CRITICALSTART® MICROSOFT®

Response Actions White Paper

All Threat Responses
Are Not Created Equal

Achieving the promise of Extended Detection and Response (XDR)

Microsoft is regarded as a leader in XDR. It was named a leader in *The Forrester New Wave™: Extended Detection and Response (XDR), Q4, 2021*[i.] Its XDR architecture is built around gathering detections, telemetry data, behaviors, alerts and events from across multiple domains: identities, devices, applications, data, network and infrastructure. Microsoft adds powerful automation as part of their XDR to normalize and analyze the cross-domain data into high-fidelity incidents, enabling broad threat detection coverage. In addition, cross-domain correlation and analysis close the threat detection gaps that can exist between domain silos, like identities and applications.

Even with leading innovations, Microsoft's XDR can be a complex solution to manage, requiring the right capabilities and know-how to optimize configuration, data consumption, security operations and most importantly, response actions to legitimate threats.

The results of getting it wrong can be dire, leading to inefficiencies that degrade effectiveness or oversights that invite catastrophic security failures.

This white paper outlines how Critical Start Microsoft security experts deliver effective threat detection response for Microsoft XDR.

Cross-domain Threat Detection Requires
Cross-domain Response

The primary challenge with cross-domain threat detection is having an equally robust response capability for legitimate threats. Whereas most Managed Detection and Response (MDR) providers center their response actions around endpoint or host isolation, Critical Start leverages the breadth of Microsoft XDR to deliver response actions that get to the root of an attack kill chain from identity, applications, infrastructure, to endpoints.

We deliver comprehensive, 24/7/365 Managed Detection and Response services that address the demands and challenges of cross-domain XDR detection and response. At the same time, our team of certified Microsoft experts has the deep know-how and skills to unlock the full potential of Microsoft XDR. Additionally, we are a Microsoft Verified Managed Extended Detection and Response (MXDR) solution provider.

1. We use Microsoft XDR and widespread integrations in Microsoft 365 and connected cloud applications (Salesforce, Workday, etc.), on-premises infrastructure, and hybrid cloud technologies (Google and AWS, etc.) to analyze and respond to all alerts regardless of disposition (high, medium, or low). Critical Start, by analyzing every alert, can discover low and slow cross-domain breaches and eliminate false positives at scale. (Fig 1)

2. Every legitimate threat goes through in-depth analysis by the Critical Start SOC team to determine the most effective response actions.

3. Critical Start leverages Microsoft XDR breadth to deliver an equally comprehensive set of cross-domain response actions to stop attackers in their tracks.

