Email Security Agent - Configuration & Usage Guide

1. Introduction

The **Email Security Agent** automates the investigation of suspicious emails by querying your Microsoft Sentinel and Defender data, analyzing email content for psychological triggers, and checking URLs against threat intelligence.

2. Prerequisites

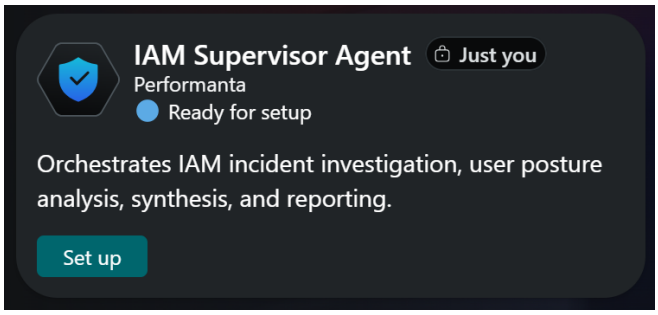
Before configuring or running the agent, ensure you have the following information available from your Azure Portal. The agent requires these details to locate your security data:

1. **Workspace Name:** The name of your Microsoft Sentinel / Log Analytics workspace.
2. **Tenant ID:** Your Azure Active Directory (Entra ID) Tenant GUID.
3. **Subscription Name:** The name of the Azure Subscription hosting the workspace.
4. **Resource Group Name:** The name of the Resource Group hosting the workspace.

Note: The user account running this agent must have at least **Reader** permissions on the Sentinel Workspace to fetch incidents.

3. Installation & Configuration

1. **Add the agent:**
    - Find Performanta IAM Supervisor Agent in the Microsoft Security Store
    - Click on “Set up”



    - Grant any necessary permissions
    - Sign in with a user that has all necessary access

- Configure the agent settings:

  timeframe: The window to look for new incidents (Default: 1h).

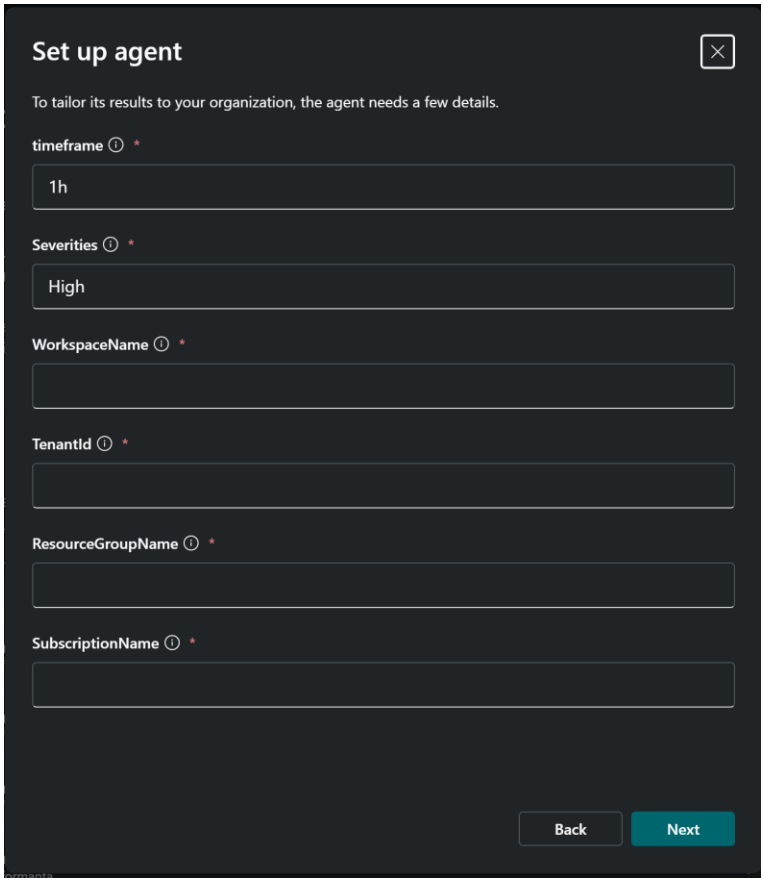
  Severities: A comma-separated list of severities to monitor (e.g., High or High,Medium).

