CYBERARK®
The Identity Security Company™

PAM Administration

Privileged Threat Analytics

Agenda

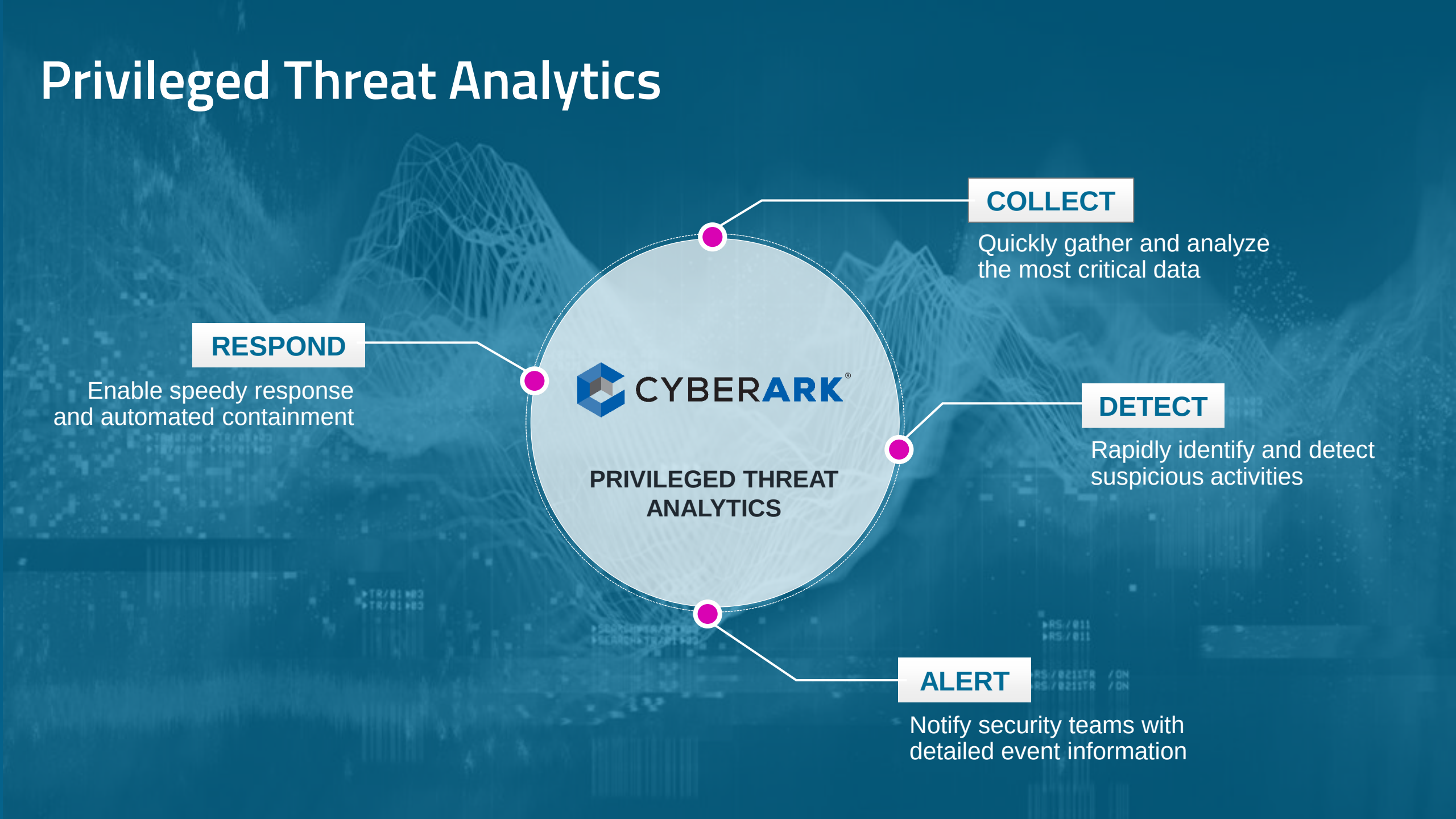
By the end of this session the participant will be able to:

