eBook

3 Step Guide to Materializing the Power of Microsoft Security

CRITICALSTART®

Congratulations!

You are either moving to E5 Security (or other licenses) or you are looking to optimize your existing Microsoft licensing investment. Microsoft Security solutions provide you with cross-enterprise visibility and robust threat detection and auto investigation capabilities to rapidly respond to threats. However, if you are like most other security leaders, you are feeling the pain of number of security challenges:

- ✓ **Lack of visibility to report on security posture**
- ✓ **Expanded attack surface with changes happening every day**
- ✓ **Talent shortage – it's hard to find the skills and expertise**
- ✓ **Advanced persistent threats are only getting more complex**

These challenges can make it feel impossible to rationalize the investments you've made and build a business case for new investments – security controls and people - to help you increase your return and ability to protect your organization.

This guide has been designed to help you move past those security challenges. Within, you'll find step by step guidance to help you mature your Microsoft Security tools and approach breach prevention with simplified threat detection and response.

LET'S GET STARTED

CRITICALSTART®

82% of security leaders have been surprised by a security event, incident or breach that evaded a control(s) thought to be in place.[1]

On an average, an event, incident or breach is the result of five control failures.

STEP 1

Feed & Care for Your Tools

No security tool can detect every attack

Security teams are dealing with a growing volume of data and alerts, across a growing number of security controls. They don't have the time or people to manage, maintain and optimize their tools' ability to stop breaches. It can feel like a no-win situation. A common refrain heard in IT security circles is "We bought these tools to help us streamline and improve our ability to detect and respond to threats – but these tools are underperforming in their ability to disrupt attacks."

Similar to being an athlete, or working with a racehorse, proper care and feeding of security solutions is needed to drive ultimate performance and obtain winning outcomes.

Organizations invested in Microsoft Security should work with experts who fully understand these tools, can assess areas of risk in your unique organization, help you deploy the tools properly, apply the right threat detection use cases and adapt play books to automate investigation and response actions.

In knowing your security tools better, you'll gain visibility into areas of risk exposure and control, reduce operating expenses and drive better security outcomes with your Microsoft investment.

1 – Panaseer 2022 Security Leaders Peer Report

NEXT STEP

277 days:
Average time to identify and contain a data breach[2]

STEP 2

Monitor & Resolve Every Alert

People prevent attacks, not tools

Don't let the skills gap impede your ability to detect and disrupt attackers. Managed detection and response (MDR) service providers give your existing security teams increased speed to investigate and respond to threats with the right actions.

Now, there are many service providers to choose from. You may already be working with a Managed Security Services Provider (MSSP) but have felt like your team is still doing a lot of work, or they are missing threats. The challenge with the majority of security services providers offering MDR services is that they only sign up to do so some of the work.

- ✓ **They prioritize and address the critical and high-level alerts**
- ✓ **They cannot take a response action with your security tools**
- ✓ **They provide service level agreements that have small print language**

As a Microsoft Gold Partner and member of the Microsoft Intelligence Security Association, Critical Start has been invested with Microsoft from the beginning of the design of Microsoft Defender. As a leader in MDR, we do something uniquely, that no one else can prove they do.

On average, 99% alert reduction across all alert types.

Practicing alert suppression comes at the price of accepting risk. Many MDR service providers disable lower priority alerts, change thresholds and prioritize Critical and High priority alerts while ignoring Medium and Lows. **This means many threats are evading security controls and escaping investigation.**

Critical Start built its MDR service on the most advanced analytics and automation platform to resolve every alert. Specifically, the Zero Trust Analytics Platform™ (ZTAP™), featuring the Zero Trust Behavior Registry™ (TBR), auto-resolves false positives. The unknown alerts are escalated to our security team for further investigation and response on your behalf.

Critical Start built a comprehensive integration with the Microsoft Security stack so you gain end-to-end solutions and services to shield your hybrid, multi-cloud environment and speed up investigation beyond the endpoint – all in one portal.

2 – IBM Security. Cost of a Data Breach Report 2022

NEXT STEP

USD $550,000

Average data breach cost savings of a sufficiently staffed organization versus insufficiently staffed[2]

STEP 3

Let the Experts Support Your Crew

You're investing in a great foundation – Microsoft Security.

But you still need complete security operations or a partner to help you build and optimize your existing security operations center (SOC) with Microsoft.

Organizations should look for a partner who not only can help them deploy their tools and monitor alerts, but who can provide other advanced threat detection and response capabilities to stay ahead of advanced threats – and adapt to your changing business requirements.

We might be a little biased, but at Critical Start we believe that a security service provider should go beyond the minimal requirements of monitoring and response recommendations. A true MDR should support your team by handling the critical security functions so that your team is freed up to focus on strategic business initiatives. Our MDR service includes detection engineering, Indicator of Compromise (IOC) management, detection engineering, continuous threat hunting and optional Incident Response services in the event of a security incident.

