Managed Detection and Response for SIEM

SOLUTION OVERVIEW

CRITICALSTART®

They're good. We're better.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Critical Start Managed Detection and Response (MDR) for Security Information and Event Management (SIEM) integrates our trust-oriented approach to MDR with leading SIEM platforms to help customers achieve the full operating potential of their SIEM investments for the most effective threat detection.

SIEM implementations can be complex. You must make choices about what to ingest based on the value of your data and make adjustments as your needs change. Critical Start MDR for SIEM simplifies this process by prioritizing data based on what we have observed with other customers and MITRE ATT&CK® coverage, then our trust-oriented approach to MDR eliminates false positives at scale to streamline the investigation and response process. We become deeply familiar with your business and take the entire SIEM journey with you--from onboarding to personalization to investigation to continuously maturing your security platform—to ensure the best outcomes.

Critical Start MDR for SIEM offers unique benefits to enterprise customers who are deploying SIEM solutions to detect sophisticated attacks:

Reduce the noise. SIEMs can generate so many alerts that your security team becomes overwhelmed. Our Zero Trust Analytics Platform™ (ZTAP™) ingests source data across all users, devices, applications, and infrastructure. ZTAP does the heavy lifting, looking for the known good, then sends everything it considers bad to a SOC analyst for review. The SOC analyst provides a guided response or takes remediation on your behalf, as appropriate for SIEM implementations.

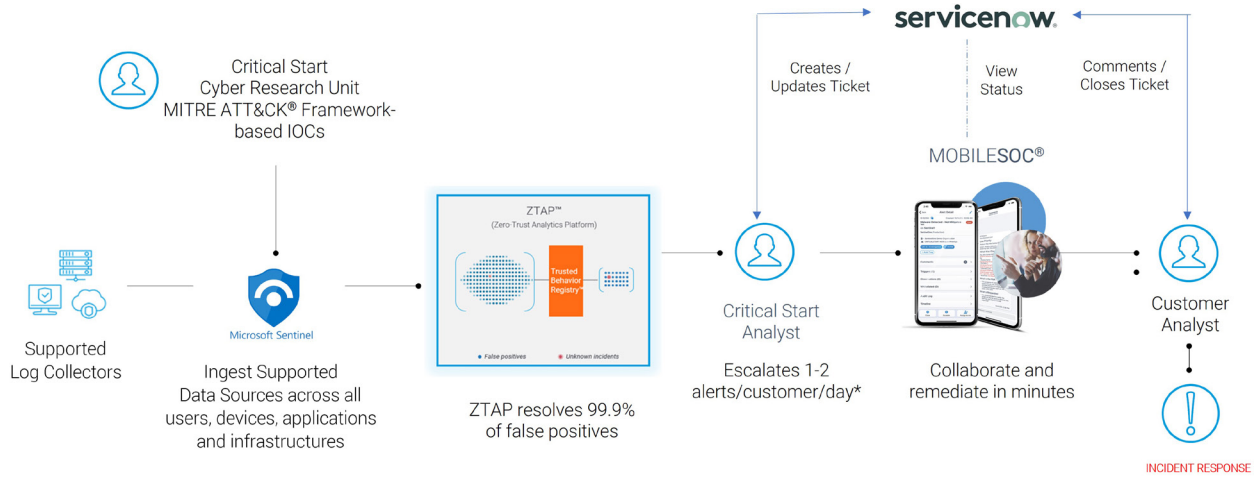
Continuously mature your security program. Implementing SIEM is a journey, and unfortunately, many businesses do not reach the maturity phase of that journey. Critical Start stays with you every step of the way to help verify coverage in your attack framework and add more data sources to address new IT initiatives, such as cloud migration, BYOD, and multi-factor authentication.

Increase visibility across your security environment. ZTAP is built on the promise of unfettered transparency. You see what our SOC analysts see, and you can view performance against SLAs right from the dashboard. In addition, our MOBILE**SOC**® app allows you to view ZTAP and take actions directly from your mobile phone.

Stop breaches. With 24x7x365 expert security analysts, and the Cyber Research Unit (CRU), we monitor, investigate, and remediate alerts swiftly and effectively, via contractual Service Level Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR).

When you combine these benefits with the many advantages offered by Critical Start, such as our MobileSOC, Customer Success Management Team and SOC, you can see how Critical Start MDR for SIEM simplifies breach prevention.

HOW WE DO IT



The backbone of our MDR service is the Zero Trust Analytics Platform (ZTAP). It delivers the scalability to resolve every alert. ZTAP features the Trusted Behavior Registry (TBR), the only purpose-built registry of known good behaviors.

Most SIEM platforms let you ingest whatever you want— but being able to do something with that content is a different story.

To effectively drive threat detection and provide content needed for investigations, you must make choices about what you want to ingest into the SIEM platform and manage that against the value those data sources provide to your security mission.

We help you prioritize your data onboarding by separating it into:

- ✓ Threat Detection Sources that are rich in threat detection value and contain actionable signals
- ✓ Investigation Sources that contain information about what is going on in your environment and will be the primary data corpus for investigations when threats are detected, as well as select targeted detections
- ✓ Enrichment Sources that help provide more context to threat detections and investigations but have limited security value.

After feeding all your log sources into ZTAP, we add all the threat detection content needed to turn your data into meaningful alerts.

ZTAP PROVIDES:

- ✓ Immediate notification of alerts escalated by the Critical Start SOC
- ✓ Triage information for full context and analyst recommendations
- ✓ Direct communication with our analysts to collaborate, make quick decisions, and act with confidence
- ✓ Threat analysis plug-ins to pivot to your security tools and gather more data to enhance investigation

HOW WE DO IT

PLAYBOOKS

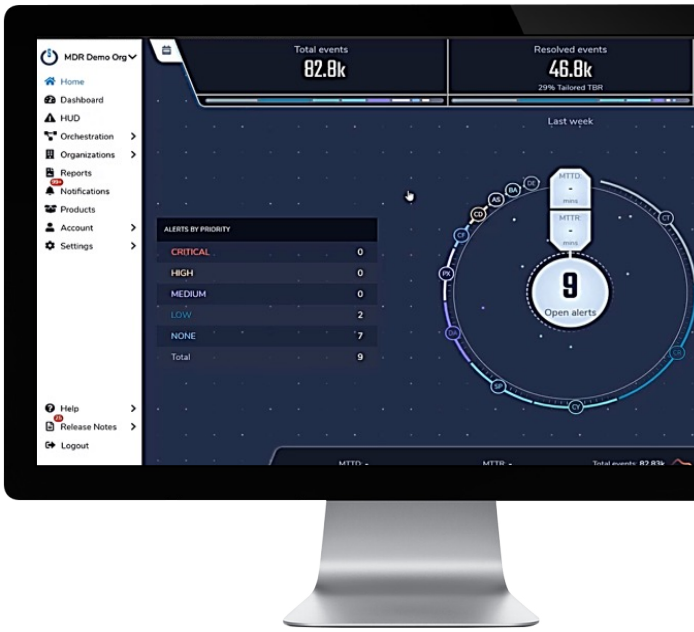
The TBR consists of over 40,000 playbooks that provide confirmed and automated investigations. TBR playbooks automatically resolve known good alerts using key-value pairs that are generated by security tools. Key-value pairs provide the context needed to accurately identify good versus bad behavior. Examples of keys include host name, IP address, hashes, paths, command lines and more.

