CYBERARK®

PAM Administration

Privileged Threat Analytics

CYBERARK®

Agenda

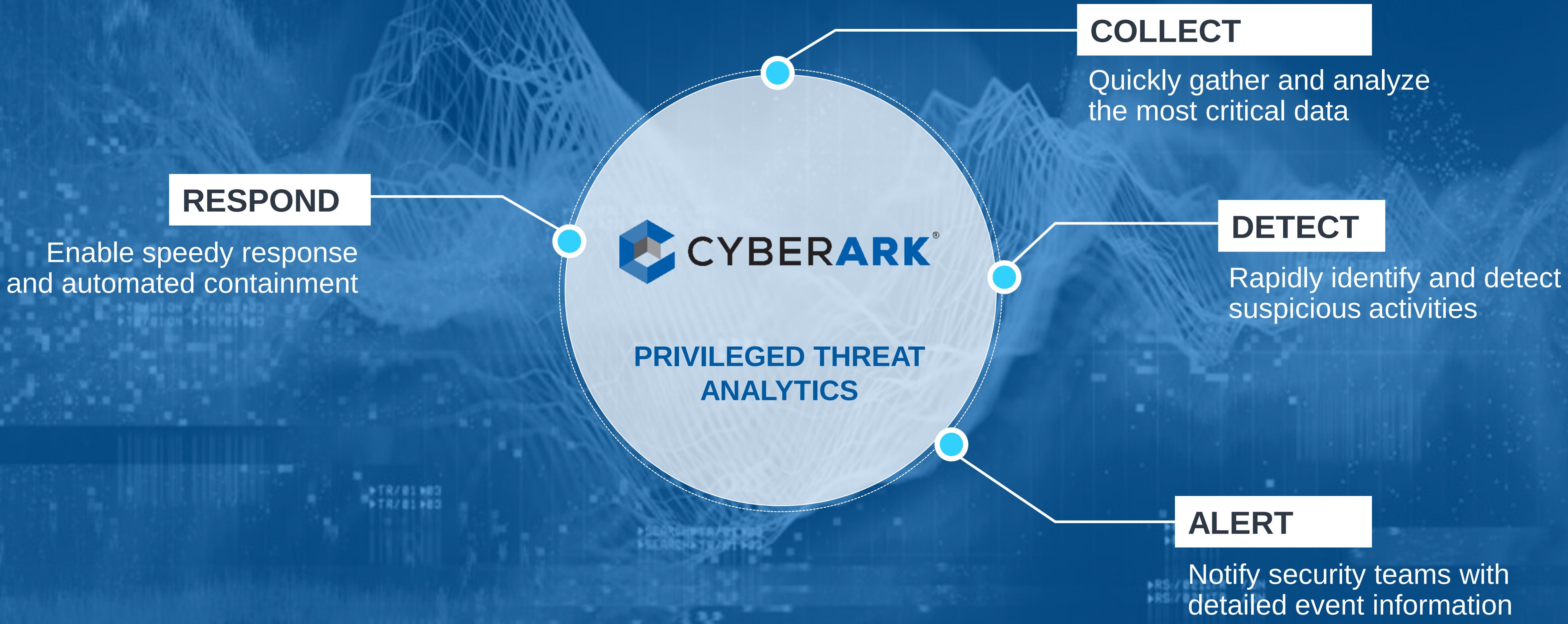
By the end of this session the participant will be able to:

- Describe the main functionality of **Privileged Threat Analytics** (**PTA**)
- Describe the different data sources used by the **PTA**
- Describe the different attacks and risks detected by the **PTA**
- Describe the alert flow by the **PTA**
- Configure and test **PTA** automatic responses
- Describe the session analysis and response flow

Overview:

Privileged Threat Analytics

Privileged Threat Analytics



COLLECT

Quickly gather and analyze the most critical data

DETECT

Rapidly identify and detect suspicious activities

ALERT

Notify security teams with detailed event information

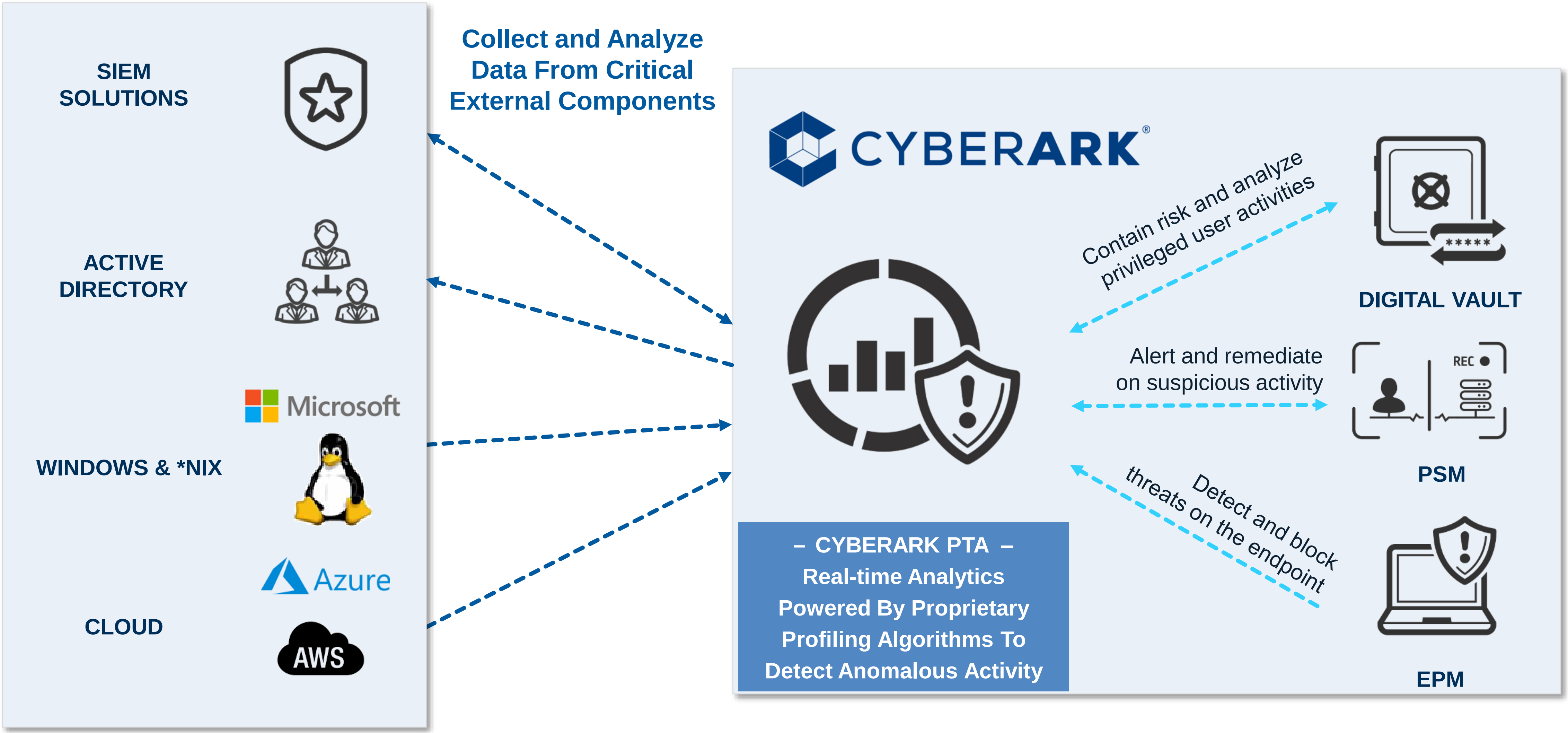
RESPOND

Enable speedy response and automated containment

Collect

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

Collect and Analyze the Right Data



SIEM SOLUTIONS

ACTIVE DIRECTORY

WINDOWS & *NIX

CLOUD

Collect and Analyze Data From Critical External Components

Contain risk and analyze privileged user activities

Alert and remediate on suspicious activity

Detect and block threats on the endpoint

DIGITAL VAULT

PSM

EPM

– CYBERARK PTA –
Real-time Analytics Powered By Proprietary Profiling Algorithms To Detect Anomalous Activity

