

# Take your threat detection to next level

IBM QRadar SIEM  
IBM Verify Identity Protection

[tomasz.zalewski@pl.ibm.com](mailto:tomasz.zalewski@pl.ibm.com)

IBM Security QRadar

Offenses / ID: 73

# Process Created a Thread into System Process preceded by Detected a New or Updated COM Component in User Registry Hive preceded by De...

ID : 73    Type : Log Source Hostname (custom)    Actions

Offense Type Log Source Hostname (custom)	Offense Source DESKTOP-UEJFMTT	Source IPs ● INT 172.16.60.31	Destination IPs ● INT 172.16.60.31
Status Open	Assigned Unassigned	Start June 4, 2020 4:08 PM	Duration 7 minutes
Events 549	Flows 0	Categories 2	Networks LocalNetwork.QRadarNetwork

### Insights (4)

- Process Created a Thread into System Process
- Malware Persistence: An AutoRun Key Has Been Added To Windows Registry
- Detected Possible COM Malicious Usage - InProcServer32 Registry Key Pointing to a File in Users Directory
- Detected a New or Updated COM Component in User Registry Hive

### Recent Events

View Events

### Magnitude

Relevance 6  
Credibility 3  
Severity 7

### Notes (0)

Add note +

Internal IPs    External IPs    Users    Log Sources

# What is IBM QRadar SIEM?

It turns events into offenses




# How does it do it?




Via correlations!


Rule (Click on an underlined value to edit it)

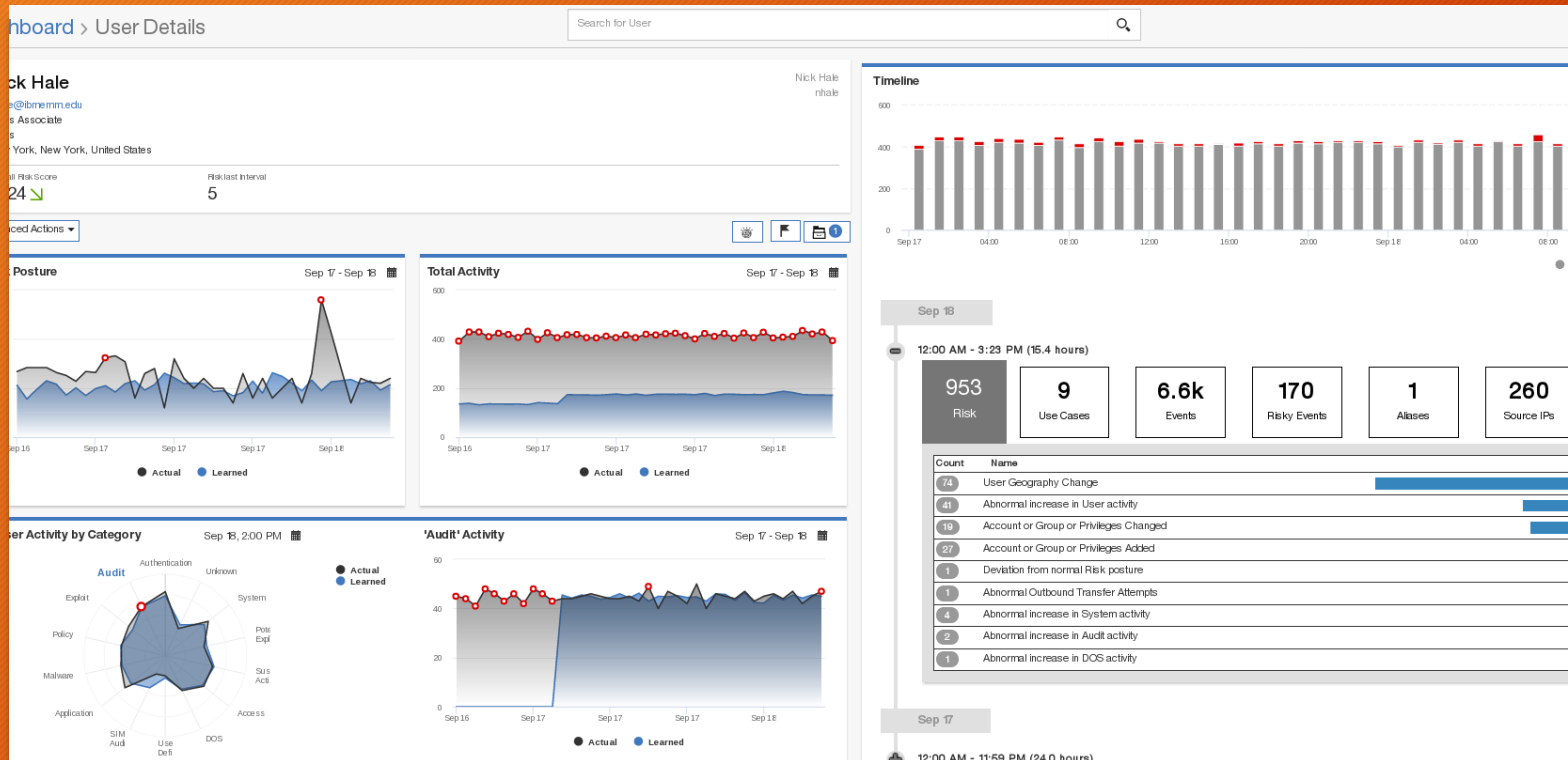
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by the  system

   and when an event matches all of the following [BB:UBA : Common Event Filters](#)

   and NOT when the source is located in other

   and when at least 2 events are seen with the same Username and different Source Geographic Country/Region in 15 minutes