2 – IBM Security, Cost of a Data Breach Report 2022

SHOW ME THE VALUE

Use Case

INDUSTRY

Pharmaceutical Manufacturing

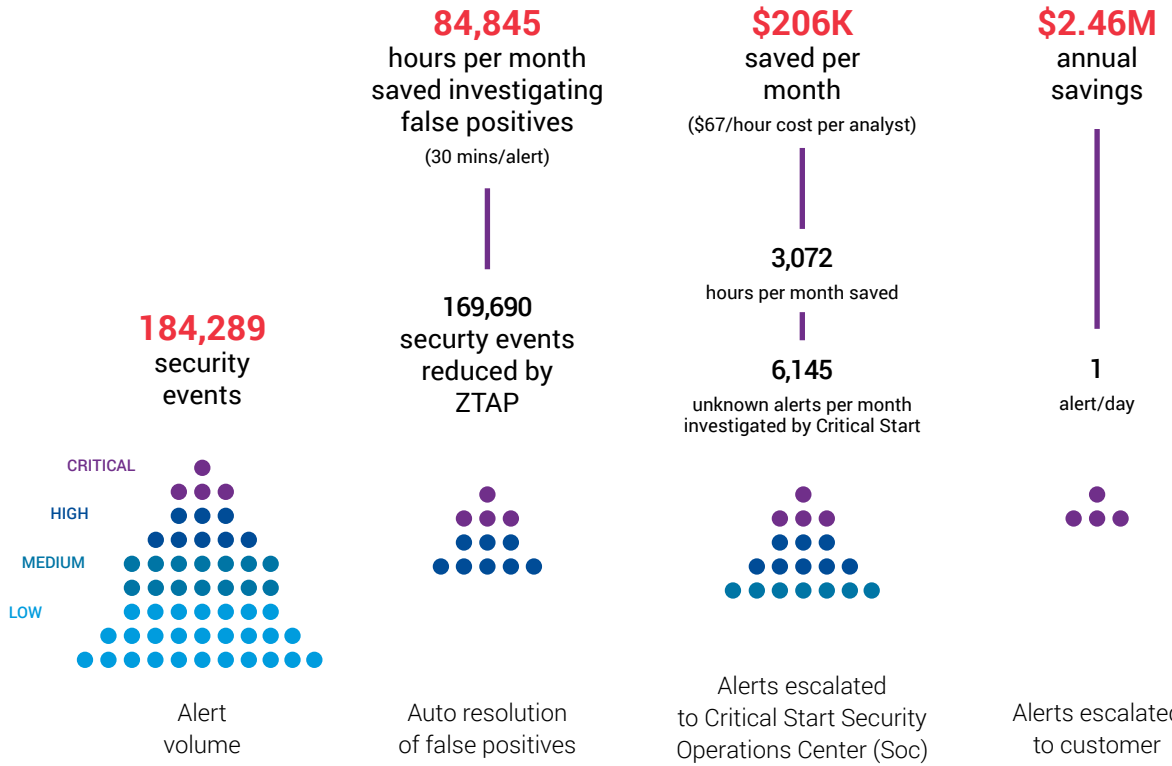
MICROSOFT PRODUCTS

Microsoft Sentinel | Microsoft Defender for Endpoint

This customer experienced a significant breach that made a huge impact on their brand and caused substantial financial losses. Realizing they needed help, the IT team began working with a managed security services provider. After a year into the engagement, however, the provider was not meeting expectations with regards to response capabilities, and was not providing the visibility and transparency this large enterprise expected.

Additionally, the customer was looking to move to the Microsoft security stack. The customer decided to work with Critical Start because of our deep Microsoft bench across the team – including on SIEM/Sentinel deployments and our detection and response capabilities – being able to resolve every alert and prevent breaches. Today we monitor Microsoft Defender for Endpoint – 18,000 endpoints and Microsoft Sentinel. The customer is now speaking with us about monitoring Microsoft 365 Defender as their next security maturity move is email and identity.

In the first month of monitoring, we collected 184,289 events from their tools. With our service we were able to cut down the number of alerts per day to 1. Without Critical Start it would take them 84,845 hours/month investigating false positives and 3,072 hours per month resolving unknown alerts. This is nearly $206K a month in savings and $2.46M yearly. Over the life of the engagement, we've saved them $3.5M.