Detect

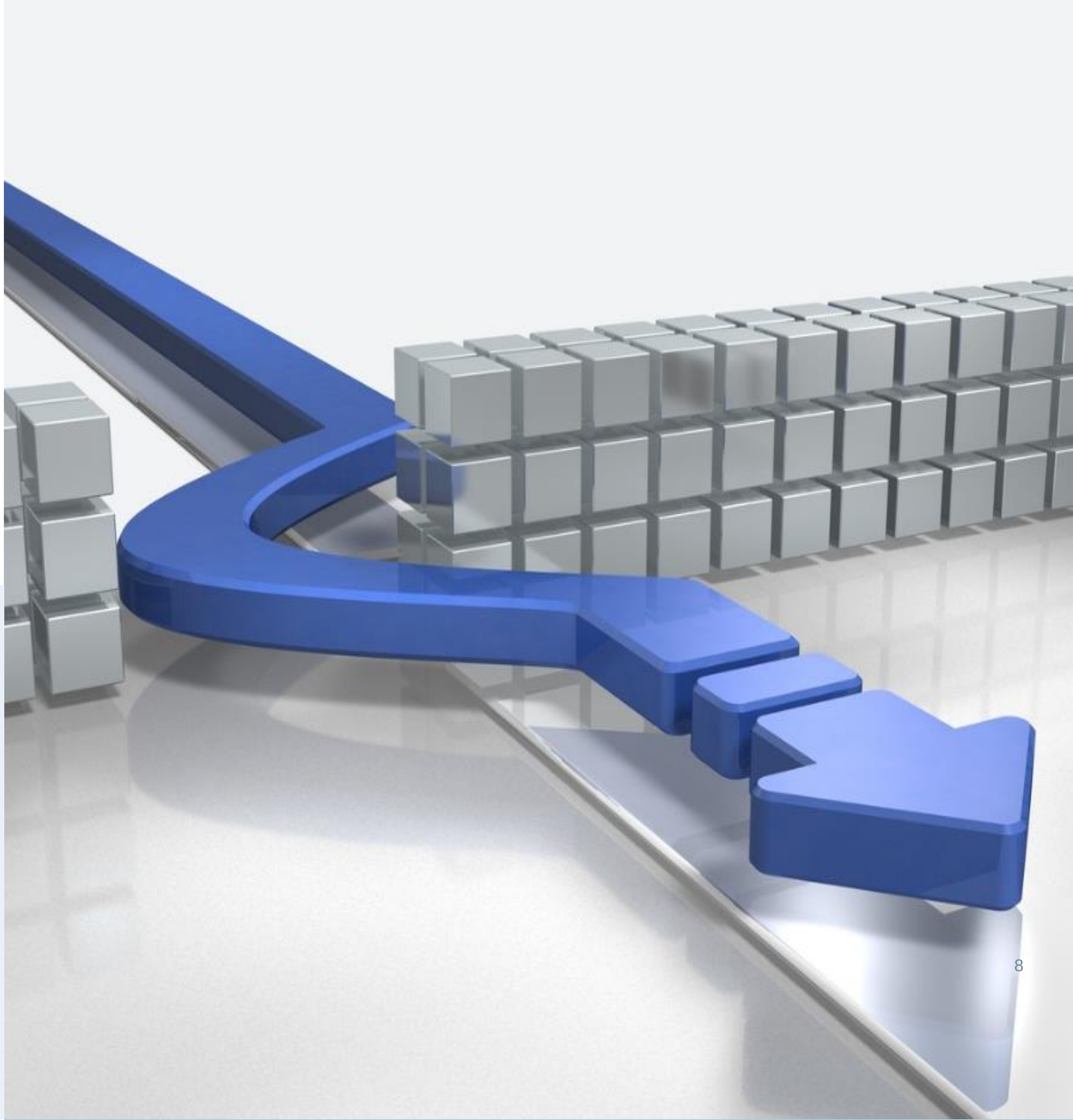
- Attacks that bypass security controls
- Statistical anomalies
- Active Directory risks

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

PTA DETECTION	VAULT	LOGS	AD	EPM
Suspected credentials theft	🟦	🟦		
Unmanaged privileged access	🟦	🟦	■	
Unconstrained delegation			🟦	
Service account logged on interactively	■	🟦	■	
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		🟦		

PTA Detections with EPM

PTA DETECTION	VAULT	LOGS	AD	EPM
Suspected LSASS credentials harvesting				
Suspected SAM hash harvesting				
Suspected credentials theft from Chrome				
Suspected credentials theft from Firefox				
Suspected credentials theft from VNC				
Suspected credentials theft from WinSCP				
Suspected credentials theft from service account				
Suspected domain credentials theft from local cache				

Alert

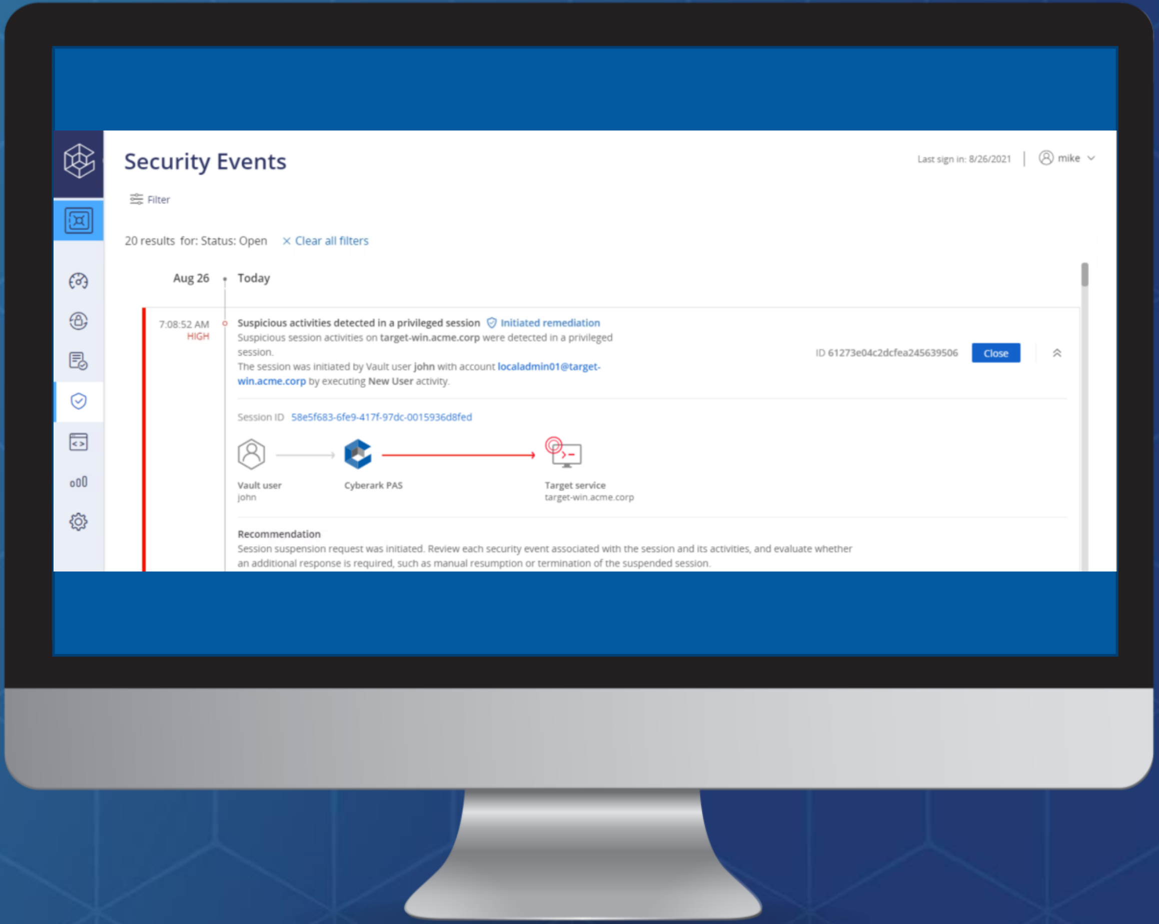
- Security Events
- Security Monitoring Navigation

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

Last sign in: 8/26/2021 | mike

Filter

20 results for: Status: Open × Clear all filters

Aug 26 Today

7:08:52 AM HIGH

Suspicious activities detected in a privileged session Initiated remediation

Suspicious session activities on **target-win.acme.corp** were detected in a privileged session.