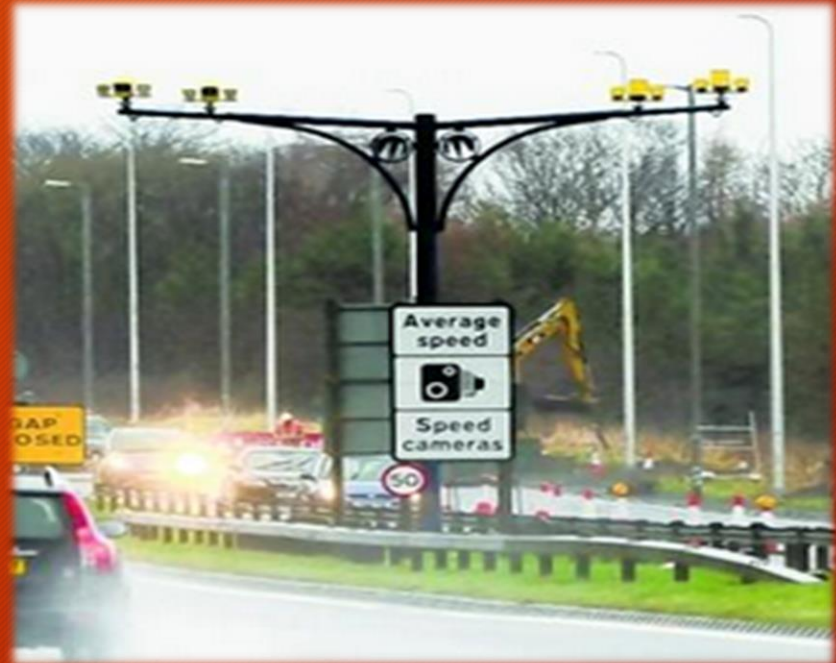


Insiders monitoring is free!

(Network) traffic monitoring is important!



VS



# Free applications!

- Enhancements
- Integrations
- Rule sets

The screenshot displays the IBM X-Force Exchange / App Exchange interface. At the top, there is a navigation bar with the text "IBM X-Force Exchange / App Exchange" and a search bar labeled "Search by Application". Below the navigation bar, there are three featured application cards:

- AWS Security Hub for SOAR**: Orchestrates AWS Security Hub actions with QRadar SOAR.
- Tenable for QRadar App**: Correlates Tenable findings with offenses in QRadar.
- AWS GuardDuty**: Process and respond to AWS GuardDuty findings.

Below the featured cards, there is a "Featured" section with a "Refine By" filter and a "Products" list. The "Products" list includes:

Product	Count
<input type="checkbox"/> Cloud Pak for Security	59
<input type="checkbox"/> MaaS360	29
<input type="checkbox"/> QRadar SIEM	314
<input type="checkbox"/> QRadar SOAR	317
<input type="checkbox"/> Verify Identity and Access	33

The "Featured" section contains four application cards:

- QRadar SIEM QRadar Advisor With Watson - v7.5.0+** (Premier): Enrich security incidents with insights from Watson to rapidly respond to threats.
- QRadar SIEM IBM Security QRadar Analyst Workflow - QRadar 7.5.0 UP7+ only** (Updated): QRadar Analyst Workflow simplifies and expedites the offense response process.
- QRadar SIEM IBM Security QRadar Network Threat Analytics - QRadar v7.5.0 UP3+**: Analyze network traffic to identify threats.
- QRadar SIEM User Behavior Analytics - QRadar v7.5.0 UP3+**: UBA app is a tool for detecting insider threats in your organization.

# Quick deployment

- Is POC in 1 hour possible?
- 180 OOTB rules
- Log source autodetection





How many integrations do we have?



