IDC

In Cybersecurity Every Alert Matters

RESEARCH BY:

Craig Robinson
Program Director, Security Services, IDC

October 2021 | IDC Doc. #US48277521

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Situation Overview

A cybersecurity practitioner has one of the hardest jobs to tackle today. Constant vigilance is required because of the serious repercussions that could arise if a cyberattacker were to gain access to critical data. Consider a data lake that holds private medical data, an industrial control system that monitors the water temperature in a nuclear power plant, or a credit bureau that holds personal financial information; all present ripe targets for enterprising cybercriminals.

The attack vectors that cybersecurity professionals must monitor are many.

Among the challenges are:

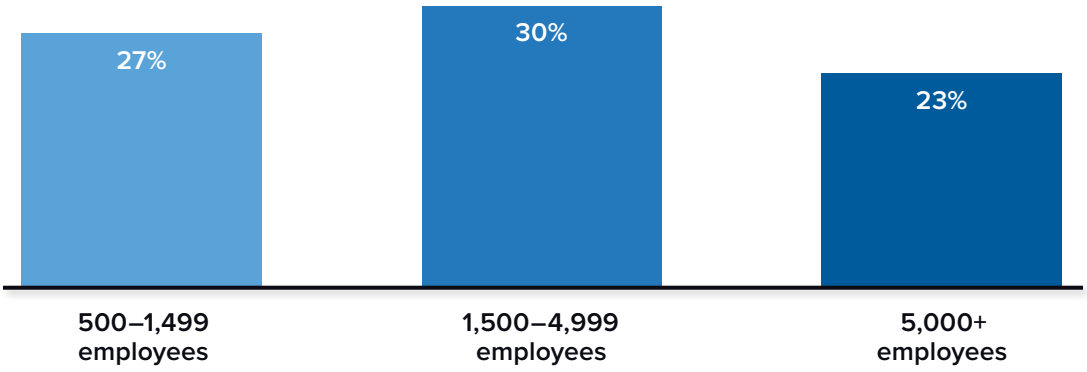
- **Third-party software** utilized to monitor and secure networks can be weaponized.
- **Distracted employees working outside the confines of an office** can fall prey to phishing emails.
- **Hybrid environments** mean that employees are not always working in monitored conditions behind a corporate firewall, making insider threats more difficult to detect.

Even the telemetry that must be monitored across the network, cloud, and endpoints has become more complicated and thus presents a challenge. Increased connectivity enabled by 5G has exponentially increased the Internet of things (IoT) and operational technology (OT) data that cybersecurity professionals must monitor. Line-of-business executives crave the data that has been made possible by the OT/IT convergence. But securing that data is an additional cost and an extra burden, as increased telemetry requires investigating the number of alerts that this at-risk data contains—and companies can't keep up with the alert volume (see **Figure 1**).

FIGURE 1

Firms of All Sizes Struggle with Investigating Alerts

Q. What percentage of alerts that your team receives are ignored or not investigated?
(% of alerts)



n = 310, Source: IDC's *U.S. Critical Start MSS MDR Performance Survey,* May 2021

IN THIS WHITE PAPER

IDC recently launched a survey that looks at some of challenges organizations are facing due to the heightened quantity and quality of threats. Key questions that were asked included how much time and effort organizations spend investigating and responding to alerts, what are the challenges organizations face in regard to security analyst talent, what operational security information is of interest to the board, and the increasing role of managed detection and response (MDR) services in helping companies respond to threats. Over 300 United States based respondents, director level or above, who utilize or plan to utilize MDR services were surveyed in this study.

A History of Solutions That Have Fallen Short

For many organizations, the capacity to ingest, correlate to, and respond to potential threats was difficult even before the mad dash to the cloud during the COVID-19 pandemic. Organizations have responded to the growing threats by adding evermore security tools while simultaneously struggling to fill the vacant seats in their security operations centers (SOCs).

Not surprisingly, organizations have turned to using managed security service providers (SPs) to try and bring some order to their short-staffed SOCs. The idea is that managed security SPs can take all of the tools sitting on the virtual shelf and configure those tools to do the job that they were created to do.