The session was initiated by Vault user **john** with account localadmin01@target-win.acme.corp by executing **New User** activity.

ID 61273e04c2dcfea245639506 Close

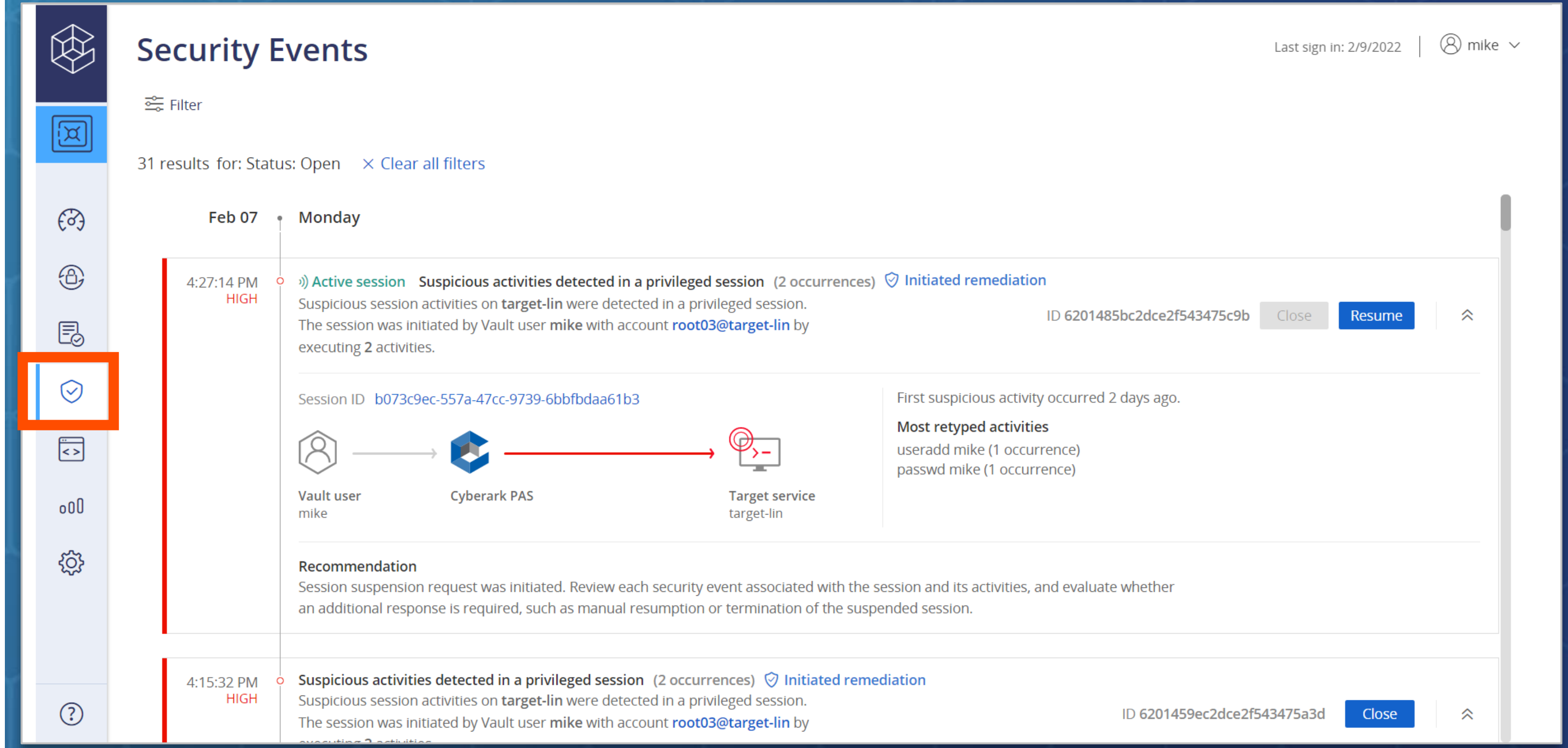
Session ID 58e5f683-6fe9-417f-97dc-0015936d8fed

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.

Security Events

- Visible in the **PVWA** under the ***Security*** pane
- 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



Security Events

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

Session ID b073c9ec-557a-47cc-9739-6bbfbdaa61b3

First suspicious activity occurred 2 days ago.

Most retyped activities
useradd mike (1 occurrence)
passwd mike (1 occurrence)

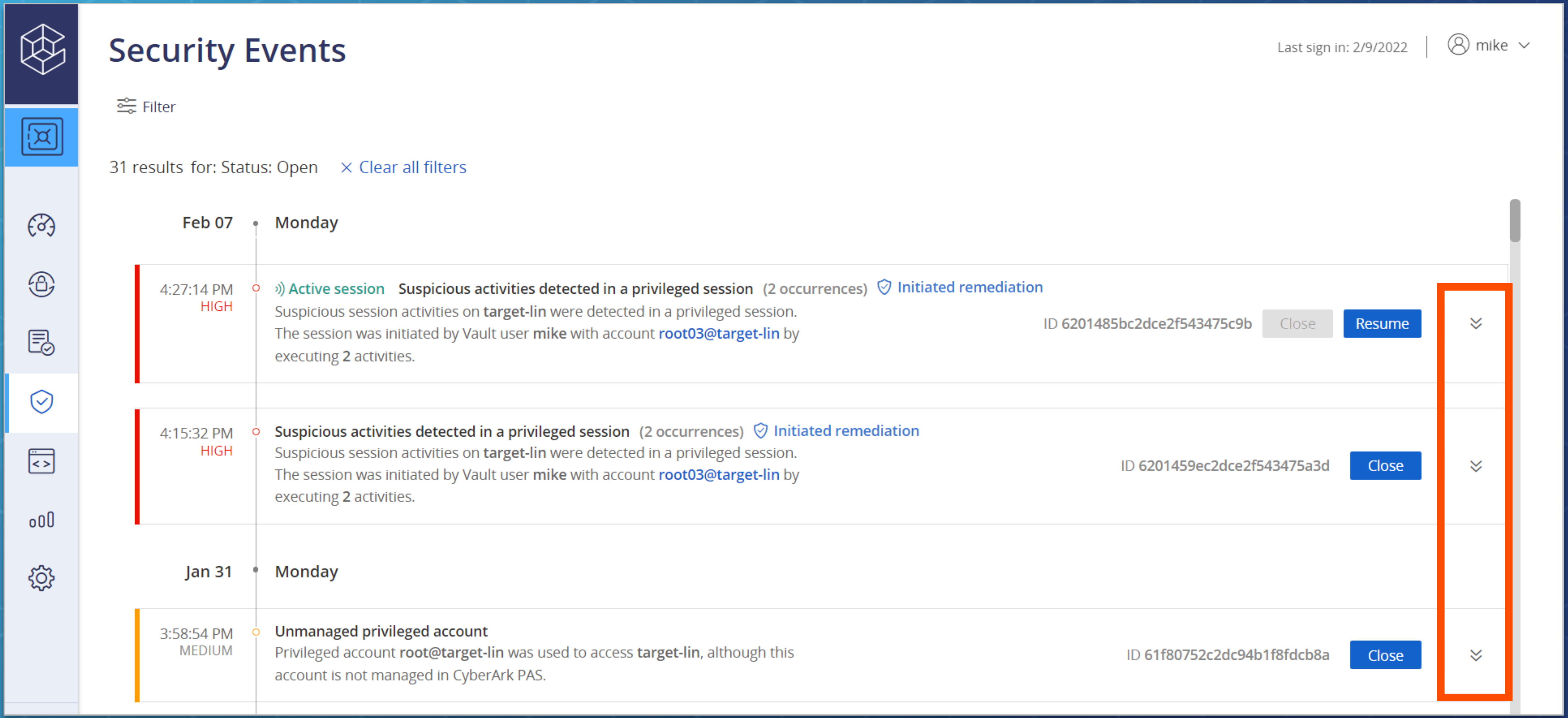
Recommendation
Session suspension request was initiated. Review each security event associated with the session and its activities, and evaluate whether an additional response is required, such as manual resumption or termination of the suspended session.

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

ID 6201459ec2dce2f543475a3d

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.

