

EPM SOC Response with Palo Alto Networks

Name of Company: Palo Alto Networks

Website: <https://www.paloaltonetworks.com>

Name of Product: EPM SOC Response

Version: General Available - V1.0

Date: April 2026

1. Solution Overview

The integration between CyberArk Endpoint Privilege Manager (EPM) and Palo Alto Networks Cortex XSOAR and XSIAM enables SOC teams to contain threats without disrupting users.

Traditional SOAR and XDR responses often isolate the entire machine or run generalized remediation scripts. These methods can disrupt critical operations. The EPM SOC Response integration introduces privilege-based controls, allowing analysts to respond with precision.

When Cortex detects an incident, analysts can trigger a predefined EPM policy to block privilege elevation, enforce multi-factor authentication (MFA), or restrict application access. The integration supports both manual and automated playbook triggers to accelerate containment and reduce dwell time.

2. Key Benefits

- Accelerated incident response: Trigger privilege-based EPM SOC Response directly from Cortex XSIAM or XSOAR incidents.
 - Reduced business disruption: Contain threats without isolating endpoints or interrupting user activity.
 - Risk-based containment: Apply medium or high-risk EPM policies depending on the incident type or severity.
 - Unified SOC and IAM collaboration: Combine Palo Alto Networks detection and orchestration with CyberArk privilege control.
 - Simplified automation: Use playbooks to automate response workflows that invoke CyberArk EPM actions.
-

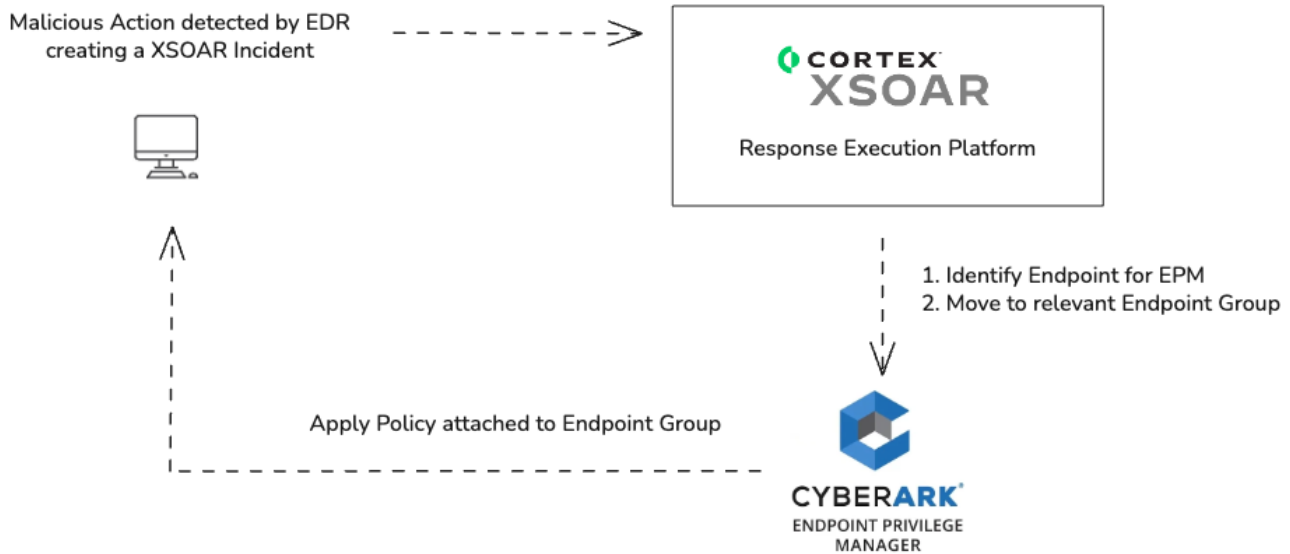
3. Integration Description and Diagram

The **CyberArk EPM Content Pack** for Cortex XSOAR/XSIAM integrates directly with Palo Alto Networks' incident response workflows.