Some progress has been made, but the lack of a cohesive system to detect and respond to threats remains. Detections are up, but the tickets created to make sure these threats are investigated, contained, and remediated come at the cost of a large number of false positives that are triaged.

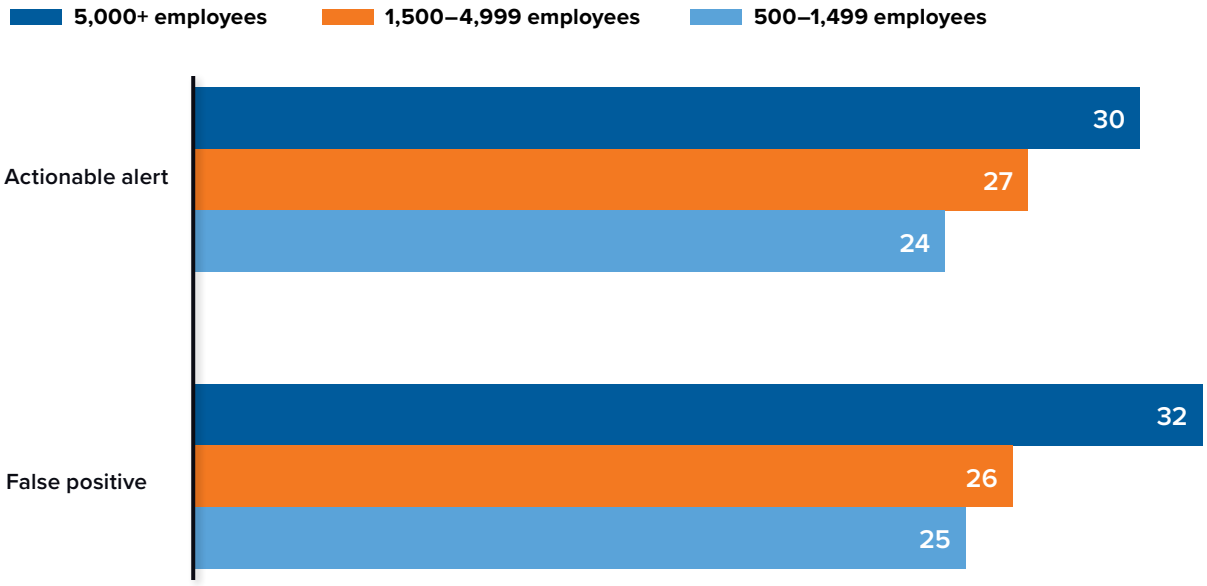
A well-trained and seasoned cybersecurity professional who can rapidly triage, contain, and eradicate threats—that rarity of rarities—does not enjoy wasting time on chasing ghosts. Yet this is the case when systems or managed security SPs fail to properly weed out false positives, as shown in **Figure 2** (next page).

Also as shown in **Figure 2**, larger companies take additional time to investigate all alerts. Even when organizations investigate detections that turned out to be real issues, the lack of automation that could be applied to any response action has allowed the cybercriminals to persist in environments far longer than they should be.

FIGURE 2

Time Required to Investigate False Positives and Actual Alerts

Q. How much time does it typically take for your team to investigate the following types of alerts?
(minutes required to investigate false positives and actual alerts)



n = 291
Base = respondents who indicated that their team receives more than 0% alerts that turn out to be false
Source: IDC's *U.S. Critical Start MSS MDR Performance Survey,* May 2021

This lack of productivity and the frustration with chasing false positives have been escalated to the top of the organizational chain of command. Chief information security officers (CISOs), CIOs, and others who are responsible for security must explain to the board and other members of the C-suite why they are experiencing high turnover and empty seats in their SOCs while ransomware and other high-profile exploits dominate news cycles.

Responding to the ever-growing number and sophistication of threats is onerous, yet organizations must deal with them. In addition, there are other areas that need attention from the security team:

- **The security department must recognize, reduce, and/or transfer risk** through the utilization of cyberinsurance.
- **SOCs must test their capability of thwarting a zero-day cyberattack** through the use of a red/blue/purple team exercise.
- **To raise awareness of management across the board, security teams should run** through ransomware tabletop exercises.

