SOLUTION QUICK CARD

Critical Start Response Authorizations

Managed Detection and Response, Your Way

KEY BENEFITS

- ✓ **Start with industry best practice default rules** for common response actions.
- ✓ **Gain full visibility** into how Critical Start responds to alerts in your environment.
- ✓ **Tailor response actions** with an easy-to-use form that gives you flexibility and control.
- ✓ **Maximize your team's productivity** by offloading response actions to Critical Start's MDR experts.
- ✓ **Only respond to the alerts that need your attention.**

Too many Managed Detection and Response (**MDR**) providers expect your environment to fit neatly into their idea of what detection and response should be. At CRITICAL**START**®, we know that the cookie-cutter approach doesn't work. Our job is to make detection and response easier for your organization so that your team is only alerted when required. That means you need transparent, customizable Rules of Engagement that work for your unique organization.

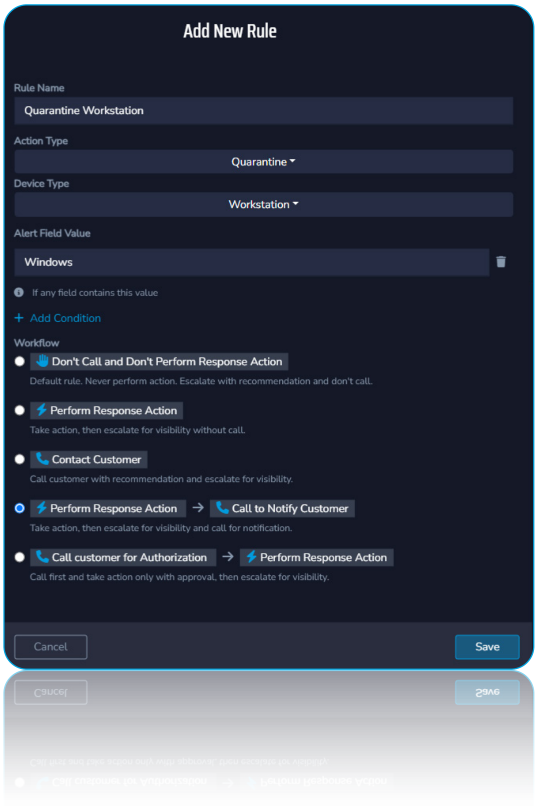
Critical Start response authorizations give you control over your rules of engagement, making it easy for you to see – and change – how Critical Start responds to alerts in your environment. With response authorizations, you can define workflows and actions based on device type and conditional data. These rules provide a detailed guide for the Critical Start Security Operations Center (**SOC**) so that we handle your alerts in the manner that best fits your organization's needs.

How it works

Response authorizations make it easy to add, update, or remove custom Rules of Engagement. You start by either adding or updating a rule. Using the form, you select the action type, device type, and alert field value for the rule. You can add custom conditions, if desired, and you can name your rules using a convention that makes sense for your organization and team. For each rule that you add or edit, you can define detailed workflows that include:

- ✓ When the Critical Start SOC contacts your team
- ✓ Default response actions that the Critical Start SOC should take on your behalf
- ✓ Specific devices that apply for the response action
- ✓ Conditions that must be met to initiate the response action
- ✓ Multi-step operations that include response and customer contact actions

When an alert triggers your pre-defined response authorization, the Critical Start SOC follows your directions on how to respond. Additionally, our quality assurance measures apply to all investigation procedures, meaning that your response authorizations follow our two-person approval process for comprehensive analysis and accurate conclusions.



Add New Rule

Rule Name: Quarantine Workstation

Action Type: Quarantine

Device Type: Workstation

Alert Field Value: Windows

If any field contains this value

+ Add Condition

Workflow

○ Don't Call and Don't Perform Response Action
Default rule. Never perform action. Escalate with recommendation and don't call.

○ Perform Response Action
Take action, then escalate for visibility without call.

○ Contact Customer
Call customer with recommendation and escalate for visibility.

● Perform Response Action → Call to Notify Customer
Take action, then escalate for visibility and call for notification.

○ Call customer for Authorization → Perform Response Action
Call first and take action only with approval, then escalate for visibility.

criticalstart.com