



CYBERARK®
The Identity Security Company™

PAM Administration

Privileged Threat Analytics



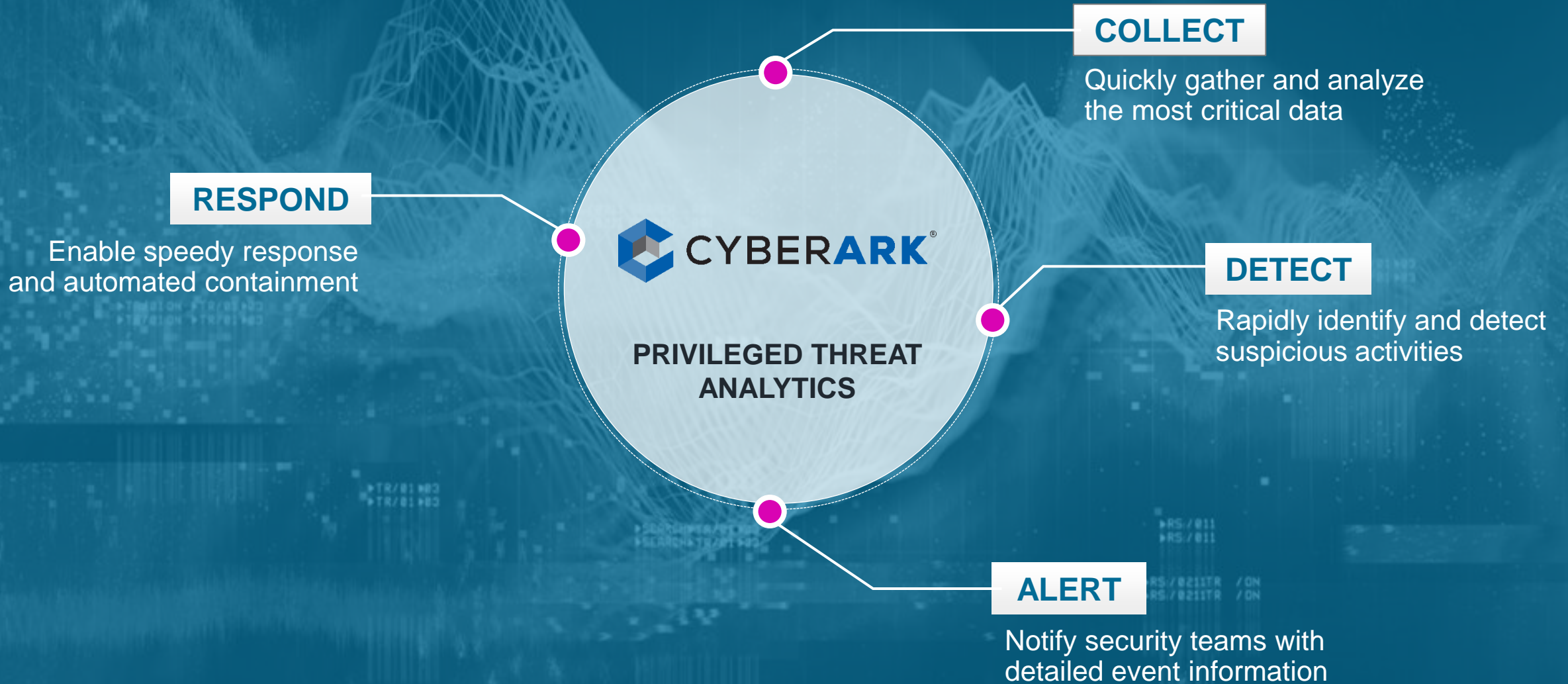
Agenda

By the end of this session the participant will be able to:

1. Describe the main functionality of **Privileged Threat Analytics (PTA)**
2. Describe the different data sources used by the **PTA**
3. Describe the different attacks and risks detected by the **PTA**
4. Describe the alert flow by the **PTA**
5. Configure and test **PTA** automatic responses
6. Describe the session analysis and response flow

