# SentinelOne – EPM SOC Response Integration Guide

**Company:** SentinelOne
**Website:** https://www.sentinelone.com
**Product:** CyberArk EPM & SentinelOne Singularity HyperAutomation **Version:** Early Availability - V1.0
**Date:** January 2026

---

## Table of Contents



---

## Solution Overview

The integration between **CyberArk Endpoint Privilege Manager (EPM)** and **SentinelOne** enables SOC teams to take direct containment and remediation actions on endpoints without interrupting business operations.

Traditional XDR tools offer binary response options—either isolate the endpoint or allow it to remain online—creating operational challenges. This integration introduces **EPM SOC Response**, giving SOC teams granular control to respond precisely and proportionally.

When a SentinelOne alert is triggered, it can automatically or manually invoke an **EPM policy action** on the targeted endpoint. The policy can restrict privilege elevation, enforce MFA, or apply stricter application control, reducing attacker dwell time while preserving productivity.

---

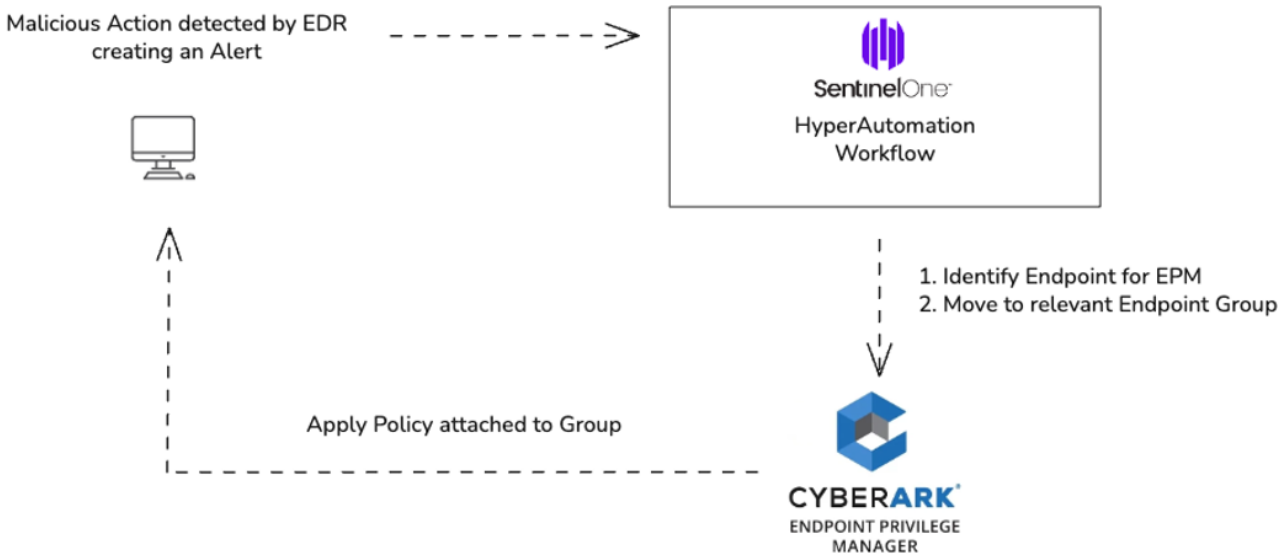
## Key Benefits

- **Accelerated incident response:** Take immediate action on SentinelOne alerts using CyberArk EPM controls.
- **Reduced business disruption:** Contain threats without isolating endpoints or interrupting end-user activity.

- **Granular control:** Apply risk-based SOC response plans that adjust to threat severity.
- **Unified SOC and IAM operations:** Combine endpoint detection and privilege management for coordinated response.
- **Streamlined automation:** Use SentinelOne HyperAutomation to automatically invoke EPM SOC Response based on alert type or risk level.