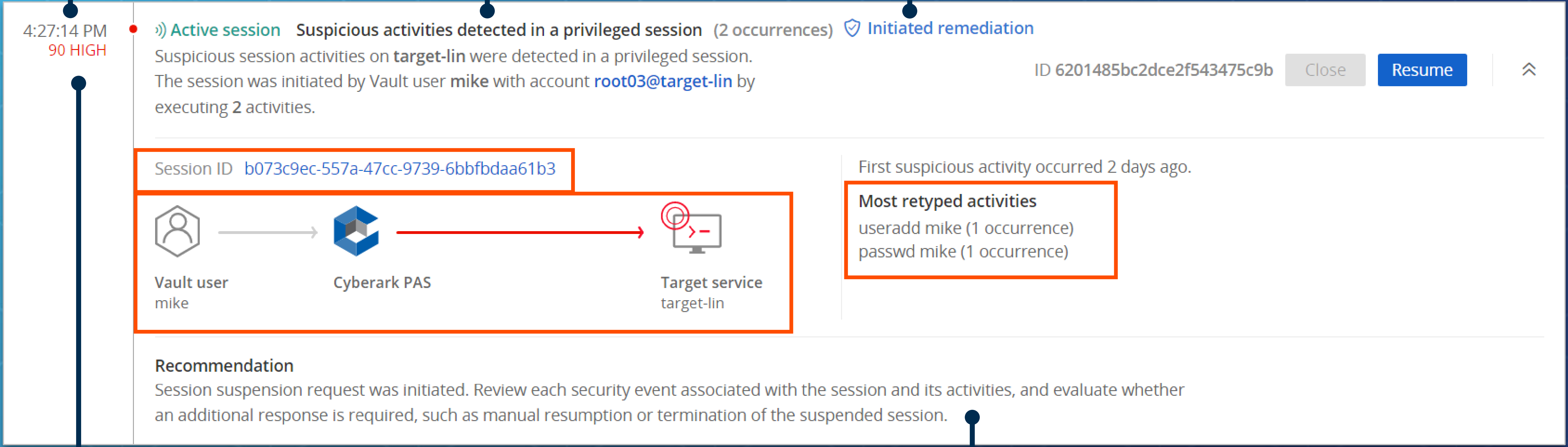
ID **61f80752c2dc94b1f8fdcb8a** Close

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

Session ID b073c9ec-557a-47cc-9739-6bbfbdaa61b3

First suspicious activity occurred 2 days ago.

Most retyped activities
useradd mike (1 occurrence)
passwd mike (1 occurrence)

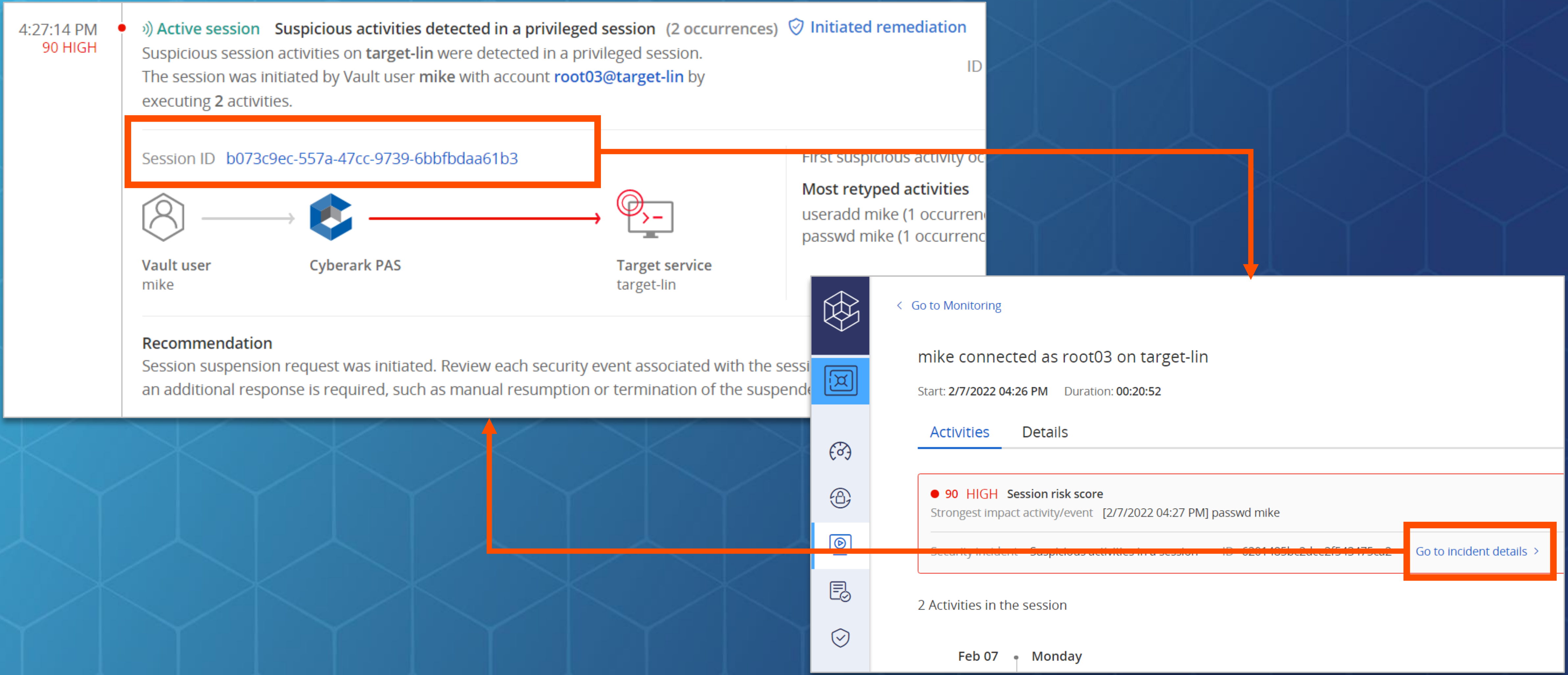
Recommendation

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



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

Session ID b073c9ec-557a-47cc-9739-6bbfbdaa61b3

First suspicious activity oc

Most retyped activities
useradd mike (1 occurren
passwd mike (1 occurrenc

Recommendation
Session suspension request was initiated. Review each security event associated with the sessi
an additional response is required, such as manual resumption or termination of the suspende

< Go to Monitoring

mike connected as root03 on target-lin

Start: 2/7/2022 04:26 PM Duration: 00:20:52

● 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 6201485bc2dcc2f543475ca2 Go to incident details >

