digital hands®

Force Multiply Your Cybersecurity Team With MDR

Learn how MDR can force multiply your team, boost your detection times and help you orchestrate a ruthless response to cyber threats.

Introduction

In a hostile, rapidly-evolving threat landscape, being able to quickly detect cyber threats and effectively remediate them has become all-important. It's predicted that one trillion dollars in losses are associated with cybercrime in 2020 globally[1] and that figure is expected to be even higher in 2021.

With so many businesses suffering from cyberattacks, your business needs the capability to quickly detect and immediately respond to cyberattacks. This is where a managed detection and response (MDR) service plays its part in dramatically improving cyber defenses and hardening your overall cybersecurity posture.

MDR is an advanced detection and response service. It combines the latest cybersecurity technologies (SOAR & SIEM), a dedicated team of experienced cybersecurity threat analysts, and the threat intelligence organizations need to thwart advanced threat actors and malicious insiders capable of bypassing traditional cybersecurity measures.

MDR is not just about technology. A robust MDR service will stand out thanks to the human element behind it. MDR requires seasoned and skillful analysts with specific threat-hunting and incident response domain expertise, as well as tenured resources to regularly update detection rules. These first responders are the ones who will come to your aid when the worst-case scenario occurs and a cyber attacker penetrates your defenses.

In this white paper, we explore how a managed detection and response service can yield positive outcomes in detecting advanced persistent and insider threats and responding to them before they erupt into a full-blown security incident.

WHAT SECURITY CHALLENGES DOES MDR ADDRESS?

AN EXPANDING ATTACK SURFACE

An increasing number of devices and endpoints, changes to IT infrastructure, new technologies, a growing remote workforce and the increasing use of big data. For most businesses, however, their security posture remains stagnant while the threat landscape continuously evolves. Adoption of new technologies may bring cost and productivity benefits, but they also broaden the surface through which organized cybercriminals can get inside your business.

The job of managing both your legacy systems and new technologies can complicate your efforts and inadvertently help cybercriminals crack into your IT infrastructure. You need to secure all endpoints and systems, but your attackers only need to find one vulnerability to successfully attack you, tilting the scales in their favor.

CYBERCRIMINALS ARE GETTING SMARTER

Over the last ten years, we have seen the tools, techniques and procedures (TTP) cybercriminals utilize become significantly more sophisticated. These tools are also more widely available to would-be attackers, either through the dark web or hacker communities, and traditional cybersecurity defenses can’t keep up.

Despite providing you with a base level of security, traditional cybersecurity tools like firewalls and anti-virus are preventative in nature and ineffective at blocking advanced persistent threats and malicious insiders. Attackers can exploit unknown vulnerabilities to get inside your business and this trend is only set to escalate everyday

ROBUST IN-HOUSE CYBERSECURITY IS EXPENSIVE & HIGH-MAINTENANCE

Defending your IT infrastructure against a rapidly-evolving threat landscape requires cybersecurity technologies that help prevent attacks and give visibility into malicious activity across your entire IT infrastructure.

Buying all of this technology requires a large CAPEX, and with so many different technology solutions on the market, choosing the best can quickly become a major research exercise. You must also consider that some of these technologies rapidly become obsolete. Not to mention, deploying, managing, and monitoring these cybersecurity technologies can be both time and resource-intensive and require experienced cybersecurity professionals. Modern cybersecurity technologies generate an enormous volume of alerts that each need to be investigated.

COMPLIANCE REGULATIONS ARE BECOMING MORE DEMANDING AND COMPLEX

The increasing need for data security means that compliance regulators are bearing down on businesses that fail to implement effective cybersecurity measures. The HIPAA, SOX, GDPR and NIST are good examples of regulations and frameworks that aim to improve the way those businesses who fall beneath its remit handle data, report attacks, and deal with cyber breaches.