---

## Integration Description and Diagram




---

## Requirements

- CyberArk Endpoint Privilege Manager (EPM)
- SentinelOne HyperAutomation module
- SentinelOne Agent deployed on target endpoints
- Service User with API Key in SentinelOne
- Network connectivity between SentinelOne platform and EPM tenant

---

## Limitations

- Endpoint matching uses **FQDN** and **IP Address**.
- Only one active EPM SOC Response workflow per endpoint at a time.
- API key expiration may cause workflow failures if not renewed.
- Local Admins should already be removed from endpoints to enforce response actions.

---

## Installation

1. Go to the CyberArk Marketplace.
2. Download the **SentinelOne EPM Adaptive Risk Reduction package**.
3. Save the downloaded file locally for later import into SentinelOne HyperAutomation.

---

## Configuration

### Set-up EPM Policies

- Create or review EPM policies according to CyberArk Documentation.
- Define **Medium Risk** and **High Risk** Reduction Plans within CyberArk EPM application groups.

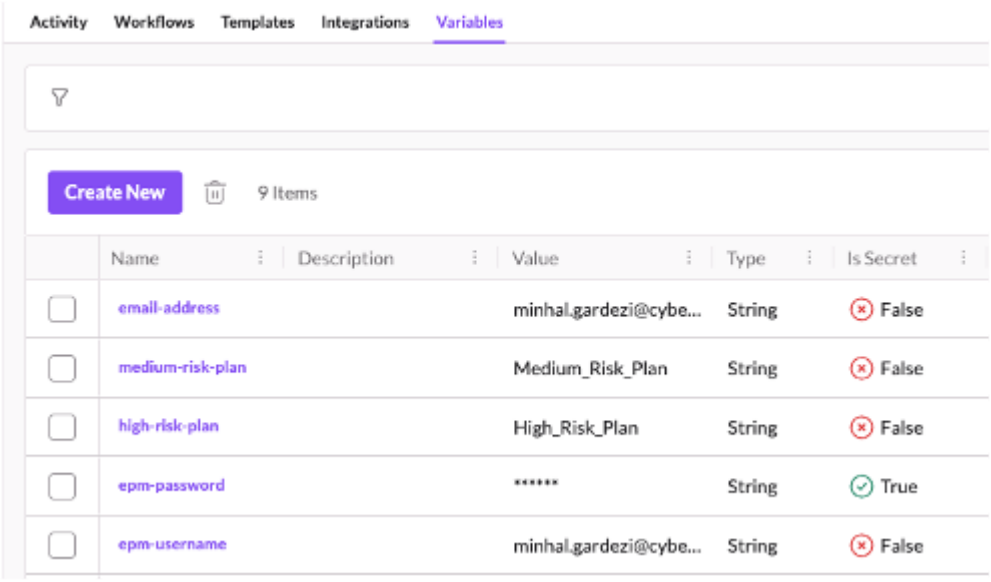
### Import SentinelOne HyperAutomation Flows

1. Open the HyperAutomation console in SentinelOne.
2. Navigate to **Actions → Import**.
3. Upload the JSON files:
    - `CyberArk EPM SOC Response Activate.json`
    - `CyberArk EPM SOC Response Deactivate.json`
4. Verify the imported flow appears in the workflow list.

### Configure SentinelOne HyperAutomation Variables

Configure these **case-sensitive** variables:

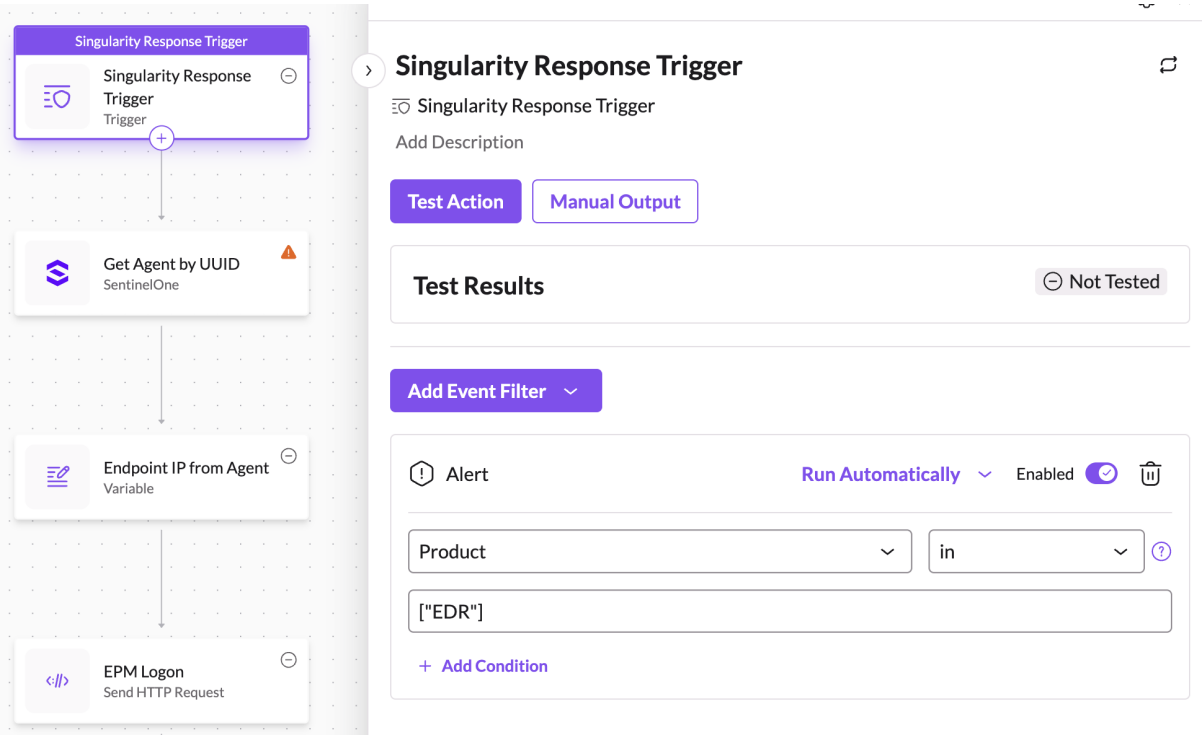
- `epm-username`: Username for EPM logon
- `epm-password`: Password for EPM logon
- `medium-risk-plan`: Name of Medium Risk Plan in EPM
- `high-risk-plan`: Name of High Risk Plan in EPM
- `email-address`: Email recipient if no endpoint is matched




### Configure SentinelOne HyperAutomation Workflow

1. Open the Singularity Workflow.
2. Open the **Singularity Response Trigger** at the top of the workflow.
    - Use the Toggle for **automatic** or **on-demand** invocation.
    - Example: Automate low/medium severity alerts; on-demand for higher severity.

- The different scenarios can be configured within the same workflow.




3. Open the **EPM Logon Node**.
4. Replace beta.epm.cyberark.com with your tenant URL.
5. Navigate to node **Get Agent by UUID**.
    - Create a new **Static Connection**.
6. In the Authentication section, we recommend creating a Service User for which the API key will be used. Steps to create Service User:

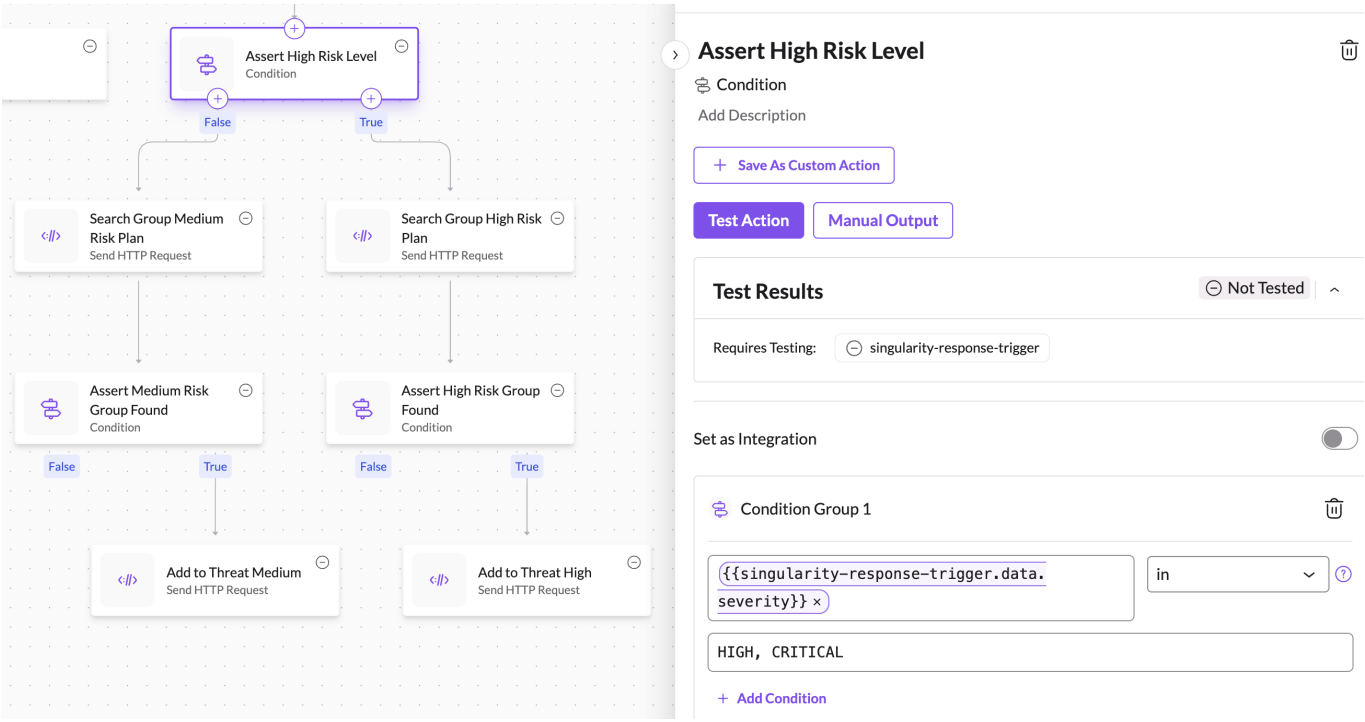
    a. Go to Policy & Settings -> Service Users and click on: “New Service User” b. Choose name, API Key expiration period and check the Account for it to cover c. Click on Create Service user and copy the display API key **NOTE:** Upon key expiration Workflow may result in error so make sure to renew it prior to expiration data
7. Enter SentinelOne tenant host and API credentials.
8. Enable workflow by clicking **Activate**.

---

## How to Use the Integration

**How to trigger the Medium or High risk reduction plan:** In this workflow, a decision point is used to navigate between Medium and High risk plans, based on input from the Alert. The shipped preset is to classify Medium and High on Alert severity, such as low and medium severity will be mapped to Medium Risk Plan and any higher value will divert to High Risk Plan. This assertion can be changed adding additional conditions, based on your specific environment and business logic. Alternatively, workflows can be

duplicated to differentiate between the Medium or High Risk Reduction Plan.