CRITICALSTART – Enterprise-wide Detection and Response

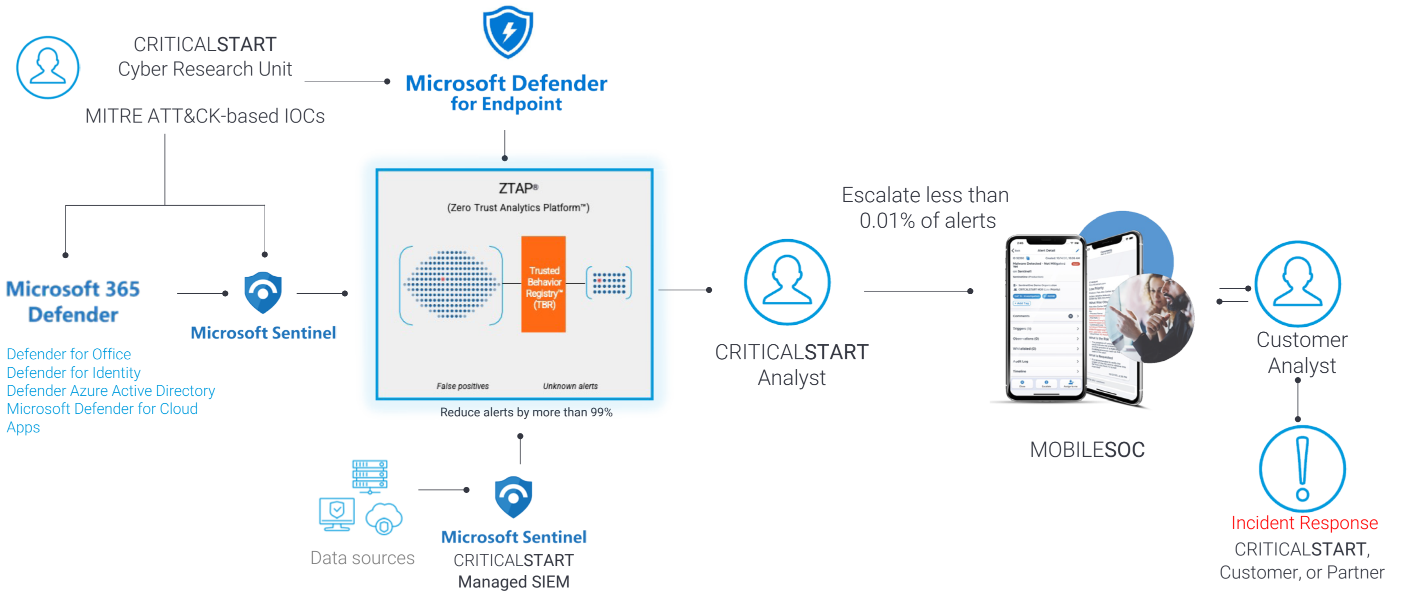


Figure 1: Critical Start Microsoft verified MXDR architecture and cross-domain response capabilities

Identity

Last Line of Response

Identity is the new security permitter and a foundation for Zero Trust Architecture in the modern world. **Over 60% of all breaches involve credentials[ii] and weak identity security remains a top security risk for companies and organizations worldwide[iii].** Unique to MDR service providers, Critical Start acts at the identity layer to help prevent these pervasive attacks.

In addition, Critical Start leverages identity data in combination with cross-domain threat detections and telemetry to identify and map breach activity to the **MITRE ATT&CK® Framework.** Not only does this allow Critical Start to prioritize response actions based on the criticality of an identity or asset, but it also enables us to respond holistically to multiple components of a breach within the kill chain.

HOW WE DO IT

Using a multitude of threat signals and detections via bi-directional API integrations with Defender for Identity for on-premises Active Directory and Azure Active Directory for cloud identities, Critical Start addresses identity-based attacks with the following pervasive response actions:

- ✓ **Block user sign-in** — Immediately prevents a user from being able to sign into Azure AD from any device or application.
- ✓ **Revoke all sessions and MFA tokens** — Prevents all existing sessions and tokens from being used for continued access or new authentications.
- ✓ **Confirm/Dismiss Risky User status** — Marks a user as compromised to initiate additional workflows such as the actions listed above. Conversely, flagged User Risk in Azure AD that is a false-positive can be reinstated.

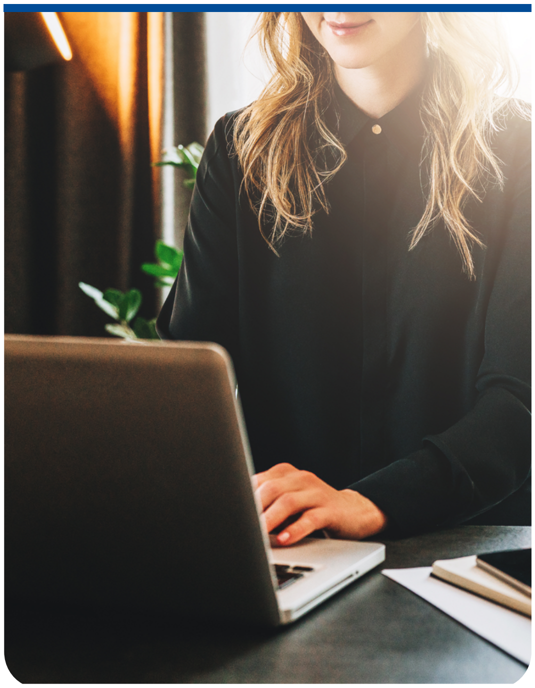
Response That
Goes Beyond Email

With increased attacks in collaboration tools like Microsoft Teams[iv], it is more important than ever to protect users beyond email. Plus, it is impossible for all phishing and spoofing emails to be stopped with automated policies—especially in circumstances where a business partner or vendor becomes compromised and attackers use legitimate accounts to try to infiltrate your environment.

Email security solutions like Proofpoint® and Mimecast® do an excellent job at protecting users from malware, phishing, spoofing and malicious links within Microsoft Exchange Online email. However, they may be blind to threats within the broader Microsoft Office 365 toolset.

Microsoft Defender for Office 365 takes it to the next level with protection for all collaboration and productivity tools in Office 365. Critical Start leverages this breadth of protection coverage and deep integration to take decisive response actions to mitigate attacks or further spread of malicious communications when automated tools and policies fail.

