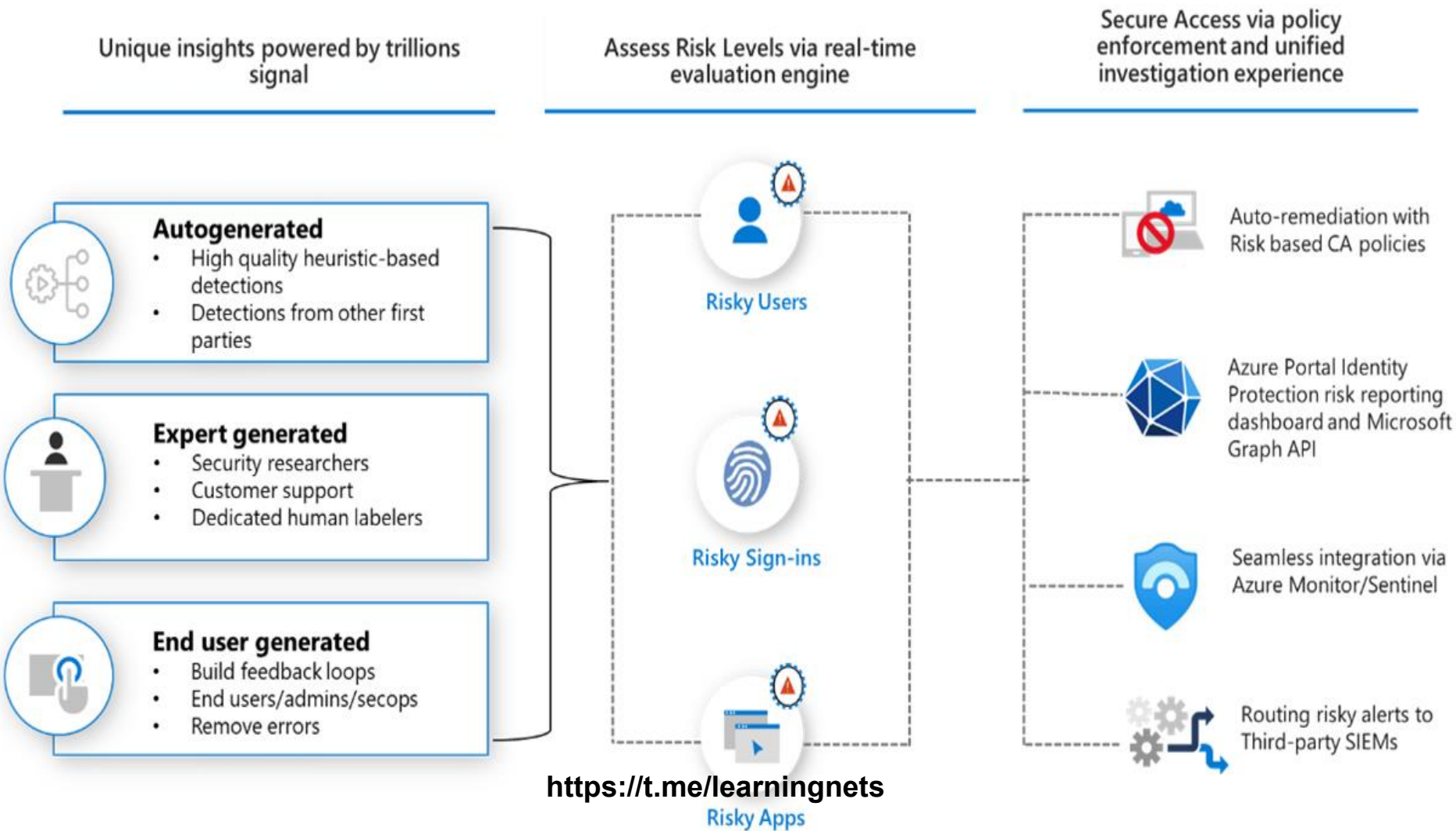
Microsoft Entra Identity Protection

examlabpractice.com

What is Entra Identity Protection?

- Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks.
- These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.