Overview: Privileged Threat Analytics

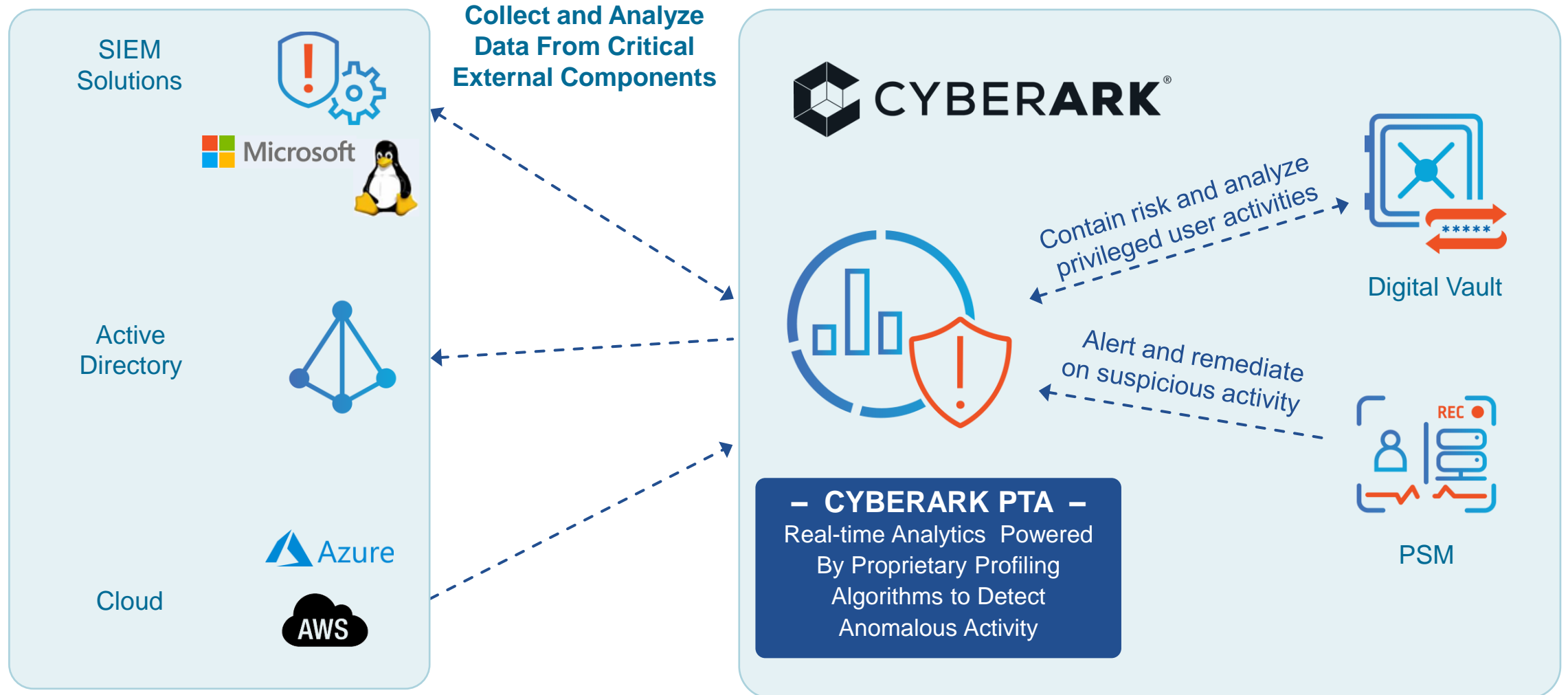
Privileged Threat Analytics



Collect

The **CyberArk Privileged Threat Analytics** collects data from a wide variety of sources

Collect and Analyze the Right Data



Detect

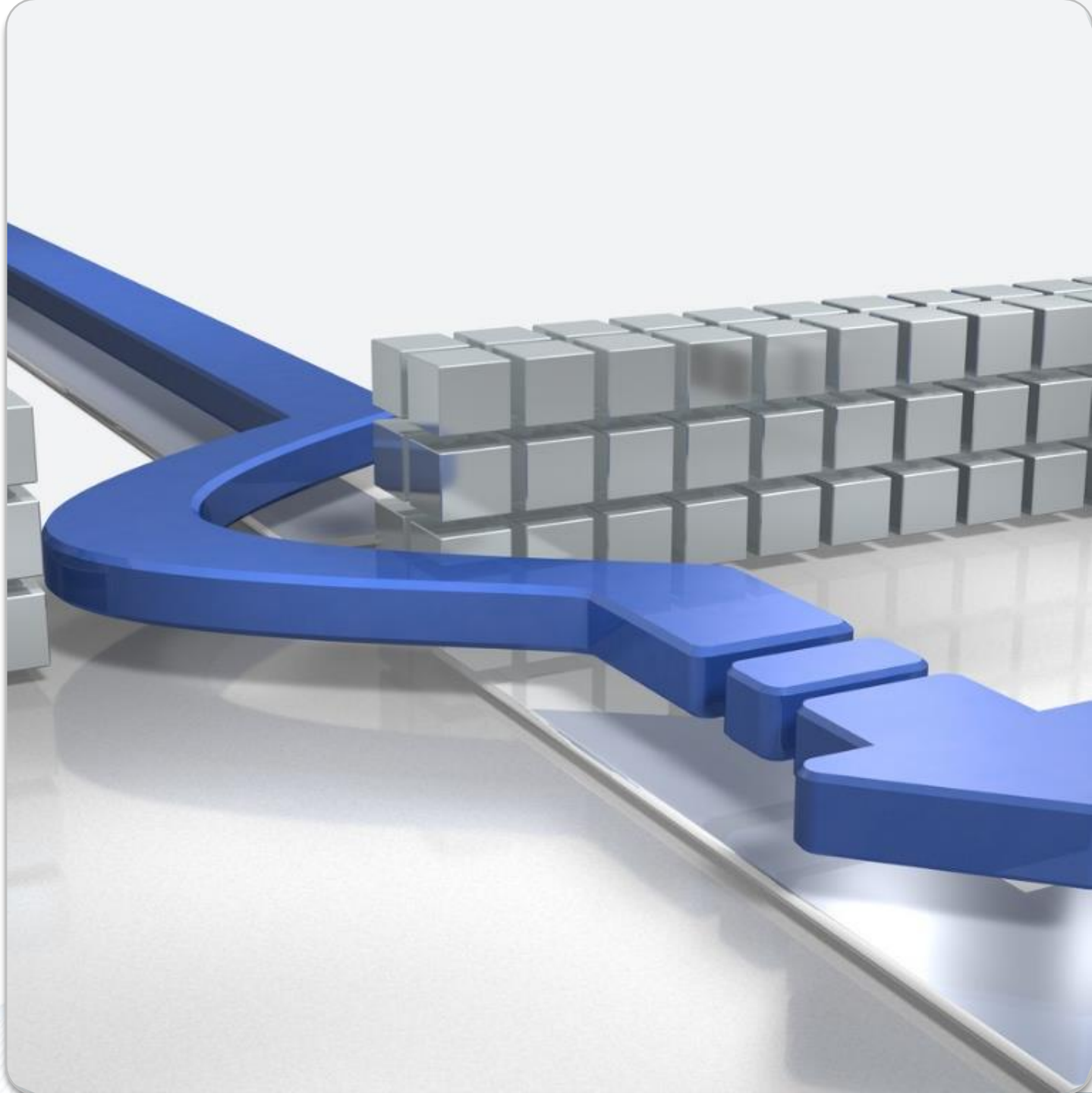
- Attacks that bypass security controls
- Statistical anomalies
- Active Directory risks

Abuse or Bypass of PAM Controls

PTA continuously monitors the use of privileged accounts that are managed by **CyberArk**, as well as privileged accounts that are not yet managed, and looks for indications of abuse or misuse of the **CyberArk** platform.

