SECURONIX™ | CYBERARK®

SOLUTION BRIEF

Protect Privileged User Accounts with Securonix and CyberArk

Cybersecurity grows more complex over time and is increasingly critical for profitable businesses. Attackers continue to evolve more sophisticated attacks that legacy perimeter defenses fail to detect and protect, while modern business technologies generate increasing volumes of data that need to be sorted through to find the attacks.

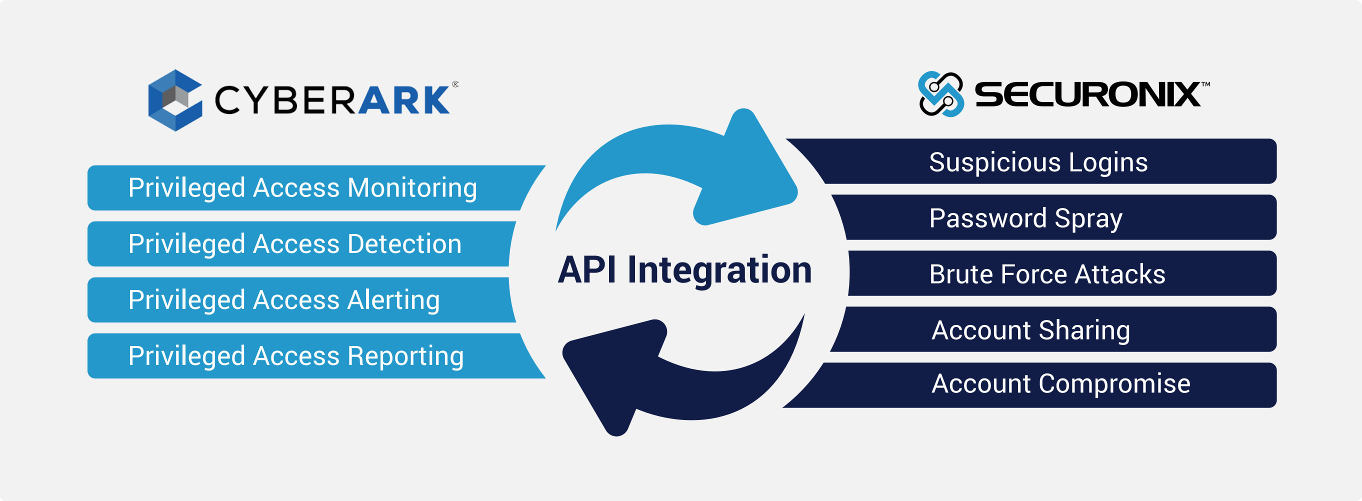
Securonix Next-Generation SIEM transforms big data into actionable security intelligence, leveraging machine learning to power advanced threat detection, rapid investigation, and intelligent incident response. It collects enormous volumes of data in real-time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

The CyberArk Privileged Access Security Solution delivers risk-based credential protection and session management to detect and prevent attacks involving privileged access. The solution provides multi-layered security to mitigate the risk of advanced attacks across on-premises, cloud, and hybrid environments in order to help organizations defend against advanced persistent threats and insider threats.

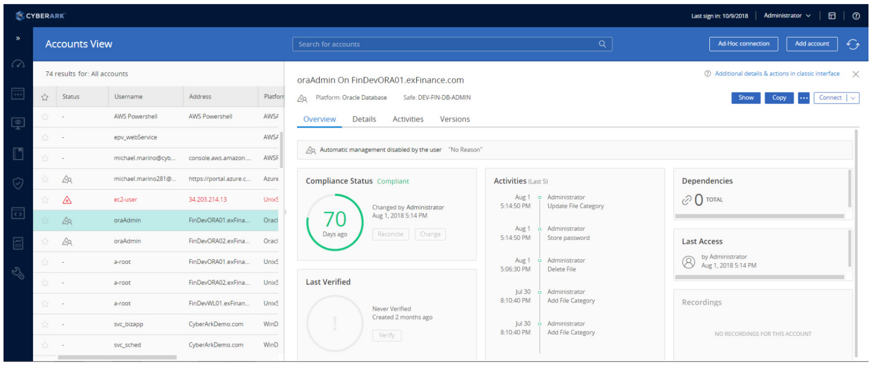
By integrating Securonix and CyberArk, organizations receive a world-class comprehensive protection and prevention solution for mission-critical identity management and privileged access security. Proactively, CyberArk detects and prevents the latest sophisticated attacks that attempt to misuse privileged access.

Integration Benefits

- Artificial intelligence-driven prevention through behavioral baselining of password retrievals.
- Backdoor account creation detection.
- CyberArk account modification detection.
- Continuous detection for terminated user activity, high number of failed login attempts, and multiple host logins.



Securonix API integration with CyberArk provides a playbook to quickly create an incident response case.



