

Varonis (DLP)

Purpose

This document outlines the procedure to integrate **Varonis DatAlert** or **DatAdvantage** with a SIEM platform using **Syslog (CEF)**. The integration provides visibility into sensitive data access, permissions changes, and threat alerts.

Prerequisites

- Admin access to **Varonis DatAlert Console**
- IP address and port of your **SIEM/syslog collector**
- Network/firewall access from Varonis to SIEM (UDP or TCP port open)
- (Optional) CEF parsing support in your SIEM

Step 1: Configure Syslog Server in Varonis

1. Log in to the **Varonis DatAlert Console**.
2. Navigate to:
Tools → DatAlert → Configuration → Syslog
3. Click **Add Syslog Server**.
4. Input the following:
 - **Server Name:** Descriptive name (e.g., CinchSyslog)
 - **IP Address:** Your SIEM or Cinch collector IP
 - **Port:** Common options: , , or
 - **Protocol:** Choose or (enable encryption if needed)
 - **Message Format:** Choose **CEF**
5. Click **Save**.

Step 2: Set Up an Alert Template

1. Go to:
Tools → DatAlert → Templates
2. Click **New Template** or edit an existing one.
3. Enter:
 - **Template Name:** e.g., “Syslog CEF Export”
 - **Description:** Template for sending alerts to SIEM
4. In the **Alert Outputs** section:
 - Check **Syslog Message**
 - Choose the syslog server created in Step 1

5. Set the **Message Format** to **External system default template (CEF)**
6. Click **Save Template**

Step 3: Enable Alerts to Send via Syslog

1. Navigate to:
DatAlert → **Rules**
2. Select a rule (e.g., “Mass file access” or “Sensitive File Access”)
3. Click **Edit** on the rule
4. Go to the **Outputs** section:
 - Check **Syslog Message**
 - Assign your custom template (e.g., “Syslog CEF Export”)
5. Click **Save**
6. Repeat for each alert rule you want to forward to your SIEM

Step 4: Configure Your SIEM to Ingest Logs

1. Create a **new log source** or **syslog input**:
 - **Source Type**: Syslog (TCP/UDP)
 - **Port**: Match what you configured in Varonis
 - **Log Format**: CEF (or Custom parser for Varonis CEF)
2. Create a **parser** to extract CEF fields:
 - Example fields: **suser**, **src**, **filePath**, **act**, **deviceSeverity**
 - Many SIEMs (like Splunk, Elastic, QRadar) include CEF parsers

Step 5: Test and Validate

1. Simulate an alert in Varonis (e.g., access a sensitive file or trigger a test alert).
2. Check your SIEM/Cinch logs for messages like:
CEF:0|Varonis|DatAlert|1.0|100|Sensitive File Access|10|src=10.0.1.15
suser=john.doe filePath=\\server\hr\payroll.xls act=access
3. Confirm:
 - Syslog message is received
 - Parsed fields are correct
 - Alerts or dashboards are populating as expected

(Optional) Step 6: API Integration for Enrichment

Varonis also offers a REST API for:

- User activity reports
- File system access logs
- Sensitive data classification results

For enrichment:

1. Obtain API credentials from Varonis admin portal
 2. Poll /api/alerts, /api/files, or /api/permissions
 3. Ingest results into your SIEM/Cinch as contextual data
-

Revision #1

Created 19 June 2025 07:34:35 by Albert Alombro

Updated 19 June 2025 07:52:12 by Albert Alombro