2 Activities in the session

Feb 07 • Monday

Respond

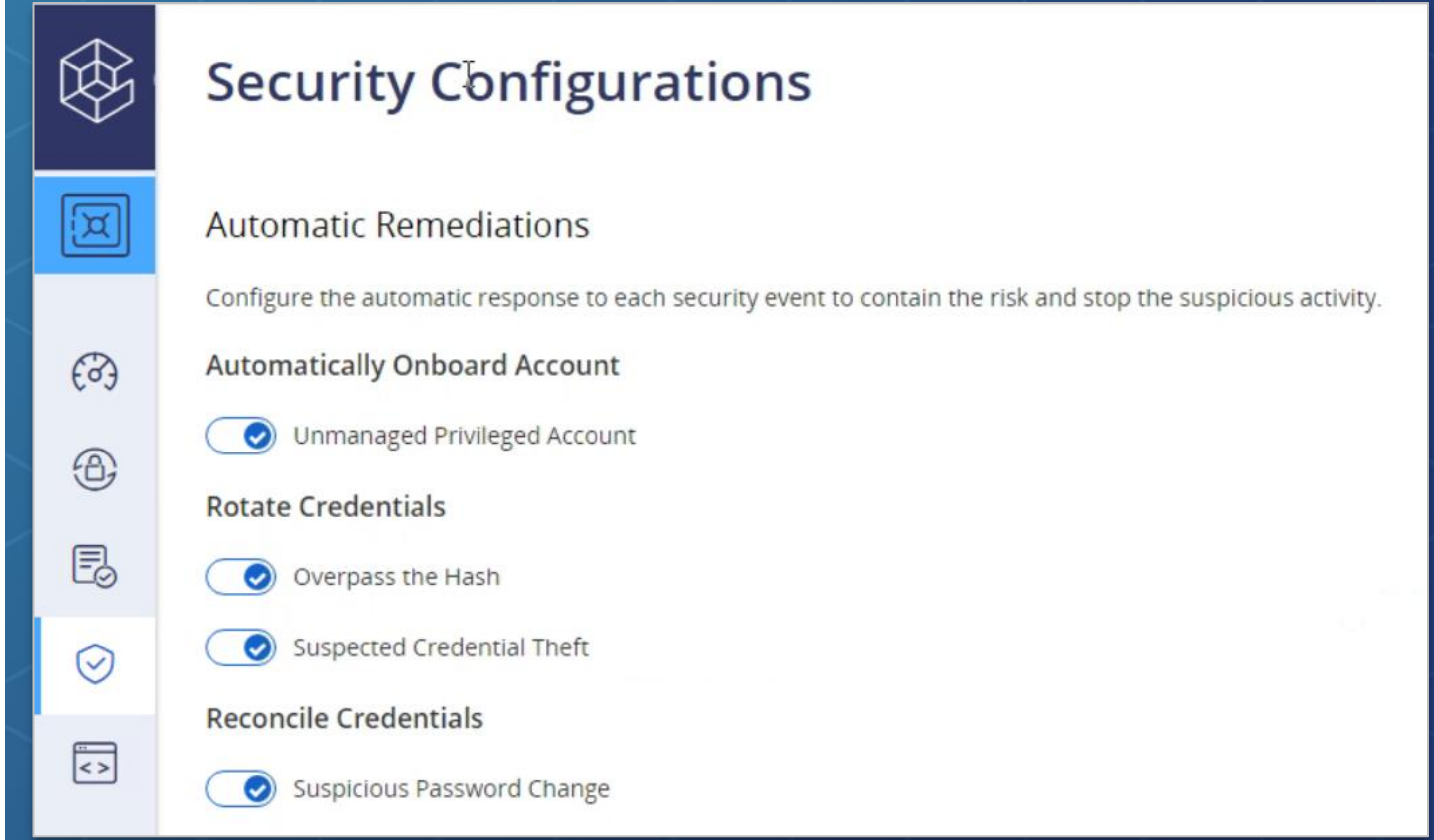
- Automatic Remediation
- PSM – PTA Integration
- Session Analysis and Response
- Risk-based Prioritization
- Configuring Session Analysis and Response Rules
- The Session Analysis and Response Life Cycle

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



Security Configurations

Automatic Remediations

Configure the automatic response to each security event to contain the risk and stop the suspicious activity.

Automatically Onboard Account

☑ Unmanaged Privileged Account

Rotate Credentials

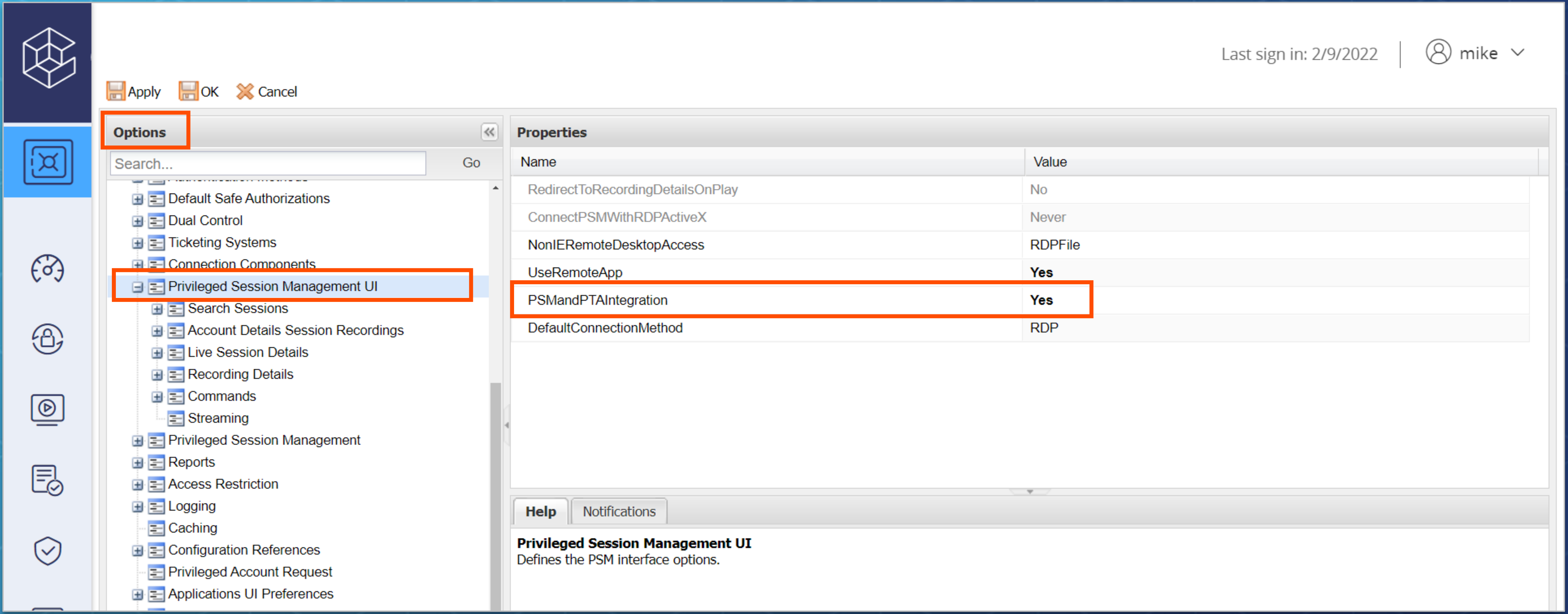
☑ Overpass the Hash

☑ Suspected Credential Theft

Reconcile Credentials

☑ Suspicious Password Change

PSM – PTA Integration



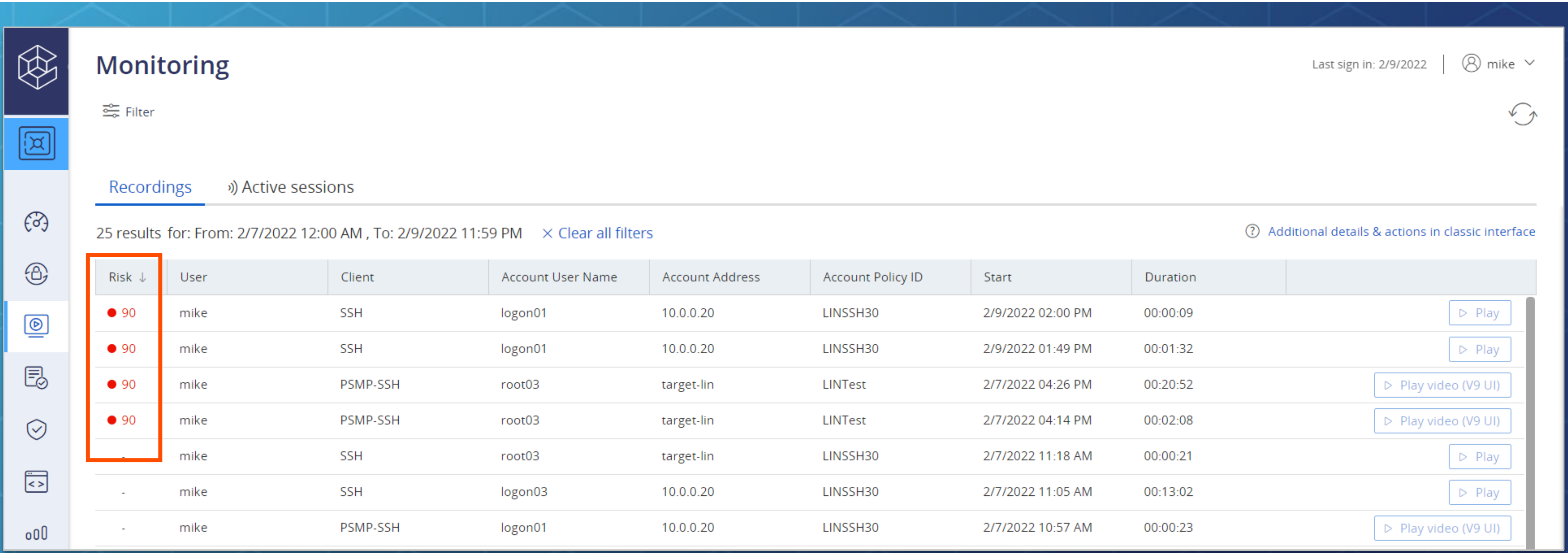
- Default Safe Authorizations
- Dual Control
- Ticketing Systems
- Connection Components
- Privileged Session Management UI
  - Search Sessions
  - Account Details Session Recordings
  - Live Session Details
  - Recording Details
  - Commands
  - Streaming
- Privileged Session Management
- Reports
- Access Restriction
- Logging
- Caching
- Configuration References
- Privileged Account Request
- Applications UI Preferences

Name	Value
RedirectToRecordingDetailsOnPlay	No
ConnectPSMWithRDPActiveX	Never
NonIERemoteDesktopAccess	RDPFile
UseRemoteApp	**Yes**
PSMandPTAIntegration	**Yes**
DefaultConnectionMethod	RDP

Privileged Session Management UI
Defines the PSM interface options.

