peopleXTECH

A **Quest Global**Company

CREDENTIAL THEFT HUNT 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 Content

01. Purpose of the Agent

The **Credential Theft Hunt** Agent detects and validates potential credential theft by correlating multiple security signals across the environment.

Instead of relying on single alerts, the agent performs automated cross-source analysis by linking suspicious endpoint activity from **Microsoft Defender XDR**, identity anomalies from **Microsoft Entra ID**. This correlation-driven approach reduces false positives and minimizes alert noise.

When strong evidence of credential theft is identified, the agent assigns a confidence score and creates enriched incidents in **Microsoft Sentinel**, including timelines, MITRE ATT&CK mappings, and actionable response guidance.

By automating investigation and validation, the agent helps SOC teams reduce alert fatigue, improve detection accuracy, and focus on high-fidelity incidents.

Associated Microsoft Products:
- Microsoft Sentinel
- Microsoft Defender XDR
- Microsoft Entra ID

02. Functional Design

Our agent will:
- Hunt for threats by running KQL queries in Sentinel over the last 6 hours for LSASS access, credential dumping tools, or suspicious PowerShell activity.
- Correlate endpoint activity with Entra ID Sign-in logs using KQL joins, focusing on anomalies within ±1 hour of the event.
- Check for potential lateral movement by analyzing DeviceNetworkEvents (RDP/SMB connections) after suspicious activity.
- Enrich findings with known IOCs from MSTIC or other threat intelligence feeds in Sentinel.
- Calculate a confidence score (0–1); if the score exceeds 0.8, automatically create a Sentinel incident.
- Generate a Credential Theft Incident Summary (Markdown/JSON) including affected users, devices, timeline, MITRE mapping, IOCs, and confidence score.

03. Triggers for Agent Activation

The agent can run in two modes:

Scheduled scan: Runs daily at 02:00 UTC to hunt for credential theft patterns.

Event-driven scan: Runs immediately when high-risk signals are observed, such as:
- Detection of suspicious credential access behavior on an endpoint.

- High-risk or anomalous Entra ID sign-in events.
- Unusual lateral movement activity between devices.

04. Plugins or Data Signals

Required Data Sources in Microsoft Sentinel:

- Microsoft Defender XDR: DeviceProcessEvents and DeviceNetworkEvents.
- Microsoft Entra ID: SigninLogs and AADRiskyUsers.
- MSTIC Threat Intelligence (optional but recommended).

Required Permissions:

- Log Analytics Reader: to run KQL hunting queries.
- Microsoft Sentinel Contributor: to create incidents.
- Microsoft Sentinel Responder (optional): to trigger automated playbooks.

05. Customer Onboarding / Deployment

Preconditions:

- An active Microsoft Sentinel workspace must exist.
- Data connectors for Microsoft Defender XDR and Microsoft Entra ID must be enabled.
- The agent must be granted Log Analytics Reader and Sentinel Contributor roles.

Deployment Steps:

1. Install the agent from the Security Copilot Agents gallery.
2. Run the agent in Observe Mode to review findings without creating incidents.
3. Tune KQL logic to match the customer environment (process names, command lines, etc.).
4. Maintain an allowlist for legitimate administrative tools.
5. Enable full incident creation and optional automated remediation playbooks.