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

CYBERARK®

Privileged Threat Analytics

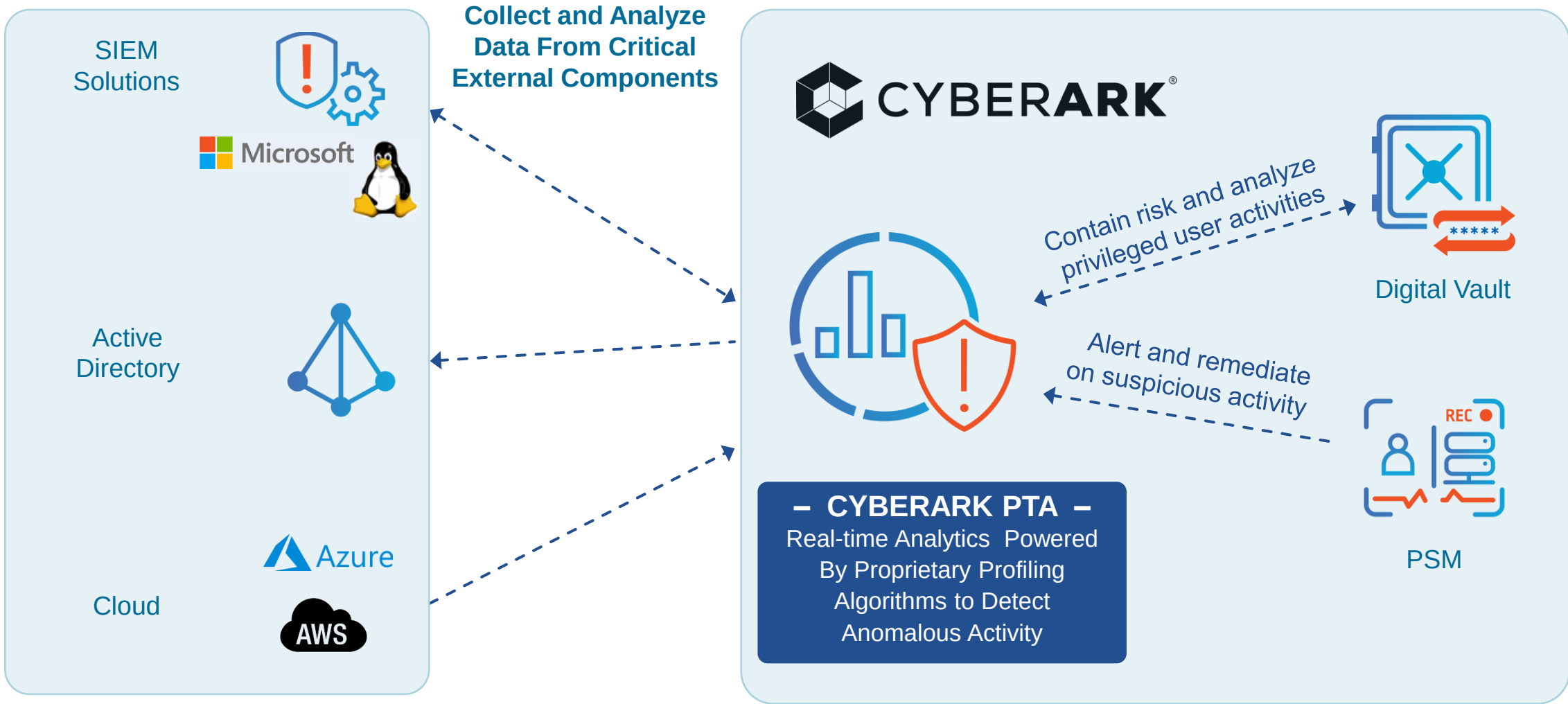


Collect

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

CYBERARK®

Collect and Analyze the Right Data



Detect

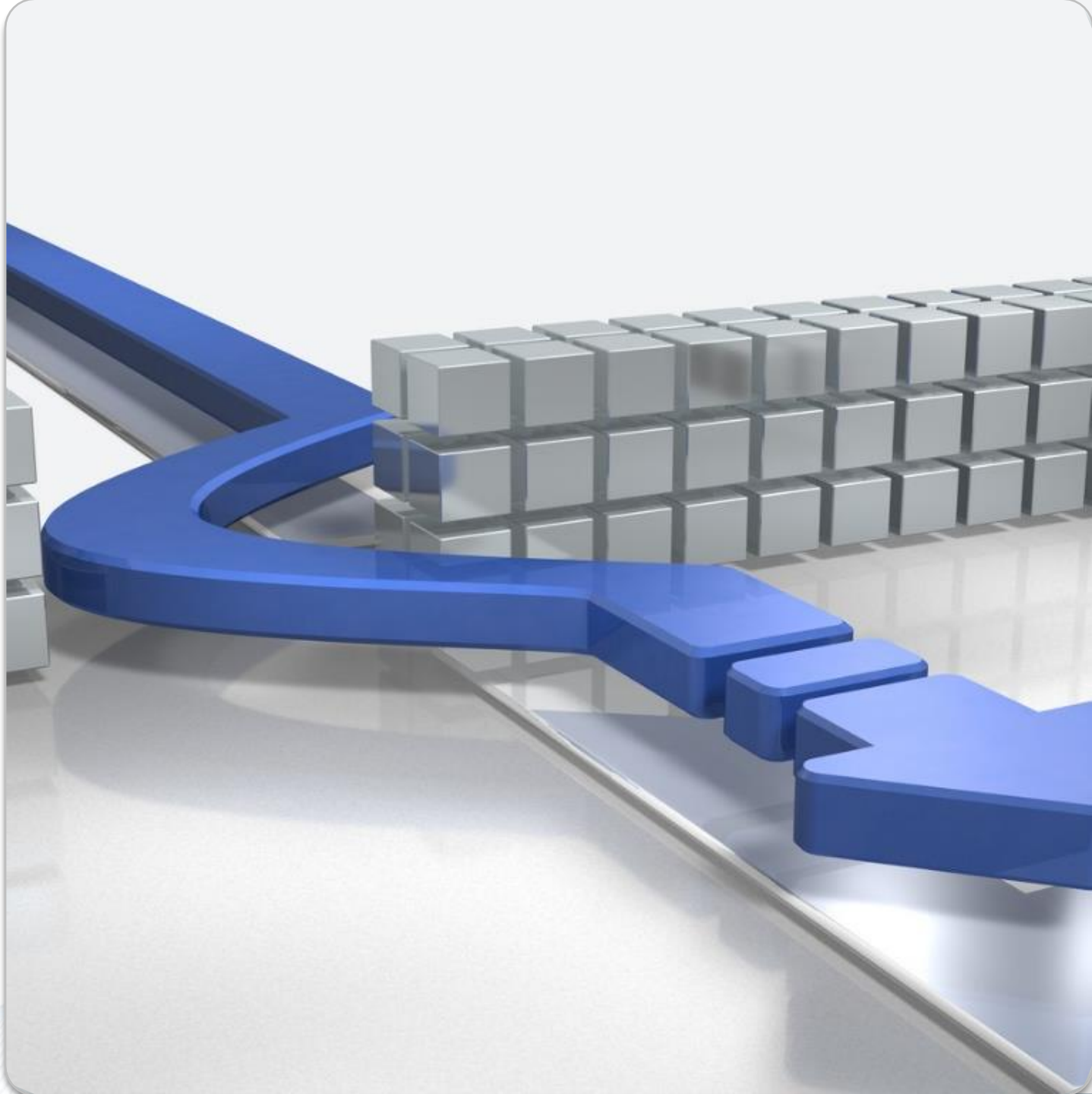
- Attacks that bypass security controls
- Statistical anomalies
- Active Directory risks