When an alert or incident is generated within Cortex, a playbook can trigger an **EPM Response Action** to contain the threat. This response applies the appropriate EPM policy to the endpoint identified in the alert, based on parameters such as FQDN or IP address.

Integration Diagram

This integration can be applied to alerts originating from **Cortex XSIAM**, or extended to **alerts from other EDR tools** that feed into Cortex.



4. Requirements

- CyberArk Endpoint Privilege Manager (EPM)
- Palo Alto Networks Cortex: XDR, XSOAR, XSIAM, Agentix or Cloud
- CyberArk EPM Content Pack installed from the Cortex Marketplace
- API access credentials (username and key) for CyberArk EPM
- Connectivity between Cortex and EPM APIs

5. Limitations

- Endpoint matching is performed using FQDN and IP Address.
- A single Cortex instance can connect to one EPM tenant at a time.
- Playbook customization is required to align with each organization's incident workflows.

6. Installation

1. Go to the [CyberArk Marketplace](#).
2. Download the **Palo Alto Networks EPM SOC Response** package.
3. Save the downloaded file locally for reference during Cortex configuration.

7. Configuration

7.1 Set up the EPM Policies

1. Create or update EPM policies according to the official [CyberArk documentation](#).
2. Define two response plans for use in the integration:
 - **Medium Risk Plan:** Limit privilege elevation or enforce MFA.
 - **High Risk Plan:** Block privilege elevation and restrict application access.
3. Save and publish the policies before configuring the integration.

7.2 Install the CyberArk EPM Content Pack

1. Log in to **Cortex XSOAR or XSIAM**.
2. Navigate to **Marketplace → Browse Packs**.
3. Search for **CyberArk EPM**.
4. Click **Install** to add the content pack to your environment.

This content pack includes API commands, sample playbooks, and layout templates that can be customized for your use case.

7.3 Configure the Instance

1. In Cortex, go to **Settings → Integrations → Instances**.
2. Search for **CyberArk EPM**.
3. Click **Add Instance** and provide the following details:
 - **EPM URL:** The base URL of your CyberArk EPM tenant.
 - **Username:** The account name used to authenticate API access.
 - **API Key or Password:** The credentials or key for authentication.
 - **Verify Connection:** Test the configuration to confirm access.
4. Save and enable the instance.

Your Cortex environment is now connected to EPM and can invoke response actions.

8. How to Use the Integration

The **CyberArk EPM SOC Response** integration with **Palo Alto Networks Cortex XSIAM and XSOAR** provides the foundational components needed to automate or manually trigger privilege-based response actions from within your SOC workflows.

The integration package includes **API commands** and **example playbooks** that demonstrate how to invoke CyberArk EPM actions based on incident data.

As a customer, you should review these examples and **adapt them to fit their existing automation logic and security processes**.

8.1 Using the Integration in Cortex XSIAM

In Cortex XSIAM, the integration can be used to connect **CyberArk EPM SOC Response** directly to **cases and issues** detected in your environment.

Configuring the Playbook in XSIAM

1. Import the **CyberArk EPM SOC Response Playbook** included in the content pack.
2. Use playbook conditions to decide when to invoke the CyberArk EPM SOC Response, based on attributes such as severity, alert type, or indicator reputation. The default condition, implemented in **EPM SOC Response** playbook uses severity to classify between medium and high response actions.
3. Edit Playbook inputs to ingest hostname and LoggedInUser from target issues context.
 - Open Playbook and go to inputs and outputs
 - Map `${issue.hostname}` to endpoint_name

- Map `{{issue.username}}` to `logged_in_user`
- 4. Save edited playbook.
- 5. The playbook can now be associated to an issue or case.
 - Open the target incident and click **Edit**.
 - In the **Playbook** dropdown, select **CyberArk EPM SOC Response**.
 - Click **Update Incident** to apply the playbook.

