3 Steps to Materializing the Power of Your Security Tools

CRITICALSTART®

Table Of Contents

Introduction

Unfortunately, multiple security tools don't prevent cyber attacks

As cyber threats grow, it's tempting to acquire more security tools to proactively prevent attacks. However, tool overload is a serious issue: security teams from big enterprises now have 76 tools to manage and those with 10,000 employees or more have, on average, 96 tools.[1]

Even with this massive number of security solutions in place, breaches are still occurring. Seventy-nine percent of enterprises have experienced cyber incidents that should have been prevented with current safeguards. **And nine out of 10 security leaders state that failure of an expected control is the primary cause of breaches.[2]**

Why do security tools fail to protect organizations?

For example:

- **Lack of integration** results in coverage gaps that attackers can exploit
- **Difficulty configuring and maintaining so many tools**–especially for short-handed security teams
- **Poor detection effectiveness** makes it difficult to identify true threats
- **Limited visibility** makes it challenging to monitor and improve detection coverage
- **Lack of outcome-based metrics** means it's challenging to make well-informed, risk-based decisions

Control failures and gaps are also a major source of frustration: the inability to continuously measure their enterprises' security posture and identify control failures is ranked first among senior cyber professionals' dissatisfaction.[3]

Integrating security controls with managed detection and response

This emphasis on outcomes can be tough to achieve without a Managed Detection and Response (**MDR**) service. CRITICAL**START**® MDR brings skilled security experts who will deeply understand your environment. We partner with you to detect, investigate and respond to threats specific to your organization.

The Zero-Trust Analytics Platform® (**ZTAP®**) integrates all your security tools and brings together risk and operational metrics that align with cybersecurity and business outcomes, all within a single management platform.

By integrating with multiple vendors' technologies, Critical Start MDR services consolidate visibility across security tools, so you have a clear picture of performance and your controls' coverage gaps. You'll have metrics you can trust and confidently share with executives and board members.

The three steps outlined in this eBook will help you realize the value of your security tools and get the most out of them.

According to a Gartner® report, "organizations must stop investing in security tools and start investing in outcomes…. CIOs must evolve the way they measure and report on security to reflect levels of protection for key business outcomes."[3]

[1] *2022 Security Leaders Peer Report, Panaseer*
[2] *2023 Security Leaders Peer Report, Panaseer*
[3] *Gartner® Use Value and Cost to Treat Cybersecurity as a Business Decision, Gartner, March 30, 2022*

3 Steps to Materializing the Power of Your Security Tools

- **Consolidate visibility across disparate security tools**
- **Measure performance while focusing on business outcomes**
- **Let the Critical Start security experts support your team**

Consolidate visibility across disparate security tools

View security performance across all your systems in real-time.

The bottom line is you don't need more security solutions to increase your effectiveness in detecting threats. Instead, it's important to make your existing tools work better together and preserve your investment in them.

If organizations had better insight into their security tools' performance, they would be in a better position to reduce risk, improve their team's efficiency, boost detection effectiveness and measure levels of detection to guide investments.

Our MDR services integrates with your existing security solutions to help monitor and improve detection coverage. As a result, you'll enhance operational efficiency and reduce risk. With this new level of visibility, you can measure controls' effectiveness and take action to address coverage gaps.

Real-time dashboards map alerts and threat detection to the industry standard **MITRE ATT&CK® Framework** to enforce, manage and maintain effective detection content. You'll can have your security tools' detection coverage mapped to this framework and use these metrics to identify gaps in your security tool set.

82% of security leaders agree that monitoring and addressing expected controls' failure and risk would have a bigger impact on their security posture than buying additional tools that provide more controls.[4]

[4] *52022 Security Leaders Peer Report, Panaseer.*

Measure performance while focusing on business outcomes

Get the data you need to reduce risk and drive security investments.

In the absence of outcome-based metrics, it's difficult to articulate your security program's value to guide future investments. With Critical Start MDR services, you'll no longer be in the dark when it comes to your security operation's performance.

Our MDR service brings together risk and operational metrics, such as measuring your team's performance against peer benchmark data and detection coverage across controls mapped to the MITRE ATT&CK Framework, so you can make informed decisions about resource and staffing investments.