  WorkspaceName: Your Sentinel Workspace Name.

  TenantId: Your Directory (Tenant) ID.

  ResourceGroupName: Your Resource Group Name.

  SubscriptionName: Your Subscription Name.

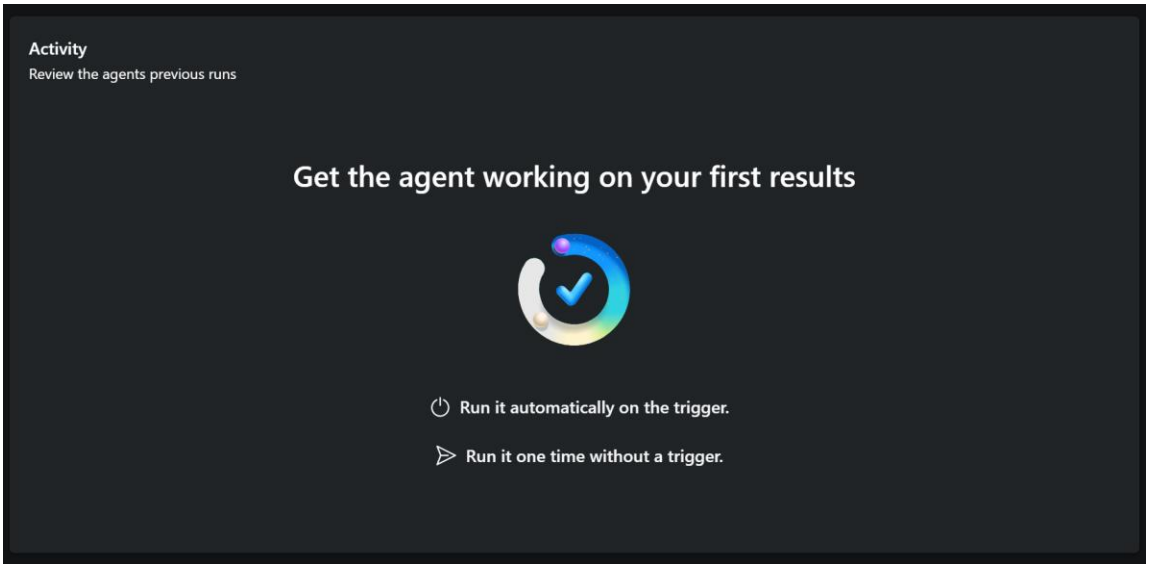


- Once configuration is finished, you may go to the agent and run manually, or set up to run on a schedule.