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

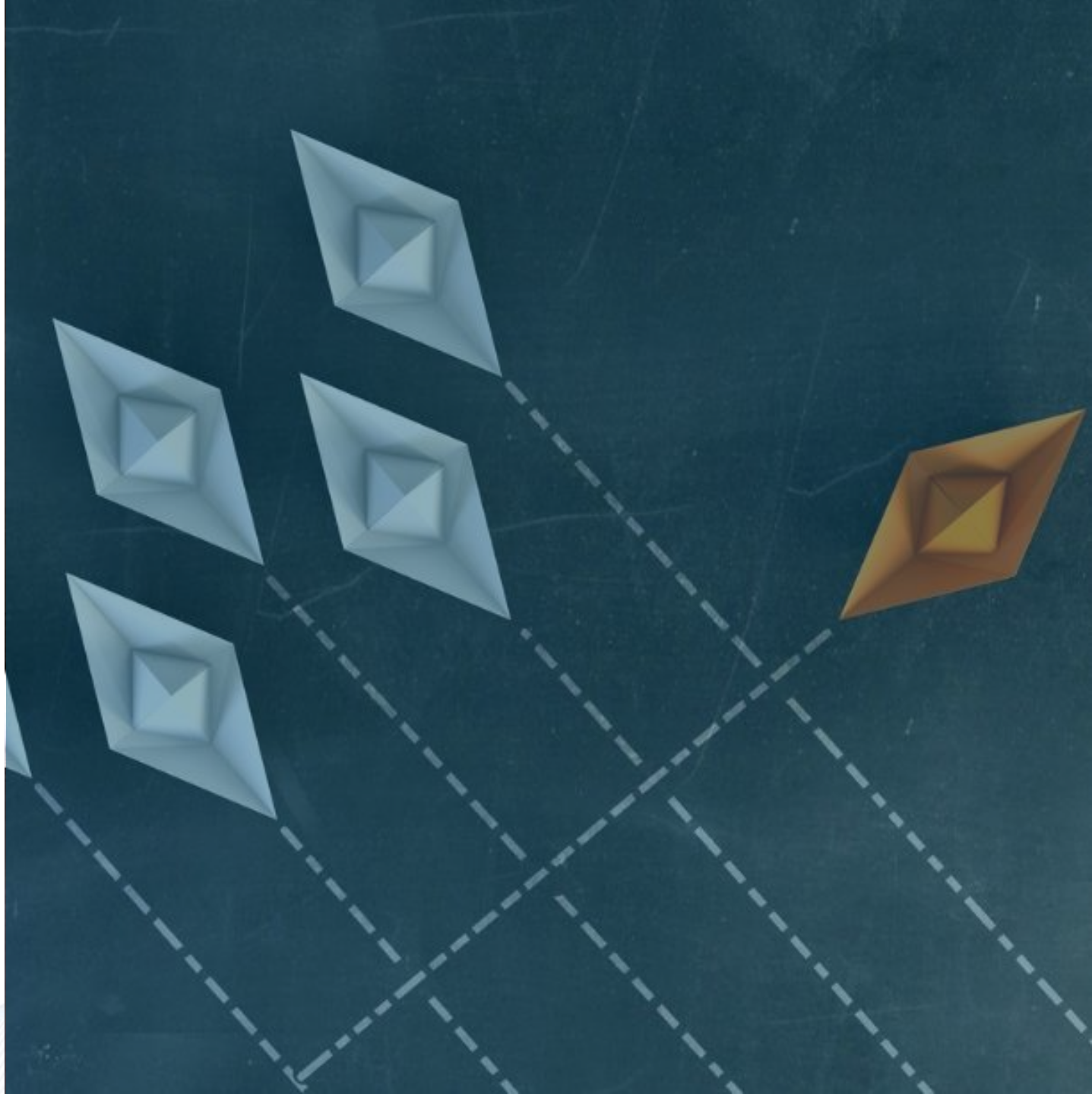


Statistical Anomalies

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	✗	✓	✗	✗

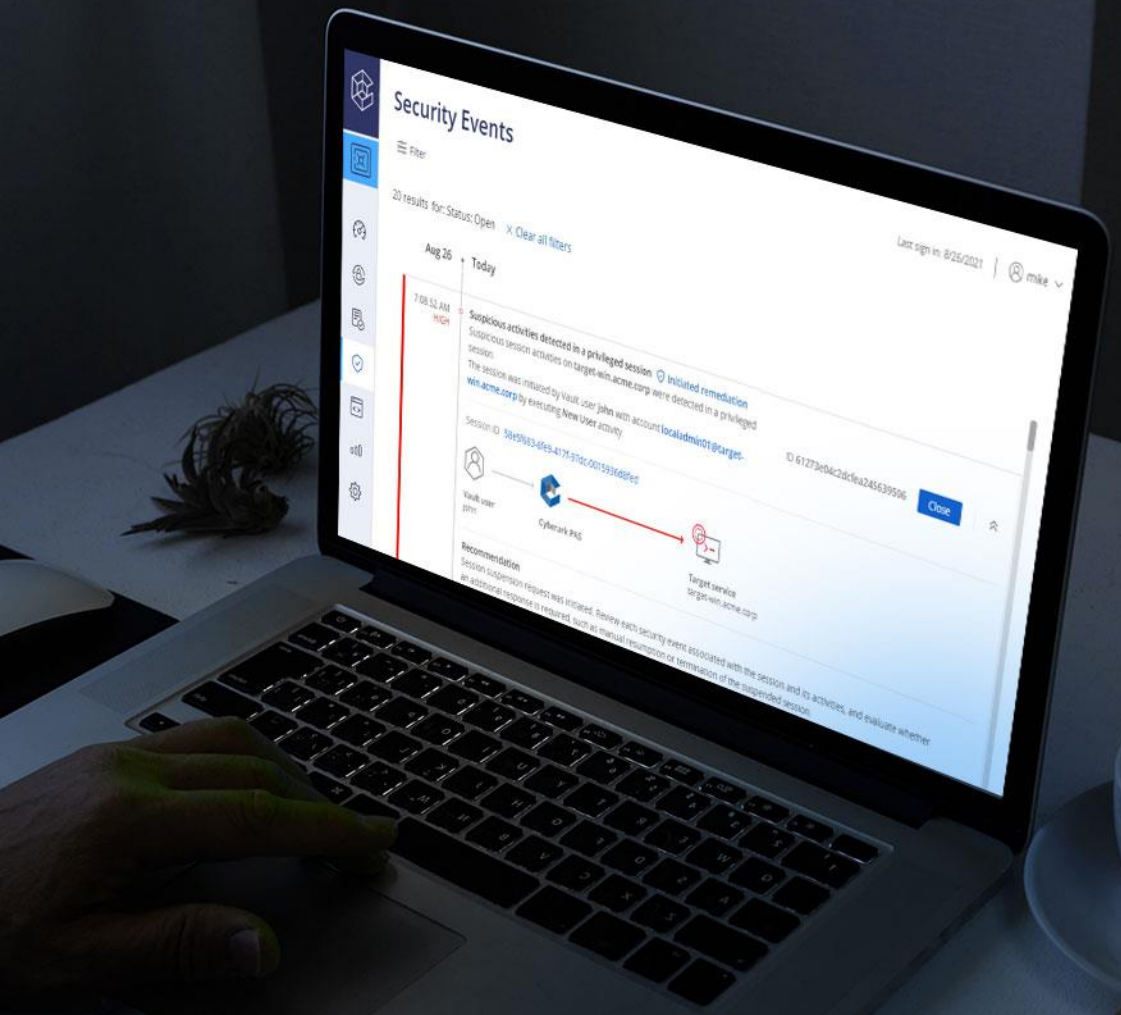
CYBERARK®

Alert

- Security Events
- Security Monitoring Navigation

CYBERARK®

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:

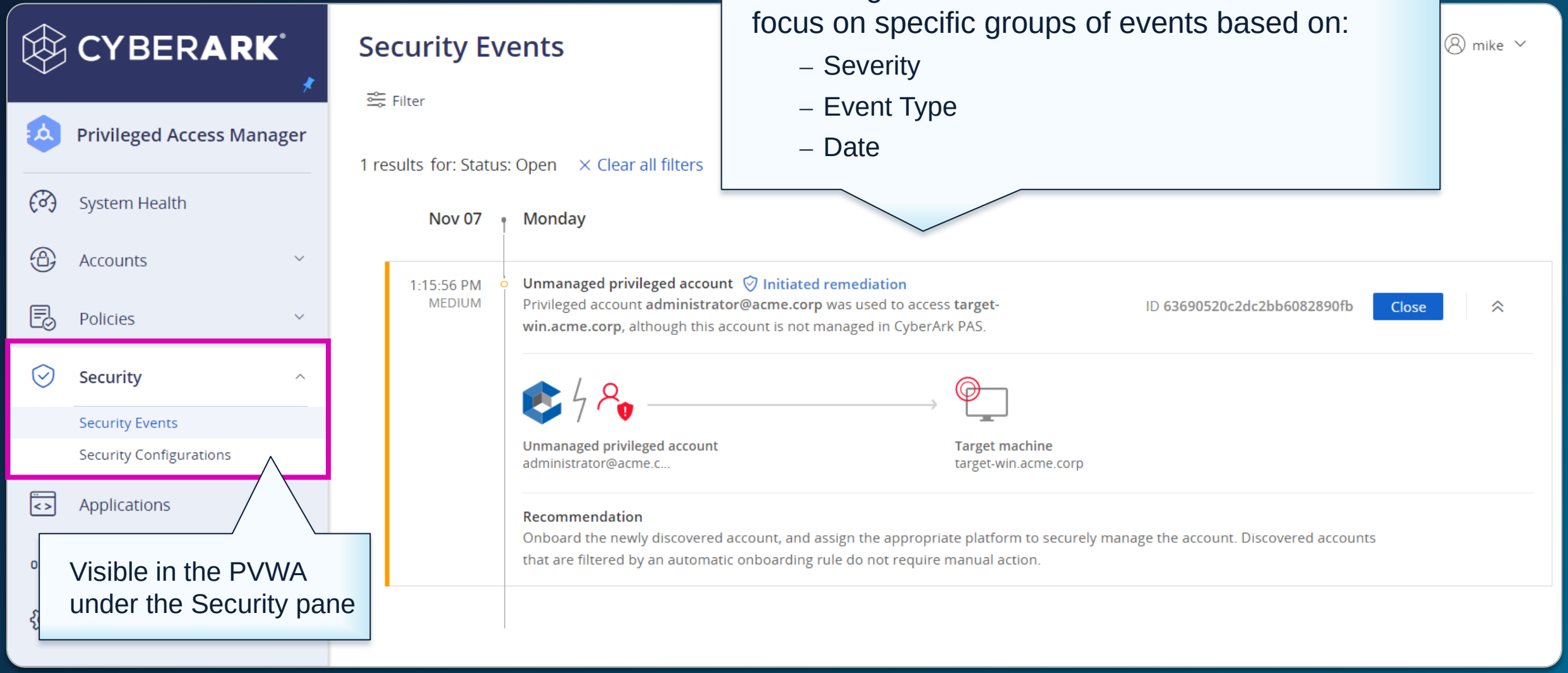
- Are assigned risk scores based on severity of the detected anomaly
- Contain granular details related to the suspected attack
- Can easily be reviewed in the PVWA and/or in a SIEM dashboard