Such abuse or bypasses include:

- Unmanaged privileged access
- Suspected credential theft
- Suspicious password change
- Suspicious activities detected in a privileged session

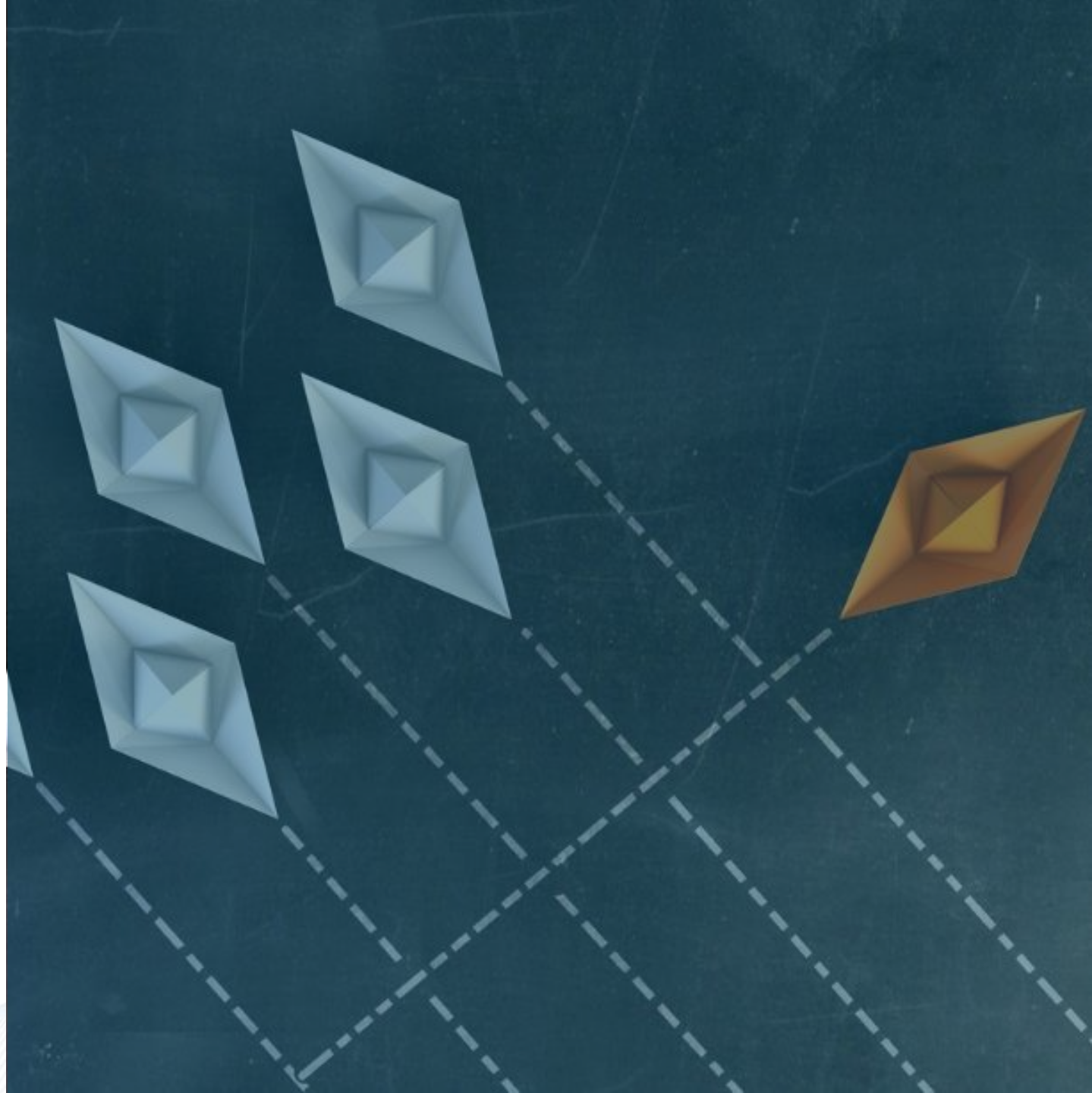


Statistical Anomalies

Using proprietary profiling algorithms, the **PTA** distinguishes in real time between normal and abnormal behavior and raises alerts when abnormal activity is detected.

Such abnormal behavior includes:

- Access to the Vault during irregular hours or days
- Access to the Vault from irregular IP addresses
- Excessive access to privileged accounts in the Vault
- Activity by dormant vault users



Active Directory Risks

PTA proactively monitors risks related to accounts in Active Directory that can be abused by attackers and sends alerts to the security team to handle these risks before attackers abuse them.

Such risks include:

- Unconstrained Delegation
- Dual Usage



PTA Detections – Standard

PTA DETECTION	VAULT	LOGS	AD	EPM
Suspected credentials theft	✓	✓	×	×
→ Unmanaged privileged access	✓	✓	OPTIONAL	×
Unconstrained delegation	×	×	✓	×
Service account logged on interactively	OPTIONAL	✓	OPTIONAL	×
Risky SPN	×	×	✓	×
Suspicious activities detected in a privileged session	✓	×	×	×
Privileged access to the Vault during irregular hours	✓	×	×	×
Excessive access to privileged accounts in the Vault	✓	×	×	×
Privileged access to the Vault from irregular IP	✓	×	×	×
Active dormant Vault user	✓	×	×	×
Machine accessed during irregular hours	×	✓	×	×

Alert

- Security Events
- Security Monitoring Navigation

Alerts On Suspicious Activity and Behavior

PTA enables security teams to prioritize and respond to the most critical incidents.