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.

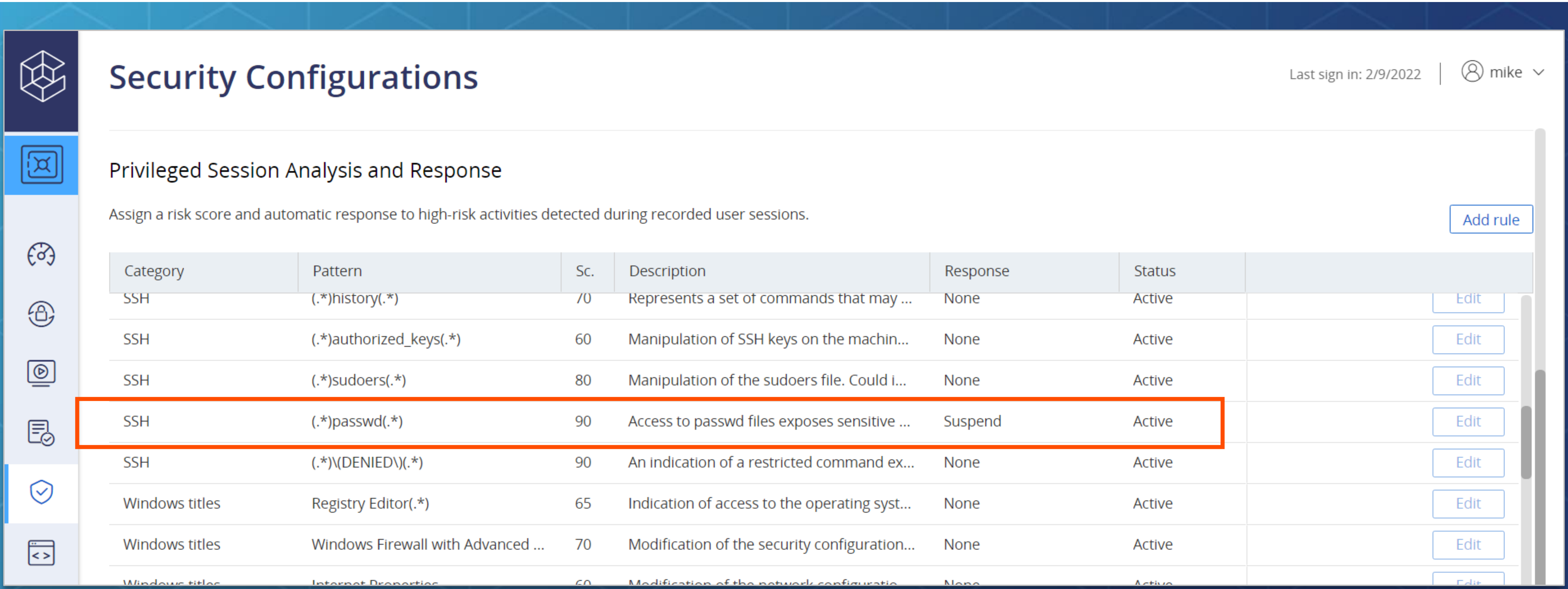


25 results for: From: 2/7/2022 12:00 AM , To: 2/9/2022 11:59 PM

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

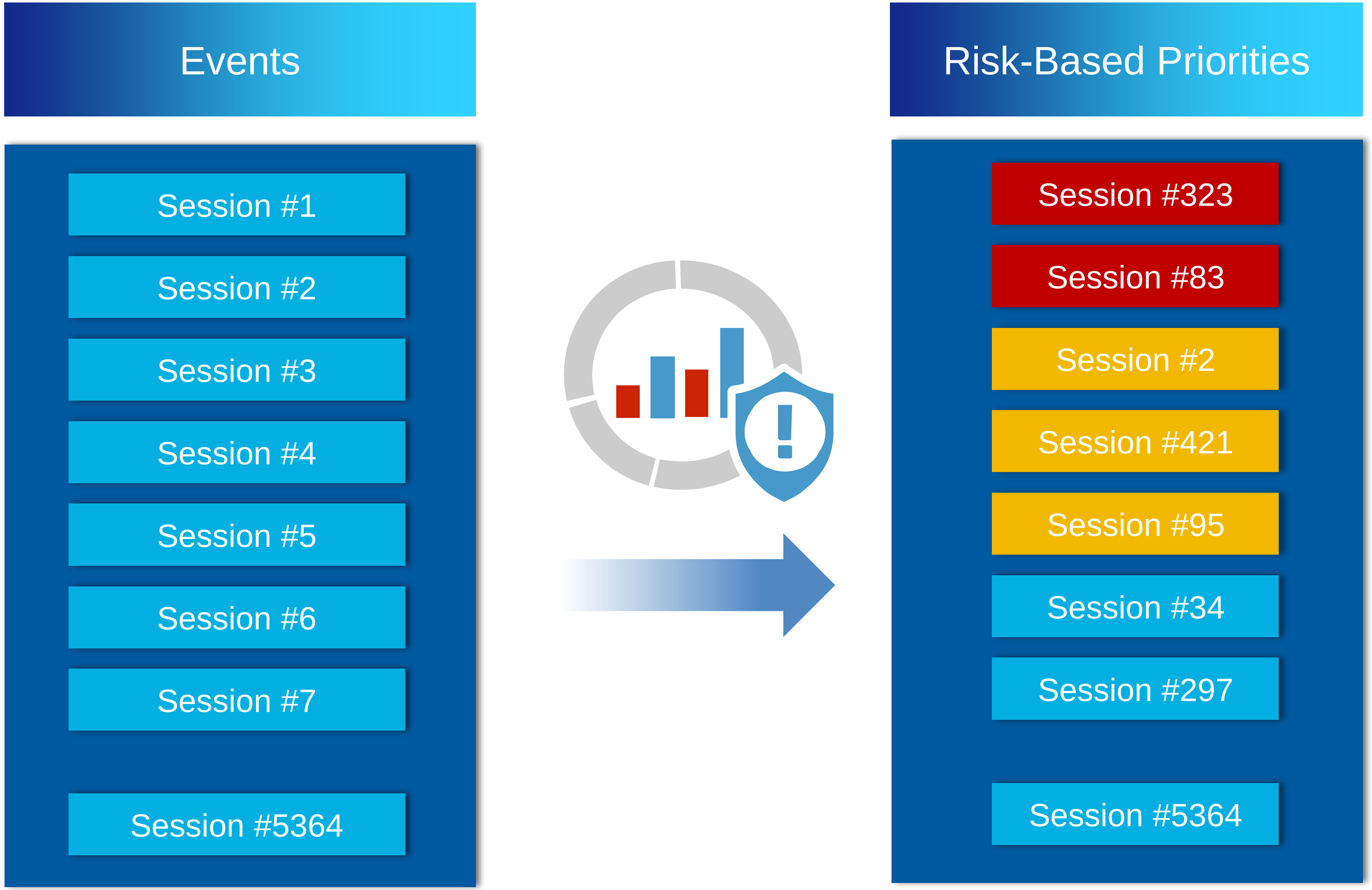
Last sign in: 2/9/2022 | mike

Privileged Session Analysis and Response

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

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

Session #1