All of these activities take time. Proactively raising the cybersecurity maturity of a security team is next to impossible when the SOC lacks the resources to handle the day-to-day threat detection and response requirements.

Technology and security leaders have responded to escalating threats and subsequent timely detection and response requirements by implementing a variety of tools. Extended detection and response (XDR) was created to tackle the lack of automation capabilities and address the deficiencies that endpoint detection and response (EDR), security information and event management (SIEM), and other tools have in detecting threats away from the endpoint. To that end, XDR has shown some promise as a platform that can solve some of the previously mentioned pain points, yet it still lacks the human element that is a key piece to obtaining the full protection and detection that organizations are seeking. Cybersecurity practitioners cannot be trained overnight, and without the backing of a fully qualified staff to manage and utilize it, XDR will fall short.

XDR or any of the tools that CISOs are attempting to utilize without qualified analysts to manage and run them are not going to be up to the task.

Relying on tools that are not fully implemented or that do not have the proper visibility and automation to detect and respond to threats — combined with overwhelmed or insufficient staffing — is not acceptable to an organization's stakeholders.

Adding More Tools Is Not the Solution

The launch of managed detection and response services goes against the prior pattern of layering security tools with more security tools to try and match up against the cyber adversary's increasingly sophisticated attacks. Instead of layering more tools, a proper MDR offering complements an organization's technology stack with additional people, processes, and integrated technology to deliver tactical 24 x 7 monitoring, as well as investigation and response capabilities.

IDC defines MDR as an elevated part of managed security services that includes a response capability for when threats are detected within an organization. Response can mean different things to different organizations. Early versions of managed security service (MSS) that attempted to provide response often just provided guidance or advice to their clients, who were left to take the full response action on their own. When alerts were kicked off with a 2:00 a.m. notification from the managed security SP, it was up to the organization to do remote containment, eradication, and remediation. **Figure 3** (next page) illustrates how MDR has evolved to the point where providers are managing the entire alert life cycle.

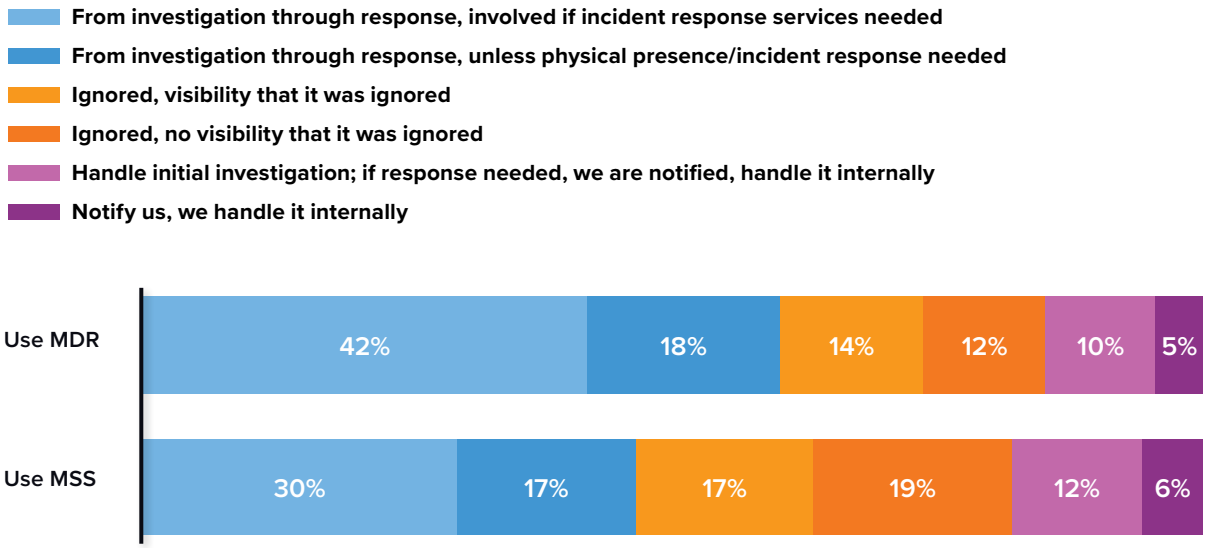
FIGURE 3

Complete Alert Life-Cycle Trends

Firms currently using MDR are more likely to have the MDR provider handle the complete alert life cycle than firms that utilize just MSS.

