GuardianIQ Documentation

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 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 (Defender for Office 365)**, **file collaboration (SharePoint/OneDrive)**, 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 Defender (Endpoint, Office 365, Cloud Apps), Microsoft Entra ID, Microsoft SharePoint.

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 (Defender, Entra, 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, and cloud activity sources to provide comprehensive monitoring of employees flagged for offboarding. These connectors provide the logs and telemetry needed to detect anomalous or malicious activity in the critical window between HRMS last working day (LWD) notification and exit.

Core Connectors (Required):

- **Microsoft Sentinel** → Primary aggregation and correlation engine for all telemetry.
- **Microsoft Entra ID (Azure AD)** → Identity activity logs (sign-ins, conditional access, privileged role assignments/usage).
- **Microsoft Defender for Endpoint** → Device logs (process creation, USB usage, lateral movement attempts).
- **Office 365** → Email and collaboration logs (suspicious forwarding rules, mass sends, attachments).

4. Deployment

Customers will configure the Security Copilot Agent through the **Secure Exchnage** following an onboarding tutorial. The setup process ensures the agent can ingest HR updates, monitor employee activity, and surface actionable insights.

Prerequisites:

- Active Microsoft Sentinel workspace with connectors enabled.
- Licenses for Microsoft Defender (Endpoint, Office 365, Cloud Apps), Microsoft Entra ID, and Microsoft SharePoint.

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: Entra ID, Defender for Endpoint, Defender for Office 365, Defender for Cloud Apps, SharePoint/OneDrive, and DevOps/GitHub (if applicable).
4. **Validate signals** by running the agent on a test offboarding case and reviewing the report in Security Copilot.