Over 90% of the TBR playbooks are common to all customers and applications. During the on-boarding process the Critical Start implementation team will adapt an additional 9% of playbooks to a specific customer environment. An unlimited number of key-value pairs can be applied to filter an alert. The more context you add, the less risk you must accept.

DASHBOARD

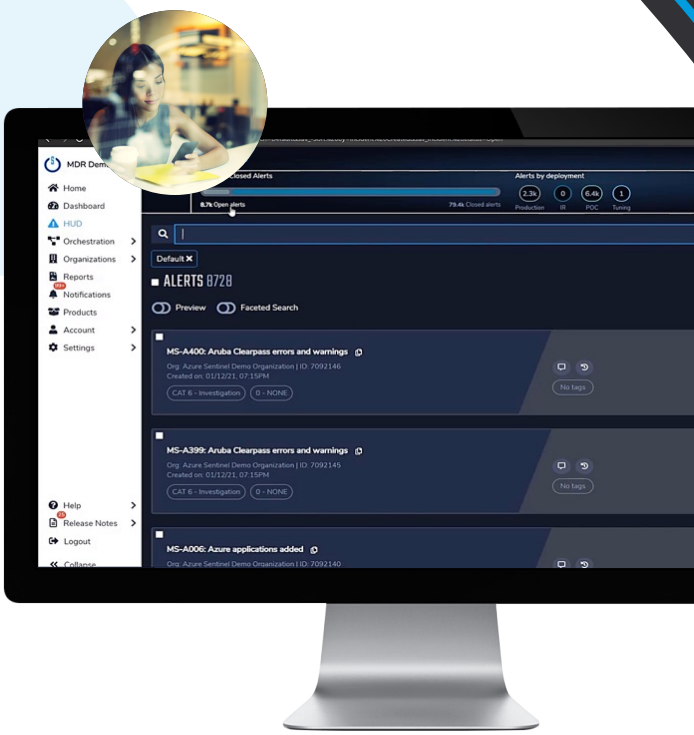
The ZTAP™ Dashboard provides executive insights into the effectiveness of the TBR, the responsiveness of the Critical Start SOC and the next steps required by customer security teams. The Dashboard provides four key data points.

- ✓ The total events collected from the security tools.
- ✓ The total number of alerts resolved. These are the alerts that are automatically resolved by global or adapted TBR playbooks.
- ✓ The number of alerts escalated by the Critical Start SOC to the customer.
- ✓ Critical Start Service Level Agreement (SLA) performance in real-time. Our SLAs are one hour Time-To-Detect and one hour Median-Time-To-Respond.



HOW WE DO IT

HEADS-UP DISPLAY



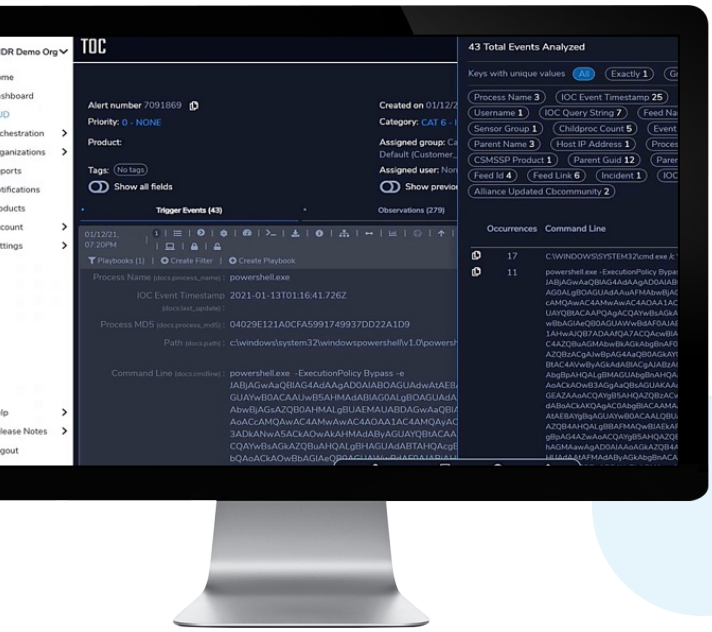
The Heads-Up Display (HUD) is where the analysis, triage and response to alerts occur. All SOC investigations and response actions are tracked and audited within the HUD. The HUD displays:

- **Alert classification** – Displays open and closed alerts. Both are actionable. Selecting Open shows all alerts opened within the last week.
- **Alerts by deployment** – Displays alerts by Production, IR, POC and Tuning. As customers are onboarding, they are put into the Tuning deployment state. At this time, you are transitioned to full production monitoring. Each deployment status is actionable.
- **Queries** – Searches for all Key-Value Pairs from the alerts ingested into ZTAP™. These are intelligent queries, not raw log searches. Raw log searches can be performed by pivoting to the security tools.

Within each alert are the actual events that are generated. ZTAP aggregates events based on parameters that are dependent on the security tool monitored. Aggregations can be viewed in the HUD.

ZTAP classifies alerts into Trigger and Observation events. Trigger events are unknown and cannot be confirmed by the TBR as good. These alerts are investigated by Critical Start analysts. Observations are events that have been confirmed as known good by the TBR and automatically resolved. Known good events are often used as components of complex attacks. Observation events can provide additional context to Trigger event investigations.

HOW WE DO IT



EVENT ANALYSIS

Event Analysis looks for how often or how infrequently we see Key-Value pairs, such as looking at all command line arguments seen in Trigger events. Event Analysis allows us to quickly determine if an event was good or bad and to quickly pivot into a response.

THREAT ANALYSIS PLUGINS

TBR playbooks can go deeper in investigation. Threat Analysis Plugins (TAPS) are APIs between ZTAP and security tools. For SIEM, we use in-line triage TAPs that take certain data points inside an alert and make the alert link to additional threat intelligence, allowing analysts to search for an IP address or hash in a threat intelligence repository.

While MDR for SIEM does not include response capabilities such as host isolation, we do enhance and simplify the investigation process through targeted TAPs that automatically apply themselves into alerts in ZTAP.