Q. How does your current MDR provider or managed security SP handle critical/high alerts?

(% of respondents)



Note: Numbers may not add to 100% due to rounding.
Source: IDC's *U.S. Critical Start MSS MDR Performance Survey,* May 2021

As shown in **Figure 3**, MDR providers are more likely to take the entire detection, containment, and response function all the way through to completion. As part of the process of onboarding a new organization to an MDR service, there should be a discussion between provider and client to identify the various threats and assets and establish an appropriate response. Given its 24 x 7 x 365 monitoring and response capabilities, the MDR provider is often in the best position to take certain response actions, and such responsibility should be authorized accordingly.

Another key benefit of utilizing an MDR service is the use of threat hunting. Reactive threat hunts are important. They are typically done when an MDR provider finds a compromised application in one customer's environment. The provider can then search all of their clients' environments for the same compromised application. A full-featured MDR provider will also rely on threat intelligence from multiple sources and apply that intelligence to similar clients by region or industry—or even to a specific client if that client has been targeted by name in any intelligence gathered. An MDR provider may also take a proactive approach by using threat intelligence to examine potential areas where attackers may be residing within a client's environment.

In the case of a zero-day exploit breaking through (and no system is 100% immune to a targeted attack), organizations should assess capabilities during a "break the glass" scenario, which calls for bringing in a highly skilled cybersecurity team to fully forensically investigate, eradicate, and remediate the damage. For these situations, MDR providers will often offer an incident response (IR) retainer (see **Figure 4**), which gives their clients the peace of mind of knowing that help with their situation (either in person or remote) is readily available. Utilizing an MDR provider that already knows a client's network topology is an added bonus, as it is not optimal for an incident response provider to show up for the first time during a crisis.

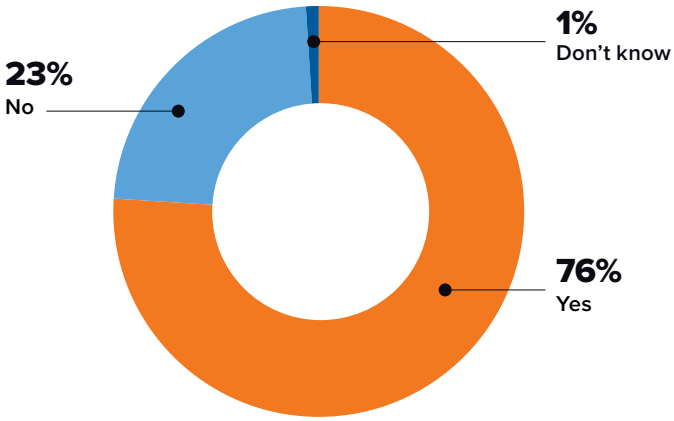
FIGURE 4

MDR Providers and Incident Response

Organizations that utilize an MDR service find that their provider offers an incident response retainer.

Q. Does your provider have an incident response retainer?

(% of respondents)



n = 310, Source: IDC's *U.S. Critical Start MSS MDR Performance Survey,* May 2021

As cybersecurity continues to become a critical agenda item for boards to review, the utilization of an incident response retainer will help elevate the stature and status of the CISO and security team.

Incident response demonstrates that an organization's security posture is migrating from a reactive to a proactive stance. In the event when no issues arise, the CFO and CEO will appreciate the cost certainty benefits of having an incident response retainer that can be utilized for proactive exercises, such as to see how well prepared an organization is for a ransomware attack.

