SOLUTION BRIEF

Align Your Cybersecurity Spending with Business Outcomes

Managed Detection & Response Services

Quantifying value in cybersecurity spend is a challenge

Success in cybersecurity has historically meant no breaches, data theft, or business downtime. Quantifying value in today's is accomplished through using complex data models. Historically, this has proven difficult. If a security solution is performing optimally, useable data can be scarce. And without it, generating insight into key security metrics is tough as is justifying cybersecurity spend. **In fact, according to Gartner®, " While 88% of the corporate directors Gartner surveyed view cybersecurity as a business risk, 1 only 11% formally track its impact on business decisions through quantitative and qualitative metrics, and only 36% can provide the required level of transparency on security budgets to make them understandable to business units (BUs)."[1]**

This lack of metrics results in:

- Inability to demonstrate results, Return on Investment (**ROI**) and risk
- Difficulty articulating why cybersecurity budget requests should be prioritized versus competing IT budget items
- Challenges in creating a business case for new cybersecurity projects

Drive business decisions with key operational metrics

Even though cybersecurity is critical to your organization, investments in security tools and services aren't often treated as business decisions. The inability to measure security investments makes it challenging to quantify a security program's value to key stakeholders, because they may not understand the risk.

My board was unclear how our security program was performing in relation to business outcomes they understood. I didn't have the data I needed to clearly articulate my business case.

With CRITICAL**START**® *MDR services, I now have real-time, operational metrics that help me align cybersecurity spend to business outcomes. This helps me clearly justify cybersecurity investment requests.*

- CISO, TECHNOLOGY INDUSTRY

Our Approach

Our Managed Detection and Response (**MDR**) services give you meaningful operational metrics that help you tie your security program's results to business outcomes.

As a result, you'll have actionable insights to prioritize investments and gain executives' buy-in.

Our metrics not only report on traditional measurements, such as Median Time to Detection (**MTTD**) and Median Time to Respond (**MTTR**), but also our security operations center's (**SOC's**) performance. You'll always have 100% transparency into how we're performing against contractual service level agreements.

Figure 1: Use operational metrics to quantify efficiency and effectiveness.

[1]—Gartner® "Measure the Real Cost of Cybersecurity Protection" Published 30 March 2022 - ID G00764671 - 10 min read By Analyst(s): Stewart Buchanan, Paul Proctor, Bryan Hayes.

KEY SOLUTION BENEFITS

Give your executives the data they need

It's important to articulate how your cybersecurity spend influences business outcomes – from an executive's perspective. Our real-time dashboards help answer key questions such as, "What level of risk are we taking by not investing in cybersecurity in a specific area?" Our customer success teams partner with you to build an efficient solution that meets your expectations and delivers insights into the effectiveness of your security tools. Our MDR services are 100% transparent, enabling customers to track service level agreements.

Measure levels of detection and reduce risk

Demonstrating value in an investment into cybersecurity services is challenging enough without data justification. The Critical Start Zero Trust Analytics Platform™ **(ZTAP®)** helps users to produce detailed reports and build visibility into all service delivery metrics across your security toolchain, including MTTD and MTTR along with the equivalent operational costs. By measuring detection levels, you'll have a new level of visibility including understanding exactly how many events our MDR services have detected and the value they provide.

Improve efficiency of people and tools

A lack of meaningful metrics makes it challenging to simplify resource management, such as identifying appropriate staffing levels and pinpointing security tools' coverage gaps. Dashboards measure your security analysts' MTTR and track trends over time to help your team become more efficient. You can also benchmark their performance against other companies to assess if there's additional room for improvement.

Our MDR services integrate with your existing security tools so you can determine if there are coverage gaps that need to be addressed. As a result, your team has the data it needs so it can focus on real and emerging threats rather than an overwhelming number of false positives.

CRITICALSTART®

For more information about Critical Start services and solutions for Microsoft Security, schedule a demo at:
www.criticalstart.com/contact/request-a-demo/