### How to trigger the response actions

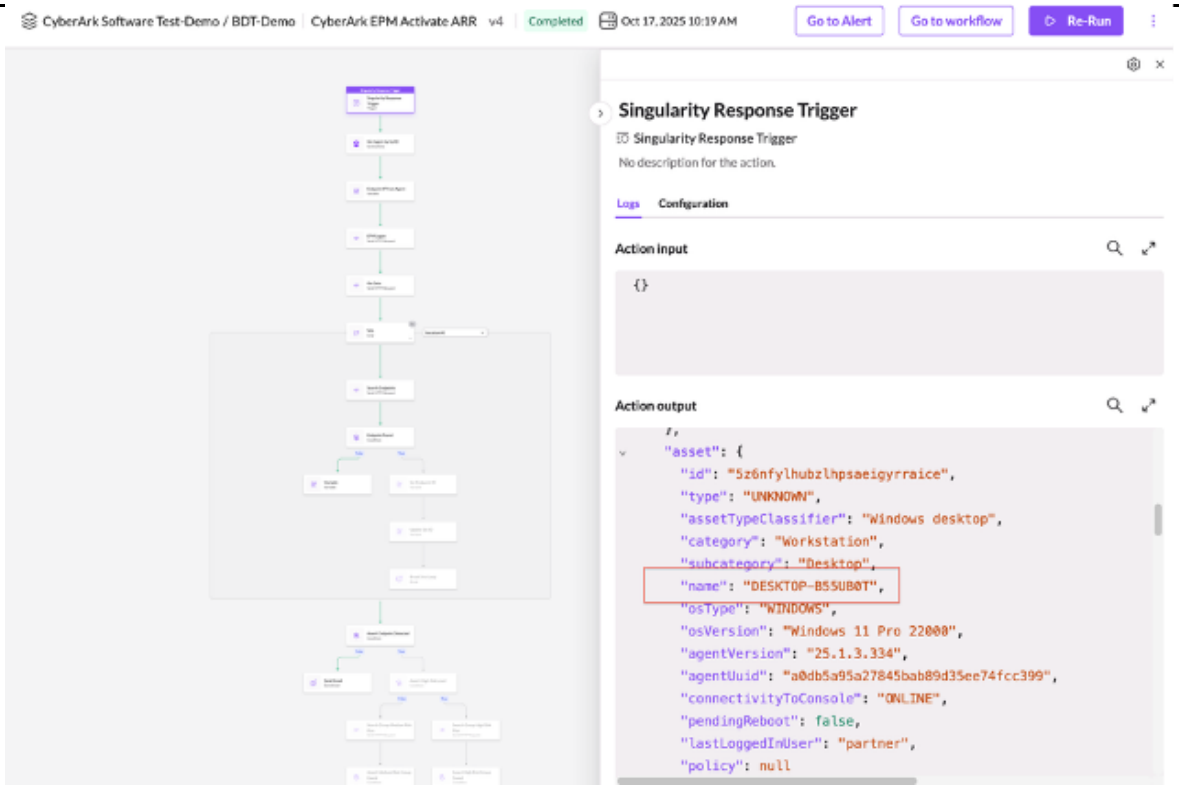
1. Open an **Alert** that you want to respond to
2. Click **Automate**
3. Open the **CyberArk EPM SOC Response Activate** workflow in “Ready” state.
4. To revert to initial policy, run **CyberArk EPM SOC Response Deactivate** workflow.
5. For completed workflows, you can explore results by clicking on “View Execution”.