Other industries are increasingly introducing more stringent standards and regulations governing cybersecurity, too. For example, Society for Worldwide Interbank Financial Telecommunications' (SWIFT) Customer Security Program and the Directive on Security of Network and Information Systems both seek to impose regulations on businesses handling sensitive customer data.

CLOSES THE CYBERSECURITY TALENT GAP

There is a global shortage of good cybersecurity talent and recent research from the Information Systems Security Association (ISSA) indicates that the situation is getting worse, with more than 70% [2] of cybersecurity professionals claiming that their organization has been impacted by the shortage. This skills shortage means that it can be both difficult and expensive for your business to find and hire the experienced cybersecurity professionals that you need. Retaining any cyber talent is challenging as they are so in demand they receive enticing competitive job offers. To further compound matters, cybersecurity teams are being overwhelmed by the sheer number of alerts and security events that they have to wade through in order to identify the alerts that count and detect the real threats which could cause damage.

ISSA research finds

70%

of organizations surveyed are affected by the lack of strong cybersecurity talent.

Given this shortage, leveraging your existing IT team to handle your cybersecurity may seem like a good idea, but IT and cybersecurity are

two separate functions with competing priorities. Acquiring a level of maturity in your cybersecurity efforts can only be accomplished with properly qualified and experienced cybersecurity professionals - people who know how cybercriminals operate and the various techniques they use. Only they know how to defend your business against modern cybersecurity threats and are able to improve their skills, your IT team is simply not up to the task, especially if they are expected to retain their traditional duties.

BUILDING THE CAPABILITIES INTERNALLY ISN'T EASY

Building a threat detection and response capability within your own organization can be incredibly hard to accomplish, especially if you want it to operate 24x7x365. Plus, it can consume a huge portion of your overall information technology budget.

Many organizations lack qualified employees working 24/7/365 and a cybersecurity operations center (SOC) with the right technologies deployed. Building out internal threat detection and incident response capabilities is simply unrealistic for most businesses.

TESTING CYBERSECURITY TECHNOLOGIES

Good MDR providers continuously test and review the latest cybersecurity technologies, putting them to work in the real world and ensuring they have the best technology to manage the workflows at hand. When you hire an MDR provider, they bring these technologies and their capabilities to work in your environments, handling deployment, configuration, and management.

They also integrate them into other tools so that their SOAR, SIEM, IDS/IPS, endpoint protection, behavioral monitoring, and analytics tools all work together. To try and replicate this kind of technological innovation and effort within your own organization is next to impossible unless you are a very large enterprise with a diverse user base that comes close to an MDR provider's customer footprint.

> *Security leaders are increasingly cognizant that reducing the time to detect a threat is meaningless without a corresponding reduction in the time to respond to a threat to enable a return to a known good state.*

Source: Gartner [4]

HOW MDR SERVICES AUGMENT YOUR SECURITY

Managed detection and response services have evolved to meet the cybersecurity challenges described above. MDR service providers supply their customers with a dedicated team of experienced cybersecurity analysts, the benefits of a mature SOC operation that can deliver the latest threat detection and response capabilities, and live threat intelligence data from around the globe. MDR providers give businesses the ability to leverage advanced cybersecurity defenses and hunt for cyber threats, plus incident response capability to remediate these threats.

By 2025,

50%

of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities."

Source: Gartner [4]

HUMAN LED INTELLIGENCE AND CAPABILITY

A good MDR service consists of highly trained professionals specializing in their own domains. Think threat analysts, security engineers, and experienced incident responders. They provide you with 24/7/365 infrastructure monitoring and proactive threat-hunting capabilities to quickly detect, isolate and remove threats.

These practitioners also bring the experience they gained from dealing with a large variety of incidents from across their entire customer base - something that can not be replaced internally.

PROCESS

An experienced MDR provider like Digital Hands has decades of experience dealing with the cybersecurity of many different kinds of customers. During this time, they develop and mature their processes and playbooks, putting an internal cybersecurity team's processes to shame.

We have the ability to share threat intelligence across hundreds of clients so when we see malicious activity or an attack with one client we can closely monitor other clients for similar activity or proactively block the indicators of compromise.