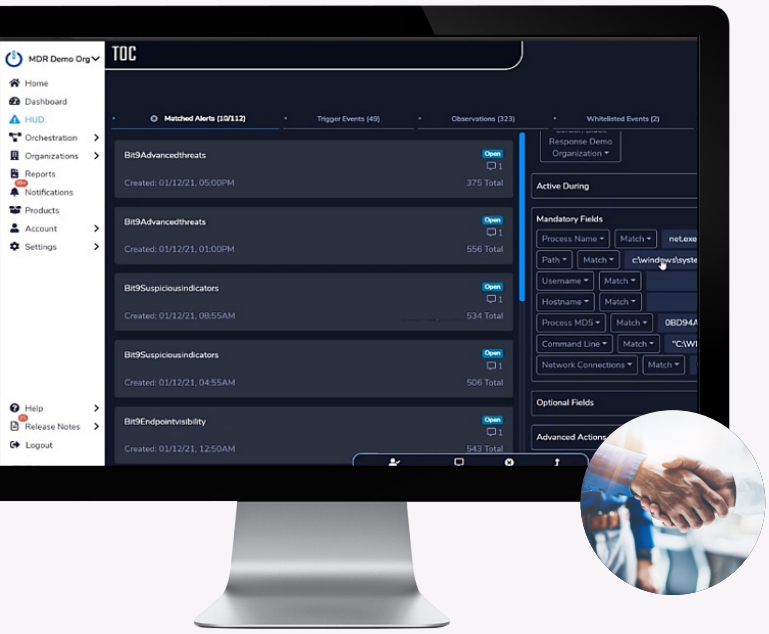
HOW WE DO IT

ADDING PLAYBOOKS

If we determine that an event was expected by the customer, and therefore good, the Critical Start analysts will update the TBR with an additional playbook to auto-resolve the alert as a false positive. Our analyst will work with customer security teams to determine the Key-Value pairs that will confirm this event is known good. In the example above, if the Process Name is run from a known good Path, with a known Username and Hostname, then this is known good and a false positive to be automatically resolved.

By using the capabilities of the customer's solution we can add more granular Key-Value pairs. Continuing with our example, net.exe must have a confirmed MD5 Hash, a confirmed Command Line argument and there must be no corresponding Network Connections. In the future, all seven variables must be a match for the playbook to automatically resolve this alert.

Before we add a new adapted playbook to the TBR, Critical Start enforces a two-person integrity system. Any customer or Critical Start analyst can create and save a playbook. However, we require a second set of eyes to perform the same investigation to validate the playbook before deploying it.



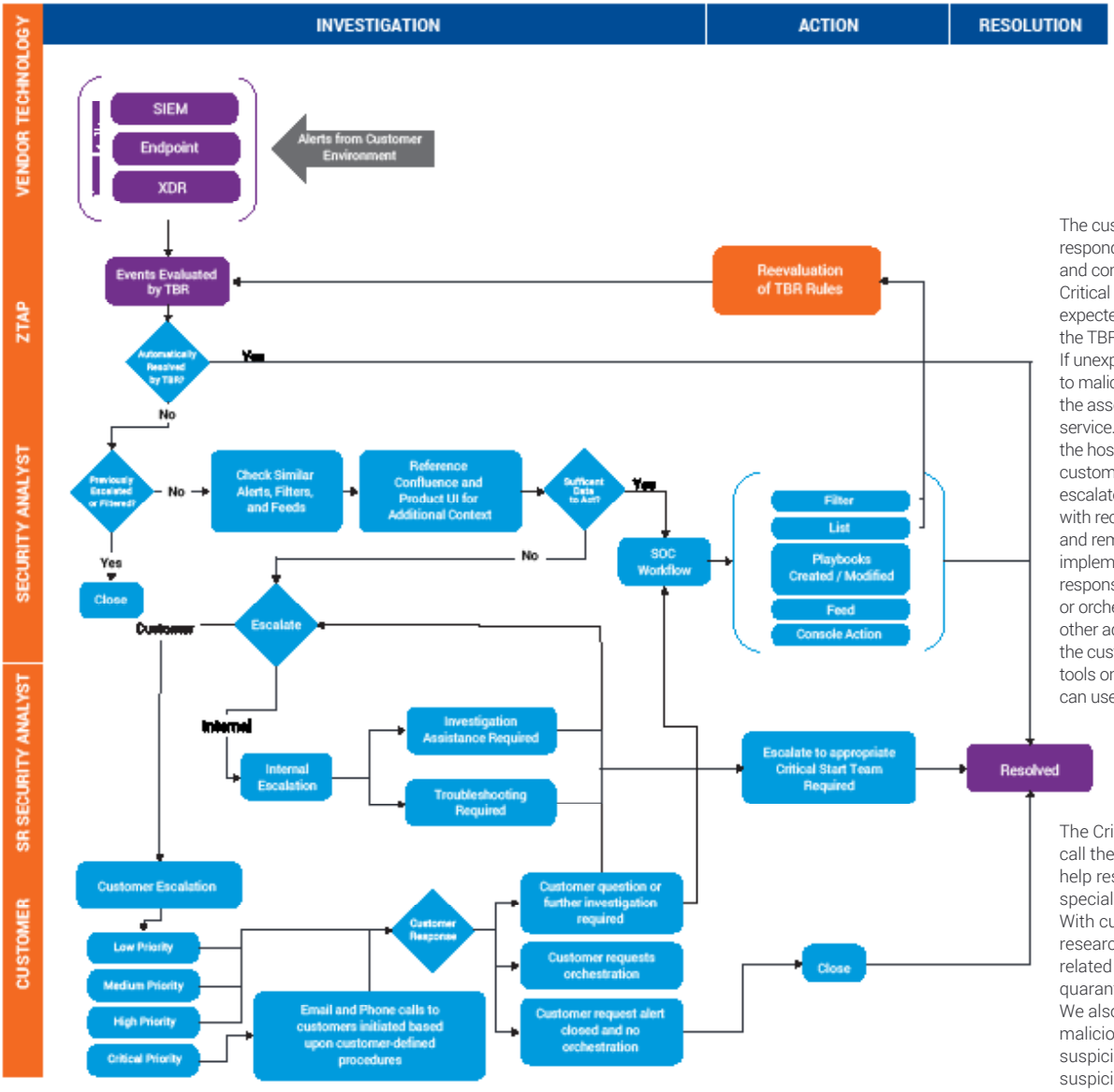
PLAYBOOK VALIDATION

The Playbook Validation function shows how many alerts and security events will be resolved by the new playbook. If we created a playbook to resolve a single event, and we see multiple other events that will be resolved, we know the playbook lacks granularity. On the other hand, a playbook that resolves multiple alerts can serve as a force-multiplier that extends our auto-resolution coverage.

HOW WE DO IT

INVESTIGATION AND ESCALATION

This diagram displays the decision tree for alert investigation and resolution. Alerts are ingested into ZTAP where they are analyzed by the TBR. If an alert matches the Key-Value pairs in a TBR playbook, it is automatically resolved. If it does not, it is unknown and sent to the Critical Start SOC for triage and investigation. If the SOC determines the alert is good, we update the TBR and resolve the alert. If the alert remains unknown the Critical Start SOC escalates to the customer, in accordance with the established SLAs.