Configuring EPM SOC Response in XSIAM

1. Ensure the **CyberArk EPM instance** has been configured in the integration page.
2. Use the **EPM Playbooks or API Commands** included in the content pack to call response actions directly from an existing **XSIAM playbook** or **automation rule**.
3. Add conditions to your playbooks or automation rules to determine which EPM plan to apply based on context — for example:
 - Medium severity incidents trigger the *Medium Risk Plan*.
 - High severity incidents trigger the *High Risk Plan*.
4. Test the response flow in a non-production environment before applying in production.

Integrating with XSIAM Issues

The EPM SOC Response Action can be invoked either manually or automatically via several mechanisms

1. Automation Rule

- Go to **Investigation & Response → Automation Rules**.
- Define a rule that targets relevant issues based on triggering conditions.
- Under **Action**, select the **CyberArk EPM SOC Response** playbook.

2. EPM SOC Response Layout Button

- Navigate to the **Incident Layout Editor** in XSIAM.
- Add **custom sections or widgets** to allow direct invocation of response actions, for example:
 - Buttons for *Medium Risk Plan*, *High Risk Plan*, and *Deactivate Plan*.
- For step-by-step guidance, see the official [Palo Alto Networks XSIAM documentation](#).

3. Direct Playbook Assignment

- On the target issue, go to the **Work Plan** section.
- Select the **CyberArk EPM SOC Response** playbook.
- Follow execution results in the **War Room** section.

8.2 Using the Integration in Cortex XSOAR

In Cortex XSOAR, the integration intended to be used on **incidents produced both internally by XSOAR or from external EDR vendors** such as SentinelOne, CrowdStrike, or Microsoft Defender.

Integrating with XSOAR Incidents

1. Import the **CyberArk EPM SOC Response Playbook** included in the content pack.

2. Use playbook conditions to decide when to invoke the CyberArk EPM SOC Response, based on attributes such as severity, alert type, or indicator reputation. The default condition, implemented in **EPM SOC Response** playbook uses severity to classify between medium and high response actions.
3. Edit the playbook inputs to ingest the Hostname and Logged-in username from the target incident's context:
 - Open Playbook and to inputs and outputs
 - Map `${incident.devicename}` to endpoint_name
 - Map `${incident.deviceusername}` to logged_in_user
4. Save edited playbook.
5. Associate the playbook with an incident:
 - Open the target incident and click **Edit**.
 - In the **Playbook** dropdown, select **CyberArk EPM SOC Response**.
 - Click **Update Incident** to apply the playbook.

8.3 Recommendations and Best Practices

- Begin with **manual or semi-automated triggers** to understand operational impact before enabling full automation.
- Ensure your EPM policies are aligned with your organization's **incident severity and escalation framework**.
- Validate endpoint matching (FQDN and IP) across Cortex and EPM to ensure consistent policy enforcement.
- Use **periodic enrichment** within playbooks to fetch current EPM policy or group data for affected endpoints before executing a response action.
- Review and customize the example playbooks to reflect your **incident taxonomy, naming conventions, and approval workflows**.

9. Troubleshooting

Error	Possible Cause	Resolution
"Failed to connect to EPM"	Incorrect API credentials or URL	Verify the EPM URL and authentication credentials
"Endpoint not found"	FQDN or IP does not match between Cortex and EPM	Check endpoint naming conventions in both systems
"Playbook error"	Missing parameters in playbook configuration	Ensure all required fields are correctly mapped
"No response from EPM"	Network or policy configuration issue	Verify EPM connectivity and policy activation

10. Partner Contact Information

Contact Type	Name	Email
--------------	------	-------

Contact Type	Name	Email
Technical Contact	Nitsan Tzur	ntzur@paloaltonetworks.com
Support Contact	Business Development Technology	cybr-bizdevtech@paloaltonetworks.com