peopleXTECH

A **Quest Global**Company

GuardianIQ Documentation

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

The Security Copilot Agent is designed to detect insider threats during the employee offboarding process by continuously monitoring employees who have recorded a last working day (LWD) in the HRMS.

Unlike traditional IAM offboarding, this agent focuses on security-analyst workflows — enriching telemetry, highlighting anomalies, and delivering actionable intelligence.

Key benefits for customers:

• Insider threat detection: Monitors for anomalous or malicious actions in the critical window before employee departure.

• Comprehensive visibility: Correlates activity across identity (Entra ID), devices (Defender for Endpoint), communications (Microsoft 365) and development platforms (Azure DevOps/GitHub).

• Analyst productivity: Replaces hours of manual log correlation with structured evidence bundles and anomaly scoring.

• Risk reduction: Prevents last-minute data exfiltration, privilege abuse, or intellectual property theft.

• Policy-driven logic: Supports custom business rules (e.g., flag privileged role usage after LWD notification).

Products used:

Microsoft Sentinel, Microsoft 365, Microsoft Defender for Endpoint, Microsoft Entra ID

2. Functional Design

Our agent will:

1. Ingest HRMS updates to detect when an employee has an upcoming LWD.

2. Add employees to a watchlist for heightened monitoring until exit is complete.

3. Collect logs from Sentinel connectors (Microsoft 365, Microsoft Defender for Endpoint, Microsoft Entra ID, etc.).

4. Analyze activity against historical baseline and peer group behaviors.

5. Apply business logic/policy rules (e.g., flag privileged actions after LWD notification).

6. Generate structured reports for SOC analysts with findings, anomalies, and evidence bundles.

7. Optionally trigger escalations (e.g., Sentinel incident, ticket creation).

3. Plugins or Data Signals

The agent requires integration with HR, identity, endpoint, email sources to provide comprehensive monitoring of employees flagged for offboarding.

Core Connectors (Required):

• Microsoft Sentinel – Primary aggregation and correlation engine for all telemetry.

• Microsoft Entra ID – Identity activity logs (sign-ins, conditional access, privileged role assignments/usage).

• Microsoft Defender for Endpoint – Device logs (process creation, USB usage, lateral movement attempts).

• Microsoft 365 – Email and collaboration logs (suspicious forwarding rules, mass sends, attachments).

4. Deployment

Customers will configure the Security Copilot Agent through the Secure Exchange following an onboarding tutorial.

Prerequisites:

• Active Microsoft Sentinel workspace with connectors enabled.

• Licenses for Microsoft Defender (Endpoint, Microsoft 365), Microsoft Entra ID.

5. Onboarding Steps:

1. Install and enable the agent via the Security Copilot Agents gallery.

2. Connect HRMS as the source of truth for last working day (LWD) updates.

3. Enable Microsoft Sentinel connectors for Microsoft Entra ID, Microsoft Defender for Endpoint, Microsoft 365.

4. Validate signals by running the agent on a test offboarding case and reviewing the report in Security Copilot.