CRITICALSTART®
MDR Onboarding Guide

Here's what to expect and how we can simplify the complexity of your cybersecurity.

CRITICALSTART®
They're good. We're better.

Executive Summary

The unknown can be a powerful motivator. The reason you're probably considering managed detection and response is that you're dealing with unknown gaps in your cybersecurity coverage and unknown threats that are waiting to exploit them.

But MDR itself could also be considered an unknown. If an organization has not worked with an MDR provider, it's understandable that there will be questions:

- How will this impact my environment?
- What is the implementation plan?
- What resources can I expect from my MDR partner?
- What are the responsibilities of my team?
- What kind of deployment timeline can I expect?

At CRITICAL**START, our primary focus is on simplifying the complexity of cybersecurity for our customers.** That takes the form of tools such as our Zero Trust Analytics platform and Trusted Behavioral Registry, which can resolve all alerts, escalating less than 0.01% of alerts that require your attention. But it also means that we've developed an onboarding process to strengthen both your visibility and comfort level with the entire process.

Let's take a quick look at what this process entails and what it takes to ensure every alert is resolved to dramatically increase the cyberprotection level for your organization.

Topics Include

- ✓ An overview of the resources we provide to ensure a successful transition to resolving all alerts through MDR
- ✓ An overview of the resources a customer needs to provide to ensure successful onboarding as well as ongoing monitoring and resolution
- ✓ Detailed outlines of the onboarding lifecycle and implementation workflow
- ✓ Action items required at each phase to ensure a successful move to live production monitoring through MDR

How to Get Started

The key to a smooth onboarding launch is understanding. We've built a process to make you completely comfortable—including a comprehensive understanding of the resources we make available to enable success. We also want to build understanding of the internal resources you need to leverage so that your organization is making the most of the resources we provide.

An effective onboarding and implementation process should take into the account an organization's unique environment and existing security tools and processes. We want to make the effort and spend the time with you to learn this environment and build out a dedicated team to work effectively within it.

One of our primary values is that we provide resources that stay with you throughout the project. We want to build a strong relationship between your resources and ours to work together daily, with a common purpose and understanding, to respond as a fluid, cohesive unit any time a threat presents itself.

Dedicated resources we provide during onboarding:

Project Manager

- Point of contact for project plan, timeline and milestones
- Will host cadence calls to make sure project is on track and on schedule

Customer Success Manager

- Will build relationship and ensure that all goals and primary business objectives are met

Endpoint or SIEM (depending on specific project need) Engineers

- Will assist with event reduction, playbooking and technical integration into ZTAP

Support Analyst

- Provides additional support before moving into production monitoring and continues after launch

Customer to provide resources with the capabilities to perform the following tasks:

- ✓ Deploy/install endpoint/XDR/SIEM agents on hosts
- ✓ Review security events as escalated by Critical Start
- ✓ Modify firewall rules to accommodate endpoint/XDR/SIEM connectivity
- ✓ Knowledge of network environment to work with Critical Start on baselining security events

The Onboarding Lifecycle

From start-to-finish, the onboarding process can be outlined through three stages:

Stage 1: Kick-off

During our initial kick-off call, you can meet your Critical Start team and review project milestones.

Customer Action Items

- ✓ Be sure to fill out and return questionnaire prior to kick-off.
- ✓ Download the MobileSOC app and sign-up for ZTAP training.
- ✓ Be sure to approve project plan after review.

Stage 2: Implementation

Access and Integration During this phase we will perform a health check of your current cybersecurity policies to uncover and address any gaps in coverage. Detections and indicators of compromise are infused directly into the tools used by our MDR team. Through this approach, we can create a high-fidelity threat detection and validation platform that uses specific detection logic customized to your environment. At this stage, we will need access to your security product in order to build and connect the ZTAP environment.

Event Reduction We will develop playbooks to reduce the volume of alerts and security events. Additionally, threat intelligence includes a curation of original and third-party data to derive new detections with everything mapped to the MITRE ATT&CK® framework to reduce complexity and improve SOC effectiveness.

ZTAP Training Your team will have multiple options for self-paced training through video instruction, or through online instruction for both console-based ZTAP and our MobileSOC application.

Customer Action Items

- ✓ Provide security product tenant access.
- ✓ Assist in event reduction through handling of escalated alerts.
- ✓ Work with the Critical Start team to develop alert exclusions in security product.

Stage 3: Production

Final Health Check We work with you to ensure the technology, processes and people are in place to resolve alerts and mitigate threats to your enterprise.

Move to Production Monitoring Managed Detection and Response goes live, and monitoring and response are transitioned to our customer success team. This is another dedicated team to provide you with a consistent point of contact to ensure dynamic and adaptive protection.

Customer Action Items

- ✓ Approve move to production monitoring.

