CRITICALSTART®

SOLUTION BRIEF

Measure Key Operational Metrics to Continuously Improve Your Security Program

Managed Detection & Response Services

Do you have sufficient data to measure the performance of your security program?

Searching through a morass of data metrics to understand the performance of your security tools can be powerful. **Today's massive data lake repositories and security solutions are able to correlate from multiple sources, analyze and monitor quickly, and generate genuine alerts better than ever. Yet, a fundamental challenge continues to persist- organizations are unable to quantify the effectiveness of their cybersecurity programs**.

In the absence of key metrics, you can experience these challenges:

- **Actionable data** to understand your team's performance and practice effective resource management
- **Operational metrics** for improving alert detections, quantifying risk and identifying areas of improvement
- **Pressure to reduce time to detect and respond**
- **Difficulty articulating the value** of your cybersecurity program

With increasing pressure to detect and respond to threats, you need to deploy your resources effectively. CRITICAL**START**® Managed Detection and Response (MDR) services provide real-time information and data to make guided decisions on staffing coverage and investment requests.

Our Approach

Our Managed Detection and Response (**MDR**) services simplify resource management and help improve your team's efficiency and productivity.

By giving you visibility into critical operational metrics, such as each analyst's Median Time to Respond (**MTTR**), you'll have the data you need to make smart resource decisions.

The security experts at our 24x7x365 security operations center (**SOC**) also augment your team to provide complete coverage while preventing breaches.

> *It was a struggle to understand if my team needed additional resources. Without that data, we were running blind and potentially letting threats slip by.*
>
> *Now I have the metrics to make smart business decisions tied to threat activity, and I understand how my individual team members are performing.*
>
> **- DIRECTOR OF SECURITY OPERATIONS, RETAIL INDUSTRY**

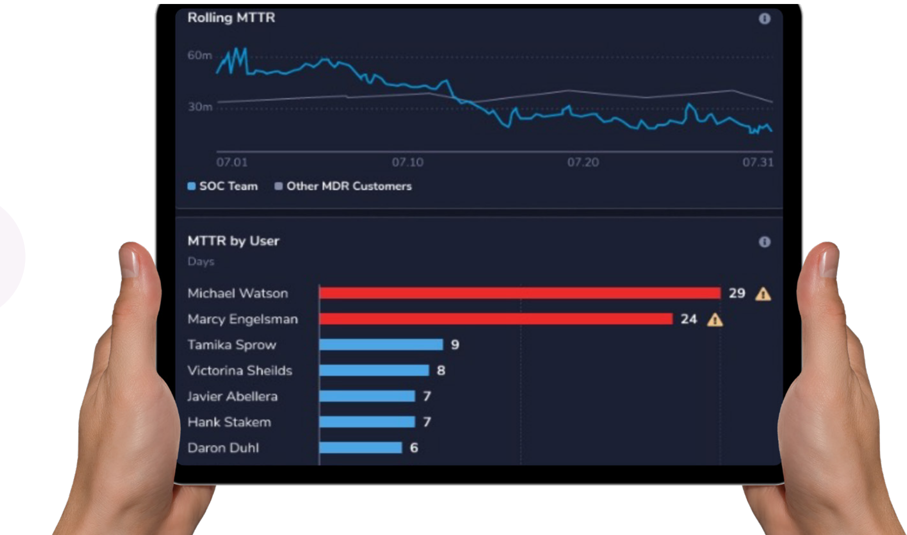

Figure 1: ZTAP displays MTTR by analyst. SOC managers can identify bottlenecks, allocate resources as needed, thereby reducing MTTR further.

KEY SOLUTION BENEFITS

Simplify resource management & justify investment requests

Resource management is critical since understaffing can result in threats slipping through. However, measuring your team's coverage in detecting and responding to potential attacks can be difficult if you don't have access to the right data.

Our Zero Trust Analytics Platform™ (**ZTAP®**) allows you to build the most efficient team possible. It correlates risk and operational metrics and builds performance benchmarks at a team and analyst levels. Management can use this data to trend past performance, forecast budget requests, and allocate resources where needed.

Inform decision-making

Leverage peer comparison insights and security controls' performance mapped to industry frameworks, such as the **MITRE ATT&CK® Framework**, to succinctly report on risk and set goals for security outcomes. As a result, you'll be in a better position to calibrate detection and response capabilities.

Improve your team's productivity and efficiency

By reducing the number of alerts required to initiate an investigation and reducing false positives rates, SOC teams can reduce workloads significantly. ZTAP's intuitive dashboards display all unresolved alerts by analyst, providing a granular view of each person's workload. Ability to compare workloads across teams is a powerful method of allocating resources, identifying underperformers and taking measures to improve.

With insight into key metrics, such as your team's performance compared against company defined MTTR, you'll have the ability to spot trends and business continuity . You'll have the required data to determine which team members require additional training or if escalation policies need to be updated.

If your team is struggling with a high workload and at risk for burnout, Critical Start SOC experts can balance your analysts' capacity via customized rules of engagement. We handle L1 and L2 triage so your employees can focus on higher level responsibilities.

CRITICALSTART®

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