peopleXTECH

A **Quest Global**Company

Compliance Drift & Configuration Deviation Agent

USA : +1 206-858-9902
INDIA : +91 40 41239999

18300 NE Union Hill Road
Suite 210 Redmond, WA 98052

Info@peopletech.com
www.peopletech.com

Table of Contents

1. Purpose of the Agent.....3
2. Functional Design 3
3. Triggers for Agent Activation 3
4. Plugins or Data Signals 4
5. Customer Onboarding / Deployment 4

1. Purpose of the Agent

The Compliance Drift & Configuration Deviation Agent helps organizations detect and prioritize deviations from defined security baselines across their Azure cloud services and managed endpoints. It identifies unhealthy recommendations from **Microsoft Defender for Cloud** (e.g., misconfigurations) and endpoint compliance drift (e.g., non-compliant devices) that violate Zero-Trust principles. This enables security teams to reduce the attack surface, enforce configuration standards, and maintain continuous visibility of their compliance posture. The agent produces a consolidated "Drift Report" of prioritized deviations, affected resources, and recommended remediation actions.

Associated Microsoft Products:

- Microsoft Sentinel
- Microsoft Defender for Cloud
- Microsoft Entra ID
- Microsoft Intune (via Entra ID logs)

2. Functional Design

- Pull top-severity, unhealthy recommendations from the SecurityRecommendation table (fed by Microsoft Defender for Cloud).
- Collect SigninLogs from Microsoft Entra ID to identify endpoint compliance drift, specifically users successfully signing in from non-compliant devices.
- Aggregate findings from both cloud posture (SecurityRecommendation) and device posture (SigninLogs) into a single, normalized dataset.
- Group findings by owner (e.g., subscription or user) and prioritize them based on risk and severity.
- Generate a daily "Drift Report" summarizing all findings with risk categorization and recommended remediation actions in a structured format (Control, Affected Resource, Owner, Fix Steps).

3. Triggers for Agent Activation

The agent runs automatically in two ways:

- **Scheduled scan:** Performs a daily scan (e.g., at 01:00 UTC) to check the entire environment for new or persistent drifts.
- **Event-driven:** Triggers immediately when a new **critical** recommendation is created in the SecurityRecommendation table (detected by the FetchNewCriticalRecommendations skill).

4. Plugins or Data Signals

Required Data Sources

1. **Microsoft Defender for Cloud** – Uses the SecurityRecommendation table to detect unhealthy resources and posture drift.
2. **Microsoft Entra ID** – Uses SigninLogs to detect non-compliant device access.

Required Integrations:

1. Microsoft Sentinel data connection.
2. Log Analytics Reader permission for workspace access.

Sentinel KQL plugin for cross-source data retrieval.

5. Customer Onboarding / Deployment

Preconditions

- Microsoft Sentinel workspace configured with Log Analytics.
- Data connector for **Microsoft Entra ID** (for SigninLogs) enabled.
- **Microsoft Defender for Cloud** data (recommendations) must be successfully exporting to the Sentinel workspace (populating the SecurityRecommendation table). This is typically configured via "Continuous export" in Defender for Cloud.

Deployment Procedure

1. Install the agent from the Security Copilot Agent Gallery.
2. Configure the following parameters:
    - Tenant ID
    - Subscription ID
    - Resource Group Name
    - Workspace Name
3. Assign the **Log Analytics Reader** role to the agent identity.
4. Confirm that data is present in both the SecurityRecommendation and SigninLogs tables.
5. (Optional) Configure an exemption workflow (e.g., using a Sentinel Watchlist) for justified deviations.
6. (Optional) Configure automated remediation or ticketing via Microsoft Logic Apps.