THREAT INTELLIGENCE & HUMAN ANALYSIS

Good MDR providers subscribe to a wide range of different threat intelligence feeds from a number of different global providers, government agencies and intelligence associations. They also leverage internal custom research and forensic data collected from other incidents to properly inform their defense actions, as well as develop custom rulesets that help detect previously unknown threats.

280
days

Average time to identify and contain a data breach

$1.0
million

Average savings from containing a breach in less than 200 days vs. more than 200 days

39%

Average share of data breach costs incurred more than a year after the data breach

Source[3]

The ability to detect unknown threats capable of bypassing traditional IT security (firewalls and AV software), as well as stop phishing, ransomware, and malware attacks is a hallmark of good threat intelligence. It's hard to compete with MDR providers on this.

PROACTIVE RESPONSE

Proven MDR providers deliver end to end response services and resources. Threat analysts receive alerts from their SOAR platform for any malicious activity on their network. From there analysts can launch the remediation process to identify threats before they get a foothold on your network, and utilize tested playbooks to mitigate the impact of a threat. Forensic investigations, which can be deployed remotely, are critical to determine exactly what happened so you can re-secure your business.

BEST PRACTICES FOR MDR OUTSOURCING

When it comes to making MDR outsourcing a success, deep collaboration between customer and provider matters. Without collaboration and communication, an MDR service cannot tailor their service and ease a business's pain points. You can never outsource the knowledge of your own business and industry, which is really what a good MDR provider needs to deliver an effective service. Work closely with them and communicate constantly.

Many organizations think that the best place to begin is a traditional combination of a SOC and a SIEM. This is no longer the case. A SIEM alone is not enough to achieve full visibility. Securing and monitoring networks and endpoints is vitally important. Good MDR solutions are increasingly cloud-native and contain good EDR (endpoint detection and response) and NDR (network detection and response capabilities) to deal with modern-day hybrid (cloud, onsite, and offsite) IT infrastructures.

Good MDR providers have matured their services to the point where their EDR and NDR capabilities form a strong foundation for their overall MDR service. They make sure that they are cloud-native and able to accommodate any number of cloud-based IaaS, PaaS, productivity, and communication services.

They explicitly model their services to match your unique environment and provide visibility across the entire service delivery and kill chain. They continuously look at ways they can improve upon this, too. It is by seeing the MDR provider's work that you can verify they are doing their job.

CONTACT DIGITAL HANDS

Digital Hands provides a fully-managed detection and response service. We go above and beyond to supply your organization with dedicated analysts and white-glove service. We integrate your environment with our own internal SOAR and SIEM tools, providing us with visibility and a huge amount of threat intelligence that we use to protect you and your users.

If you have questions or need a competent partner to help you manage your detection and response efforts, get in touch via (855) 511-5114 or info@digitalhands.com.

About Digital Hands:

Digital Hands is a trusted global cybersecurity leader continuously taking action to protect our customers' most valuable assets against relentless threats.

Digital Hands is proud to offer extensive security expertise and advanced monitoring and reporting capabilities. Our robust set of innovative cybersecurity services and solutions ensures your organization, customers and employees are defended against cybersecurity attacks and data breaches round the clock.

We are proactive in our response orchestration that includes in-depth analysis and business context. Digital Hands enables our customers to harden their security posture, outmatch bad actors and benefit from our complementary white glove service and excellence in delivery. Our industry – leading customer retention rate and Net Promoter Score of 94 reflects how we go above and beyond every day for our customers.

December 2020

CITATIONS

[1] https://www.csis.org/analysis/hidden-costs-cybercrime

[2] https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

[3] https://www.ibm.com/security/digital-assets/cost-data-breach-report

[4] https://www.gartner.com/doc/reprints?id=1-249ZX5YK&ct=200930&st=sb

digital hands®

(855) 511-5114
sales@digitalhands.com
www.digitalhands.com