# What do others say?

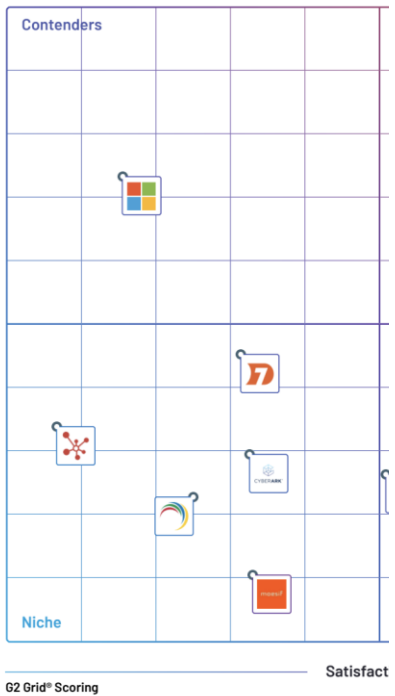
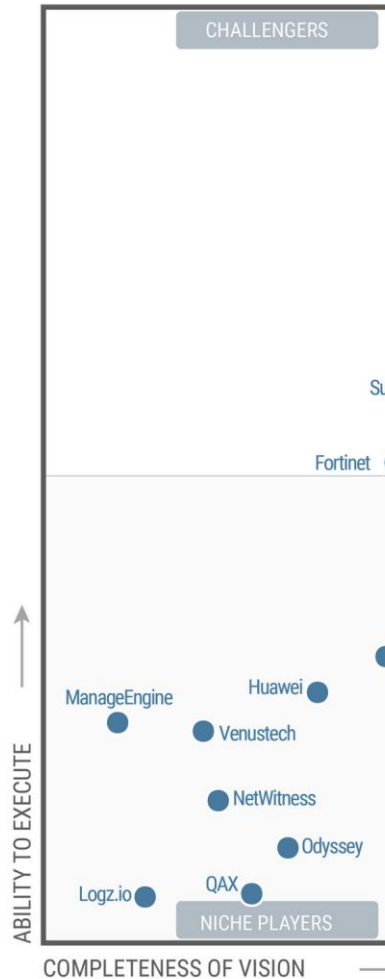


Grid® Report for S  
Information and E  
Management (SIEI  
Summer 2023

Grid® Report for Us  
Behavior Analytics  
Analysis (NTA) | Summer 2023

Security Information and E User and Entity Behavior

Network Traffic Analysis (NTA) Software





IBM QRadar Security Intelligence - Community Edition



Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Quick Filter

Search

Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:04...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Failure Audit: Authentication Ticket Denied	WindowsAuthServer @ micro...	1	Jul 22, 2020, 1:50:04...	Auth Server Session Closed	192.168.108.176	0	127.0.0.1	0	maiken	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:03...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
MSSQL Login failed for user	WindowsAuthServer @ micro...	1	Jul 22, 2020, 1:50:03...	Database Login Failed	127.0.0.1	0	127.0.0.1	0	larmitage	
User failed to login to SSH, incorrect password	LinuxServer @ apple.macosx....	1	Jul 22, 2020, 1:50:02...	SSH Login Failed	56.69.169.215	62199	127.0.0.1	0	tkane	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:01...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:01...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
<b>UBA : New Account Use Detected</b>	<b>Custom Rule Engine-8 :: lab</b>	<b>1</b>	<b>Jul 22, 2020, 1:50:01...</b>	<b>User Access</b>	<b>192.168.227.138</b>	<b>54815</b>	<b>127.0.0.1</b>	<b>0</b>	<b>jwilliams</b>	
Success Audit: A Kerberos service ticket was granted	WindowsAuthServer @ micro...	1	Jul 22, 2020, 1:50:01...	Kerberos Session Opened	192.168.227.138	54815	127.0.0.1	0	jwilliams	
Account Logon Failed	WindowsAuthServer @ micro...	1	Jul 22, 2020, 1:50:00...	Auth Server Login Failed	127.0.0.1	0	127.0.0.1	0	mrose	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Information Message	System Notification-2 :: lab	1	Jul 22, 2020, 1:50:00...	Information	192.168.226.12	0	127.0.0.1	0	N/A	
Linux login messages Message	LinuxServer @ apple.macosx....	1	Jul 22, 2020, 1:49:59...	Stored	127.0.0.1	0	127.0.0.1	0	N/A	
MSSQL Permission Denied	WindowsAuthServer @ micro...	1	Jul 22, 2020, 1:49:58...	Database Action Denied	127.0.0.1	0	127.0.0.1	0	taquil	

# What is the most popular attack vector?

- 60% of attacks are identity-based
  - At least 😊
  - <https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023>
  - <https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022>
- 2024 update:
  - <https://www.cloudrangecyber.com/news/analyzing-the-2024-ticketmaster-breach>
- “Hackers do not break in, hackers log in”



# Hybrid cloud adoption Digital transformation

**67%**  
of enterprises will use  
three or more clouds



# Why is that?

So  
Ticketmaster/Snowflake  
does not use PAM or MFA?

So why they didn't use it?



