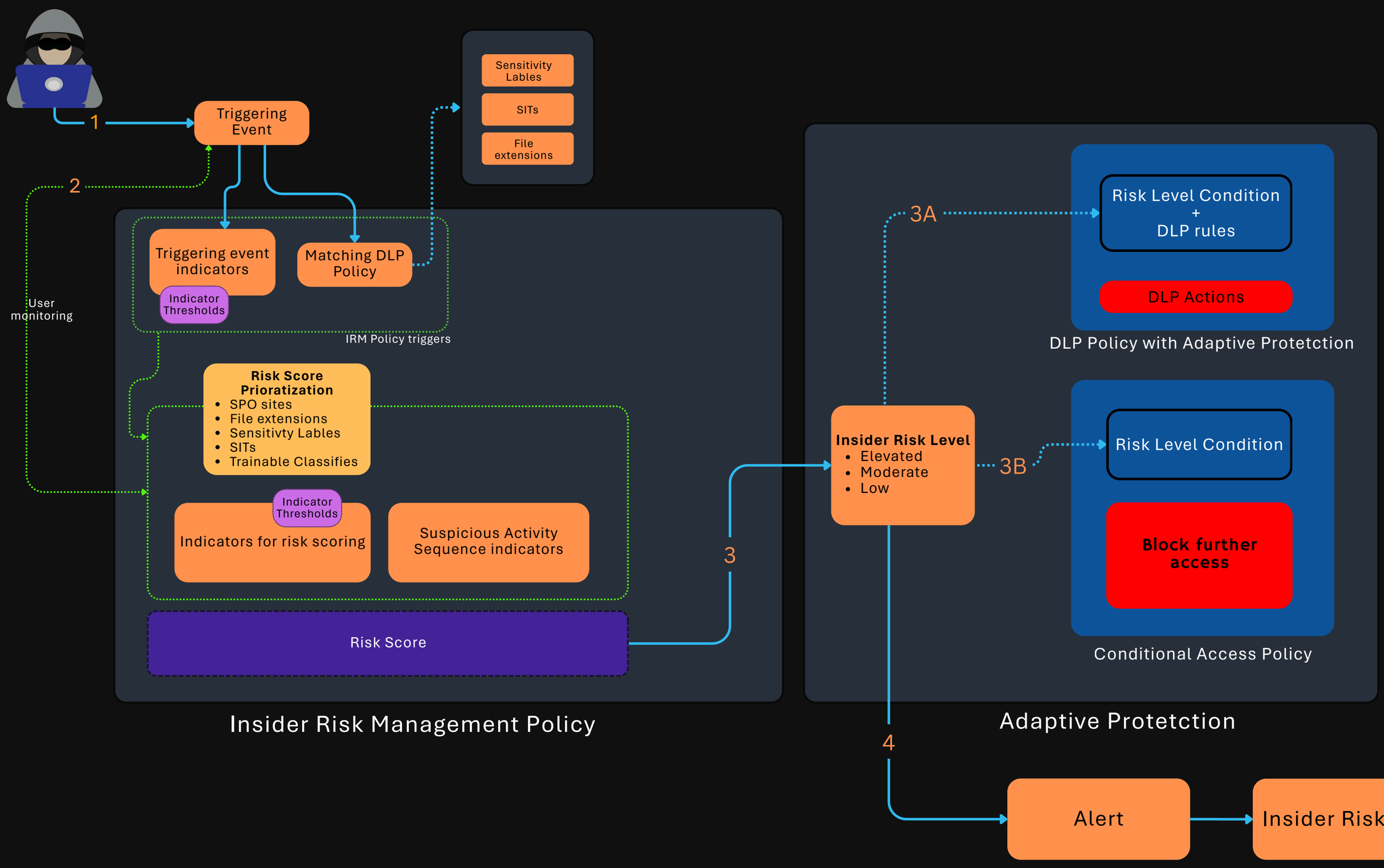
Dissecting a Microsoft Purview Insider Risk Management Policy

Blog emsroute.com @shehanperera85

EMS ROUTE A Guide to Microsoft's Enterprise Mobility and Security Realm
MVP Microsoft® Most Valuable Professional
emsroute.com



1	Triggering activity by the user or by the HR - This will add the user into the IRM policy and will start the policy.
2	IRM policy engine will now inspect the user activities. Risk score will be elevated depending on the matching indicators' threshold levels and the activity sequences. Risk score can be further elevated by prioritizing on selected elements.
3	Activity risk score for that user will now be evaluated against the risk levels defined in adaptive protection. The Adaptive Protection will have the Risk Levels defined. This Risk level will help you to create 3A and 3B.
3A	Conditional Access Policies to block further access depending on the risk level condition.
3B	DLP policies with adaptive protection to further strengthen the data leak detection and prevention.
4	Alerts can be added depending on the risk level using tools like Power Automate and open insider risk cases for further investigate incidents.

Triggering Events (starts the IRM engine for the in-scope user)

- Matching DLP policy
- HR setting up employee leave date which flags the account in Purview (HR Connector required)
- Downloading files from cloud endpoints
- Data exfiltration activities

Prioritise items which you think that matters the most to the business (Risk score will increase)

- SPO sites
- Sensitivity labels
- SITs
- File extensions
- Trainable classifiers

Indicators for risk scoring and used for sequence detection

- DLP policy matching
- Exfiltration activities
- Copying files to a USB
- etc, etc.

License Requirements

- Insider Risk Management: M365 E5, M365 E7 or Purview Suite
- Adaptive Protection: M365 E5, M365 E7 or Purview Suite

(Adaptive Protection feature is not available for users who have the Microsoft E5 Insider Risk Management add-on. Only users with Microsoft 365 E5 and the Microsoft Purview Suite add-on)

RBAC

- Microsoft Entra ID Global Administrator role
- Microsoft Entra ID Compliance Administrator role
- Microsoft Purview Organization Management role group
- Microsoft Purview Compliance Administrator role group
- Insider Risk Management role group
- Insider Risk Management Admins role group