IDC Identifies MDR as the Next Generation of Managed Security Services

FRAMINGHAM, Mass., June 23, 2020 – Protecting an organization's assets from cyberattacks remains an enormous challenge as the attackers' tactics and capabilities become more targeted and sophisticated. As organizations struggle to elevate their cybersecurity maturity level, managed detection and response (MDR) has emerged as one of the latest buzzwords in the security market. A new report from International Data Corporation (IDC) examines the role of MDR in the managed security services (MSS) market.

IDC defines managed security services (MSS) as the around-the-clock remote administration and/or monitoring of IT security functions delivered by remote personnel at security operations centers (SOCs) operated by a third party. As organizations have matured, so have the managed security service providers, moving from protection to detection by adding in more functionalities such as threat intelligence, security information and event management (SIEM) systems, incident response capabilities, and identity access management to raise the cybersecurity maturity levels for their clients.

And yet, chief information security officers (CISOs) have become increasingly frustrated at the number of attacks that have found their mark despite all the new capabilities that have been placed in the proverbial cybersecurity toolbelt. Armed with the knowledge that some attacks will inevitably make their way into an organizations' infrastructure, CISOs are coming around to the realization that having a proactive rapid response solution is just as important as having a strong defensive perimeter.

Enter MDR, a subset of managed security services (MSS) that encompasses the outsourcing of advanced security functions and utilizes a highly skilled and dedicated security team that delivers 24x7 monitoring, analysis, and rapid response to sophisticated attacks. MDR combines all 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 clients' existing capabilities, along with the cybersecurity partner-supplied tools or services, and private intellectual property. MDR services are supplied by a provider's well-trained cybersecurity staff in a 24x7x365 remote SOC.

"In the past 5–10 years, we have seen managed security services evolve in providing better detection and response capabilities. MDR represents the latest attempt by managed security service providers to give organizations a fighting chance in their quest to protect the valuable assets that they are mandated to protect. CISOs need to make sure that they utilize an MDR provider that is equipped with the latest tools, technologies, and trained personnel that their clients need to fulfill their critical mission," said Martha Vazquez, senior research analyst, Security Services.

The core capabilities a MDR service must provide at the minimum include: extended detection and response (EDR/ XDR) for endpoint/network, cloud, or messaging systems; integrated threat intelligence; regular use of human-led threat hunting; remote incident response; and the intellectual property (IP) of the methodology and procedures needed to pull these systems into a deliverable service. But the most important capabilities, as identified by CISOs in an IDC survey, are 24x7 monitoring and classification of alerts, integration of threat intelligence, and integration with existing security technologies.

"The variety of companies that are offering MDR services is substantial. While security services have grown, one thing for sure is that the breadth of services available makes it a win-win situation for customers," said C raig Robinson, program director, Security Services. "Every organization operates at a different maturity cycle in its security program, so the buyer should look at a provider to include the components that will inevitably help them achieve their long-term security program goals."

The IDC report, MDR: The Next Generation of Managed Security Services (IDC #US46427920), looks at how managed security services evolved to the advanced offering that MDR represents to the market. MDR pulls together the people, processes, and key technology functions into a cohesive service that enables CISOs to elevate their cybersecurity maturity level. Evaluating the varied MDR offerings in the market requires an understanding of the key plumbing that managed security service providers have invested in to provide a credible MDR offering to a market that sorely needs the advanced capabilities that make up an MDR service.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading tech media, data and marketing services company. To learn more about IDC, please visit www.idc.com. Follow IDC on Twitter at @IDC and LinkedIn. Subscribe to the IDC Blog for industry news and insights: http://bit.ly/IDCBlog_Subscribe.

For more information contact:

Michael Shirer
press@idc.com
508-935-4200
Martha Vazquez
mgvazquez@idc.com
210-913-2101