Session #2

Session #3

Session #4

Session #5

Session #6

Session #7

Session #5364

Risk-Based Priorities

Session #323

Session #83

Session #2

Session #421

Session #95

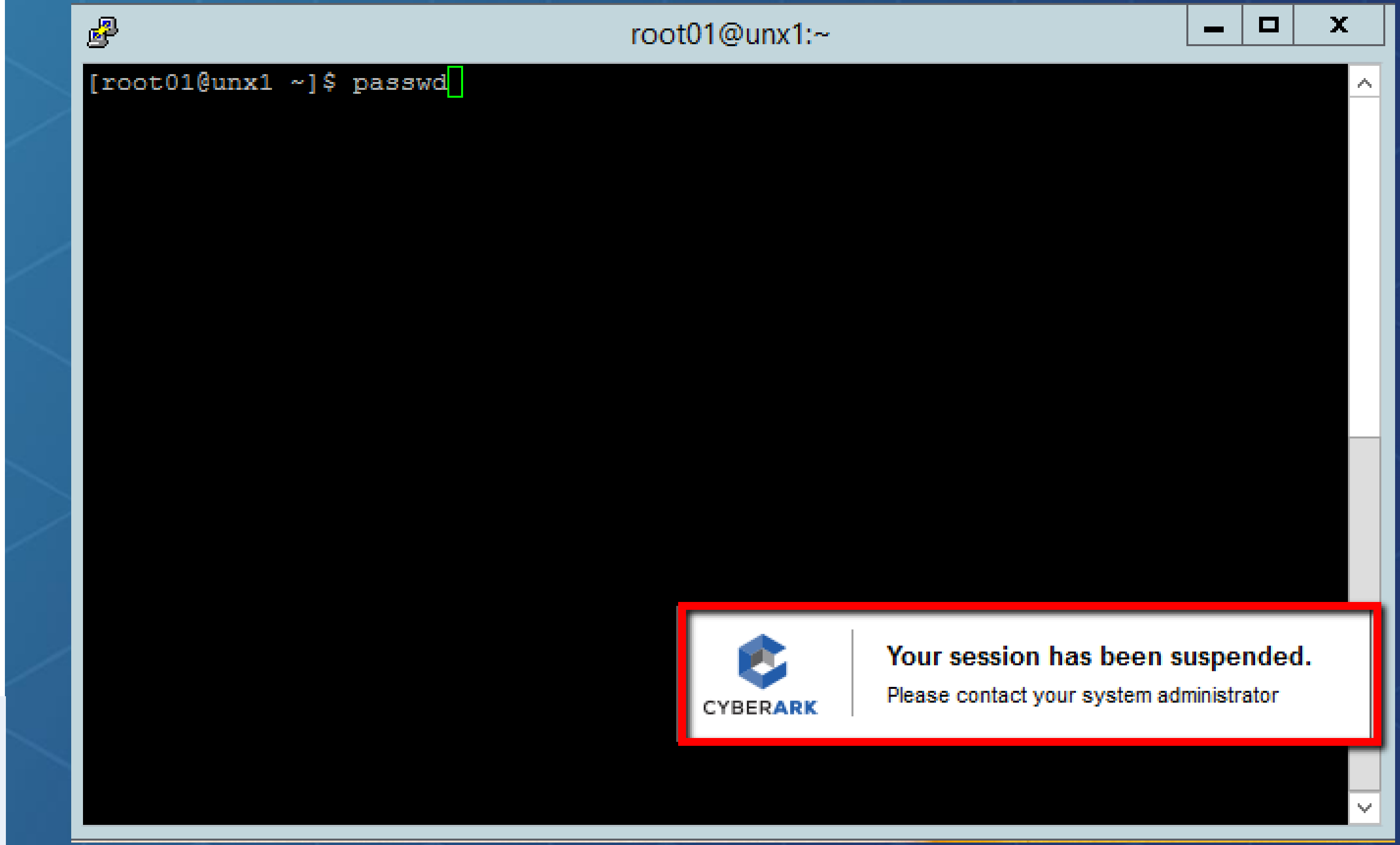
Session #34

Session #297

Session #5364

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.



```
[root01@unx1 ~]$ passwd
```

Your session has been suspended.

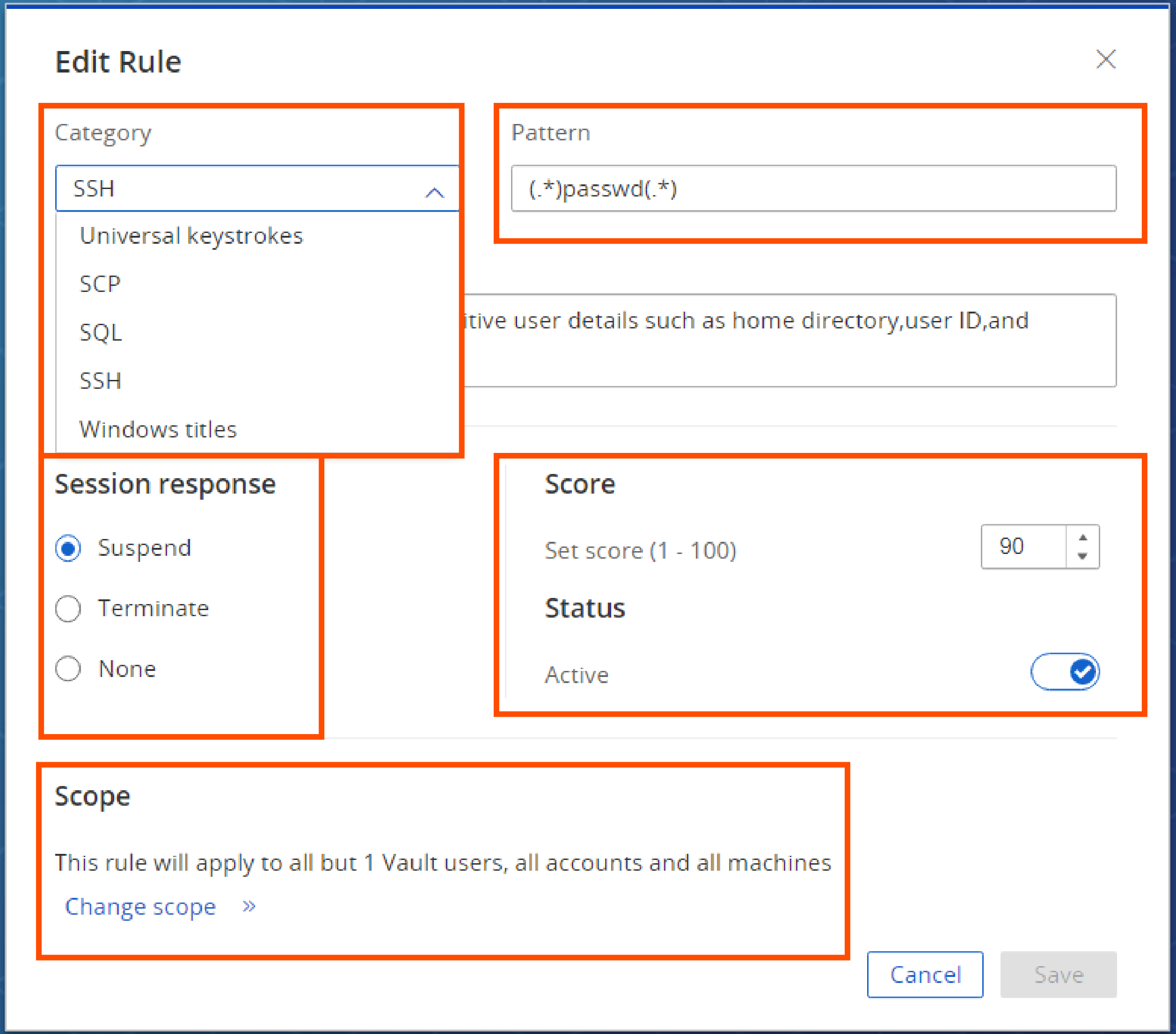
Please contact your system administrator