Risk Types

- **Risky sign-ins:**
  - A risky sign-in is reported when there are one or more risk detections reported for that sign-in.
- **Risky users:**
  - A Risky user is reported when either or both of the following are true:
  - The user has one or more Risky sign-ins.
  - One or more risk detections have been reported.

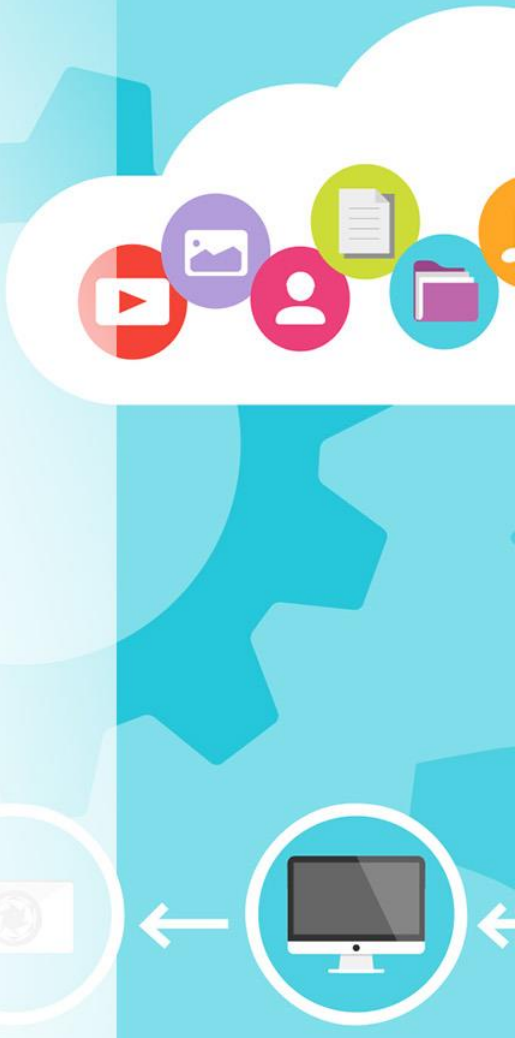
Sign-In Risk Detections

- Atypical travel
- Anomalous Token
- Malware linked IP address
- Suspicious browser
- Unfamiliar sign-in properties
- Malicious IP address
- Suspicious inbox manipulation rules
- Password spray
- Impossible travel
- New country
- Activity from anonymous IP address
- Suspicious inbox forwarding
- Mass Access to Sensitive Files
- Verified threat actor IP
- Additional risk detected
- Anonymous IP address
- Admin confirmed user compromised
- Microsoft Entra threat intelligence

DETAILED EXPLANATION OF EACH ITEM CAN BE FOUND HERE:
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

User Risk Detections

- Possible attempt to access Primary Refresh Token (PRT)
- Anomalous user activity
- User reported suspicious activity
- Additional risk detected
- Leaked credentials
- Microsoft Entra threat intelligence



DETAILED EXPLANATION OF EACH ITEM CAN BE FOUND HERE:
https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

License Requirements

Capability	Details	Microsoft Entra ID Free / Microsoft 365 Apps	Microsoft Entra ID P1	Microsoft Entra ID P2
Risk policies	Sign-in and user risk policies (via Identity Protection or Conditional Access)	No	No	Yes
Security reports	Overview	No	No	Yes
Security reports	Risky users	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Full access
Security reports	Risky sign-ins	Limited Information. No risk detail or risk level is shown.	Limited Information. No risk detail or risk level is shown.	Full access
Security reports	Risk detections	No	Limited Information. No details drawer.	Full access
Notifications	Users at risk detected alerts	No	No	Yes
Notifications	Weekly digest	No	No	Yes
MFA registration policy		No	No	Yes

Required Roles

Role	Can do	Can't do
Security Administrator	Full access to Identity Protection	Reset password for a user
Security Operator	View all Identity Protection reports and Overview Dismiss user risk, confirm safe sign-in, confirm compromise	Configure or change policies Reset password for a user Configure alerts
Security Reader	View all Identity Protection reports and Overview	Configure or change policies Reset password for a user Configure alerts Give feedback on detections
Global Reader	Read-only access to Identity Protection	
Global Administrator	Full access to Identity Protection