CYBERARK®

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:

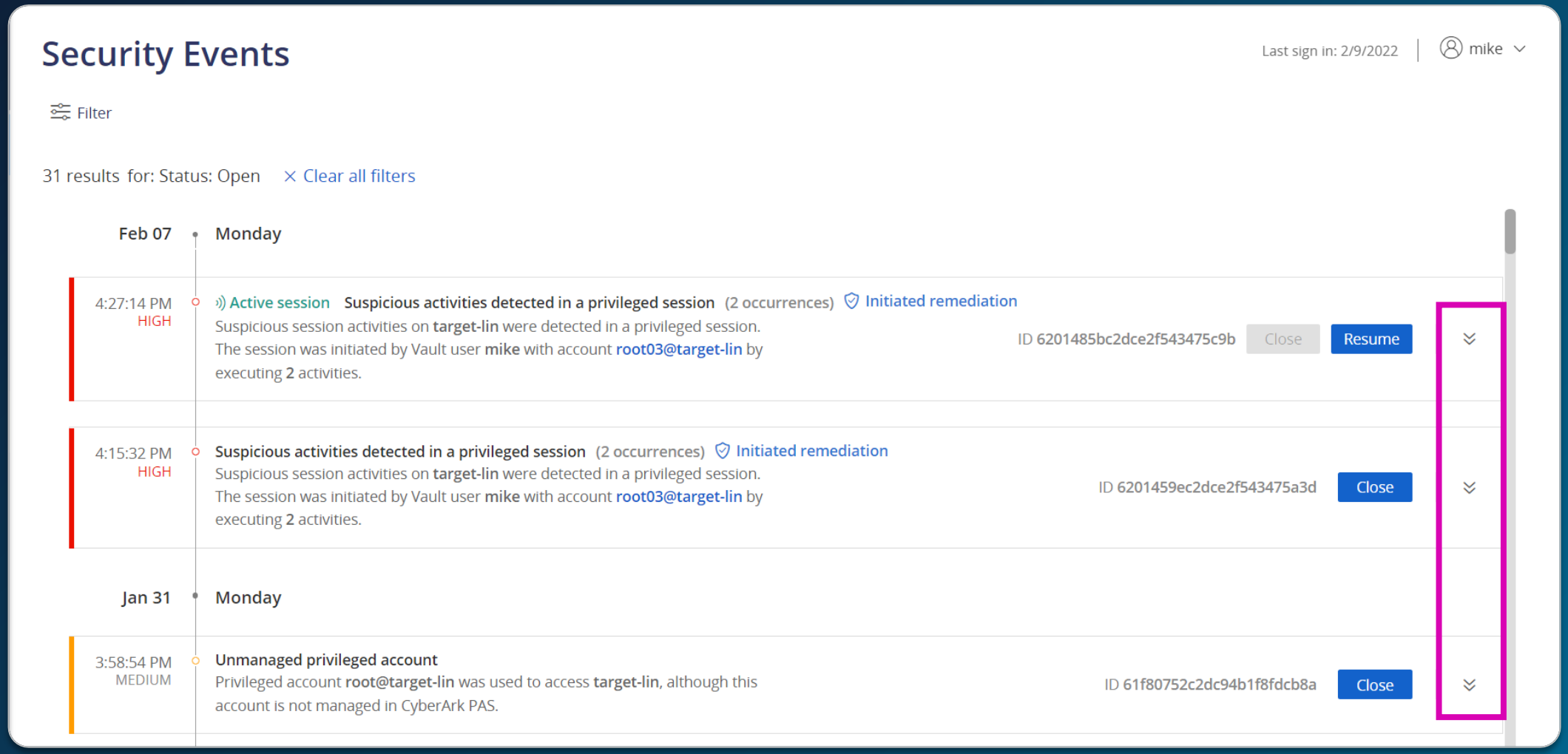
- Severity
- Event Type
- Date



Visible in the PVWA under the Security pane

CYBERARK

Security Event Compact View



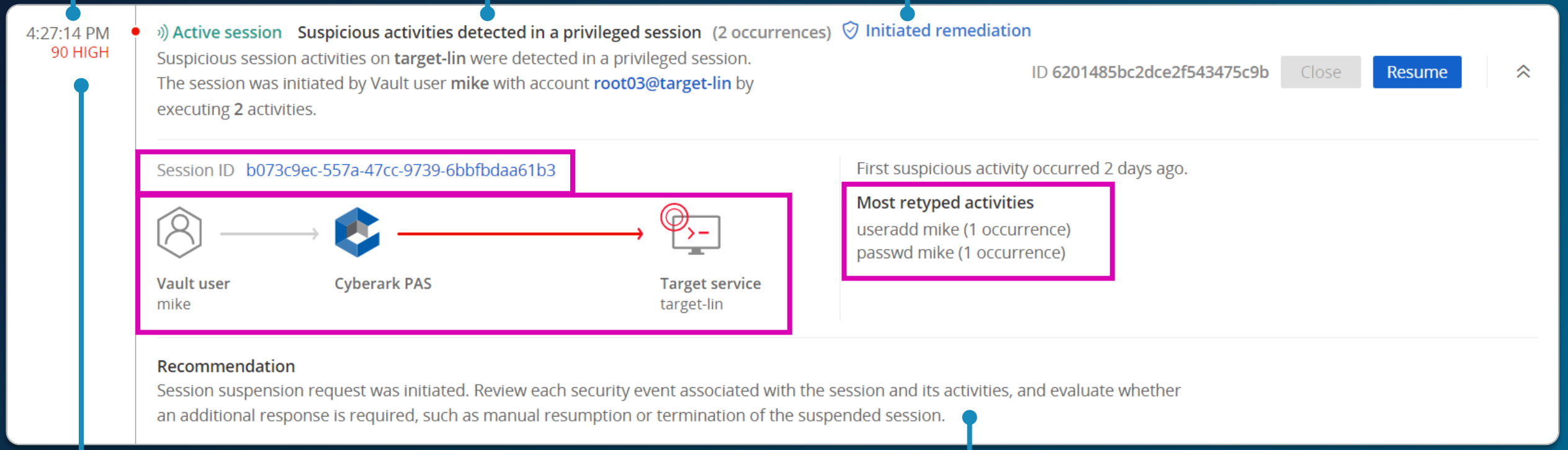
CYBERARK®

Reviewing Security Events in the PVWA

The last time the event was detected.

The name of the event

Shown when remediation has been started.