Security events coming from the PTA:

- Are assigned risk scores based on severity of the detected anomaly
- Contain granular details related to the suspected attack
- Can easily be reviewed in the PVWA and/or in a SIEM dashboard

Security Events

You can review security events in the **PVWA** according to the timeline and filter the events to focus on specific groups of events based on:

- Severity
- Event Type
- Date

CYBERARK®

Privileged Access Manager

System Health

Accounts

Policies

Security

Security Events

Security Configurations

Applications

Visible in the PVWA under the Security pane

Security Events

Filter

1 results for: Status: Open [Clear all filters](#)

Nov 07 Monday

1:15:56 PM MEDIUM

Unmanaged privileged account [Initiated remediation](#)

Privileged account `administrator@acme.corp` was used to access `target-win.acme.corp`, although this account is not managed in CyberArk PAS. ID 63690520c2dc2bb6082890fb [Close](#)

Unmanaged privileged account `administrator@acme.c...` Target machine `target-win.acme.corp`

Recommendation

Onboard the newly discovered account, and assign the appropriate platform to securely manage the account. Discovered accounts that are filtered by an automatic onboarding rule do not require manual action.

Security Event Compact View

Security Events

Last sign in: 2/9/2022 | mike ▾

Filter

31 results for: Status: Open [✕ Clear all filters](#)

Feb 07

Monday

4:27:14 PM
HIGH

» Active session

Suspicious activities detected in a privileged session (2 occurrences) Initiated remediation

Suspicious session activities on **target-lin** were detected in a privileged session. The session was initiated by Vault user **mike** with account **root03@target-lin** by executing 2 activities.

ID 6201485bc2dce2f543475c9b

Close

Resume

4:15:32 PM
HIGH

Suspicious activities detected in a privileged session (2 occurrences) Initiated remediation

Suspicious session activities on **target-lin** were detected in a privileged session. The session was initiated by Vault user **mike** with account **root03@target-lin** by executing 2 activities.

ID 6201459ec2dce2f543475a3d

Close

Jan 31

Monday

3:58:54 PM
MEDIUM

Unmanaged privileged account

Privileged account **root@target-lin** was used to access **target-lin**, although this account is not managed in CyberArk PAS.

ID 61f80752c2dc94b1f8fdbcb8a

Close

Reviewing Security Events in the PVWA

The last time the event was detected.

The name of the event

Shown when remediation has been started.

4:27:14 PM
90 HIGH

» **Active session** Suspicious activities detected in a privileged session (2 occurrences) Initiated remediation

Suspicious session activities on **target-lin** were detected in a privileged session. The session was initiated by Vault user **mike** with account **root03@target-lin** by executing 2 activities.

ID 6201485bc2dce2f543475c9b

Close

Resume



Session ID b073c9ec-557a-47cc-9739-6bbfbdad61b3



Vault user
mike



Cyberark PAS



Target service
target-lin

First suspicious activity occurred 2 days ago.

Most retyped activities

useradd mike (1 occurrence)
passwd mike (1 occurrence)

Recommendation

Session suspension request was initiated. Review each security event associated with the session and its activities, and evaluate whether an additional response is required, such as manual resumption or termination of the suspended session.

The score and severity of the event (high, medium, low).

Recommended action to take / Automatic remediation action that was taken

Easy Navigation: Security-Monitoring

The image displays a two-part interface for security monitoring. The top part shows a notification for an active session with suspicious activities. The bottom part shows the detailed view of this session, including a timeline of activities and a risk score.

Session Alert:

- Time:** 4:27:14 PM
- Severity:** 90 HIGH
- Status:** Active session
- Description:** Suspicious activities detected in a privileged session (2 occurrences). Suspicious session activities on target-lin were detected in a privileged session. The session was initiated by Vault user mike with account root03@target-lin by executing 2 activities.
- Session ID:** b073c9ec-557a-47cc-9739-6bbfbdad61b3
- Diagram:** Vault user mike → Cyberark PAS → Target service target-lin
- Recommendation:** Session suspension request was initiated. Review each security event associated with this session. If an additional response is required, such as manual resumption or termination of the session, it must be initiated.

Session Details:

- Go to Monitoring**
- Session Title:** mike connected as root03 on target-lin
- Start:** 2/7/2022 04:26 PM **Duration:** 00:20:52
- Activities** | Details
- Risk Score:** 90 HIGH Session risk score
- Strongest impact activity/event:** [2/7/2022 04:27 PM] passwd mike
- Security incident:** Suspicious activities in a session **ID:** 6201485bc2dce2f543475ca2 **Go to incident details >**
- 2 Activities in the session**
- Date:** Feb 07 Monday