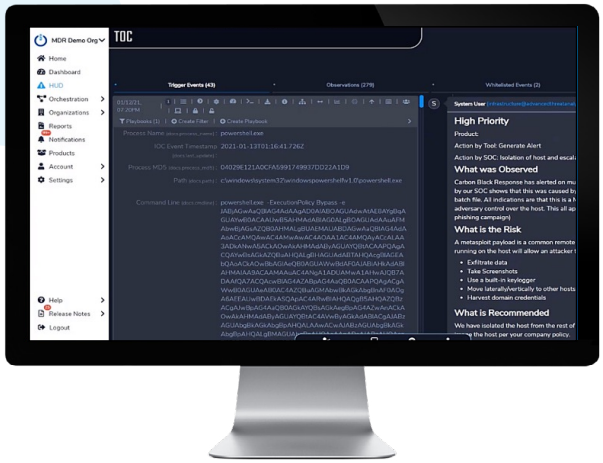


The customer is responsible for responding to escalated alerts and comments. They inform the Critical Start SOC if the event was expected. If expected, we update the TBR and resolve the alert. If unexpected and determined to malicious, we check to see if the asset is in scope of our MDR service. If in scope, we isolate the host and escalate to the customer. If out of scope, we escalate the alert to the customer with recommendation to isolate and remediate. With SIEM implementations, our SOC's only response actions are to escalate or orchestrate. They cannot take other admin actions. However, if the customer has other partner tools on their endpoints, our SOC can use those to take action.

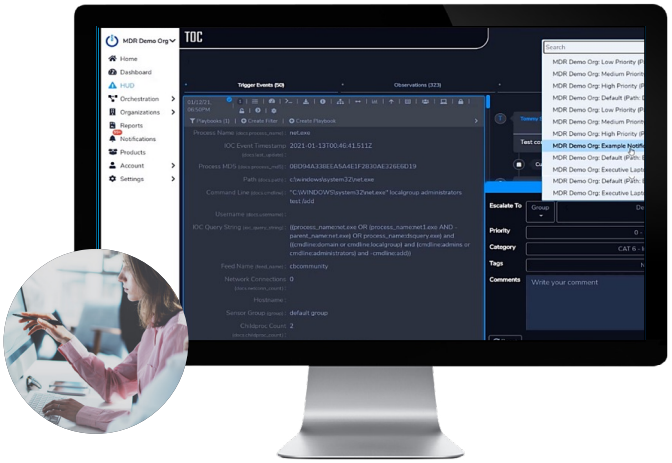
The Critical Start SOC will call the customer directly to help resolve critical, high, and special consideration alerts. With customer agreement, we research additional information related to the alert and if possible, quarantine any infected devices. We also advise on removing malicious files, terminating suspicious processes, blacklisting suspicious domains, terminating network connections, and more.

HOW WE DO IT

COMMUNICATION AND COLLABORATION

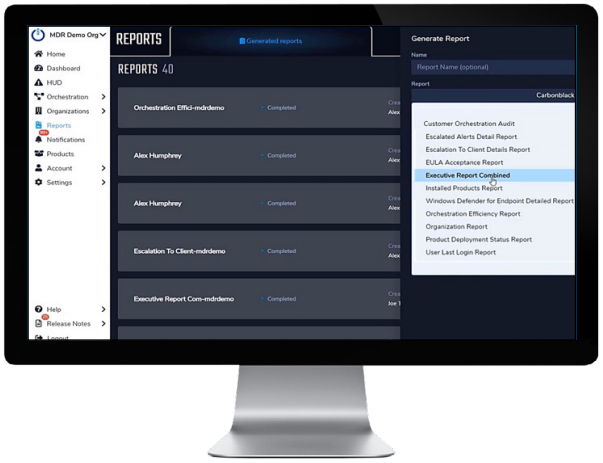


ZTAP was built to be the single portal for analysis, response, and escalation. The Critical Start SOC shares investigation information and comments through ZTAP. We assign a priority to the alert, share what was observed, the risk and recommended actions.



ZTAP provides audit logs of actions taken and by whom, for complete transparency on who is affecting the customer environment. With ZTAP, we create granular notification schedules on who an alert is escalated to and under what circumstances. Escalations can be to multiple groups or to an organization higher or lower in the security management hierarchy.

REPORTS



ZTAP can generate reports or run scheduled reports that query data relevant to the customer environment. Generated reports are reports that run on demand. Simply select any predefined report, date range, the organization, and then run the report. Reports can be emailed or downloaded from the ZTAP platform.

Scheduled reports can be configured to run daily, weekly, monthly, quarterly, and annually. Select any predefined report, the frequency of the report, the date range, the organization and then save. Reports can be emailed or downloaded from the ZTAP platform.

HOW WE DO IT

ORCHESTRATION

The Orchestration page accesses the Trusted Behavior Registry. It provides visibility into what is being applied to the customer environment, including global playbooks specific to the tools being monitored and adapted playbooks we have personalized for your organization. The Orchestration page provides access to:

FILTERS automatically categorize and resolve security events that have been previously investigated. Filters use Key- Value pairs to identify known good behavior. It automatically resolves future security events that match the logic created in the filter

PLAYBOOKS are used to route events that do not require direct investigation and escalation but should still be logged and seen by the customer organization. Playbooks allow for automatic actions to be taken on an event, such as adding comments, escalating the alert to an individual or Notification Group, and setting a schedule for when the Playbook is active. This allows the customer to maintain visibility into the traffic in their environment while reducing the number of alerts that require investigation.

Much like Filters, Playbooks use key/value pairs from security events to identify known good behavior and automatically resolve future security events.

LISTS are often referred to as either Whitelist or Blacklist. They are a key feature of orchestration within ZTAP. Lists evaluate items by their individual hash values rather than key/value pairs. Lists identify very specific files or processes. Individual hash values must be explicitly added to Lists by a user. Lists evaluate and categorize the events that match within ZTAP. Lists act as either a Tier 3 Filter (Whitelist) or Tier 1 Filter (Blacklist) that will recategorize any future events with the same hash value. Whitelisted events that are potentially related to an alert will still be shown in the Whitelisted Events tab.

Lists can utilize the APIs of the associated security tools to send a hash value to the tool's console. For example, when you create a new whitelist entry for the target file hash of a threat-quarantined event, the List entry is reviewed and activated. The event is evaluated and categorized within ZTAP and the hash is sent to the Global Whitelists so that the tool will also recognize the whitelisted hash. This is only available for products with an API that supports this functionality.

New List entries are added to the Whitelist by default. After creation of a new List item, you can modify the entry to add it to the Blacklist within ZTAP. For products that do not have a Blacklist API, this will behave similarly to a Tier 1 Filter. It will bypass any other Filter logic and create an Alert when an event with that hash is observed.

FEEDS are an important component of the Orchestration features in ZTAP. A Feed is an element that can be used in a Filter or Playbook to replace the value in a key/value pair with a list of one or more static values. Feeds allow more easily creation of Filters and Playbooks based on longer lists of known information such as server names, expected users, in-house applications, expected connections and other data. Using a Feed instead of individual values in a Filter or Playbook allows you to edit the values within the Feed without deactivating the associated Filters or Playbooks to edit the values.

HOW WE DO IT

ORGANIZATIONS

The Organizations screen presents information about how the customer organization is managed. It includes users and access permissions. Organizational Notes are kept and updated for special procedures, escalations, contacts, and other information that are relevant to the business environment. They guide authorization for response, unique escalations, and communications that may be required in specific scenarios for the organization.