74 results for: All accounts

Status	Username	Address	Platforr
-	AWS Powershell	AWS Powershell	AWSA
-	epv_webService		AWSA
-	michael.marino@cyb...	console.aws.amazon....	AWSF
	michael.marino281@...	https://portal.azure.c...	Azure
	ec2-user	34.203.214.13	UnixS
	oraAdmin	FinDevORA01.exFina...	Oracl
	oraAdmin	FinDevORA02.exFina...	Oracl
-	a-root	FinDevORA01.exFina...	UnixS
-	a-root	FinDevORA02.exFina...	UnixS
-	a-root	FinDevWL01.exFinan...	UnixS
-	svc_bizapp	CyberArkDemo.com	WinD
-	svc_sched	CyberArkDemo.com	WinD

oraAdmin On FinDevORA01.exFinance.com

Platform: Oracle Database   Safe: DEV-FIN-DB-ADMIN

Additional details & actions in classic interface

Automatic management disabled by the user "No Reason"

Compliance Status Compliant
70 Days ago
Changed by Administrator
Aug 1, 2018 5:14 PM

Last Verified
Never Verified
Created 2 months ago

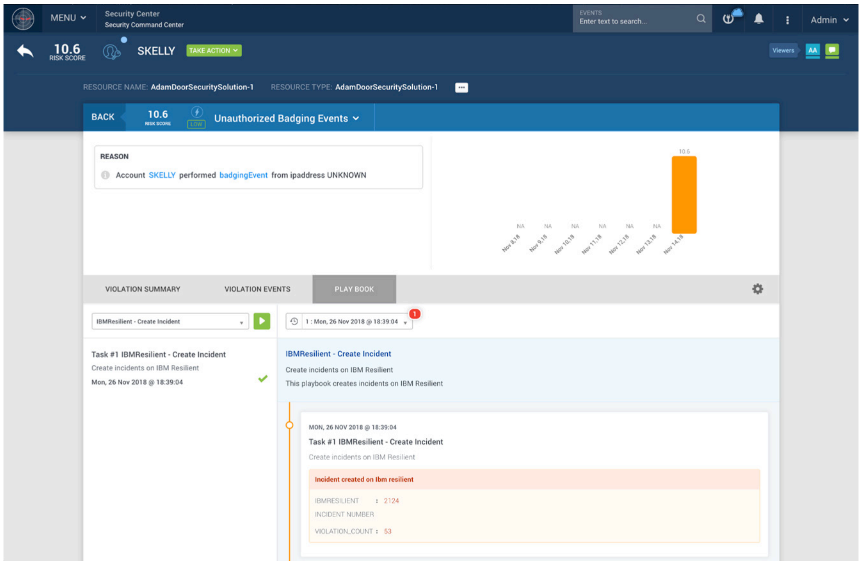
Activities (Last 5)
Aug 1 5:14:50 PM Administrator Update File Category
Aug 1 5:14:50 PM Administrator Store password
Aug 1 5:06:30 PM Administrator Delete File
Jul 30 8:10:40 PM Administrator Add File Category
Jul 30 8:10:40 PM Administrator Add File Category

Dependencies
0 TOTAL

Last Access
by Administrator
Aug 1, 2018 5:14 PM

Recordings
NO RECORDINGS FOR THIS ACCOUNT

The CyberArk dashboard provides administrators with a clear view of master policies, privileged access, session recordings, alerts on anomalous behavior, and more.



RESOURCE NAME: AdamDoorSecuritySolution-1   RESOURCE TYPE: AdamDoorSecuritySolution-1

REASON
Account SKELLY performed badgingEvent from ipaddress UNKNOWN

Task #1 IBMResilient - Create Incident
Create incidents on IBM Resilient
Mon, 26 Nov 2018 @ 18:39:04

IBMResilient - Create Incident
Create incidents on IBM Resilient
This playbook creates incidents on IBM Resilient

MON, 26 NOV 2018 @ 18:39:04
Task #1 IBMResilient - Create Incident
Create incidents on IBM Resilient

Incident created on Ibm resilient
IBMRESILIENT : 2124
INCIDENT NUMBER
VIOLATION_COUNT : 53

Securonix syslog integration with CyberArk collects and enriches the user behavior data with further activity details. Securonix then assigns a risk score to the event, using peer group context analysis to elevate the risk score as needed. Securonix can then enact predefined threat playbook actions to further mitigate the threat.

How it Works

- CyberArk provides privileged access discovery, management, detection, alerting, and response on all privileged users.
- Securonix behavioral analytics uses self-learning to baseline normal behavior patterns in your user data and detects further account misuse and anomalous behaviors.
- Securonix assigns threat risk scores and will trigger alerts when above a set threshold.
- Securonix enriches privileged access information with endpoint and user data to create further insights and helps you visualize your cybersecurity threats, risks, and compliance metrics.

About Securonix

Securonix is redefining the next generation of security monitoring using the power of machine learning and big data. Built on Hadoop, the Securonix solution provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and intelligent incident response on a single platform. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, fraud, and application security monitoring requirements. For more information visit www.securonix.com.

About CyberArk

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. For more information visit www.cyberark.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2019 Securonix