Respond

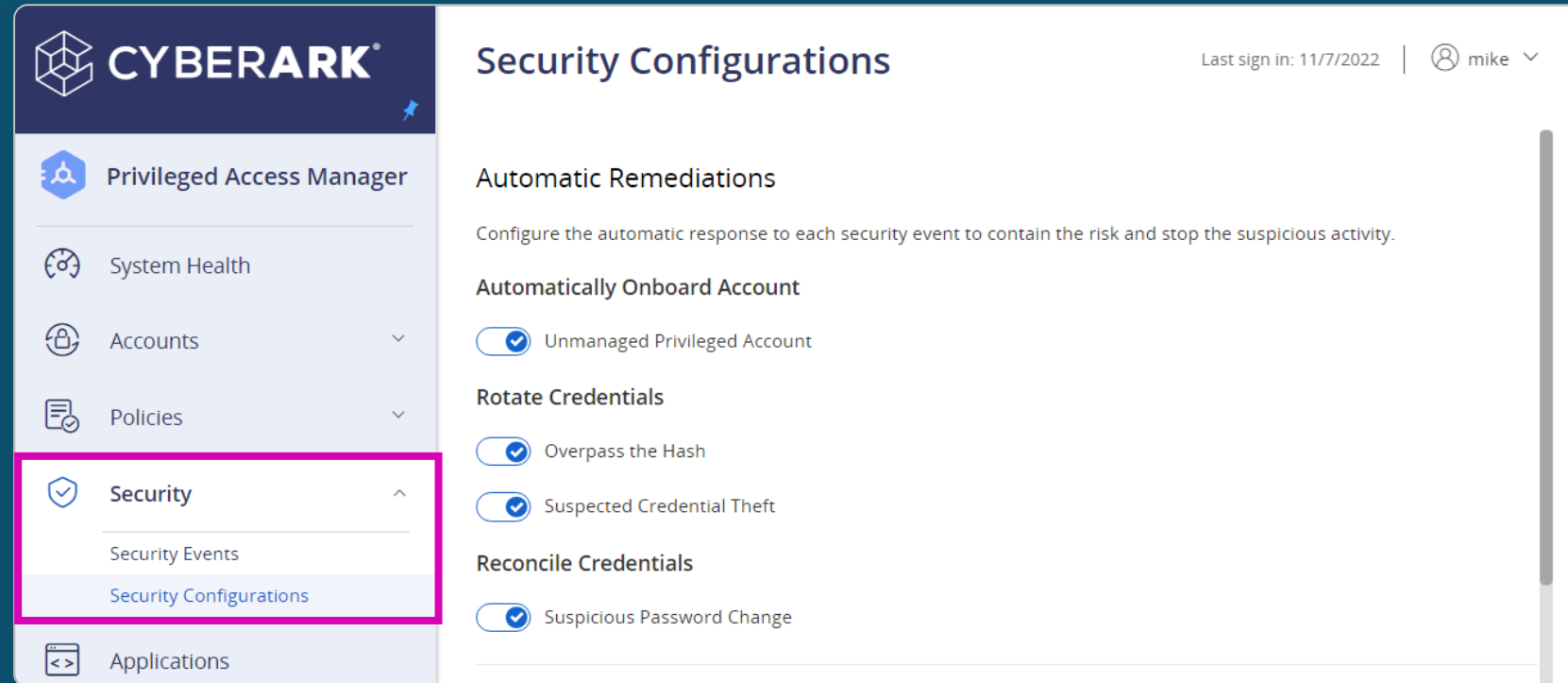
- Automatic Remediation
- PSM – PTA Integration
- Session Analysis and Response
- Risk-based Prioritization
- Configuring Session Analysis and Response Rules
- The Session Analysis and Response Life Cycle

Respond with Automatic Remediations

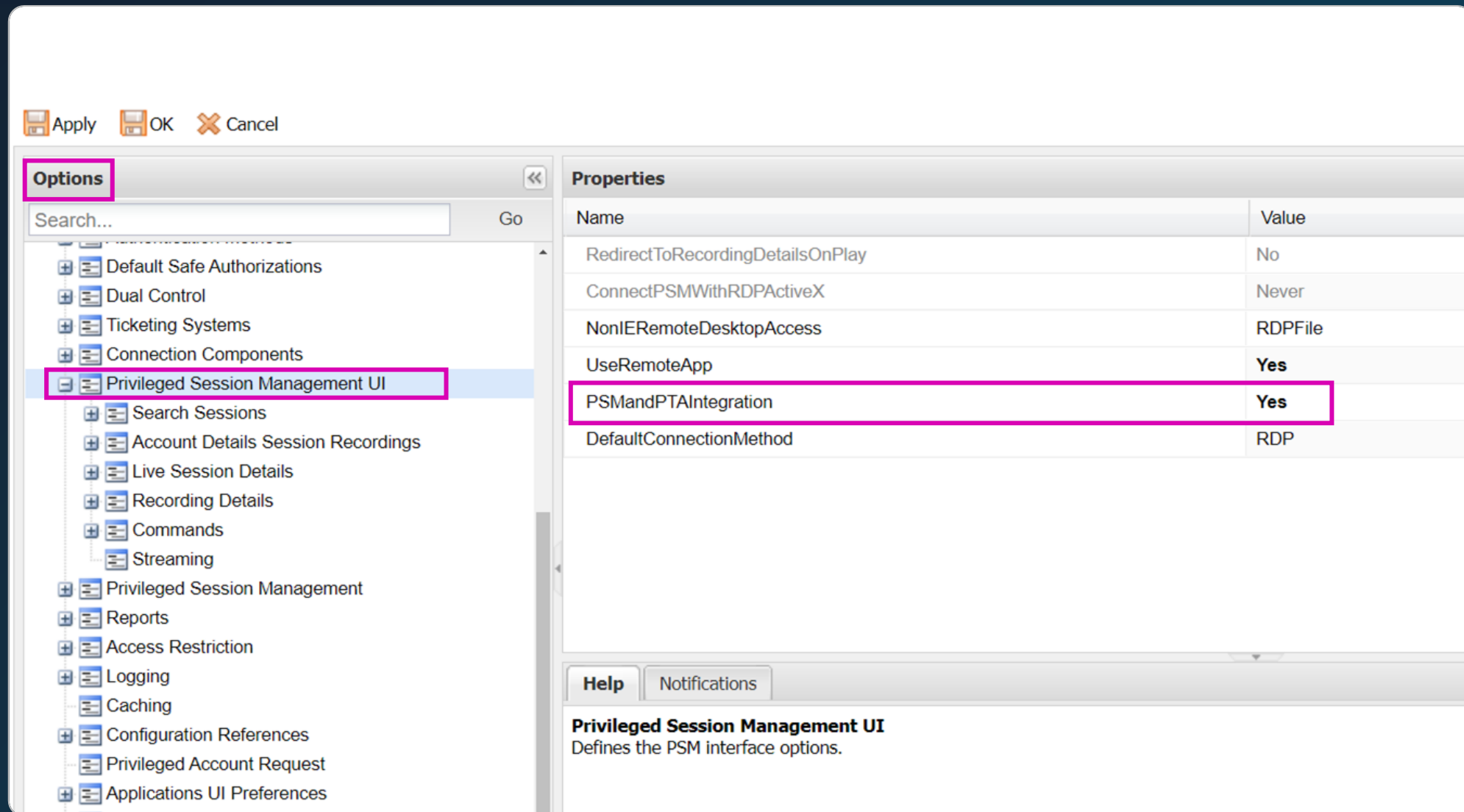
Automatic response improves your organization's security posture and mitigates risk