From this screen, customers can manage their primary Organization and any child Organizations that have been created. A primary Organization is configured by Critical Start when the MDR service becomes active.

NOTIFICATION GROUPS

Notification Groups allow for creating groups of users that can be specified to receive email and in-application notifications for different events, such as new alerts and escalations. Multiple Notification Groups can be created, based on the needs of the organization. In addition, schedules can be configured so that users who work at different times will only receive notifications during their working hours.

We can also create individual Escalation Paths. An Escalation Path is a container with its own set of unique Notification Groups. We use Escalation Paths to route events more easily to specific individuals or teams using Playbooks.

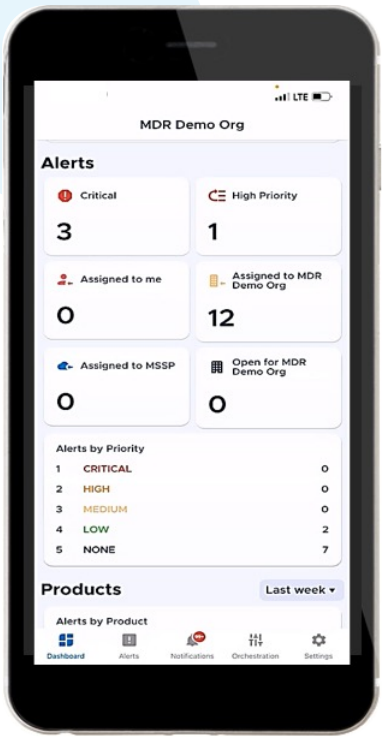
HOW WE DO IT

MOBILESOC

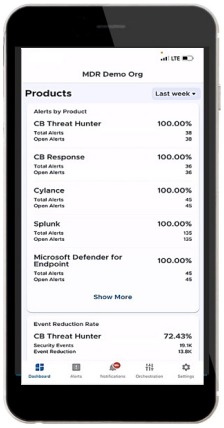
ZTAP is accessible through Critical Start's MobileSOC. It provides the full capability to investigate and respond to alerts directly from a mobile device. MobileSOC provides an immediate view of the customer environment. SOC escalations are sent directly to a mobile device, along with visibility into every alert. MobileSOC provides access to all APIs built into the platform and a direct line of communication to the Critical Start SOC.

Our mobile interface lets security teams communicate with our SOC without being tethered to a desk and collaborate remotely with full audit trails. Our SOC analysts provide guided response and this team may also be able to take response actions with other supported security solutions on your behalf.

MobileSOC can be deployed in minutes via our cloud-hosted platform. It is available for Android and iOS mobile devices.

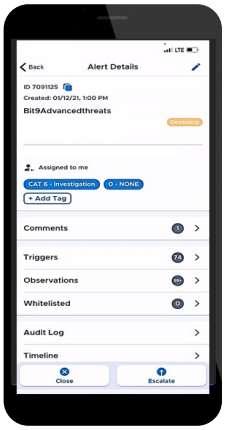


Using MobileSOC, customers can validate Critical Start SLAs and view our Time-To-Detect and Median-Time-To-Respond performance. Security teams can view all alerts in the organization, as well as get a quick glimpse of what the Critical Start SOC is asking them to do.



MobileSOC reports on each of the Products (security tools) the customer is using – How many total alerts and how many open alerts.

MobileSOC reports on the efficiency delivered by Critical Start's MDR service. It reports on the event reduction rate (the number of events automatically resolved using TBR playbooks), the efficiency for each tool, and the overall efficiency.

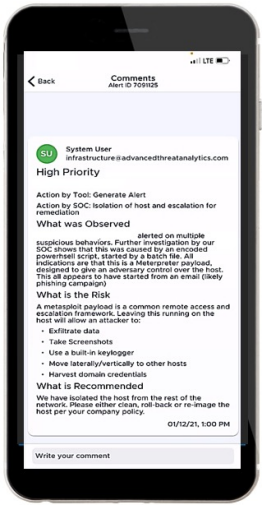


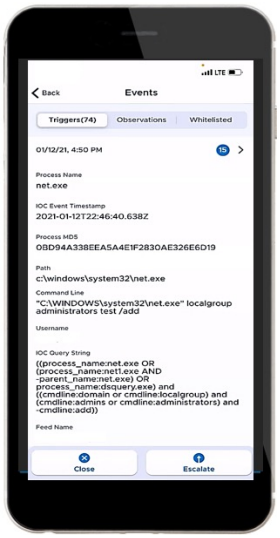
MobileSOC provides details on specific alerts. It displays Triggers, events that went through the TBR and could not be automatically resolved, and Observations, events that were automatically resolved by the TBR.

HOW WE DO IT

COMMENTS

The most common place for the security team to start is in Comments. It provides details on why an alert has been escalated, including the priority of the alert assigned by the Critical Start SOC, what was observed, the risk, and recommended actions. All communication and collaboration between the customer and the Critical Start SOC are supported within this screen.





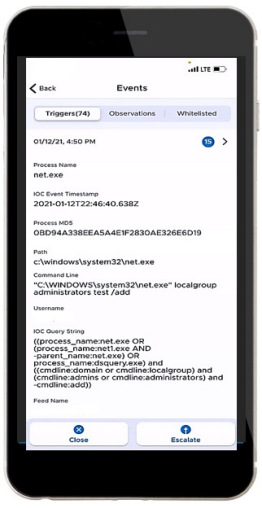
TRIGGERS

Trigger events are events that need to be responded to. The Triggers screens enables the customer to take meaningful action on an escalation. Every trigger event can be investigated from MobileSOC. It provides a view of all Key-Value pairs inside an event.

THREAT ANALYSIS PLUG-INS

MobileSOC provides direct access to supported security tools in the customer environment using Threat Analysis Plug-ins (TAPs).

For SIEM, Triage TAPs allow security teams to access more information from their security tools. For example, identifying parent processes.



HOW WE DO IT

CORTEX XSOAR AND SERVICENOW INTEGRATION

The Critical Start ZTAP bi-directional integration with Cortex™ XSOAR and ServiceNow® provides a single pane of glass for your SOC, allowing you to respond to incidents with speed and at scale—without the need to learn a new workflow or console.

CORTEX
BY PALO ALTO NETWORKS

Cortex XSOAR is a comprehensive security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration and threat intel management to serve security teams across the incident lifecycle.

Alerts from our Zero Trust Analytics Platform (ZTAP) are escalated by our SOC when end user action is required. This integration allows Cortex XSOAR to poll for these escalated alerts from ZTAP and add them as "ZTAP Alert" incidents in XSOAR so those alerts can be viewed and commented on directly from XSOAR.

Key features of the XSOAR integration include:

- ✓ When an alert is escalated, an XSOAR incident is created with all event details.
- ✓ Direct linking to the alert/incident in Cortex XDR for additional investigation.
- ✓ A customer can take actions, such as those listed below, directly in XSOAR, and they will be synched with ZTAP.
  - Add a comment, re-escalate back to Critical Start
  - Add a comment to the incident
  - Close the alert

servicenow

ServiceNow™ is a workflow automation platform that enables enterprise organizations to improve operational efficiencies by streamlining and automating routine work tasks.