# Hence, two important questions

- ISPM

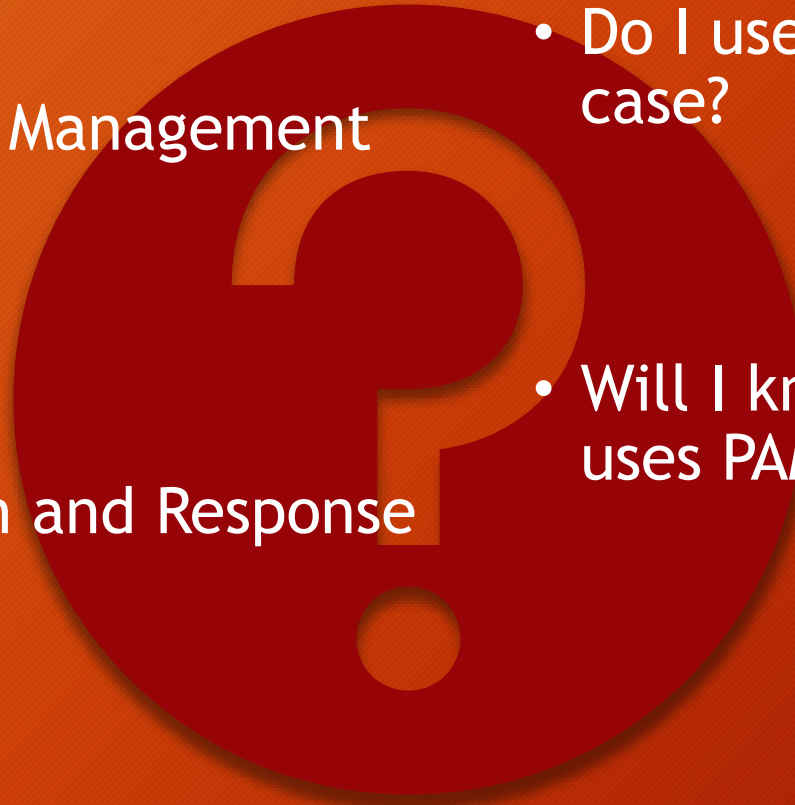
Identity Security Posture Management

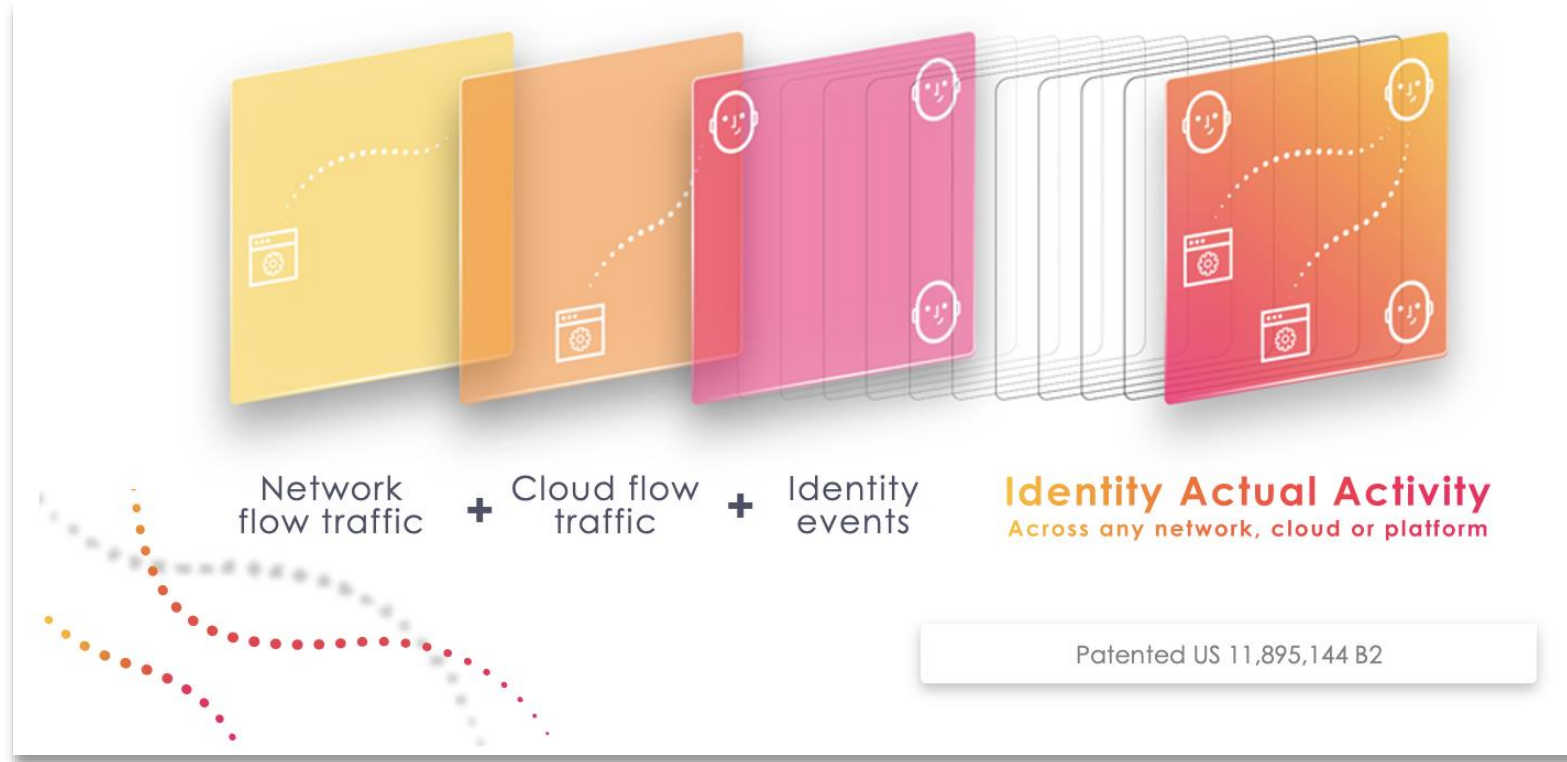
- Do I use PAM/MFA/etc in every case?

