Silverfort Identity Threat Triage Agent – User Guide

Publisher: Silverfort
Agent: Silverfort Identity Threat Triage Agent
Version: 1.0.0
Date: 2026-03

Introduction

The **Silverfort Identity Threat Triage Agent** is an identity-focused investigation and correlation agent that enables security teams to triage **user-centric identity threats** by correlating **authentication, MFA, risk, and endpoint telemetry** stored in **Microsoft Sentinel Data Lake**.

The agent analyzes identity activity for a **specific User Principal Name (UPN)** over the **last 24 hours**, surfacing suspicious authentication patterns, risky sign-ins, and post-authentication endpoint behavior without exposing raw event data.

Where it runs

- Microsoft Security Copilot

Required integrations

- Microsoft Sentinel Data Lake
- Silverfort for Microsoft Sentinel

Output

By correlating MFA activity, sign-in behavior, Entra ID risk signals, and endpoint process execution, the agent produces an **investigation-ready identity threat summary** highlighting anomalies such as MFA fatigue, risky sign-ins, and post-authentication suspicious activity.

Contents

This guide is designed for **Security Operations Center (SOC)** and **Incident Response (IR)** teams using the agent in Microsoft Security Copilot.

---

1. Overview

The **Silverfort Identity Threat Triage Agent** enables rapid investigation of **identity-related threats** by focusing on a provided user identity.

The agent correlates identity signals across:

- Silverfort's Unified Identity Protection Platform telemetry
- Microsoft Entra ID sign-in logs
- Entra ID risky user assessments
- Endpoint process execution activity

By aligning authentication, risk, and endpoint behavior in a **time-bounded (24-hour)** window, the agent helps analysts identify **post-authentication compromise patterns** such as MFA fatigue attacks, credential misuse, or living-off-the-land execution.

---

2. What the agent does

Inputs: what data the agent consumes

The agent operates **exclusively** on data already present in **Microsoft Sentinel Data Lake**:

- **CommonSecurityLog** (Silverfort logs)
- **SigninLogs** (Microsoft Entra ID authentication activity)

- **AADRiskyUsers** (user risk level and risk state)
- **DeviceProcessEvents** (endpoint process execution)

Mandatory constraint:
All queries are limited to **the last 24 hours**:

Tasks: what the agent performs

- Identity-centric threat triage for a given UPN
- MFA activity analysis (approved, blocked, timed out, auto-response)
- Authentication success and failure trend analysis
- Risky sign-in and user risk posture assessment
- Endpoint behavior analysis post-authentication
- Living-off-the-land technique detection
- Anomaly detection and investigation summarization

Outputs: what results the agent generates

The agent produces a **concise, investigation-ready summary**, including:

- MFA activity summary (approved, blocked, timed out, auto-response)
- Sign-in success and failure trends
- Distinct IP address activity summary
- User risk level and risk state snapshot
- Suspicious process execution highlights
- Correlated identity-to-endpoint insights
- Anomaly indicators (MFA fatigue, repeated denials, unexpected approvals)

No raw event logs are returned.

---

3. Prerequisites

Platform requirements

- Microsoft Security Copilot enabled
- Microsoft Sentinel workspace with **Data Lake enabled**

- Silverfort for Microsoft Sentinel - Common Event Format (CEF) and Syslog through Azure Monitor Agent (AMA) to ingest Silverfort logs into Data Lake.

Required Data Lake tables

The agent uses **only** the following tables:

- `CommonSecurityLog`
- `SigninLogs`
- `AADRiskyUsers`
- `DeviceProcessEvents`

If a table is unavailable or contains no data for the last 24 hours, the agent runs **best-effort** and documents gaps in the output.

---

4. Install the agent

1. Open **Microsoft Security Copilot**
2. Navigate to **Agents → Browse more agents**
3. Search for **Silverfort Identity Threat Triage Agent**
4. Install the agent into your Security Copilot environment

---

5. Configure access and data sources

No manual configuration is required beyond standard Sentinel access.