You'll also have the metrics you need to clearly communicate how your security program influences business outcomes. Armed with information, you will have more productive dialogues about improving business resilience.

Metrics are an effective way to measure the success of a security program. According to PwC, just 22 percent of Chief Executive Officers believe their risk exposure data is comprehensive enough to form decisions.[5]

ZTAP's dashboards give a detailed view of service delivery metrics across all security controls and alerts. You'll have a complete understanding of your risk profile and key operational metrics such as total number of events monitored, Median Time to Detection (**MTTD**), Median Time to Respond (**MTTR**) and number of false positives.

According to a Gartner report, "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).[6]

[5]https://www.pwc.com/us/en/services/risk-assurance/library/assets/pwc-2019-risk-study.pdf. (n.d.)
[6]Gartner® Measure the Real Cost of Cybersecurity Protection, March 30, 2022

Let the Critical Start security experts support your team

You don't have to do it all.

Technology that integrates with disparate tools is critical for detecting and remediating threats, but the human element is important, too.

With security experts in short supply and expensive, it's difficult to build your own Security Operations Center (**SOC**), especially for smaller security teams. You'd need a large team to staff it 24x7x365 to accommodate vacations, prevent burnout and minimize high turnover.

A true MDR service augments your team by handling critical security functions, so your employees are freed up to focus on strategic business initiatives. Our MDR services include detection engineering, Indicator of Compromise (**IOCs**) management, continuous threat hunting and optional Incident Response services in the event of security incident.

We don't use a cookie cutter approach: we tailor our services to your security operation's unique needs. As part of our onboarding process, we'll fine tune our MDR solution to your business's requirements.

A sufficiently staffed organization can save $550,000 in data breach costs versus one that's insufficiently staffed.[7]

The Critical Start Cyber Research Unit (**CRU**) acts as a force-multiplier, amplifying the effectiveness of your security tools and enhancing your team's efficiency. Our security experts monitor your environment and constantly add and update threat detections to your security tools based on the latest curated threat intelligence and other sources.

[7]*https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High*

Use-Case

Industry:

Oil and Petroleum

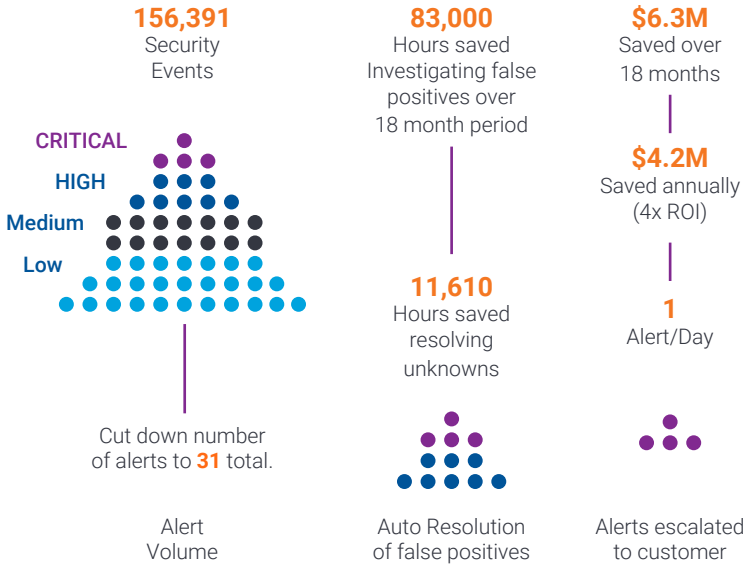
Tools:

- **Palo Alto Networks**
- **Devo SIEM**
- **Microsoft Sentinel**
- **Microsoft 365 Defender**

This customer experienced a significant breach resulting in brand damage and financial loss. Realizing they needed help, the IT team began working with a managed security services provider. Unfortunately, the provider was unable to meet visibility and Service Level Agreement (**SLA**) requirements.

The customer decided to work with Critical Start because of our experience working with both Microsoft and Palo Alto Networks customers.

In the first month of monitoring, we collected 156,391 security events from their tools. With our service we were able to cut down the number of alerts to 31 total, for an average of one per day! Over an 18-month period, this saved the company 83,000 hours of investigating false positives and 11,610 hours resolving unknowns. Results over the same time period were $6.3m in savings with an annualized total of $4.2m (4x ROI).