- ITDR

Identity Threat Detection and Response

- Will I know if somebody not uses PAM/MFA/etc

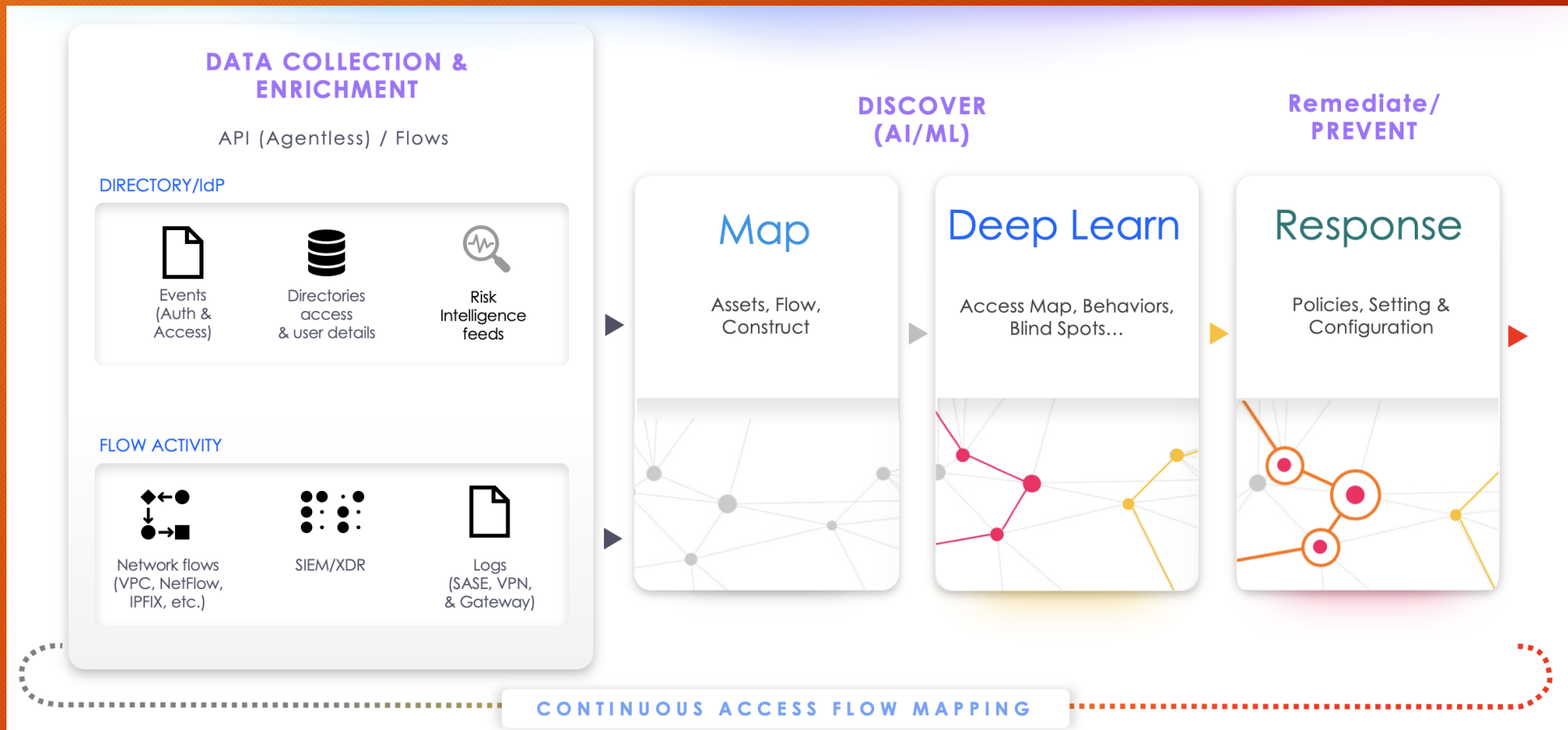




# Introducing new ITDR/ISPM tool from IBM!

Verify Identity Protection

# How does it work?





# Why would I need it?

## View Playbook: Lack of MFA

Discover accesses where MFA should have happened using a [known MFA server](#) but did not. [Learn More](#)