HOW WE DO IT



Using bi-directional API integrations with Microsoft Exchange Online and Defender for Office 365, Critical Start can take the following response actions for Exchange Online Email, Teams, SharePoint Online, OneDrive for Business and all connected apps within Microsoft 365 Groups:

- ✓ **Revoke an email —** Remove the email identified by customers, our SOC, or both as phishing out of all inboxes it was delivered to.
- ✓ **Customized end-user response** — Critical Start can communicate with end users about these communications and subsequent security actions, with predefined playbooks and governance rules created in conjunction with customers.
- ✓ **Cross-domain response** — Use the identity-based integration and responses outlined previously to stop the spread of threats in Microsoft Teams, SharePoint Online, OneDrive for Business, etc.

Endpoints
and Devices

Endpoints and devices remain a top threat vector for attackers to gain access to systems, credentials and ultimately, your data. Microsoft Defender for Endpoint was named a leader in the 2021 Gartner Magic Quadrant for Endpoint Protection Platforms. According to Gartner, Leaders "have broad capabilities in advanced malware protection, and proven management capabilities for large enterprise accounts. Increasingly, Leaders provide holistic XDR platforms that allow customers to consolidate their other tools and adopt a single-vendor solution."[v] In this regard, Defender for Endpoint delivers a broad set of detection capabilities, and consequently, a deep array of XDR signals that can be leveraged for analysis, investigation and response. This includes process information, network activities, deep optics into the kernel and memory manager, user login activities, registry and file system changes, and others.

These signals are a foundational part of Critical Start's MXDR capabilities and are core to threat investigations and response, enabling deep analysis of root causes and attack vectors. Ultimately, allowing Critical Start SOC analysts to effectively and accurately identify and respond to endpoints and devices involved in a breach, user credentials leveraged, services exploited and a timeline of events back to patient zero.

HOW WE DO IT

Critical Start has developed bi-directional API integrations with Defender for Endpoint with all its XDR signals for deep threat analysis and for taking the following response actions:

- ✓ **Isolate a host —** Prevent an endpoint from communicating with any other devices, services, or applications on the network (except for the Defender for Endpoint service) to mitigate the spread of infection or ransomware, etc.
- ✓ **Run AV scans and take response actions against malware/ransomware (stop and quarantine a file)** — Scan a disk, repository, or specific folder for threats as part of an investigation. Stop an executable or isolate a file to mitigate the spread of infection or ransomware, etc.
- ✓ **Pickup and execute failed automated response actions taken within Microsoft Defender** — Microsoft Defender's Automated Investigation and Response (AIR) capabilities can stall-out or fail, requiring human intervention.

Cloud

Enabling Response

Cloud application usage represents a substantial attack surface, with shadow IT representing a significant challenge for every organization. Microsoft Defender for Cloud Apps provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across all Microsoft and many third-party cloud services. Put simply, this is a pinnacle signal for true MXDR service capabilities across technology pillars, providing a gateway into shadow IT discovery, like the use of DropBox® to share files externally.

Additionally, it can expand entity and user behavior analytics (EUBA) beyond Microsoft 365 into the larger internet ecosystem. **Microsoft Defender for Cloud Apps uses data and integrations from Defender for Endpoint, Identity (SSO), API integrations (Salesforce®, Google® Workspace, Amazon® Web Services, etc.), and built-in connectors (Office 365) to provide rich detections, behavioral monitoring, shadow IT discovery, cloud app compliance/governance and much more.**

HOW WE DO IT

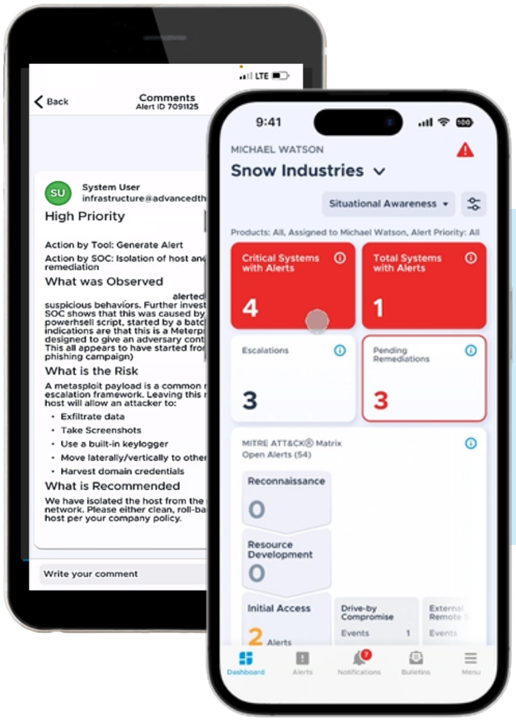
Using bi-directional API integrations with Defender for Cloud Apps Critical Start can take the below-outlined actions across identities, devices, and collaboration tools to stop attacks or nefarious behavior.