PTA can contain in-progress attacks by automatically:

- Onboarding unmanaged accounts
- Rotating credentials
- Reconciling credentials



PSM – PTA Integration



Session Analysis and Response

- Connecting the **PTA** and **PSM** leverages the analytic capabilities of the PTA, which receives details of PSM privileged sessions and user activities, analyzes them, and assigns a risk score to each session.
- Audit teams now can prioritize workloads based on risk scores.

Monitoring

Last sign in: 2/9/2022 | mike

Filter

Recordings » Active sessions

25 results for: From: 2/7/2022 12:00 AM , To: 2/9/2022 11:59 PM [Clear all filters](#) [Additional details & actions in classic interface](#)

Risk ↓	User	Client	Account User Name	Account Address	Account Policy ID	Start	Duration	
90	mike	SSH	logon01	10.0.0.20	LINSSH30	2/9/2022 02:00 PM	00:00:09	▶ Play
90	mike	SSH	logon01	10.0.0.20	LINSSH30	2/9/2022 01:49 PM	00:01:32	▶ Play
90	mike	PSMP-SSH	root03	target-lin	LINTest	2/7/2022 04:26 PM	00:20:52	▶ Play video (V9 UI)
90	mike	PSMP-SSH	root03	target-lin	LINTest	2/7/2022 04:14 PM	00:02:08	▶ Play video (V9 UI)
-	mike	SSH	root03	target-lin	LINSSH30	2/7/2022 11:18 AM	00:00:21	▶ Play
-	mike	SSH	logon03	10.0.0.20	LINSSH30	2/7/2022 11:05 AM	00:13:02	▶ Play
-	mike	PSMP-SSH	logon01	10.0.0.20	LINSSH30	2/7/2022 10:57 AM	00:00:23	▶ Play video (V9 UI)

Session Analysis and Response

Once the **PTA** and **PSM** are integrated, we can configure **Privileged Session Analysis and Response** rules to execute automatic session suspension or termination during high-risk user activity, thereby reducing response times and the risk of damage to the organization.

Security Configurations

Last sign in: 2/9/2022 | mike

Privileged Session Analysis and Response

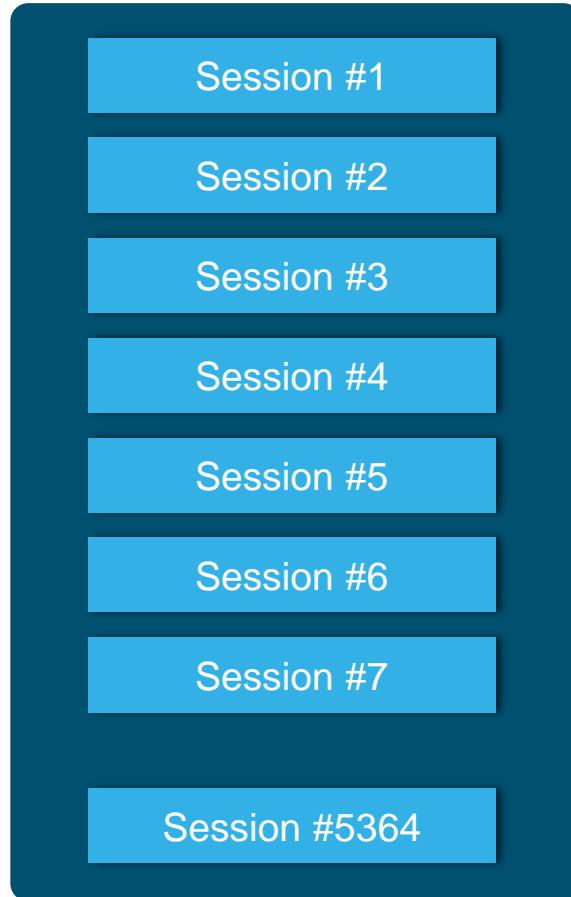
Assign a risk score and automatic response to high-risk activities detected during recorded user sessions.