The Zero Trust Analytics Platform (ZTAP) app synchronizes ServiceNow and ZTAP cases easily and conveniently so that the case management teams can quickly communicate in one place, instead of context switching from different consoles.

Key features of the ServiceNow integration include:

- ✓ Address critical incidents in real time via ServiceNow, while maintaining context in ZTAP
- ✓ Immediately synchronize updates made in ServiceNow to the corresponding alert record in ZTAP
- ✓ Restore service, mitigate threats and reduce noise without leaving the ServiceNow interface
- ✓ Use ServiceNow business logic to give access to case workers, as needed, without having to grant access to ZTAP

HOW WE DO IT

THE CRITICAL START SOC

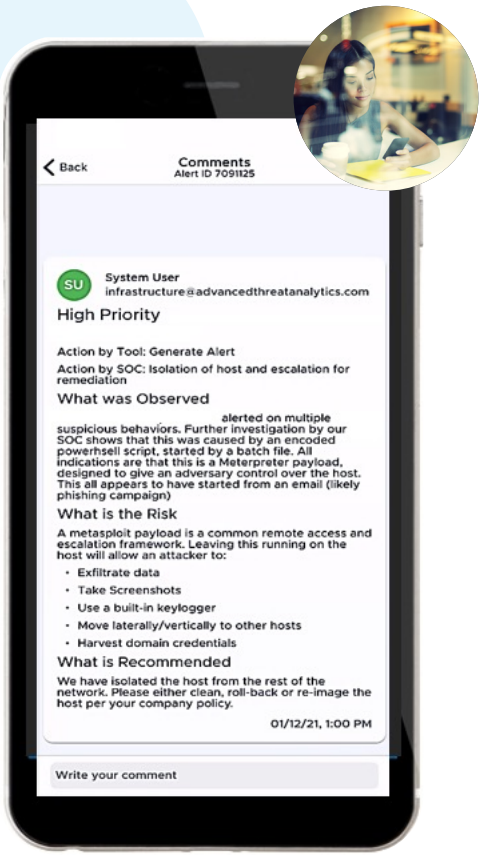
The Critical Start SOC is staffed with experienced security analysts. They undergo 300 hours of on- boarding training and are required to take an additional 60-80 hours of training annually.

Our MDR service is based on high touch to deliver customer satisfaction. Our SOC analysts triage and investigate unknown alerts that are not auto resolved by ZTAP and the TBR. They start off by determining the scope of the problem to build a full narrative of the threat – Is it just one host? Are other hosts impacted? What is actually happening?

Next, the Critical Start SOC begins the communication and collaboration process through ZTAP and MobileSOC. Based on their investigation, they assign a priority to the alert, what was observed, an assessment of the risk and recommended actions. Customers continue to communicate in real-time through comments.

Following investigation, The SOC will call the customer direct to help resolve critical, high, and special consideration alerts. We use a notification hierarchy defined in ZTAP Notification Groups during the on-boarding process.

With SIEM implementations, our SOC's only response actions are to escalate or orchestrate. They cannot take other admin actions. However, if the customer has other partner tools on their endpoints, our SOC can use those to take action.

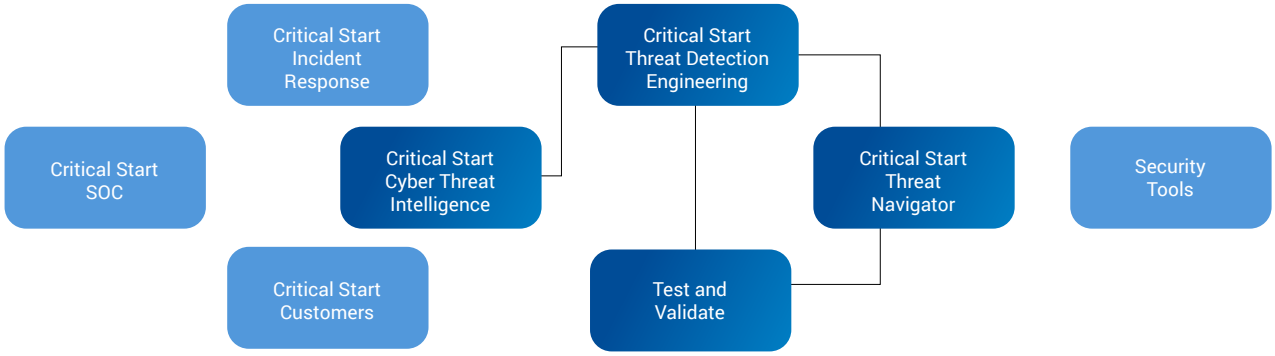


The Critical Start SOC operates under 1 hour Time-To-Detect and Median-Time-To-Resolve SLAs. These metrics are fully transparent on the ZTAP dashboard.

HOW WE DO IT

CYBER RESEARCH UNIT

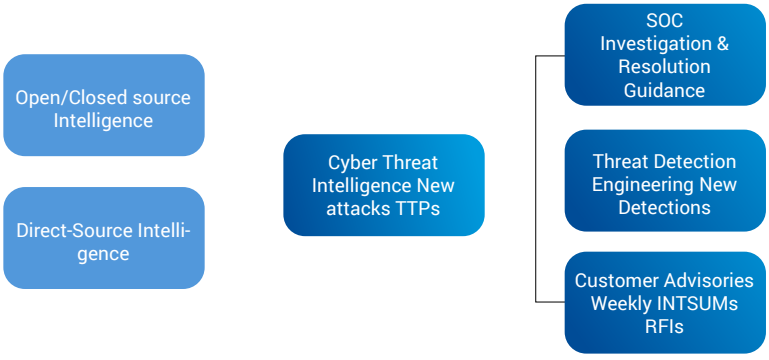
Effective SOC operations rely on effective detection management. The Critical Start Cybersecurity Research Unit (CRU) combines threat intelligence, detection engineering and the MITRE ATT&CK® framework to deliver effective detections to supported security tools. The CRU increases visibility across the attack surface area and generates actionable alerts that support efficient and effective investigation and response.



Critical Start Cyber Threat Intelligence Analysts utilize our visibility in ZTAP and Incident Response engagements to continuously build our knowledge on the rapidly evolving threat landscape. Critical Start Threat Navigator pulls in existing detections from security tools and displays them against the MITRE ATT&CK framework to help our Threat Detection Engineering team assess and optimize security tool coverage. This team enhances or creates new detections, then tests and validate the detections. After this testing and validation, Threat Navigator automatically pushes out the detections to our customers' security tools.

THE CYBER THREAT INTELLIGENCE TEAM

The Cyber Threat Intelligence (CTI) team is an essential component of detection management. This team researches and reports on new threats and suspicious TTPs requiring Critical Start and customer action.



The CTI team subscribes to paid and open-source threat intelligence feeds to collect and curate threat data. After researching new attacks and TTPs, they feed this data to the Threat Detection Engineering team to develop new detections.

The CTI team assists and provides investigative guidance to our SOC team. They also keep our customers up to date with their findings through security advisories, weekly Intelligence Summary reports, and customer requests for information.