IDENTITY	Devices	COLLABORATION
• Block user sign-in • Revoke all sessions and MFA tokens • Confirm/Dismiss Risky User status	• Isolate a host • Run AV scans • Stop and quarantine a file • Execute failed Defender response actions	• Revoke an email • Customize end-user response • Cross-domain response

Response
Rules of Engagement

Critical Start works with each client to develop a detailed governance plan to address the shared responsibility for utilizing these powerful response actions or other custom responses. In addition, Critical Start works with each client to define specific rules of engagement for their business requirements. Below are examples of some rules of engagement that are defined during the shared governance process:

- ✓ **Blocking or revoking users and sessions** — During the development of a governance plan, Critical Start works with our customers to define the rules of engagement for which sign-ins or users can be blocked or have sessions revoked for detections and threat activity.
- ✓ **Host isolation** — Critical Start will define a detailed governance plan for isolating endpoints and hosts. For example, a customer working with Critical Start may determine that factory floor devices need 24/7 customer authority to engage in response actions, like isolation.



Comments
Alert ID 7091125

System User
infrastructure@advancedth

High Priority

Action by Tool: Generate Alert

Action by SOC: Isolation of host and remediation

What was Observed

alerted
suspicious behaviors. Further invest
SOC shows that this was caused by
powerhsell script, started by a batc
indications are that this is a Meterpr
designed to give an adversary cont
This all appears to have started fro
phishing campaign)

What is the Risk

A metasploit payload is a common r
escalation framework. Leaving this r
host will allow an attacker to:

- Exfiltrate data
- Take Screenshots
- Use a built-in keylogger
- Move laterally/vertically to other
- Harvest domain credentials

What is Recommended

We have isolated the host from the
network. Please either clean, roll-ba
host per your company policy.

Write your comment

MICHAEL WATSON
Snow Industries

Situational Awareness

Products: All, Assigned to Michael Watson, Alert Priority: All

Critical Systems with Alerts	Total Systems with Alerts
4	1

Escalations	Pending Remediations
3	3

MITRE ATT&CK® Matrix
Open Alerts (54)

Reconnaissance 0
Resource Development 0
Initial Access 2 Alerts
Drive-by Compromise Events 1
External Remote Events

Lastly, customers can use the Critical Start Zero Trust Application Platform® (ZTAP®) or MOBILE**SOC**™ to directly execute the above-mentioned Microsoft Security response actions from the palm of their hand and communicate with our SOC team 24/7.

Why Critical Start

At Critical Start our focus is on delivering the most effective Managed Detection and Response for Microsoft XDR. We do this by leveraging the cross-domain security capabilities of Microsoft XDR to deliver the broadest response capabilities in the market. We work with you to define the right shared governance model to achieve your business and security outcomes.

Our team of Microsoft security experts leverages our integration with Microsoft Security to detect, investigate and respond with the right actions before threats can disrupt your business. Our outcome-based approach focuses on delivering value across areas critical to your organization:

- ✓ **Situational awareness** — By delivering actionable views of attacks in progress with clear, step-by-step response guidance, security teams gain situational awareness they can use.
- ✓ **Team efficiency** — Measuring the mean time to response (MTTR) for analysts and teams drives continuous improvement, productivity, and team efficiency.
- ✓ **Effectiveness** — Critical Start MDR maps detection content to the MITRE ATT&CK framework enabling risk-based decision-making and improving attack coverage effectiveness.
- ✓ **Investment guidance** — We deliver data and reporting that articulate the value of our MDR service to help you align cybersecurity investment with business outcomes.

[i] “Microsoft achieves a Leader placement in Forrester Wave for XDR”, October 18, 2021, https://www.microsoft.com/en-us/security/blog/2021/10/18/microsoft-achieves-a-leader-placement-in-forrester-wave-for-xdr/

[ii]“50 Identity And Access Security Stats You Should Know In 2023,” January 6, 2023, https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/#the-frequency-of-identity-and-access-breaches

[iii] ” Microsoft Digital Defense Report 2022 Executive Summary,” 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bcRe?culture=en-us&country=us

[iv] Microsoft Teams is the new frontier for phishing attacks,” February 23, 2022, https://venturebeat.com/security/microsoft-teams-is-the-new-frontier-for-phishing-attacks/#:~:text=By%20attaching%20a%20malicious%20executable,the%20Trojan%20then%20installs%20malware.

[v] “Gartner names Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant,” May 11, 2021, https://www.microsoft.com/en-us/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/