H.I.G. Capital Achieves Efficient Alert Triage and a Stronger Security Posture with CRITICAL**START®** MDR and Managed SIEM

H.I.G. Capital enhances SOC efficiency and reduces alert fatigue with Critical Start's MDR and Managed SIEM, achieving a stronger security posture.

CASE STUDY

AT A GLANCE

Industry: Venture Capital & Private Equity

Number of Employees: 1,000

CORE AGENDAS

Challenge
Incumbent MDR generated an overwhelming number of false positives, creating inefficiencies in escalations and hindered the team's ability to focus on genuine threats.

Solution
Critical Start's integration across the Microsoft Security ecosystem along with managed SIEM, and mobile monitoring eliminated alert fatigue and enhanced threat detection and response.

Results
Immediate improvements in alert quality, a significant reduction in false positives, and more efficient alert management, enabling the SOC team to focus on true security threats.

Background

H.I.G. Capital (**H.I.G.**), a prominent private equity firm, faced significant challenges with alert triage and prioritization in their Security Operations Center (**SOC**). Their incumbent MDR generated an overwhelming number of false positives, creating inefficiencies in escalations. They also lacked the ability to work with their MDR provider to flag known behaviors and tune their detection rules based on business context. They needed a solution that allowed their limited SOC team to rapidly respond to true positives in their technology environment that included both Microsoft and other platforms. To address these challenges, H.I.G. turned to Critical Start, a leading provider of Managed Detection and Response (**MDR**) services.

Challenges

The H.I.G. security team was overwhelmed by the quantity of alerts – and the lack of quality – being escalated by their existing MDR provider. They struggled to differentiate between false positives and genuine threats. Additionally, their MDR provider offered limited recourse to customize their detection rules based on business context. They needed a solution that closely aligned with their technology environment, including Microsoft and other platforms, for rapid and easy onboarding and accelerated time to value, and that could solve their challenges and inefficiencies quickly.

> **Critical Start escalates the tickets we need to look at. It helps reduce the noise on our end and allows the team to focus on other aspects of their roles on a day-to-day basis.**
>
> **- Sergio Fernandez, Cybersecurity Operations Supervisor**

Solution

H.I.G. selected Critical Start for their seamless integration with H.I.G.'s existing technology ecosystem, including 365 Defender, Defender for Endpoint, Sentinel, along with many other non-Microsoft technologies. Critical Start offered multiple compelling factors that all influenced H.I.G.'s decision, including their status as a Microsoft Managed XDR (**MXDR**) partner, the fact that they offered Managed SIEM, the MOBILE**SOC**® application for on-the-go monitoring, and the single pane of glass for alert management. H.I.G. also welcomed the added layer of contextualization that Critical Start brought to the table beyond Managed Detection and Response services, including the Trusted Behavior Register® (**TBR**®), which they saw as a powerful solution to eliminate alert fatigue.

The Critical Start team worked closely with H.I.G. to ensure a smooth deployment into their environment, providing valuable insights and recommendations to optimize their security operations. They realized improvements right from the start. Christian Diaz, Information Security Analyst of H.I.G. noted, "What I really like about this platform is the close integration with Microsoft Security products like Defender and Sentinel. We immediately noticed an improvement in alert quality and reduction of false positives."

Currently, H.I.G.'s SecOps team meets quarterly with Critical Start to perform a health check of their SIEM/SOAR implementation. They validate coverage and ensure that all expected controls are in place. H.I.G. is looking forward to fully turning on all the updated Asset Visibility features. Chief Information Security Officer, Marcos Marrero stated, "The team is working on turning on Asset Visibility to automate and accelerate the discovery of coverage gaps. We also plan to continue working directly with the Critical Start team. They provide valuable insights, especially when it comes to more complex changes that we need to better secure our environment."

> **The MobileSOC app is great for our on-watch hours. We can manage alerts on-the-go and take the same actions that we would if we were at our desks.**
>
> - Christian Diaz, Information Security Analyst

> **Critical Start is a breath of fresh air, doing what MDR what should have been done all along. They curate the list of events across the entire environment, cut through the noise, and provide actionable information. But there is more. Things like Asset Visibility, the TBR… the CORR platform is built for risk reduction. And the expert guidance we receive – not just with alerts and rules creation, but with maintaining a healthy SEIM/SOAR platform – has helped reduce organizational risk.**
>
> - Marcos Marrero, CISO

Outcomes

The deployment of Critical Start's MDR for Microsoft brought immediate improvements to H.I.G.'s SOC performance:

- **Improved SOC Efficiency:** With significantly improved alert quality, the SOC team can dedicate more time to genuine threats and concentrate on critical tasks and projects outside of alert management.
- **Mobile Monitoring:** The MobileSOC app provides on-the-go alert management, ensuring that alerts are addressed promptly, even outside office hours. They use the app to address alerts that were escalated, investigate alerts, and communicate with the on-call analysts at Critical Start.
- **Customization and Flexibility:** The ability to tailor Critical Start's MDR detection rules allows the H.I.G. team to better detect signals and respond to alerts in a way that aligns with their risk appetite. They create new rules directly, and they also rely on the Critical Start team to have more complex rules created when needed. These tailored alerts and rules of engagement are crucial for H.I.G.'s dynamic security environment.
- **Efficient Alert Management:** The H.I.G. team appreciates the ease of managing alerts within Critical Start's Cyber Operations Risk & Response™ platform (**CORR**™). They specifically like the TBR®, which auto-resolves false positive alerts and improves response times. This allows their team to prioritize actions while still having the capability to monitor all alerts, regardless of priority, so they can demonstrate their team's effectiveness.
- **Improved MDR Experience:** Apart from alerts, H.I.G. appreciates Critical Start's commitment to cyber risk reduction. They use the contextual information delivered through the CORR platform to detect anomalous behaviors and continually refine their rules. They rely on Critical Start's expert guidance and integrated features that allow them to continually tune their attack surface, harden their environment, and ultimately, reduce the risk of a breach.

> **Creating our own custom rules and then saying, 'hey, call us when this is detected.'... It's awesome. That communication piece and being notified of something that was picked up in our environment is a great thing.**
>
> **- Omar Burgos, Security Engineer**

Conclusion

Critical Start's MDR and Managed SIEM effectively addressed the H.I.G. SOC team's efficiency challenges by consolidating alerts and reducing the volume of false positives. The seamless integration with Microsoft and other tools, user-friendly interface, availability of mobile alert triage and threat containment, robust customization options, and human-driven MDR all made Critical Start the ideal partner for H.I.G.

The partnership between H.I.G. and Critical Start underscores the importance of choosing an MDR solution that goes beyond alert notification to manage and reduce risk across complex security environments. By reducing the flow of false positives and improving SOC efficiency, Critical Start enabled H.I.G. to focus on their core business operations with confidence while continually delivering demonstrable improvement in breach prevention and security threat containment.

> **Critical Start gives us reports that show us the volume of false positives that are filtered out. So, we get to use that data to tune our detection rules – but we're not chasing false positives. Instead, we're focusing on the alerts that matter.**
>
> - Christian Diaz, Information Security Analyst

For more information, contact us at:
https://www.criticalstart.com/contact/