HOW WE DO IT

CRITICAL START® THREAT NAVIGATOR

With the information provided by the Cyber Threat Intelligence team, Threat Detection Engineering evaluates existing detections and identify gaps in coverage for the new attack.

They use the Critical Start Threat Navigator as a framework to identify the gaps in detection coverage. Threat Navigator is a tool integrated within ZTAP. It is based on the MITRE ATT&CK framework. It provides a comprehensive view of the attack surface area and the TTPs used by threat actors.

Threat Navigator starts by pulling existing detections from your security tools. (Shown in purple). Critical Start Threat Detection Engineering evaluates the out-of-the-box detections identified by Threat Navigator. They evaluate the scope of the detections. Are they broad enough? Do they provide enough detail for effective SOC investigation? Do they work? Based on their assessments, they will enhance the detections. (Shown in green). Threat Detection Engineering also determines what new detections are needed.

The Cyber Threat Intelligence team uses Threat Navigator to determine additional information they need to research with new attacks.

NOTE: The information presented in Threat Navigator is dependent on the TTPs used in an attack and the security tools used.

CRITICAL START THREAT DETECTION ENGINEERING TEAM

The Threat Detection Engineering team applies Critical Start threat intelligence and Threat Navigator to identify gaps in detection coverage. They enhance existing out-of-the-box detections by adding to their scope or adding more context and detail to support SOC investigation. They will build new detections to fill gaps in coverage.

Enhanced and new detections are pushed out to tenant development environments where the Threat Detection Engineering team will emulate the attack to see if ZTAP has everything it needs to support investigation and resolution. The new and enhanced detections are pushed out to the customer to build up the TBR to detect and resolve any new false positives. Threat Navigator will then push out and synchronize the new and enhanced detections to all Critical Start customer security tools.

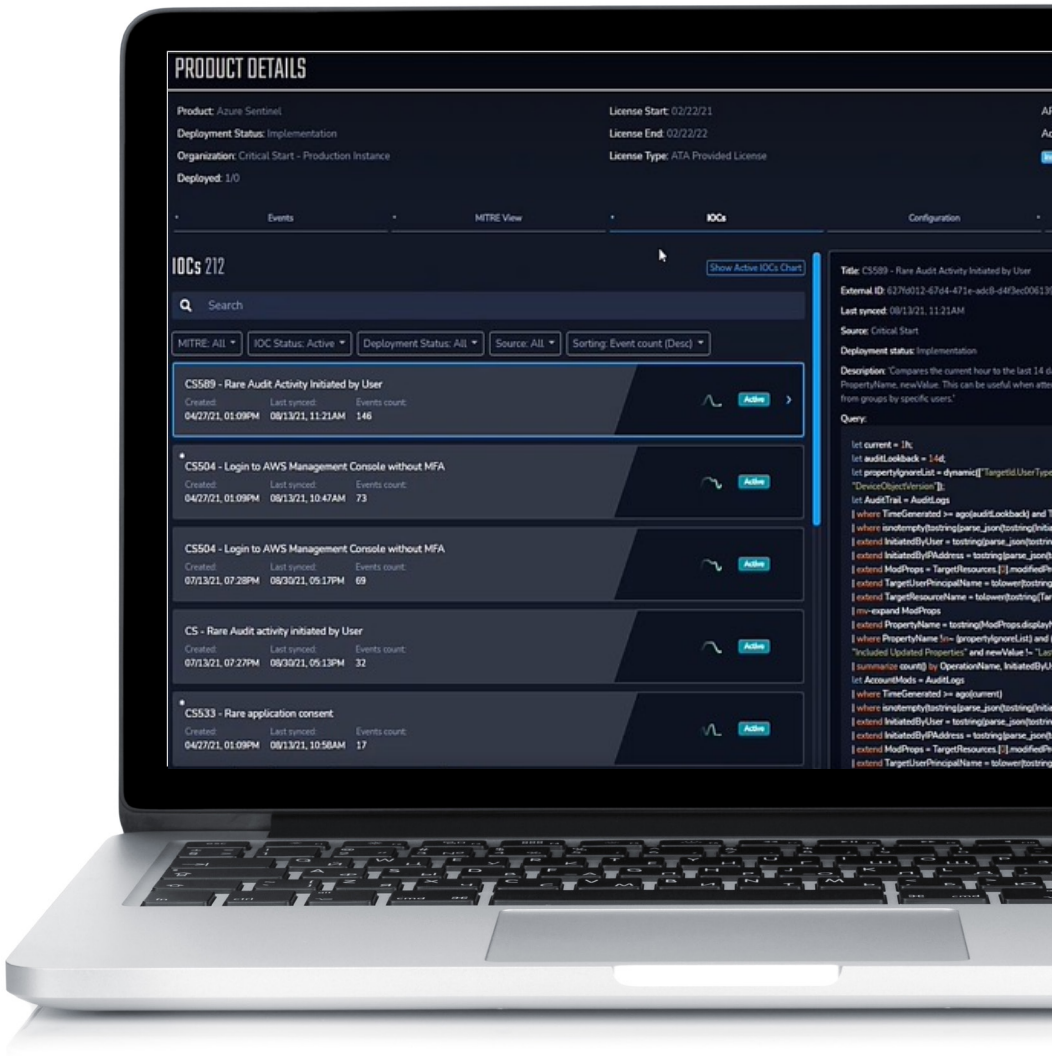
HOW WE DO IT

TRANSPARENCY THROUGH THREAT NAVIGATOR

Transparency is a core value of Critical Start's MDR service. It is important to us that we prove our value to our customers. With Threat Navigator, our customers see what our detection engineers see. Threat Navigator provides a view the coverage delivered by your security tools and gaps in your defense. This can be helpful when considering other security investments

.

Threat Navigator also provides a view of the threat intelligence researched and curated by our Cyber Threat Intelligence team. Customers can view the out-of-the- box detections and compare them to Critical Start detections to see the exact queries/rules we have created to enhance existing detections and to see the new detections we have created.



HOW WE DO IT

ONBOARDING AND IMPLEMENTATION

A dedicated Critical Start project manager will kick off and manage the onboarding and implementation process. Critical Start Implementation Engineers provision ZTAP. We baseline the customer environment, adapt ZTAP playbooks to their specific needs and tune out false positives.

The Implementation Engineer works with the customer and their vendors to help onboard customer data, deploy detection content and integrate with ZTAP. We also apply Critical Start-developed IOCs to enhance threat detection from the security tools.

During this process, frequent touchpoints take place between Critical Start analysts and the customer to confirm playbook creation and content.

NOTE:We are a bring-your-own-license operation. The customer is responsible for installing software and spinning up VMs.

Critical Start **Onboarding**

Timeline

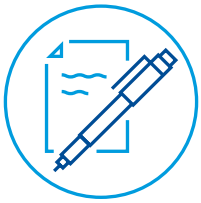
Our onboarding process is approximately 4-6 weeks.

Management

Led by our project management team, we identify key personal roles, responsibilities, and permissions, as well as holding weekly touch point meetings.