Name

Lack of MFA

Risk

● High

### Rules

#	Parameters	Identity/Source	Access Control	Asset/Destination
1	<ul style="list-style-type: none"><li>• MFA servers to be checked: AzureAD; IBM Verify SaaS;<ul style="list-style-type: none"><li>◦ MFA session is valid for 0 days and 1 hours</li></ul></li></ul>	All Identities	Any Access Control	All Assets

### Related Global Exceptions


There are a total of 6 exceptions found for Lack of MFA. [View Here](#)


### Actions


By default, Playbooks will always create incidents. In addition, the following actions can be optionally configured:

Notify Admins (email)     Notify Users (email)     Create Ticket

# Why else?

Compromised User		<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>Parameters</b> - A user will be considered compromised:<ul style="list-style-type: none"><li>◦ if his/her identity information is found in: Have I Been Pwned or Dehashed</li></ul></li><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
------------------	---	---

Suspected Directory/IdP Password Spray Attack		<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>Parameters</b> - A directory/IdP will be marked as under password spray attack when number of accounts with wrong / bad passwords in an hour is more than 2</li><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
---	---	---

Weak Password		<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>Parameters</b> - A password will be considered weak if:<ul style="list-style-type: none"><li>◦ Password takes less than 30 seconds to crack</li></ul></li><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
---------------	---	---

# Why else?

Auth Protocol Quality	●	<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>Parameters</b> - Authentication quality will be considered poor if:<ul style="list-style-type: none"><li>◦ Legacy (less secure) protocols SMTP, IMAP, POP, FTP, Telnet</li></ul></li><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
-----------------------	---	--

Shadow Identity Systems	●	<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>Parameters</b> - An Identity System will be considered a Shadow Identity System for the following Identity System Categories : Local Identity Systems, Cloud IAM and IGA, Clo...</li><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
-------------------------	---	--

Access to Anonymous IP	●	<p>Rule 1 of 1</p> <ul style="list-style-type: none"><li>• <b>All Identities</b></li><li>• <b>All Assets</b></li></ul>
------------------------	---	--

# Why else?

Unknown SaaS	Unknown SaaS Access	●	Rule 1 of 1 <ul style="list-style-type: none"><li>• All Identities</li><li>• Asset/Destination Category - equals - Cloud IAM and IGA, Cloud Identity Providers,</li></ul>
--------------	---------------------	---	---

Generative AI	Unknown SaaS Access	●	Rule 1 of 1 <ul style="list-style-type: none"><li>• All Identities</li><li>• Asset/Destination Category - equals - AI Applications</li></ul>
---------------	---------------------	---	--

Deviation in Daily Asset Activity	●	Rule 1 of 1 <ul style="list-style-type: none"><li>• Parameters - Access to an asset should be marked as a deviation when:<ul style="list-style-type: none"><li>◦ The current day's flow count for the asset goes 300% higher than the 7-day average</li></ul></li><li>• Asset/Destination IP - equals - 10.66.2.177</li></ul>
-----------------------------------	---	---

# ... and 28 more use cases

And all can be customized with parameters, e.g.

### Configure Impossible Travel ✕

Detect account takeovers where the latest access is suspicious based on the following criteria:

- User's displacement (distance/time) is greater than   per hour
- AND
- Distance traveled since last access is greater than
- AND
- Access from a new ISP was identified
- AND
- Access from a new IP range was identified

# Is it easy to deploy?

- SaaS (not only?)
- Just connect SIEM, AD, IdP...
- ... and more sources optionally

Visibility Source	Supported Technologies	Cloud SIEM	Local SIEM	Direct
Cloud IDPs	<ul style="list-style-type: none"> <li>• AWS Managed AD, Google Workspace, IBM Verify SaaS, Microsoft <a href="#">Entra ID</a> (aka Azure AD), Okta Workforce Identity, OneLogin Workforce Identity, <a href="#">PingOne</a> for Workforce</li> </ul>	Agentless	Flow Sensor <sup>1</sup>	Agentless
Local Active Directory	<ul style="list-style-type: none"> <li>• Active Directory (Windows Server 2012+)</li> <li>• Active Directory Lightweight Directory Service (AD-LDS)</li> </ul>	Agentless	Flow Sensor <sup>1</sup>	Active Directory Sensor
Network Access	<ul style="list-style-type: none"> <li>• Bastion SSH; Blue Coat Proxy SG, <a href="#">CheckPoint</a> (Firewalls, Perimeter 81, Remote Access VPN); Cato Networks SASE Platform; Cisco (ASA, FTD, Umbrella); <a href="#">CrowdStrike</a> Falcon, F5 (Big IP APM and LTM); Fortinet (Firewalls, SASE, and VPN); OpenVPN Cloud Access Server; Palo Alto (Firewall &amp; VPN), SonicWall (Firewall and VPN); <a href="#">ZScaler</a> (ZIA, ZPA, Firewall)</li> </ul>	Agentless	Flow Sensor <sup>1</sup>	Flow Sensor
Cloud& On-Premise Network Infrastructure	<ul style="list-style-type: none"> <li>• AWS VPC Flow Logs, AWS S3 Access Logs, Azure NSG Flow Logs, GCP VPC Flow Logs, VMware vSphere, Cisco Meraki, Generic <a href="#">Netflow</a> &amp; IPFIX, Generic <a href="#">sFlow</a></li> </ul>	Agentless	Flow Sensor <sup>1</sup>	Agentless

<sup>1</sup>Only a single flow sensor installed locally that has API access to the SIEM is required for all four visibility sources.