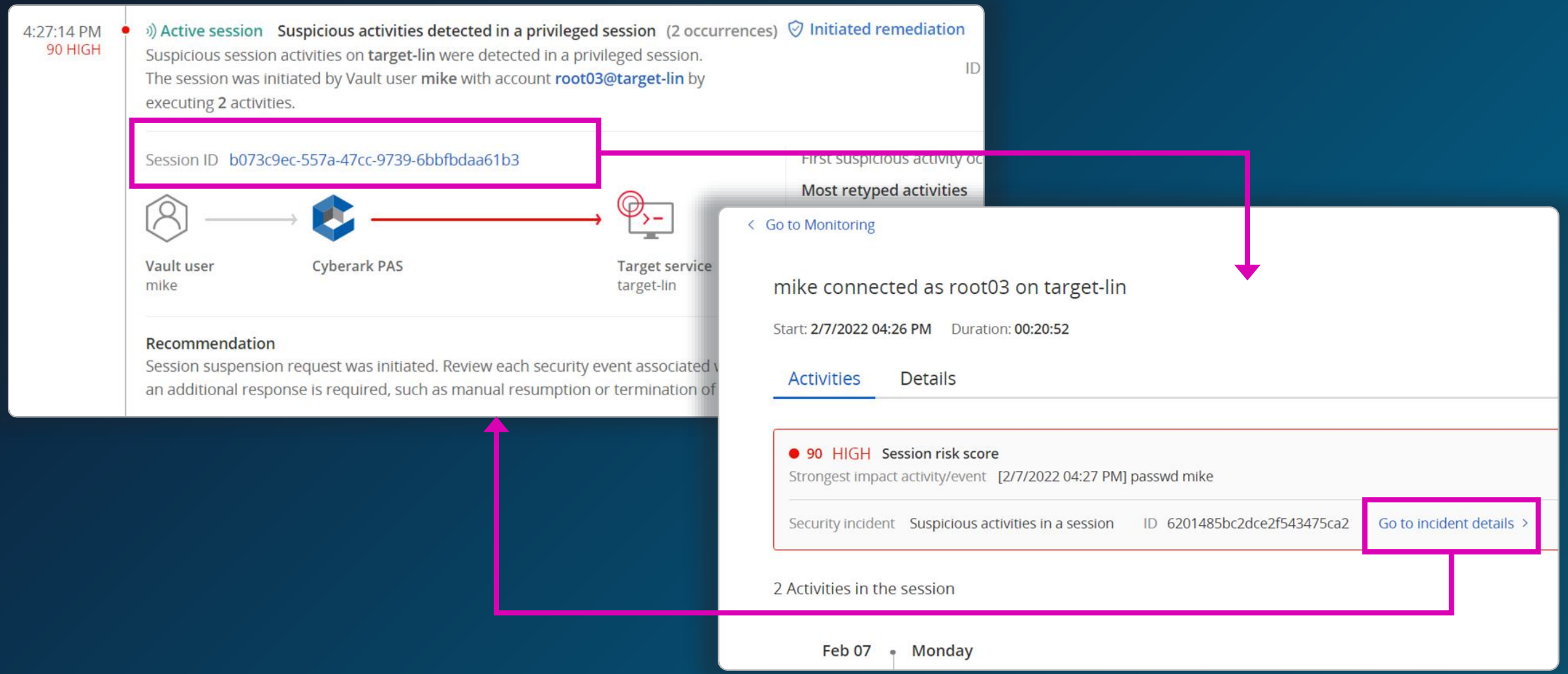


The score and severity of the event (high, medium, low).

Recommended action to take / Automatic remediation action that was taken

CYBERARK

Easy Navigation: Security-Monitoring



CYBERARK

Respond

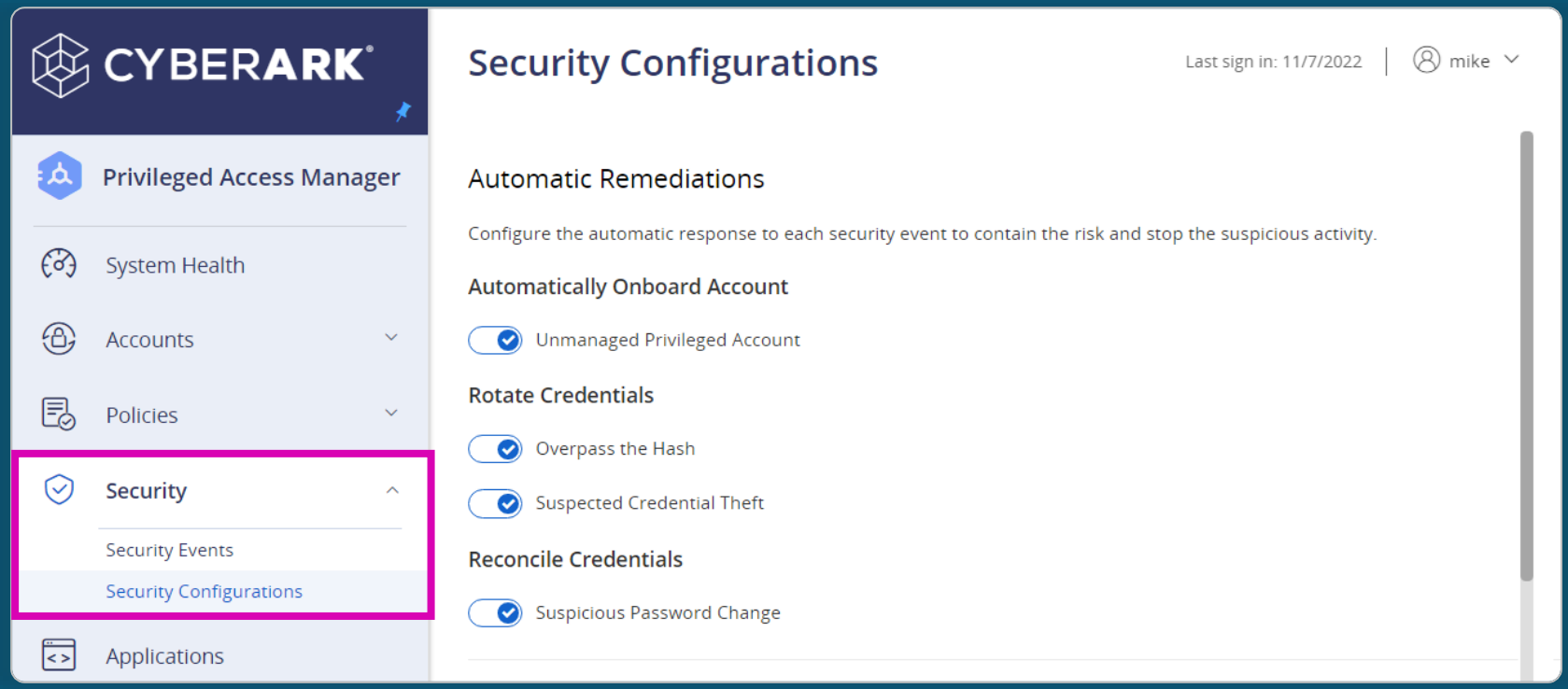
- Automatic Remediation
- PSM – PTA Integration
- Session Analysis and Response
- Risk-based Prioritization
- Configuring Session Analysis and Response Rules
- The Session Analysis and Response Life Cycle