Connection

We connect our SOC platform directly to your SIEM tool, then we begin ingesting data. You can expect an approximately 90% reduction in false positives in the first day.



Policies

We define detection & prevention policies.

Fine-Tuning

Over the remaining time, our team will fine-tune what your organization designates as “Trusted Behavior” to build your own TBR. This happens as we are identifying risk/ alerts and responding to them in communication with your technical team.

ZTAP AND THE TBR

KICKOFF

Critical Start welcome letter sent to the customer main point of contact. → A service questionnaire is sent to the customer to be filled out prior to the kick-off call. → Technical scoping calls are held with the customer to finalize project scope. → Critical StartProject Manager creates a project plan. → The Critical Start Project Manager schedules and conducts a kick-off call with the customer.

We cover:

- ✓ Review of project documents
- ✓ Executive summary of the engagement
- ✓ Scope of the project and services contracted
- ✓ Set meeting and communication cadence
- ✓ Next steps

PROVISIONING

- ✓ Critical Start assists with the provisioning of the product console/tenant where applicable.
- ✓ Critical Start provisions ZTAP organization and integrations.
- ✓ Critical Start applies best practice security polices and product configurations to the console/tenant.
- ✓ Critical Start applies our proprietary IoCs (Indicators of Compromise) to data ingested into SIEM tools.

TUNING

Critical Start conducts filtering and tuning of SIEM security tool alerts.

Critical Start works with the customer on tuning alerts and escalations.

Critical Start applies TBR global playbooks at the time of integration. Customers typically see an immediate event reduction through elimination of false positives. After initial integration, Critical Start analyzes events in ZTAP to further enhance event reduction by eliminating duplicates and false positives. From there, Critical Start will build out customized filters, playbooks, lists and feeds for the customer's unique environment.

When on-boarding is completed, with customer acceptance, Critical Start turns on 24x7x365 monitoring and begins the process of reducing risk acceptance to your organization.

THE CUSTOMER SUCCESS TEAM

To uphold our commitment to one of our founding principles that customers come first, we have designated a team of Customer Success Managers (CSMs) devoted to helping the customer achieve their security goals. Each CSM serves as a trusted advocate and Critical Start's primary point of contact to ensure the customer is receiving the tools and support needed for continued success. A few core functions of the Customer Success Manager team include:

CUSTOMER ADVOCATE. As an effective advocate for the customer, the team represents their interests, needs, and goals to meet and exceed expectations. This involves consistent engagement and holding meetings with key stakeholders. As a representative of the customer's perspective, they share their feedback for key internal business decisions and serve as a conduit for feedback into future product development. We use data collection via online Customer Satisfaction (CSAT) and Net Promoter Score (NPS) surveys to further identify customer needs and preferences.

ADOPTION. The CSM team will continuously work with the customer to facilitate successful adoption and ensure satisfaction. We make sure the customer is aware of new product releases and how they will help their organization. Although self-paced ZTAP training is available, the team is skilled in the use of ZTAP to personalize the training experience for the customer and their security teams. Whether training is for a refresh or a new staff member, the CSM is available to take training to the next level.

PROACTIVE PROBLEM RESOLUTION. Customer Success Managers are adept problem-solvers and coordinate the appropriate internal resource engagement to resolve any concerns. In addition, by focusing on trends the team works to proactively uncover potential problems to prevent future issues. In the event the customer needs additional attention on a particular request, we also partner with the customer to escalate any issues in need of a resolution.

MAXIMIZING VALUE. The CSM team is the customer's ally to align Critical Start with their business objectives to ensure value delivery. By guiding the customer to the desired outcomes and maximizing derived value from partnering with Critical Start the CSM team serves as a catalyst to success. To achieve these results, the Customer Success Management team consistently demonstrates the value of our products and services and how they positively impact the customer's organization.

TRAINING. Critical Start provides self-paced on-line training courses to our customers. The ZTAP Overview Part 1 and Part 2 courses provide training on the Zero Trust Analytics Platform (ZTAP) in separate short videos. The videos cover ZTAP capabilities, navigation, and usage.

ZTAP Overview Part 1 introduces users to:

- ✓ Navigation
- ✓ Home Page
- ✓ Dashboard
- ✓ Organization
- ✓ Notification Groups
- ✓ Reports
- ✓ Snippets
- ✓ Account
- ✓ Settings

ZTAP Overview Part 2 covers:

- ✓ Heads-Up Display (HUD)
- ✓ Event Tiers
- ✓ Orchestration
- ✓ Filters
- ✓ Playbooks
- ✓ Lists
- ✓ Feeds

In addition, the Critical Start Project Manager coordinates and schedules hands-on customer training. The Critical Start Analyst provides an in-depth training on the ZTAP console and a MobileSOC application training session.

CUSTOMER SUPPORT

Critical Start Support goes beyond assisting with our platform and technology, with L1 and L2 support for in-scope technology partner tools.

STREAMLINED INCIDENT RESOLUTION. Our goal is to streamline support for fast resolution and maximum availability. Our support team manages incidents and outages—including partner tools—from beginning to resolution, so our customers avoid the pain of bouncing back and forth between multiple vendors. This team includes Technical Support Engineers— subject matter experts, trained and certified on the tools we support.

COORDINATION WITH PARTNERS. To expedite the incident resolution process, we have a direct line with a named contact for our technology partners. We don't wait in line on a 1-800 number.

We work with our technology partners to develop a Critical Start incident response plan that is adapted to theirs to ensure maximum efficiency and fast resolution. This plan defines severity and priorities, and identifies all Critical Start stakeholders needed for resolution, including our SOC, Product Development, Customer Success, and Senior Management teams.

Our technology partners provide information on incidents, outages, and resolutions to Critical Start Support. We take ownership and communicate with our customers to keep them informed on the status of their incident, while providing guidance on any steps they need to take to resolve the problem.

CUSTOMER HELP CENTER. The Critical Start customer help center provides a single source of information, so our customers don't need to access multiple portals. The help center also includes a knowledge base with up-to-date answers to frequently asked questions about our products and services.

CAPABILITIES CHART

Key Capabilities & Features:

MDR Service for Security Information and Event Management (SIEM)

PLATFORM HEALTH & CONFIGURATION
✓ Architecture review of your existing configuration
✓ Health reporting for Supported Data Sources
SECURITY ALERT MONITORING, INVESTIGATION & ESCALATIONS
✓ Monitoring and support for Supported Log Collectors
✓ Detection personalization specific to your business, network appliances and users
✓ Review of every security alert generated by SIEM tool
✓ Playbook orchestration & alert routing to appropriate groups or users
✓ One-hour SLA for Time to Detect (TTD) and Median Time to Respond (MTTR) with security alerts
✓ Investigation
✓ Ability to take response actions on your behalf with supported security solutions
DASHBOARDS, REPORTS & EXTRAS
✓ Alert enrichment with details about IPs, hashes and domains to provide additional context
✓ Data onboarding and dashboards/app implementation for Supported Data Sources
✓ Installation of vendor-supported apps for common security vendors' dashboards and reports