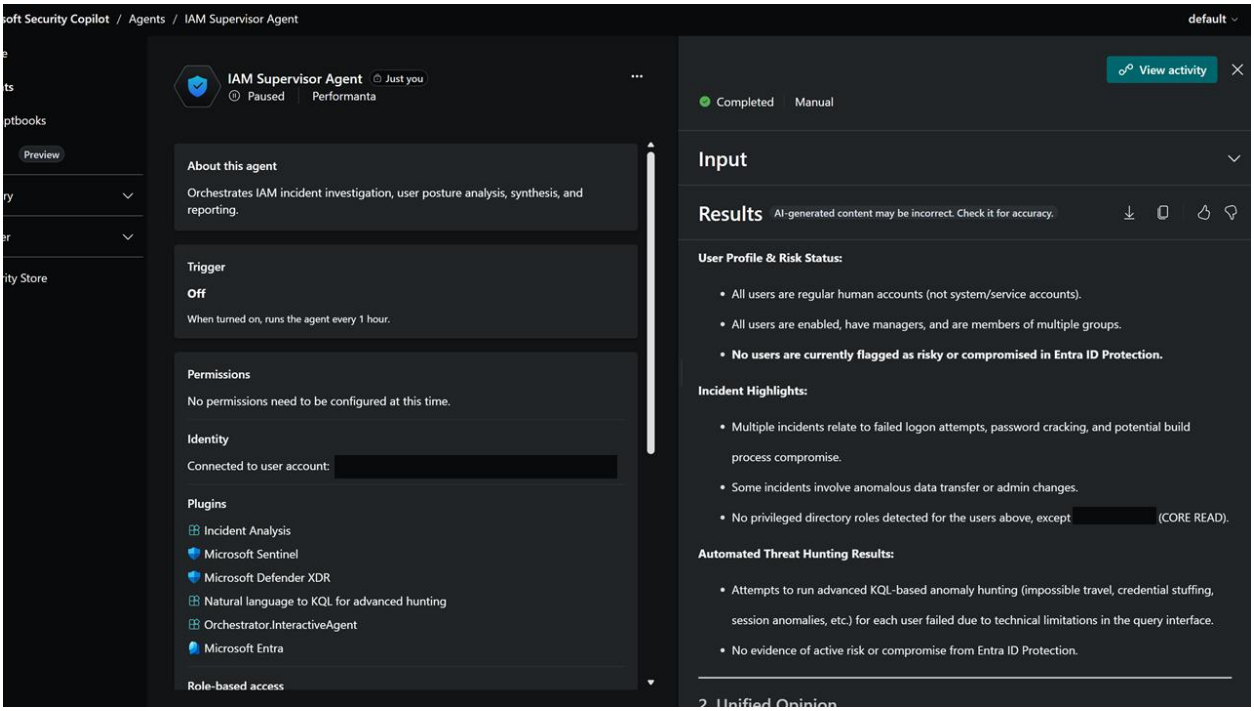
4. Running the Agent

You can choose between automatic or manual execution:

- **Automatic:** The agent is configured to run automatically once every hour (3600 seconds). It will check for **New** incidents that match your Severity criteria.
- **Manual:** You can select “Run it one time without a trigger.” You will have the chance to review the inputs (Timeframe, Severities, etc.) and click “Submit” to force an immediate check.



You will see the output of the agent as in the following example



5. Understanding the Output

If **New** incidents are found, the agent will analyze the users involved and produce a report structured into the following sections:

1. **Investigation Streams:**
    - **Compromised Credentials:** Checks for leaked passwords, impossible travel, and stuffing attacks.
    - **Account Anomalies:** Flags unusual login times or locations.
    - **Insider Risk:** Reviews data access patterns and potential exfiltration.
    - **MFA Integrity:** Looks for MFA fatigue or bypass attempts.
    - **Privileged Activity:** (If applicable) Analyzes admin actions and PIM usage.
2. **Unified Opinion:** A consolidated assessment of the user's status (e.g., *"High confidence of account compromise"*).
3. **Actionable Recommendations:** A prioritized list of remediation steps.
    - *Example:* "Revoke all active sessions for User X."
    - *Example:* "Enforce MFA registration update."

6. Troubleshooting

Issue: "No incidents found"

- **Cause:** There are no incidents in your Sentinel workspace that match the criteria.
- **Fix:**
    - Check that you have incidents with a Status of **New**. The agent ignores 'Active' or 'Closed' incidents.
    - Check your **Severities** setting. If you only listed 'High', but your incidents are 'Medium', they will be skipped.
    - Verify the **timeframe** covers when the incidents were created.

Issue: "Authorization Failed" or "Access Denied"

- **Cause:** The user context lacks permissions.

- **Fix:** Ensure the user account logged into Security Copilot has Microsoft Sentinel **Reader** or **Contributor** access to the Resource Group specified in the settings.