But I can do this in my SIEM



So why still 60% of attacks use identity exploitation?

But my identity system is ITDR



Indeed, every IdP has  
ITDR capabilities



“AuthMind is cool because... **its service has been built to work with multiple identity systems from the start.** AuthMind recognizes that a typical organization operates a complex identity fabric, and multiple identity systems may have a stake in the same identity.”

**Gartner**

**COOL  
VENDOR  
2022**

AUTHMIND

Identity-First  
Security  
Cool Vendor

AUTHMIND

**Secure all directories, IdPs and identities**

IBM Verify, Ping, Okta, One Identity, Entra ID, and more. All identities (human, non-human, managed, and unmanage)

**ISPM and ITDR primary capabilities**

**Selective identity systems and type**

- AD, Azure, and Entra ID
- Detection of known attacks on Microsoft environments
- Guidance for improving Microsoft-centric identity posture
- Okta, Ping

**Selective cloud and SaaS coverage**

- AWS, Azure, GCP
- Salesforce, Workday, GitHub

**Holistic coverage across cloud, SaaS, and on-premise**

Cloud (AWS, Azure, GCP), hybrid cloud, all SaaS apps, and on-premise assets

**Secure shadow activity, blind spots and bypass of security controls**

PA bypass, zero trust bypass, VPN bypass, local accounts, shadow directories, MFA issues, and unknown SaaS

**Observability across all identity activity and access paths**

human and non-human, across any cloud or platform

# Remember “Zero Trust”?

- Do not trust me
- Challenge me to prove it works
- Allow me to deliver a POC for you





Dashboard

Identity Security Posture

Incidents

Tickets

Playbooks

Admin



Tomasz Zalewski

PAST 24 HOURS  
Incidents 3 | 0.0%

Flows 114,142,627

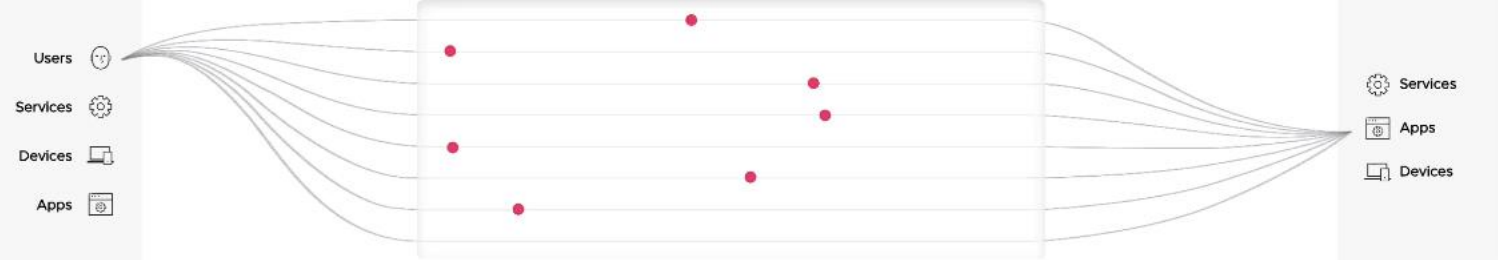


TOP NEW RISKY ENTITIES (30D)

Type	Name	Issues	Incidents	Score
👤	rajeshwar.mukund@authmind.com	Access to Public VPN, Access to Unauthorized Countries, ... (+1)	102	99.11
🔑	1Password	Shadow Identity Systems	41	98.58
⚙️	Unknown Service on se-partner-ws-1	Suspicious Outbound Access, Access to Unauthorized Co... (+1)	83	94.89

Identities

RECENT ACCESSES WITH INCIDENTS



ID AND ACCESS INFRASTRUCTURE

18 Issues | 220 incl... <sup>▲4</sup><sub>0 new</sub>

- Lack of MFA: 7 assets | 127 incidents <sup>▲1</sup><sub>0 new</sub>
- Brute-force Attack: 4 identities | 9 incidents <sup>▲1</sup><sub>1 new</sub>
- Password Spray A...: 2 directories | 57 incidents <sup>▲1</sup><sub>1 new</sub>

SHADOW ACTIVITY

206 Issues | 1.6K incl... <sup>▲45</sup><sub>0 new</sub>

- Unknown SaaS Ac...: 100 assets | 379 incidents <sup>▲18</sup><sub>25 new</sub>
- Suspicious Outbou...: 62 identities | 261 incidents <sup>▲17</sup><sub>26 new</sub>
- Shadow Assets: 24 assets | 65 incidents <sup>▲2</sup><sub>2 new</sub>