CRITICALSTART®

USE CASE

Use Case

INDUSTRY

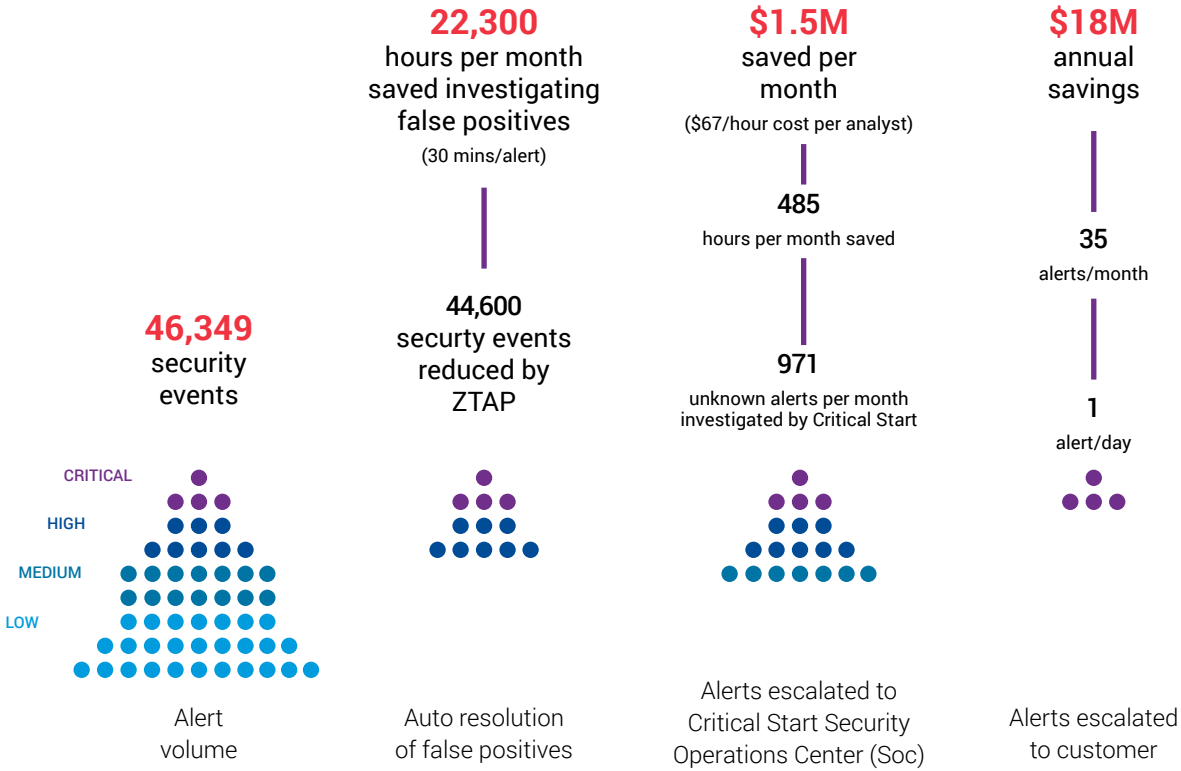
Health Insurance

MICROSOFT PRODUCTS

Microsoft Sentinel | Microsoft Defender for Endpoint | Microsoft 365 Defender

This health insurance organization engaged Critical Start to increase the scalability and efficiency of their SOC operations, augment their staff with 24x7x365 monitoring and assist in their Microsoft E5 security growth.

In one month, we collected over 46K events from their tools. Of the 35 alerts escalated to the customer, 31 were low and medium priority alerts. Critical Start reduced the number of alerts escalated to **only one per day!** We do this without ignoring or discarding a single alert. Without Critical Start it would take them over 22,300 hours/month investigating false positives and 485 hours/month resolving unknown alerts. Based on this, Critical Start costs savings would exceed $1.5M per month.



CRITICALSTART®

USE CASE

Access to the right expertise and strategy is nonnegotiable

Microsoft Security is good—really good. But we can help you make it better. The elite security expertise and unique approach to threat detection and response from Critical Start can help you derive value from your security investments, lowering your overall cost of ownership.

Deep Microsoft Relationship

- ✓ Recruited by Microsoft to be a pilot member of the MISA MSSP program
- ✓ Microsoft Gold Partner and a member of the Microsoft Security Partiner Advisory Council and Microsoft Security and Manageability Elite Partner Programs
- ✓ Advanced Development Support access

Expert Threat Detection Content

- ✓ Curated original and 3rd party threat intel
- ✓ Out-of-the box IOC management
- ✓ IOCs mapped to the MITRE ATT&CK® Framework

Microsoft Certifications

- ✓ MS-500 Microsoft 365 Security Administration
- ✓ SC-200 and AZ-500: Microsoft Azure Security Technology Certifications

Rigorous Training

- ✓ 300 hours of training required for all SOC analysts during onboarding
- ✓ 80 hours of shadowing and continuous training annually

CONTACT US

CRITICALSTART®

Ready to talk to an expert?

Let us know how we can help you make the most of everything Microsoft has to offer.

CONTACT A MICROSOFT EXPERT