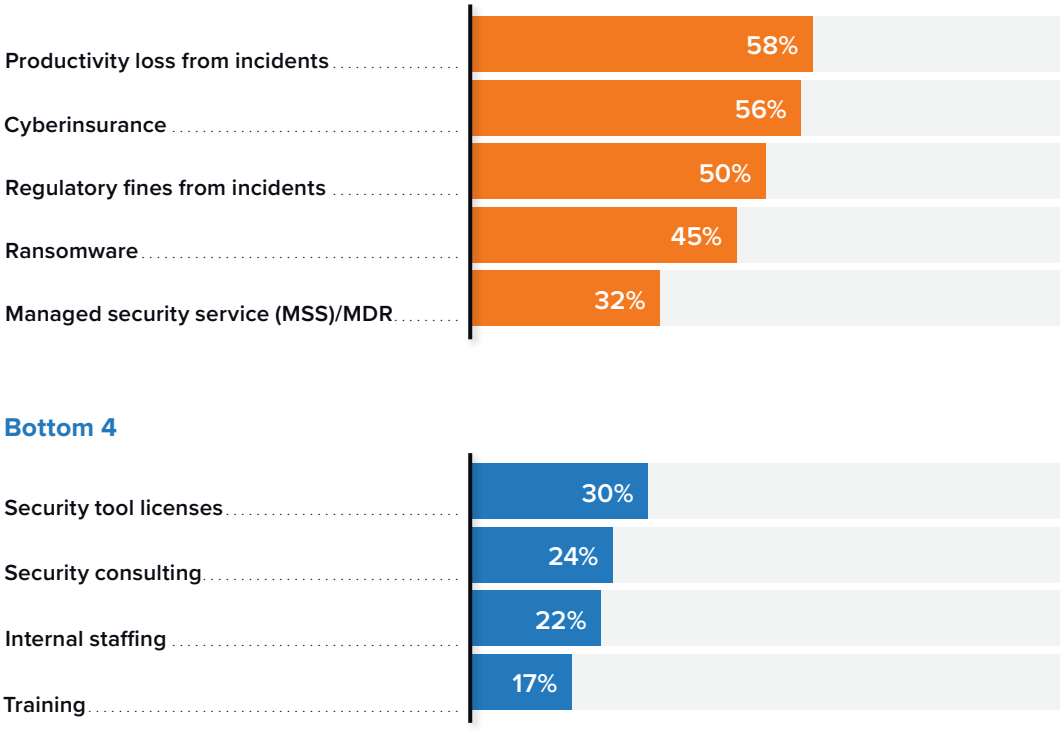
Elevating the cybersecurity maturity level of an organization will also change other items of interest in terms of cybersecurity and the board. The CIO or CISO can discuss how risk has been mitigated or reduced by utilizing an incident response retainer with their MDR provider. Specifically, boards want to know that their investments will pay dividends in reducing the costs of potential ransomware incidents and address concerns about lost productivity. Going through exercises, assessments, and simulations as part of utilizing an incident response retainer are proactive activities in that they help organizations prepare for future incidents (see **Figure 5**).

FIGURE 5

Lost Productivity and Cyberinsurance Dominate Board Issues

Q. What costs is the board most concerned with? Please select all that apply.

(% of respondents)



n = 310, Source: IDC's *U.S. Critical Start MSS MDR Performance Survey,* May 2021

Characteristics of a Well-Functioning Security Team

Utilizing a fully featured MDR service has its benefits.

The most important capabilities include the following:

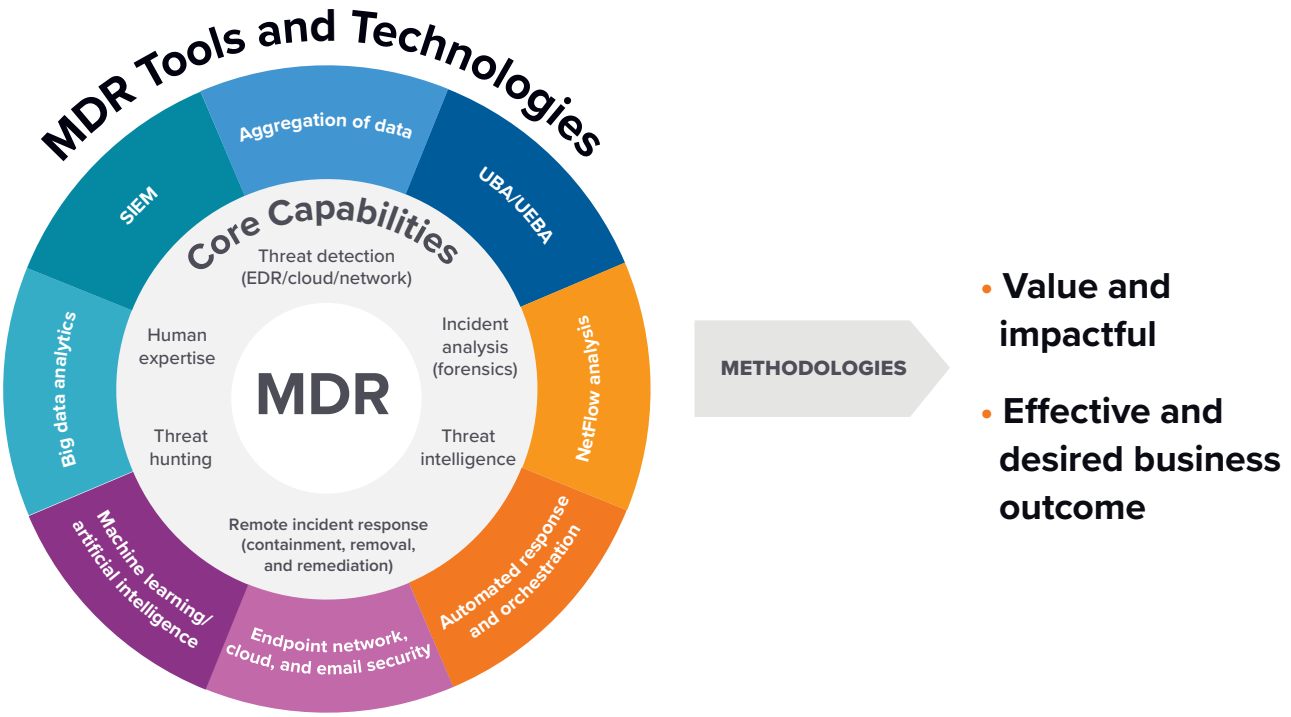
- **Alerts are fully triaged and investigated by seasoned cyber professionals** whose core focus is on detecting, stopping, and when necessary, responding to threats while using the latest technology.
- **Proactive incident readiness plans are able to be fully prepared, discussed, and practiced without the side disruption of detecting or responding to specific alerts**, such as from a laptop in sales or an IoT device in the warehouse. Instead, the MDR provider is able to take all appropriate actions on behalf of its customer.
- **Statistics, like mean time to detect (MTTD) or mean time to respond (MTTR), are readily discussed at board meetings,** without repercussions, because the trend line is toward reducing times.
- **Issues like risk reduction, governance, risk, and compliance (GRC), or third-party security concerns get the attention that they deserve** because the security, IT, and line-of-business teams can actually get together to work on these important matters without interruptions by the latest detected threat.

An MDR service is also beneficial for a CISO and the rest of the C-suite because it frees them to focus on the key business functions rather than chasing down alerts. With an MDR service, the "blocking and tackling" is handled by a team whose core purpose is to stop cybercriminals from entering a client's territory.

Success in the battle against cybercrime requires the capabilities illustrated in **Figure 6**. The core capabilities of an MDR service, such as human-led threat hunting and curated threat intelligence, is supplemented by core tools and technologies including automated response and orchestration, machine learning, artificial intelligence, and big data analytics.

FIGURE 6

An Effective MDR Solution



Source: IDC, May 2020

When an organization achieves its desired business outcomes such as fast response times and reduced risk, that is indicative of a successful cybersecurity stance.

Critical Start Solution

Critical Start provides a complete portfolio of threat detection and response capabilities that organizations can take advantage of to protect their on-premises, hybrid, and cloud environments and reduce and mitigate their risk exposure.