The Onboarding Lifecycle

Here's what the workflow of all three stages looks like in sequence:

Stage 1: Kick-off

Kick-off

- ✓ Meet your Critical Start dedicated resources
- ✓ Review Primary Business Objective and Milestones

Stage 2: Implementation

Training

- ✓ Schedule ZTAP training
- ✓ Download MobileSOC and review

Implementation

- ✓ Access and Integration
- ✓ Event Reduction
- ✓ Weekly cadences ensuring project is on track and milestones are met

Stage 3: Production

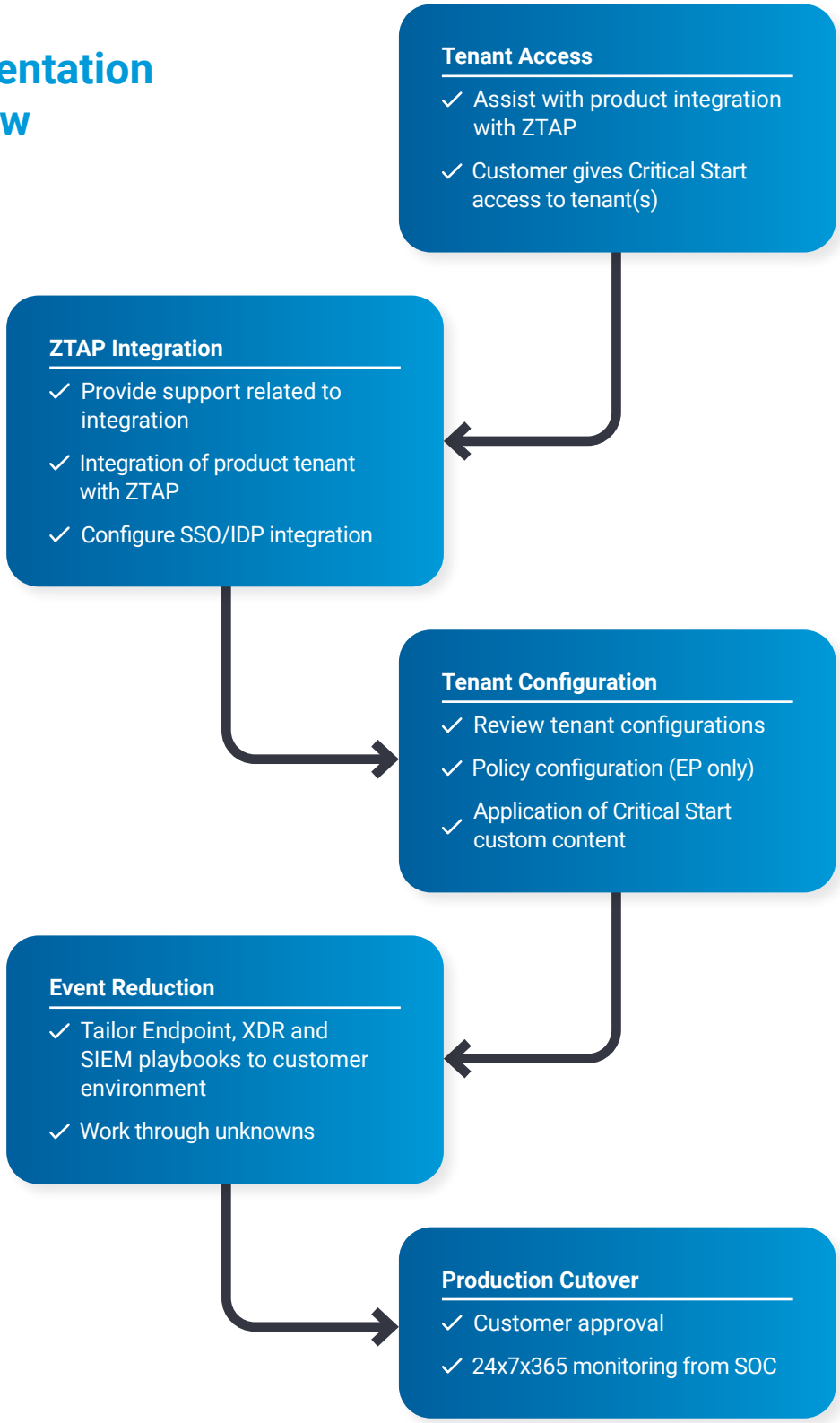
Move to Production

- ✓ Final Health Check
- ✓ Approval of move to production monitoring

Onboarding Complete

- ✓ 24x7x365 SOC monitoring
- ✓ Continue to develop known-good behavior for your environment

Implementation Workflow



But what if something changes?

Change happens, and that's ok. Our team, processes and technology are built to scale with your growth. We have a formal change management process to ensure full visibility and alignment into expectations, capabilities, timelines and performance. Just tell us what you need, and we'll advise you on the best course of action to keep your cyber protection moving forward. You need a team that can scale to accelerate your journey while constantly focusing on the mission of protecting your business, instead of just chasing a revenue stream. Our mission is to provide exactly this type of service.

Questions?

This guide is meant as an introduction to MDR onboarding and how we can help you simplify the complexity of cybersecurity, but it's not a comprehensive overview of our process. If you have questions, we have answers and we're ready to help. Just let us know the current stage of your cybersecurity journey and we'll help you plan the next step.

Contact us at information@criticalstart.com.