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



Edit Rule

Category: SSH

Universal keystrokes
SCP
SQL
SSH
Windows titles

Pattern: (.*)passwd(.*)

itive user details such as home directory,user ID,and

Session response

● Suspend
○ Terminate
○ None

Score

Set score (1 - 100): 90

Status

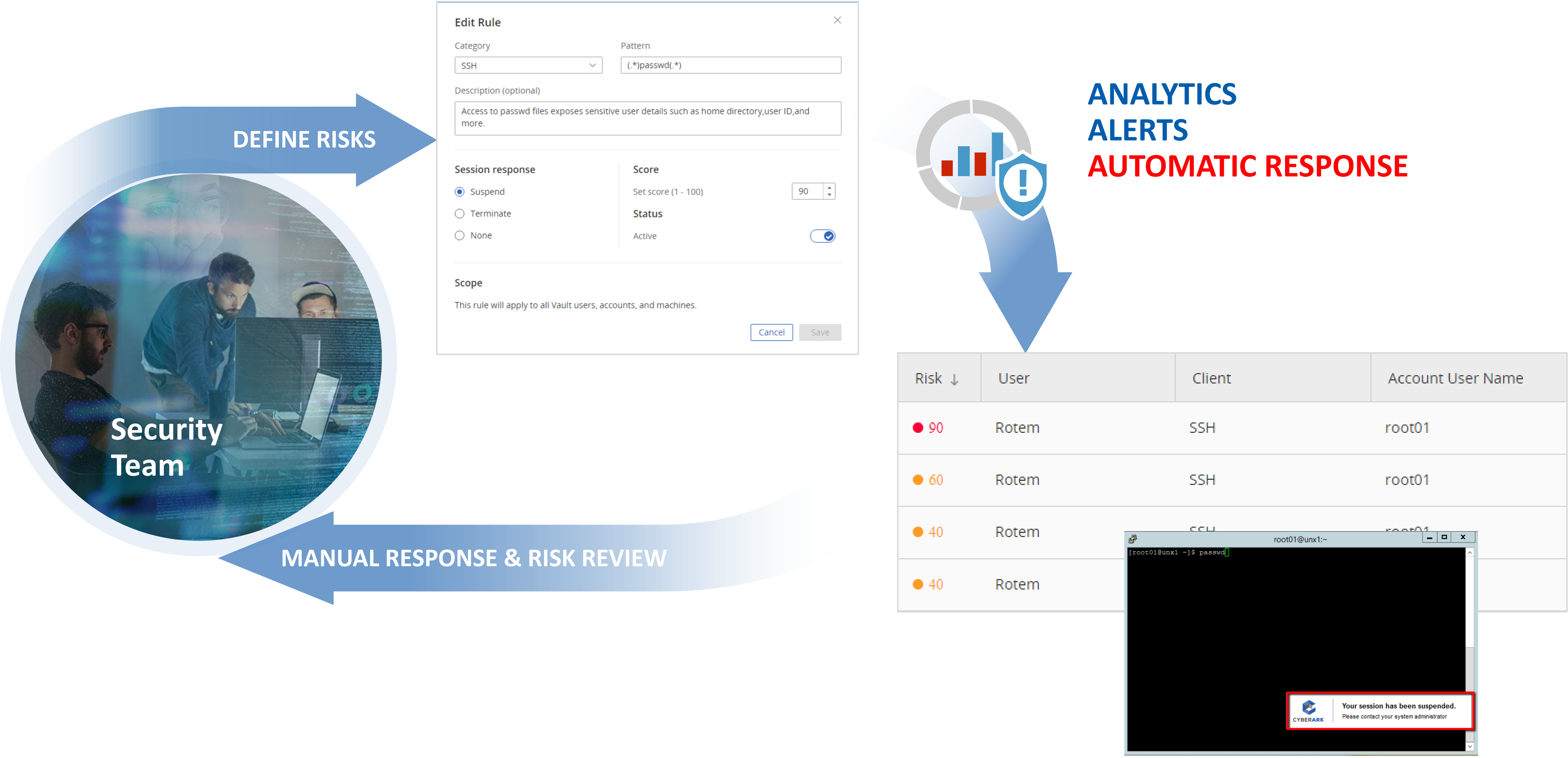
Active ☑

Scope

This rule will apply to all but 1 Vault users, all accounts and all machines

Change scope »

Session Analysis and Response Life Cycle



Edit Rule

Category: SSH

Pattern: (.*)passwd(.*)

Description (optional): Access to passwd files exposes sensitive user details such as home directory,user ID,and more.

Session response
- ● Suspend
- ○ Terminate
- ○ None

Score: Set score (1 - 100) 90

Status: Active

Scope

This rule will apply to all Vault users, accounts, and machines.

Risk ↓	User	Client	Account User Name
● 90	Rotem	SSH	root01
● 60	Rotem	SSH	root01
● 40	Rotem	SSH	root01
● 40	Rotem		

```
root01@unx1:~
[root01@unx1 ~]$ passwd
```

CYBERARK **Your session has been suspended.** Please contact your system administrator

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

Summary

Summary

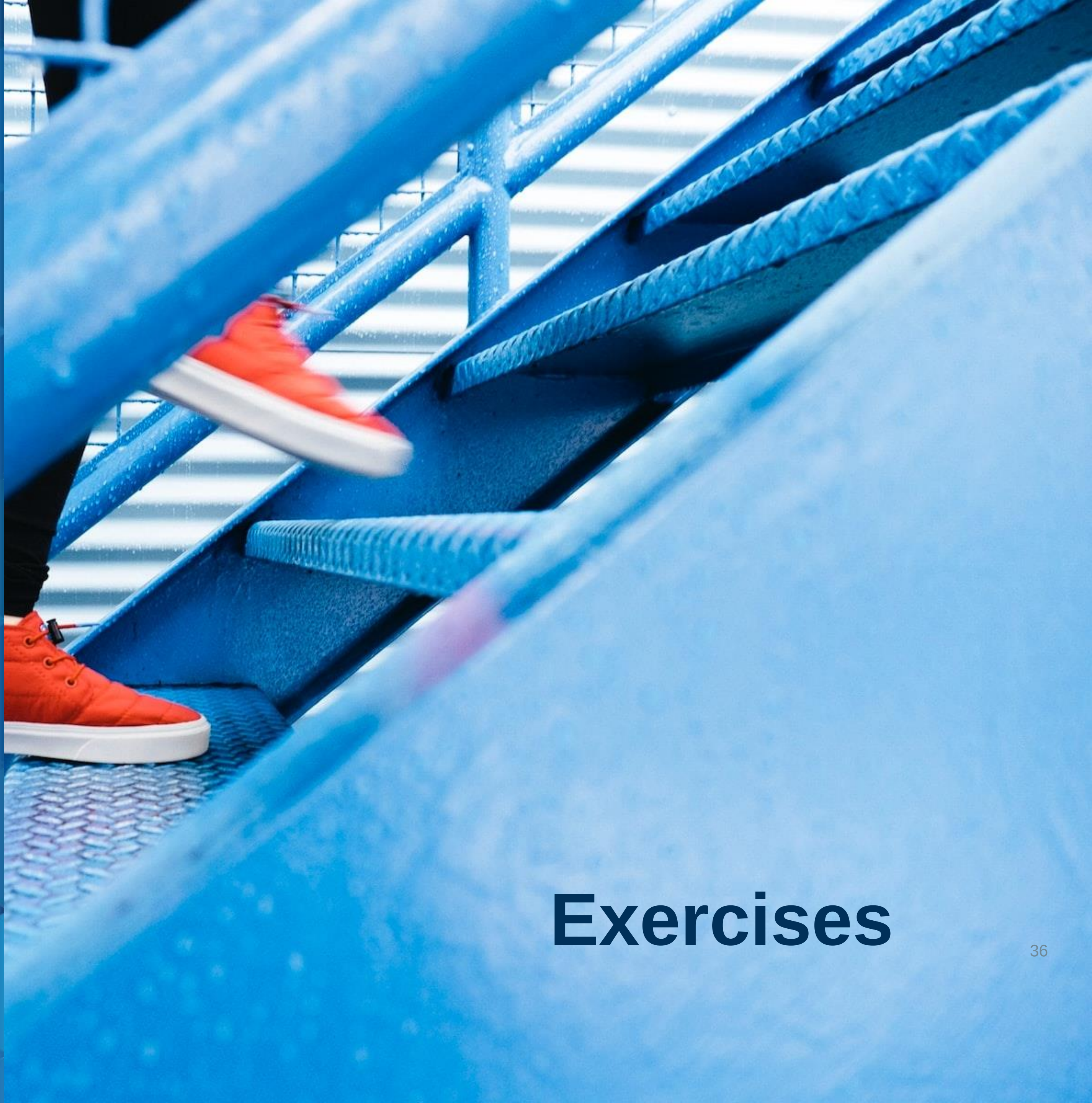
In this session we:

- 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

You may now complete the following exercise:

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



Exercises