AQUILA - 1Password Integration

1Password Events Reporting Integration Manual

With **1Password Business**, you can forward account activity to your SIEM system using the **1Password Events API**. This enables centralized monitoring, improved visibility, and enhanced response to security-related events across your organization.

Key Benefits

When integrated with your SIEM, 1Password Events Reporting allows you to:

- **Retain 1Password event data** according to your organization's policies
- **Build custom dashboards** and visualizations for insights
- **Configure custom alerts** to automate responses
- **Correlate 1Password events** with data from other systems and services

---

Permissions Required

You must be an **Owner** or **Administrator** of your 1Password Business account to configure Events Reporting.

Supported Event Types

Sign-In Attempts

Track authentication activity including:

- **Username and IP address** of the user
- **Timestamp** of the sign-in attempt
- **Success or failure status**
- **Cause of failure** (for failed attempts)

These logs help monitor account access patterns and detect unauthorized access attempts.

How to Set Up

To begin configuring the integration, refer to the official 1Password guide:

Set up Elastic Events Reporting Integration

The 1Password Events API supports JSON-formatted log delivery, which can be ingested by your SIEM using a collector or custom integration script.

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #2
Created 2 July 2025 12:03:04 by Richmond Abella
Updated 2 July 2025 12:56:36 by Richmond Abella