24 x 7 x 365 monitoring, detection, response, and remediation services are provided in response to alerts that are ingested and correlated from the organizations' Endpoint Detection and Response (EDR) / Endpoint Protection Platform (EPP), SIEM, or XDR platforms. Appropriate response capabilities are taken on behalf of the client based on previously agreed upon response plans.

Key metrics that are often reported to the board, such as mean time to detect and mean time to respond, are easier to report on as Critical Start offers service-level agreements (SLAs) with one hour or less time to detect (TTD) and median time to resolution.

The Zero Trust Analytics Platform (ZTAP) takes all of the alerts generated — regardless of source — and quickly identifies and resolves approximately 99% of the prior known-good alerts to a favorable outcome, according to Critical Start. The remaining alerts are then quickly investigated and responded to by expert security analysts.

During this whole process, customers can obtain 100% visibility to every action and every data point that is looked at by the Critical Start team. MOBILESOC—an appropriately named mobile application—goes beyond the notification and ticketing functions to allow users to perform response actions or communicate with the SOC to take the appropriate response action.

On the rare occasion that an alert gets elevated to the point that trained incident responders are required, Critical Start offers onsite and remote incident response capabilities, along with the digital forensics capabilities to fully investigate highly sensitive incidents.

Critical Start has made significant investments in the human capital that drives its offering. An example of this investment is in its Cyber Research Unit, which comprises detection engineering and cyber threat intelligence. The Cyber Threat Intelligence team curates original and third-party intelligence that the Detection Engineering team uses to develop new detections and input/output controls (IOCs). Critical Start's blue team defenders can leverage the knowledge and wisdom of the Detection Engineering and Cyber Threat Intelligence teams to gain insights into the tactics, techniques, and procedures (TTPs) that the cyber adversary is likely to use during an attack. The Cyber Research Unit also manages, maintains, and curates out-of-the-box detections and IOCs and maps detection content back to the MITRE ATT&CK Framework.

Skilled experts, like the blue teams that defend their clients' infrastructure, the red teams that test the infrastructure, or the experienced analysts in the SOC that manage the day-to-day security operations, have extensive training that is backed up by a variety of Microsoft certifications, along with relevant platform expertise on the SIEMs, EDR/EPP tools, and XDR platforms that their clients utilize.

Per Critical Start, the result is a service that ends up with only 0.1% of all alerts ever being escalated to the customer.

Challenges and Opportunities

Bringing the wide swath of technologies, services, and human capital that blends these assets — both human and machine — into a solution is not for the meek.

Critical Start brings a comprehensive offering of services that should give its clients confidence that they have a partner that can handle the critical security functions required to match up against the advanced cyberthreats that they face.

The challenge for Critical Start is similar to the one that its clients face. Finding and retaining cyber talent are just as important as the technology it utilizes to face off against cyberthreats. Critical Start will need to continue to invest in its security practitioners to offer career development opportunities to keep and attract the cyber talent that will help fuel its growing business.

CONCLUSION

There is a common statement that is repeated when it comes to the cyber teams that are tasked with defending their organizations: They need to be right 100% of the time, while their opponent needs to be right only once. As this phrase echoes over and over, it is not a stretch of the imagination in any way to start thinking about possible misses. Far too many security leaders have a hard time relaxing because they are never quite sure if their SOC team or the service provider that monitors and detects for threats will pick up every IOC that comes in.

Organizations that entrust Critical Start as their cybersecurity partner can gain some precious peace of mind. Peace that comes from knowing that *every* IOC is reviewed. Trust is gained because they get full visibility from the device of their choosing on the alerts that Critical Start is reviewing. Finally, they can gain some comfort that if a serious situation were ever to arise, they will not have to go to the back of the line because they have a working relationship with a full-featured incident response provider.

About the Analyst

Craig Robinson
Program Director, Security Services, IDC

Craig Robinson is a Program Director within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include IoT Security, Blockchain Services, Threat Detection and Response services. Craig delivers unparalleled insight and analysis, leveraging his unique experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research and guidance to vendors, service providers and clients worldwide.

More about Craig Robinson

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.