---

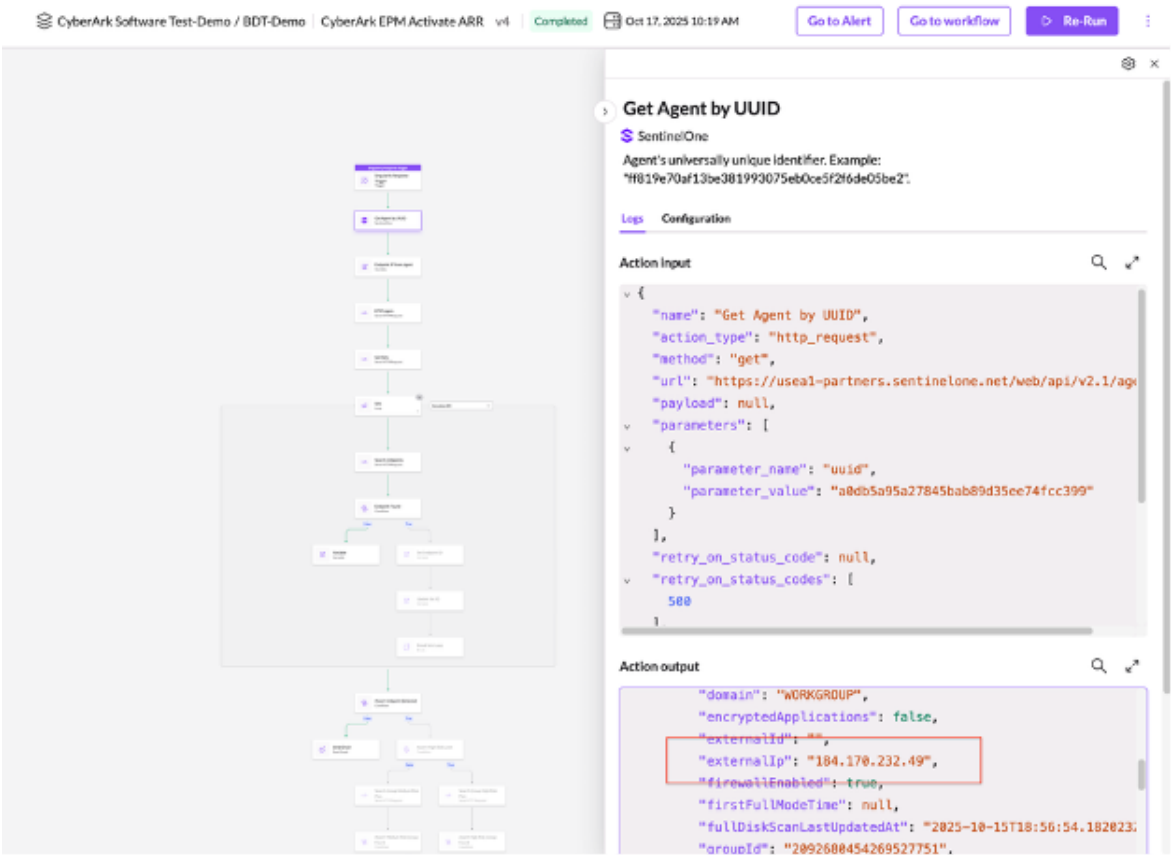
## Troubleshooting

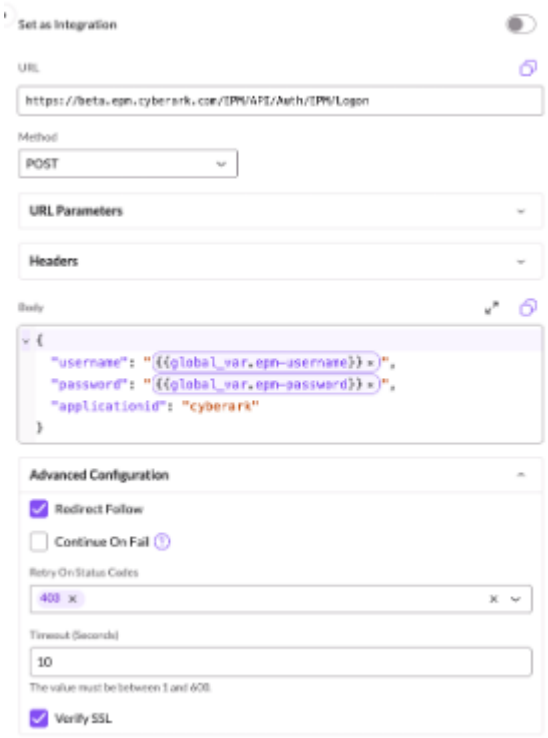
| Error | Resolution |
| --- | --- |
| No endpoint matched for Device name/IP | Verify Device Name and IP in SentinelOne and EPM You can verify these values by checking the HyperAUtomation Workflow: **Singularity Response Trigger for Device Name** |

| Error | Resolution |
| --- | --- |




**Get Agent by UUID output for External IP**



| Error | Resolution |
| --- | --- |
| 403 or 429 HTTP API errors | These errors might occur in high load environments: Try rerunning the workflow. Workflow can be configured for automatic retry on specific error codes.<br>  |

## Partner Contact Info

| Contact Type | Name | Email |
| --- | --- | --- |
| Business | Brian Carpenter (Director of Business Development) | brian.carpenter@cyberark.com |
| Technical | Business Development Technology | bizdevtech@cyberark.com |
| Support | Business Development Technology | bizdevtech@cyberark.com |