Respond with Automatic Remediations

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

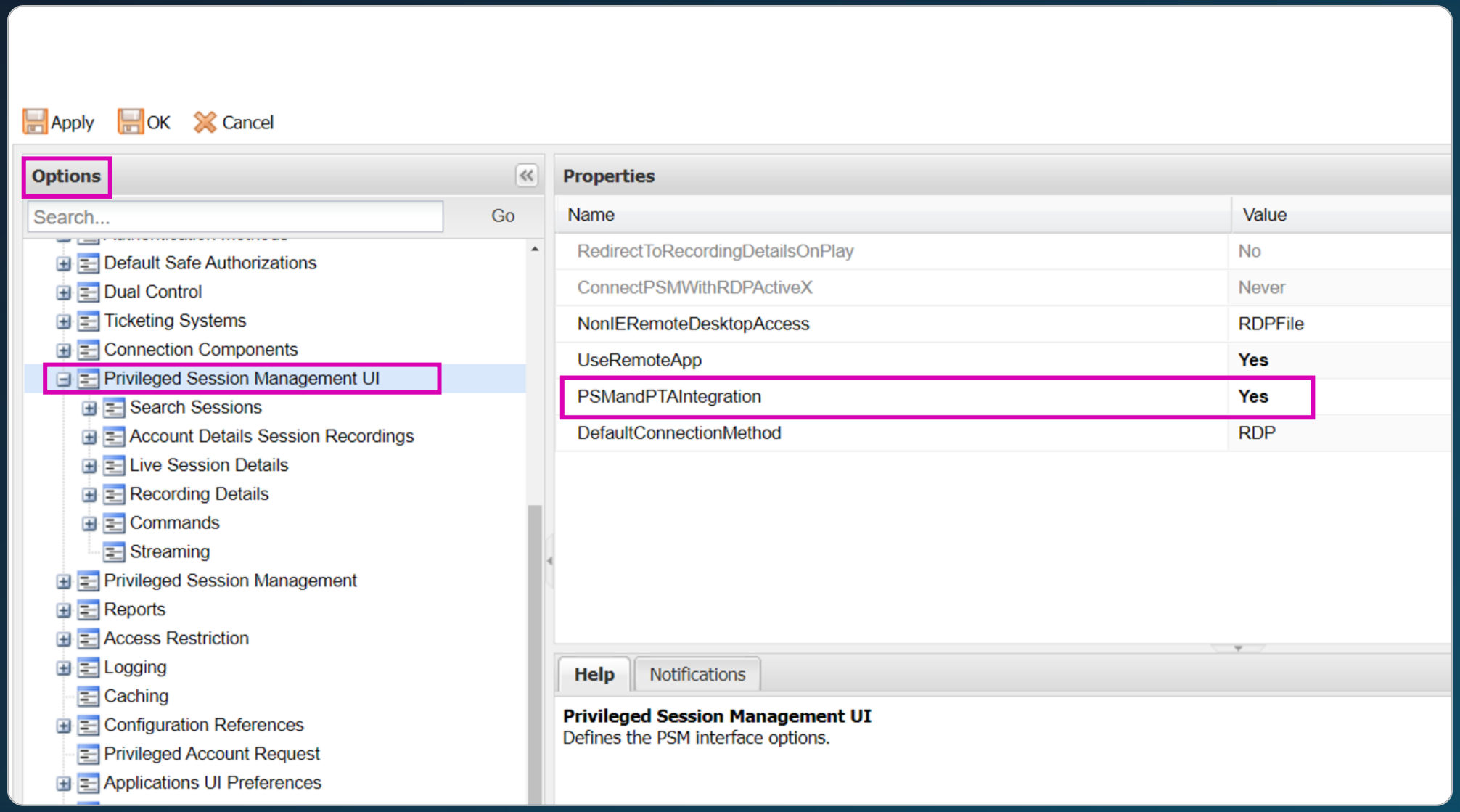
PTA can contain in-progress attacks by automatically:

- Onboarding unmanaged accounts
- Rotating credentials
- Reconciling credentials



CYBERARK

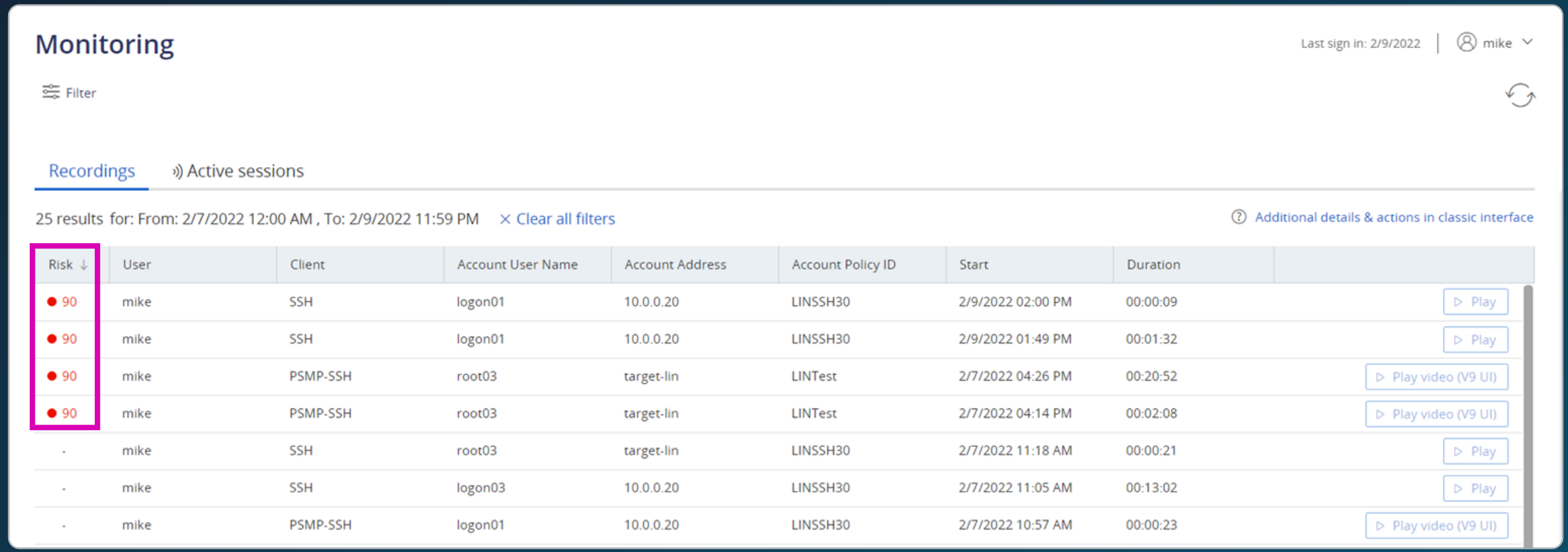
PSM – PTA Integration



CYBERARK®

Session Analysis and Response

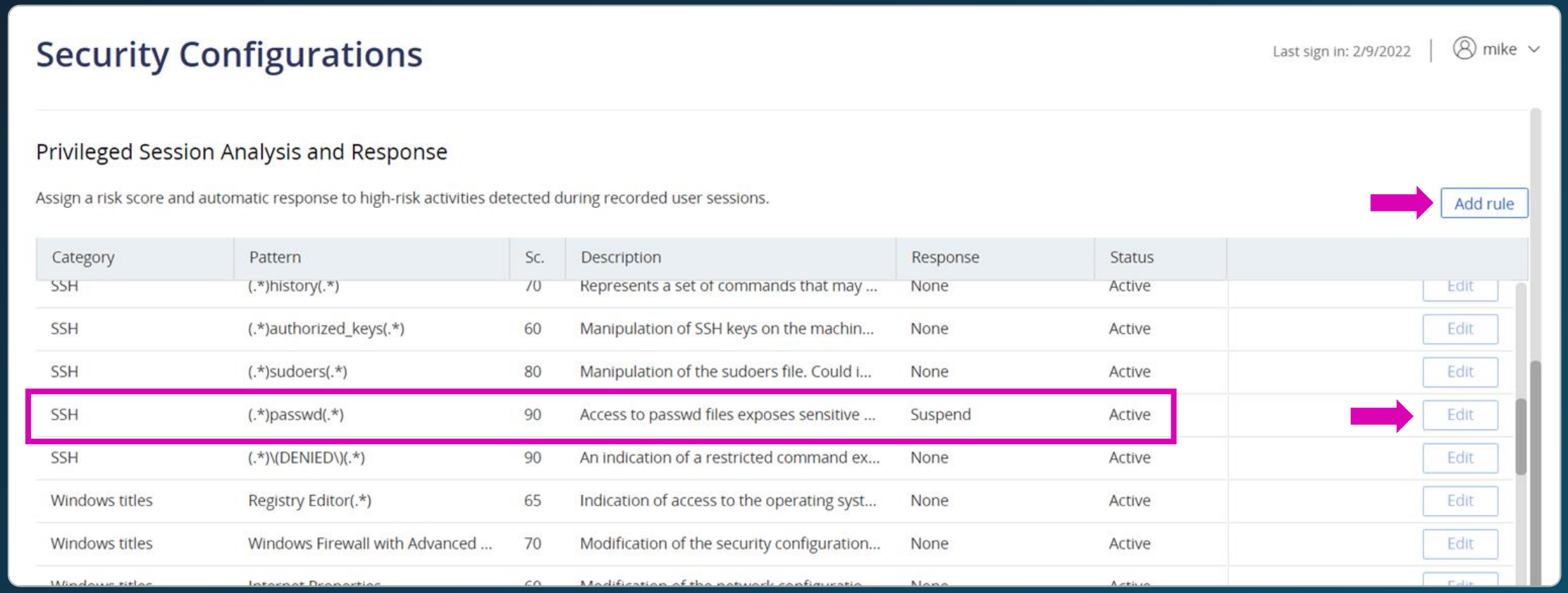
- Connecting the **PTA** and **PSM** leverages the analytic capabilities of the PTA, which receives details of PSM privileged sessions and user activities, analyzes them, and assigns a risk score to each session.
- Audit teams now can prioritize workloads based on risk scores.