Add rule

Category	Pattern	Sc.	Description	Response	Status	
SSH	(.*)history(.*)	70	Represents a set of commands that may ...	None	Active	Edit
SSH	(.*)authorized_keys(.*)	60	Manipulation of SSH keys on the machin...	None	Active	Edit
SSH	(.*)sudoers(.*)	80	Manipulation of the sudoers file. Could i...	None	Active	Edit
SSH	(.*)passwd(.*)	90	Access to passwd files exposes sensitive ...	Suspend	Active	Edit
SSH	(.*)\.(DENIED)\(.*)	90	An indication of a restricted command ex...	None	Active	Edit
Windows titles	Registry Editor(.*)	65	Indication of access to the operating syst...	None	Active	Edit
Windows titles	Windows Firewall with Advanced ...	70	Modification of the security configuration...	None	Active	Edit
Windows titles	Internet Properties	60	Modification of the network configuratio...	None	Active	Edit

Risk-based Prioritization

Events



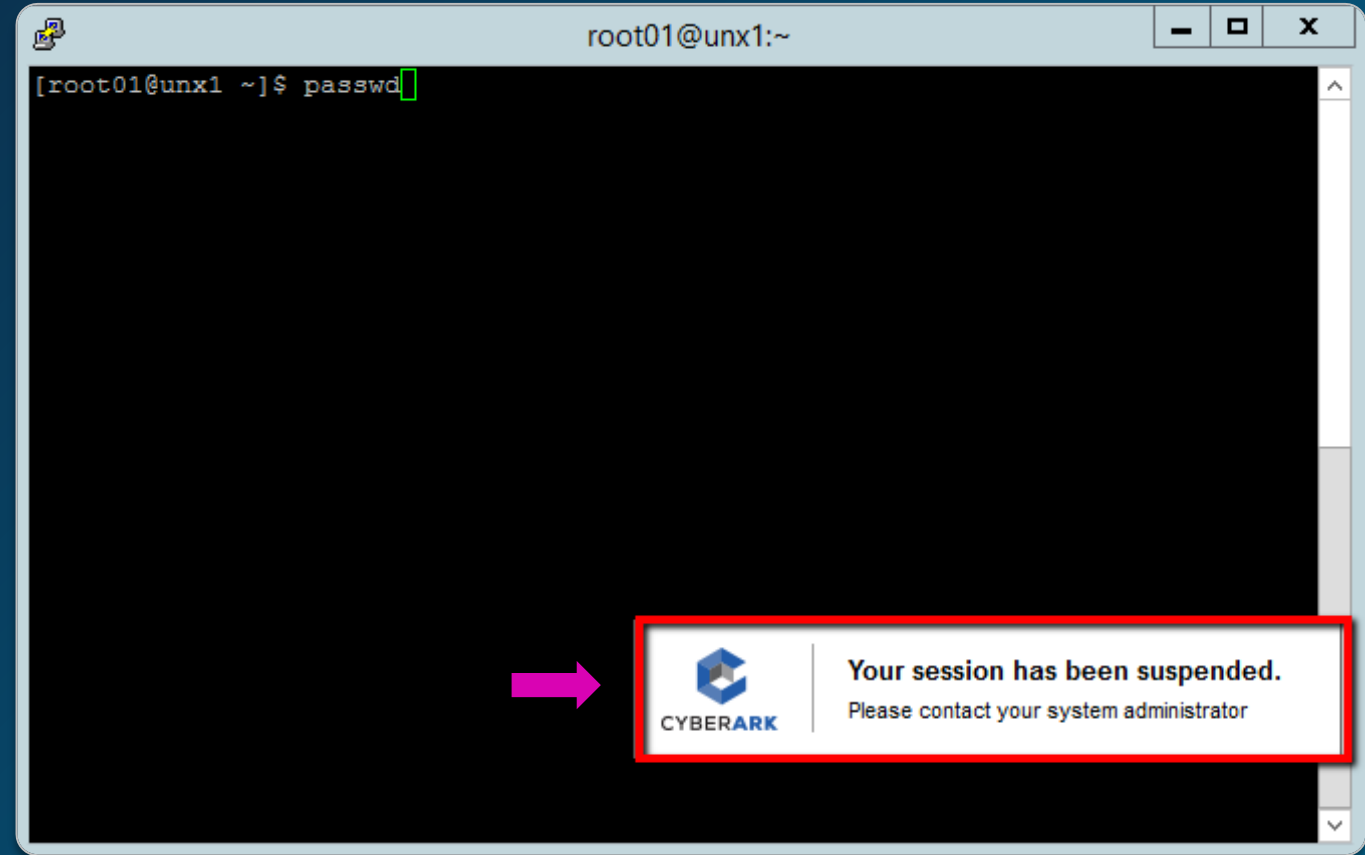
Risk-Based Priorities



Configuring Rules

- You can add new rules or customize existing rules for session analysis and response
- The scope of a rule can be granularly applied to different **Vault** users, accounts, and machines.
- In the event of high-risk activity, the **PTA** can also be configured to terminate or suspend the session.

CyberArk recommends that each organization study the predefined set of rules for suspicious session activities and then modify and add rules according to their needs.



Configuring Rules

Rules are defined by:

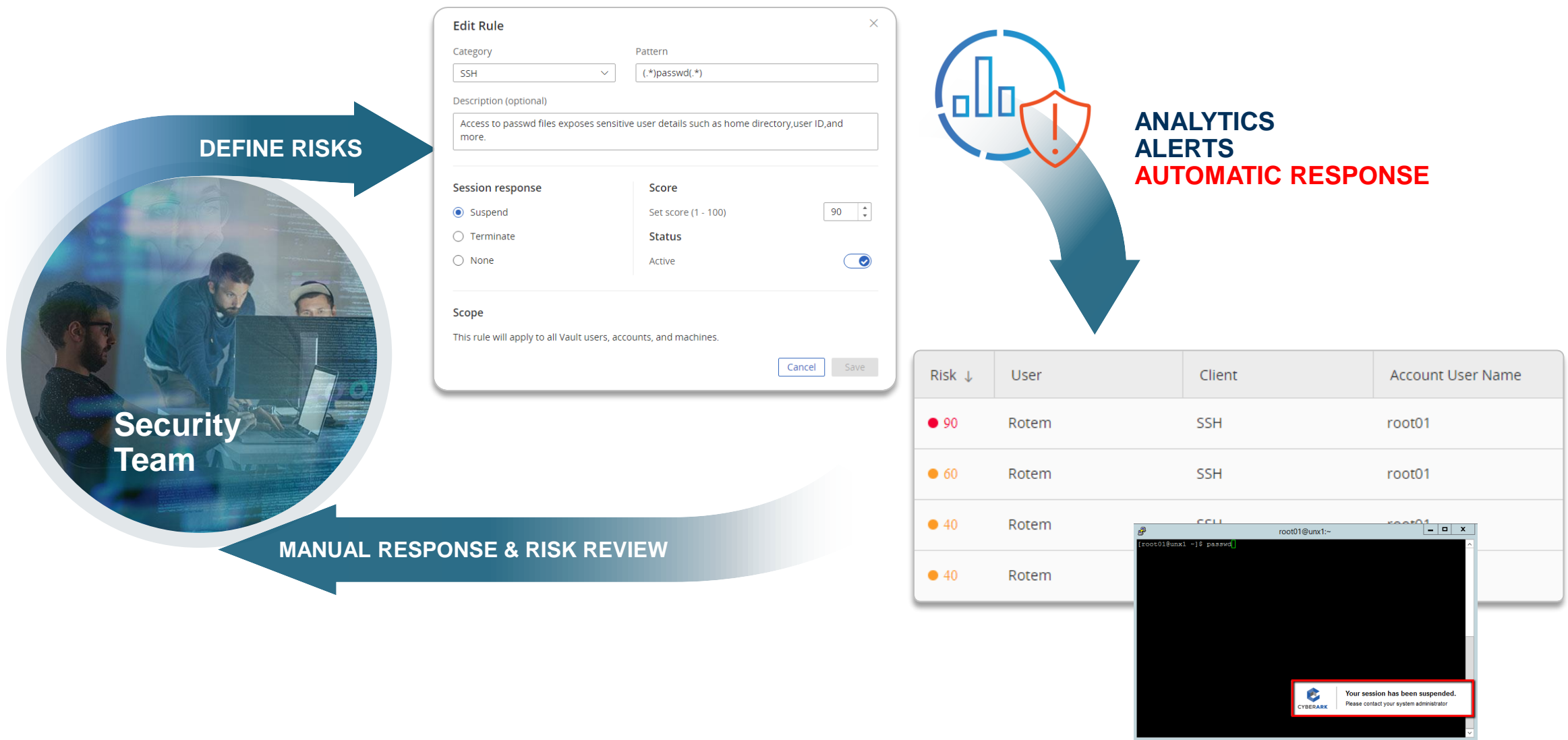
- **Category**
 - SSH
 - Universal Keystrokes
 - SCP
 - SQL
 - Windows title
- **Pattern:** a regular expression to be monitored
- **Session response**
 - Suspend
 - Terminate
 - None
- **The Threat Score (1-100)**
- **Scope:** To whom or what the rule will apply

The screenshot shows the 'Edit Rule' dialog box with the following configuration:

- Category:** A dropdown menu with 'SSH' selected. Other options include Universal keystrokes, SCP, SQL, SSH, and Windows titles.
- Pattern:** A text input field containing the regular expression '(.*)passwd(.*)'.
- Session response:** Radio buttons for 'Suspend' (selected), 'Terminate', and 'None'.
- Score:** A numeric input field set to '90' with a range of 'Set score (1 - 100)'.
- Status:** A toggle switch labeled 'Active' which is currently turned on.
- Scope:** A text area containing the text 'This rule will apply to all but 1 Vault users, all accounts and all machines' and a link 'Change scope »'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

Session Analysis and Response Life Cycle



Demos

In this section we will review recorded demos of threat detection and automatic response demos in:

- Windows
- AWS

Privileged Threat Detection and Automatic Response Demo:

Windows

Privileged Threat Detection and Automatic Response Demo:

AWS

Detect and Respond to Privileged Risks in the Cloud

To help address the challenge of monitoring Privileged Cloud users and detecting, alerting, and responding to high-risk privileged access, the **PTA** can be now used to improve the efficiency of Cloud security teams and to secure threats within Amazon Web Services (AWS) and Microsoft Azure.

- The following capabilities are supported for AWS:
 - Detect unmanaged Access Keys and Passwords for IAM accounts
 - Detect compromised privileged IAM accounts
 - Detect compromised EC2 accounts
- The following capabilities are supported for Azure:
 - Detect unmanaged privileged access
 - Detect suspected credential theft





PTA's Threat Detection and Response Capabilities within AWS



CYBERARK®
The Identity Security Company™

Automated Privileged Exploit Detection and Response

Summary



Summary

In this session we:

- Looked at overview of the main functionality of the PTA
- Viewed the different data sources used by the PTA
- Described the different attacks and risks detected by the PTA
- Discussed the alert flow by the PTA
- Looked at the PTA's automatic responses
- Described the session analysis and response flow
- Viewed some videos demonstrating PTA functionality

Exercises

You may now complete the following exercises:

Privileged Threat Analytics

Detections and Automatic remediation for UNIX/Linux

- Unmanaged Privileged Access
- Suspected Credential Theft and Automatic Password Rotation
- Suspicious Password Change and Automatic Reconciliation
- Suspicious activities in a Unix session and automatic suspension
- Security Rules Exceptions

Detections and Automatic Remediation for Windows

- Unmanaged Privileged Access
- Suspicious Activities in a Windows Session and Automatic Suspension

Connect to the PTA Administration Interface