Validation checks (recommended)

- Can the running user read Sentinel Data Lake tables?
- Is identity telemetry present for the last 24 hours?
- Are endpoint process events available for the target user?

If access is partial, the agent continues and documents limitations.

---

6. Run an investigation

When prompted, provide:

- **User Principal Name (UPN)** of the user to investigate

The agent automatically:

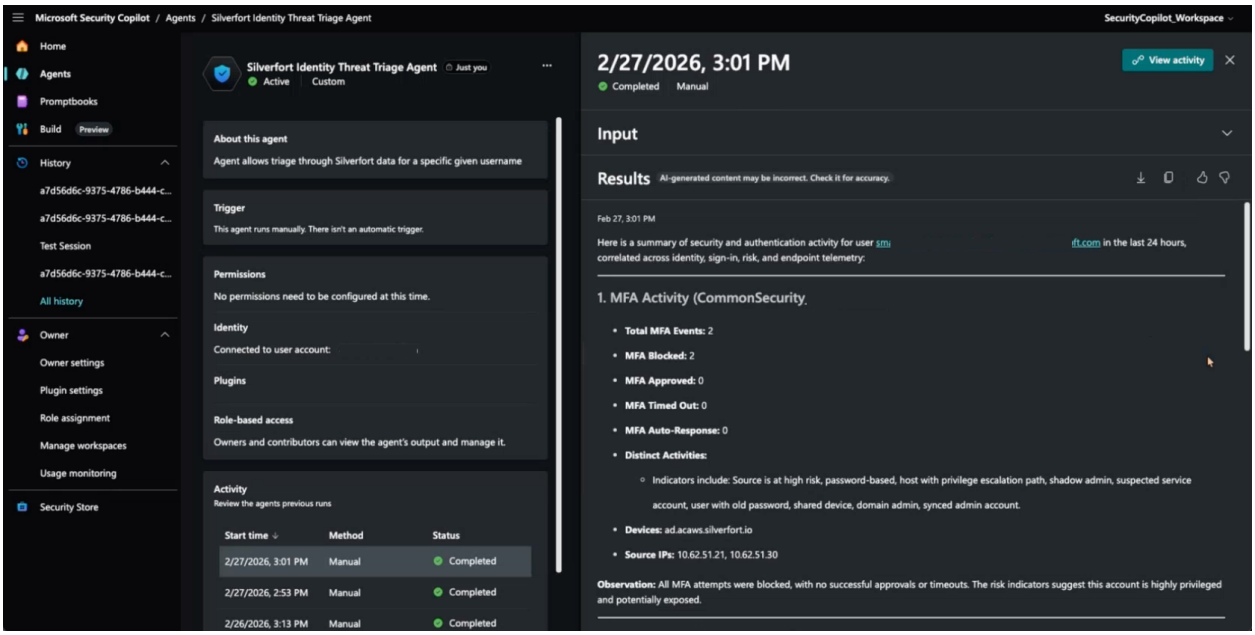
1. Queries Silverfort logs in CommonSecurityLog table.
2. Analyzes Entra ID sign-in activity
3. Evaluates user risk posture
4. Identifies suspicious endpoint execution
5. Correlates all signals using Sentinel MCP

---

7. Sample results

The agent returns a structured summary including:

- **Summary Findings**
  - Total MFA events and outcomes
  - Authentication success and failure trends
  - User risk level and state
- **Endpoint Highlights**
  - Suspicious process execution
  - Devices involved
- **Notable Observations**
  - MFA fatigue indicators
  - Repeated denials or unexpected approvals
  - Post-authentication suspicious activity



---

8. Support and feedback

When requesting support, provide:

- Tenant ID
- Security Copilot Session ID
- Agent summary output or screenshots
- Any reported data gaps

Publisher: Silverfort
Product: Silverfort Identity Threat Triage Agent