CYBERARK®

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.



CYBERARK®

Risk-based Prioritization

Events

- Session #1
- Session #2
- Session #3
- Session #4
- Session #5
- Session #6
- Session #7
- Session #5364

Risk-Based Priorities

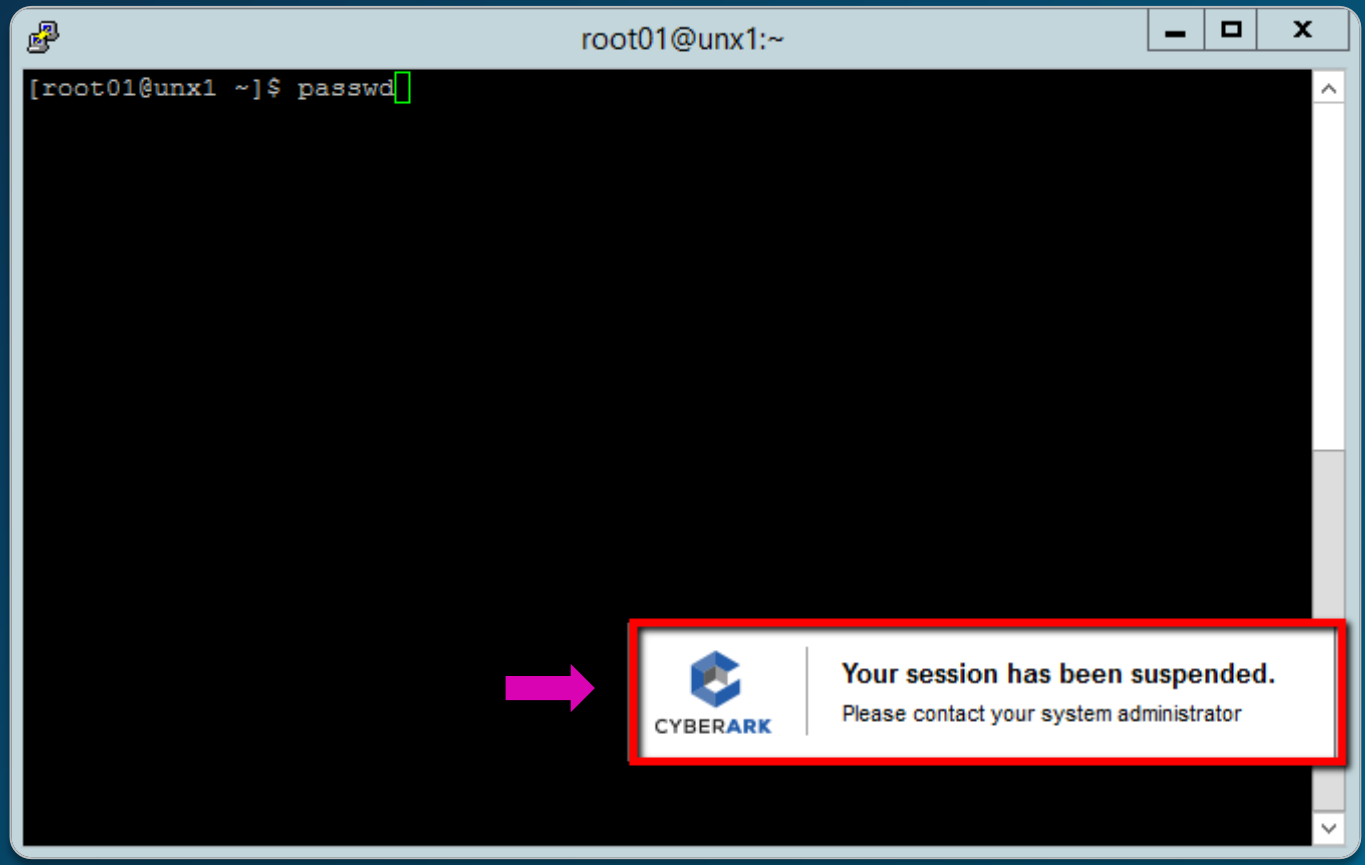
- Session #323
- Session #83
- Session #2
- Session #421
- Session #95
- Session #34
- Session #297
- Session #5364

CYBERARK®

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.

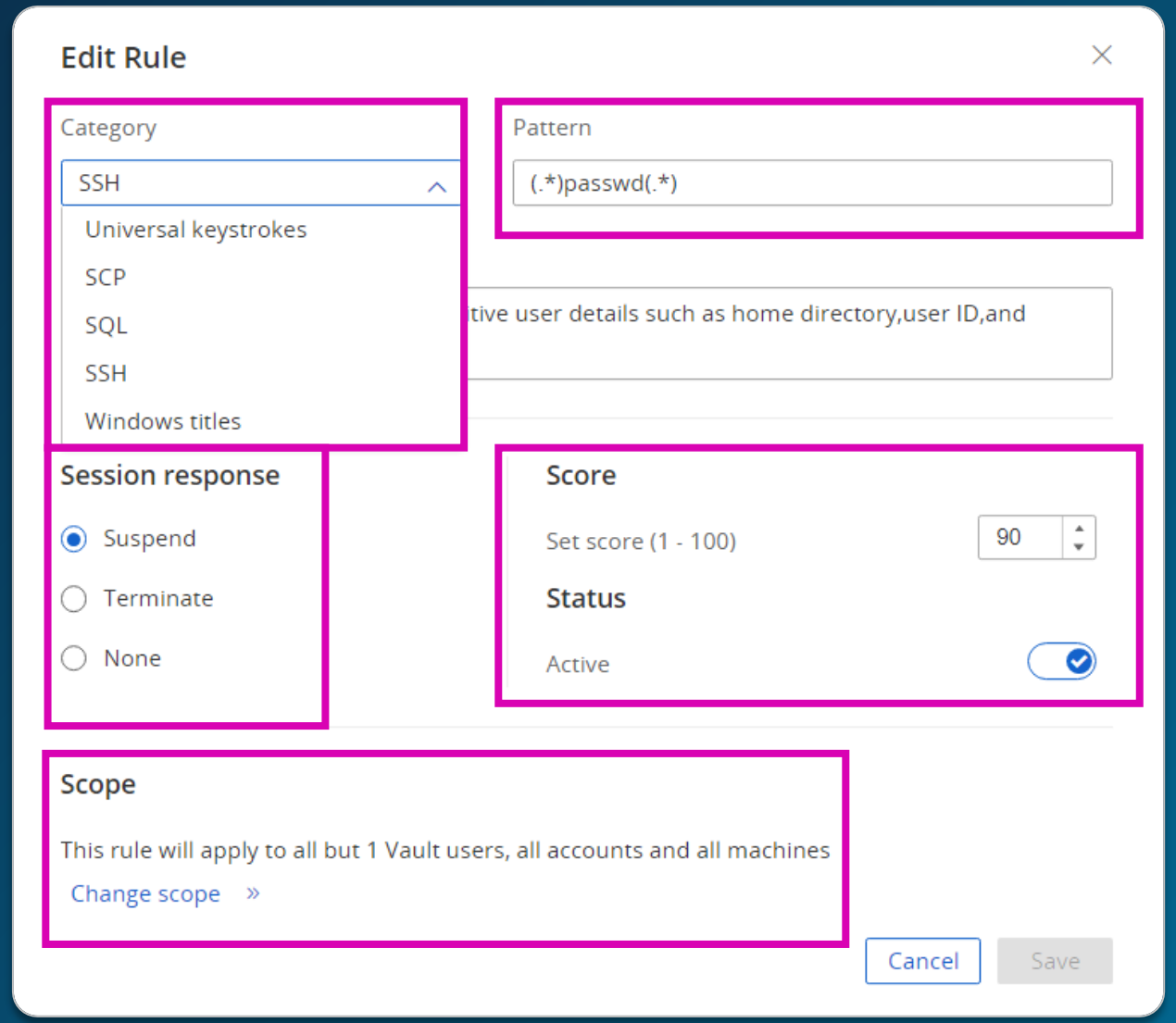


CYBERARK

Configuring Rules

Rules are defined by:

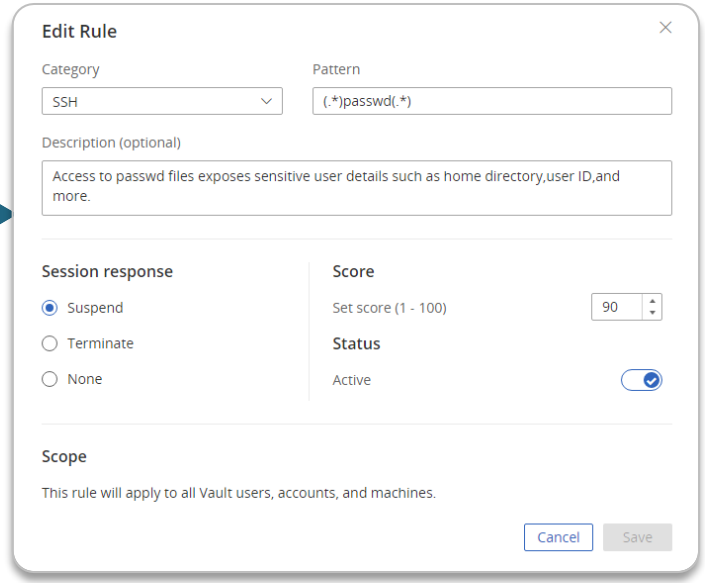
- **Category**
  - SSH
  - Universal Keystrokes
  - SCP
  - SQL
  - Windows title
- **Pattern**: a regular expression to be monitored
- **Session response**
  - Suspend
  - Terminate
  - None
- **The Threat Score** (1-100)
- **Scope**: To whom or what the rule will apply



CYBERARK®

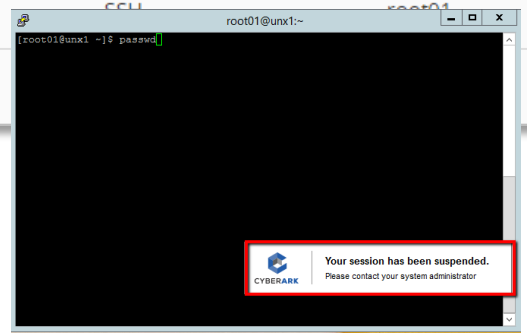
Session Analysis and Response Life Cycle

DEFINE RISKS



ANALYTICS
ALERTS
AUTOMATIC RESPONSE

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



MANUAL RESPONSE & RISK REVIEW

CYBERARK®

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

CYBERARK®

Privileged Threat Detection and Automatic Response Demo:

AWS

CYBERARK®

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

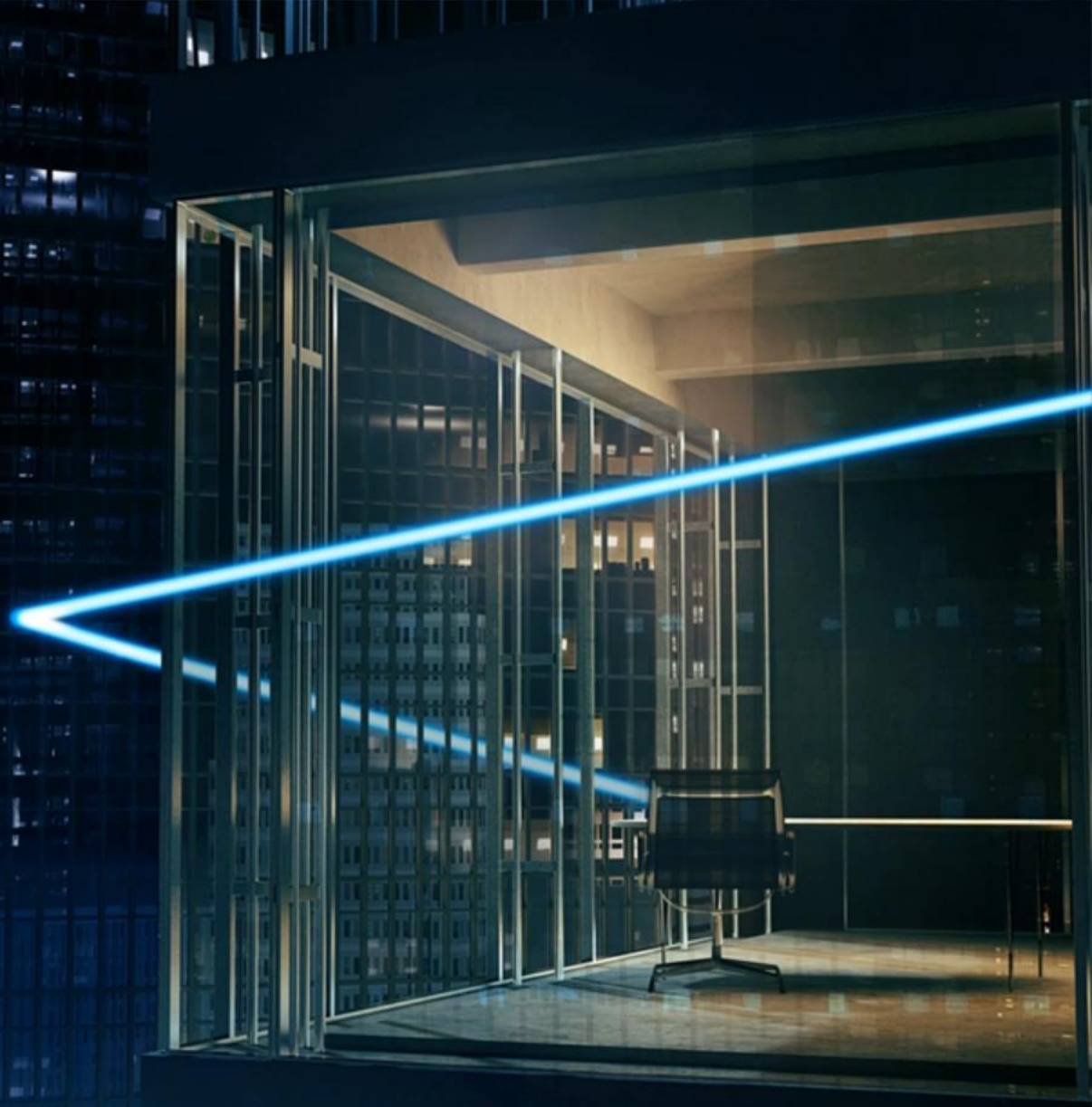
- The following capabilities are supported for Azure:
  - Detect unmanaged privileged access
  - Detect suspected credential theft

CYBERARK®
The Identity Security Company™

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

CYBERARK®

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