UNAUTHORIZED ACCESS

96 Issues | 1.2K incl... <sup>▲75</sup><sub>70 new</sub>

- To Anon. IP Access: 39 identities | 92 incidents <sup>▲10</sup><sub>10 new</sub>
- To Public VPN Acc...: 28 identities | 98 incidents <sup>▲9</sup><sub>9 new</sub>
- Unauthorized Asse...: 16 assets | 157 incidents <sup>▲28</sup><sub>28 new</sub>

CREDENTIAL RISKS

- 1 Compromised Password
- 41 Compromised User
- 1 Weak Password

SHADOW EXTERNAL ACCESS

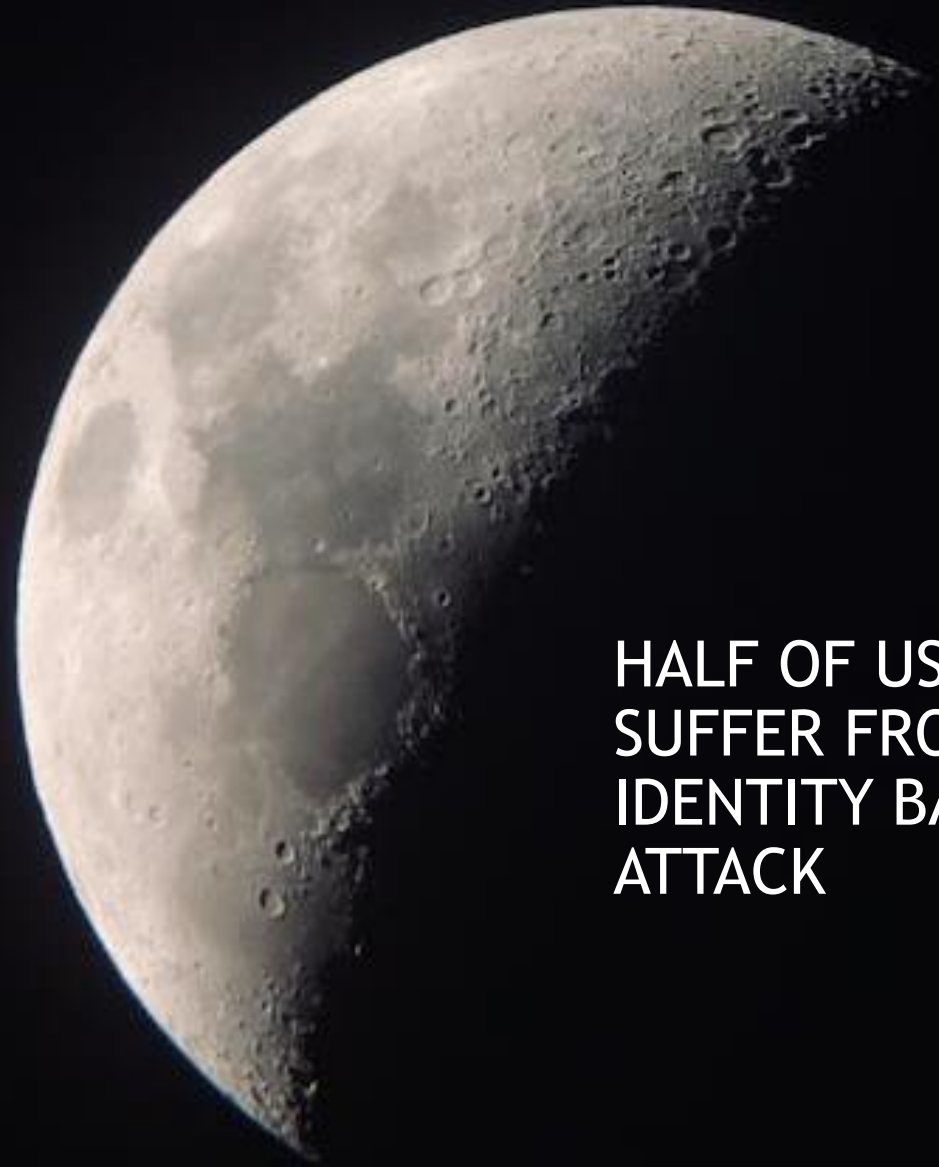
- Unknown Access: 0 assets | 0 incidents
- Shadow External A...: 39 assets | 54 incidents
- Deviation in Access: 1 assets | 396 incidents

RISKY PROTOCOLS

- FTP (2)
- HTTP (984)
- IMAP (1)

# Why a POC? Why now?

- 75% of companies will be successfully attacked in 2025
- Almost 2/3 of attacks use some form of identity exploitation



**HALF OF US WILL  
SUFFER FROM  
IDENTITY BASED  
ATTACK**

Thank you