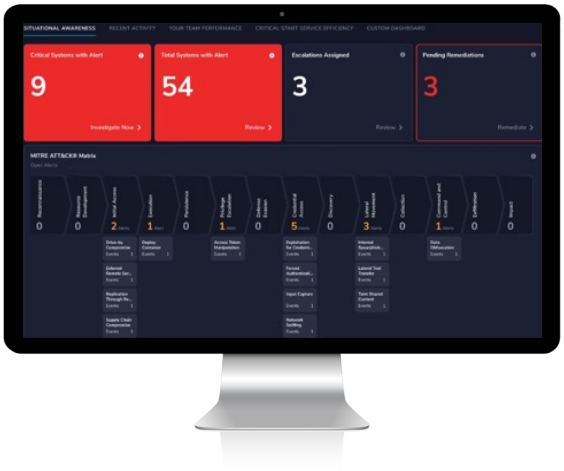


Simplify Visibility into Your Security Operation's Key Metrics

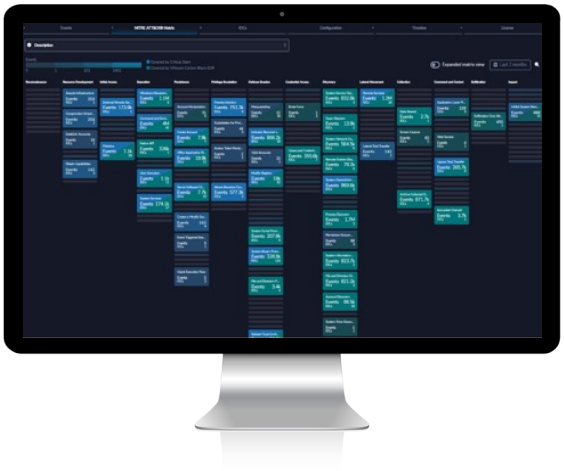
Our security expertise in MDR helps you reduce risk, improve your team's efficiency, boost detection effectiveness and measure detection and risk levels in order to guide security investments.

Here's a snapshot of what we can do for you:

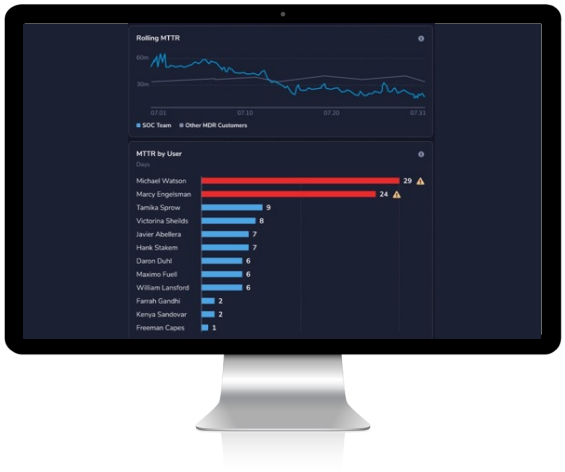
Respond and remediate faster with real-time actionable views of attacks in progress with step-by-step response guidance.



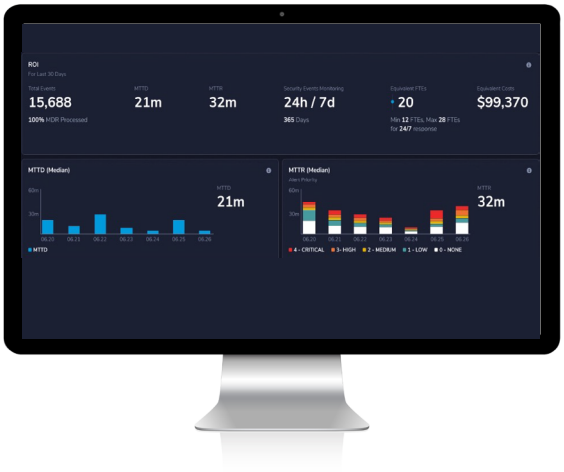
Make risk-based decisions on attack coverage that balance risk and cost.



Simplify resource management and make risk-based decisions tied to trends in threat activity and your team's performance.



Align cybersecurity spend to business outcomes by reporting on event activity and equivalent operational costs.



CRITICALSTART®

They're good. We're better.

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