration services, and automated containment. The combination of technology, human expertise, and specific methodologies allows MDR providers to move from reactive to proactive threat detection, which enables faster time to remediation. MDR services generate highly effective output on security situations with recommendations, guidance, and intelligence that help clients stay secure.

When implementing MDR solutions, organizations should keep in mind that MDR doesn't necessarily require a "rip and replace" of current core cybersecurity tools and platforms. Implementing an MDR service may involve just adding new tools or replacing a few of the current tools an organization possesses, in conjunction with the integration, orchestration, and automation of the response and remediate functions required for a true MDR solution.

Q. What's driving the need for organizations to look for a provider that offers MDR capabilities?

A. Organizations are undergoing technology changes heavily influenced by digital transformation (DX). This means that IT infrastructures are becoming more complex, with a mix of on-premises, cloud, and multicloud locations. In a recent IDC survey, 70.7% of respondents said they currently use managed services for infrastructure as a service (private or public), and an additional 22% will begin using managed services for infrastructure-as-a-service clouds (private or public) for the first time within the next 12–24 months.

As hybrid networks become ubiquitous, security is even more crucial because the attack surface grows, leaving more areas of the network exposed to threats and attacks. Gone are the days of securing only the perimeter, as the actual existence of a perimeter is fading away. As a result, organizations need to ensure highly distributed applications and data are secure, regardless of where they are located.

Gone are the days of securing only the perimeter, as the existence of an actual perimeter is fading away.

Organizations now need to take a more proactive versus reactive stance in securing their IT environments. Today, it's much harder to stay safe as attacks grow more complex and sophisticated. IDC's research has unearthed several reasons why organizations are either implementing or looking to implement MDR services, including:

- The struggle to keep up with the sophistication of threats
- The lack of 24 x 7 support, security talent, and in-house expertise
- The need to adopt emerging technologies such as artificial intelligence (AI)

As threats become more complex, organizations know they must adopt emerging technologies that go beyond just prevention and offer detection and response capabilities to rapidly lower response times to remediate security incidents and/or provide recommendations and guidance.

With legacy technologies failing to keep up with today's threat environment, organizations need help with protecting themselves from threats and responding to them more quickly and efficiently. The lack of adequate processes and tools and skilled people are hindering the effectiveness of security teams.

Q. Are MDR services available for small to midsize organizations or only for larger enterprises?

A. Historically, advanced solutions offered by MDR vendors were thought to be attractive to both large and commercial enterprises. This thinking persists, as reflected in a recent IDC security survey that showed 41% of large enterprises (5,000+ employees) choosing to outsource advanced detection techniques and services to third-party providers. With the

vast amounts of telemetry entering the network, it has become increasingly important for organizations to utilize these advanced offerings to assist in detecting threats faster and responding quickly and effectively.

As IT environments mature that MDR offerings serve, there is an increasing opportunity to push advanced capabilities down to midsize (500–4,999 employees) enterprises or organizations that have fewer internal Security Operation Center (SOC) capabilities and that lack a 24X7 staff to manage complex detection tools.

Demand for MDR services is also being driven by ever-increasing regulations that require more robust cybersecurity capabilities, regardless of the company's size. For example, even smaller organizations that deal with personal health information (PHI) as "covered entities" must adhere to HIPAA regulations. However, firms that do business in New York, for example, must hit certain financial milestones before the clock starts ticking on their requirement to implement more robust security capabilities.

Anyone who has been battling cybercrime in the dark recesses of the internet will tell you that cybercriminals are like any other criminal. They will seek the path of least resistance when trying to breach security measures. If that path leads them to target smaller size organizations, then that is where they will go.

Q. What do you recommend for enterprises that have a security team onsite but still need help analyzing advanced threats and providing rapid response?

A. Onsite security teams in larger organizations are common, but too often they lack the expertise or the people to keep up with the evolving threats in a 24 x 7 x 365 business environment. Organizations that have a security operations (SecOps) team onsite may typically have invested in traditional security tools such as firewalls, intrusion detection system/intrusion protection systems (IDS/IPS), and other systems that are part of an early-stage security maturity cycle.

As the SecOps team grows, so will the security program. As the program grows, adding more advanced detection and response methods becomes inevitable because frequently understaffed teams must pick up the skills and competencies needed to maintain legacy platforms while configuring and installing emerging technologies used by new security platforms. Doing all this work while still triaging and researching a growing number of tickets in the queue is daunting.

As the SecOps team grows, so will the security program. As the program grows, adding more advanced detection and response methods becomes inevitable.

An organization that decides to outsource part of its security program should consider several factors:

- Review the skills and expertise of the SecOps team and how an MDR provider can partner with them. It's important that the skills, the expertise, and even the cultural makeup of the team match the needs and requirements of the enterprise.

- Review internal incident response plans and processes and overall security maturity. Make sure that there is a communication plan in place for how the SecOps team will interact during an incident, as well as playbooks that match the requirements of the organization.
- Evaluate that the MDR partner is filling in the gaps for the SecOps team for any of the MDR functions that the organization is currently lacking.
- Check that the MDR provider's tools should be able to integrate into existing technologies, which can help provide that all-important single-pane-of-glass visibility for viewing the complete detection and response management life cycle.

Q. What should an organization look for when choosing an MDR provider?

A. IDC research within the cybersecurity market reveals that organizations should look for the following crucial characteristics in an MDR provider. These include:

- The ability to provide an advanced 24 x 7 SOC with the expertise to support and offer incident response capabilities. Expertise and reputation are important when selecting a vendor. Look for a vendor that is consistently involved in ongoing training, hiring, and retainment of top talent.
- The MDR provider should be able to correlate security-related data from endpoint, network, cloud, and other business systems. Providing visibility across all security tools will decrease the time needed to detect threats and provide rapid response times.
- Providers should demonstrate in-depth experience with incident response engagements. In addition, threat intelligence should be built in and provide continuous updates on the latest threats.
- Finally, the provider should demonstrate strong innovation capabilities in its core platform and use emerging technologies, such as EDR and network tools, threat intelligence, telemetry, machine learning, AI, and threat hunting.

In addition, be sure to ask for and review references from companies like yours (i.e., similar size, similar industries. Reference calls should be made in confidentiality, with just the MDR provider and the client on the call. Ask tough, open-ended questions that look at the strengths and weaknesses of the MDR offering.

About the Analyst

Martha Vazquez, *Senior Research Analyst, Infrastructure Services*

Martha Gomez Vazquez is a Senior Research Analyst for IDC's Infrastructure Services research practice focusing on Security Services and Hardware & Software Support and Deployment. In this role, she is responsible for IDC's worldwide research and analysis on enterprise and service provider security consulting, integration, and managed services as well as hardware and software support and deployment needs.

MESSAGE FROM THE SPONSOR

Detailed threat intelligence is the foundation of the MDR process at Secureworks. Only with a thorough understanding of the potential threats you might face, can you quickly and accurately identify which events require a response. Building an in-depth knowledge of the threat requires historical data analytics taken from frontline global incident response engagements, and ongoing threat research. This experience builds a detailed picture of which threats target which industries, as well as the preferred tactics, techniques, and procedures of different threat actors. Armed with robust threat intelligence, leading MDR solutions will use software-driven [automated] detection capabilities to analyze security data and increase the speed and accuracy of detection and response.

Click here to learn more about Secureworks' software-driven Managed Detection and Response solution applies threat knowledge gained from over 20 years in security operations and over 1,000 incident response engagements per year.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com