CrowdStrike to SIEM alerts and ruling

Introduction

This guide explains how to send security alerts from CrowdStrike Falcon to your Security Information and Event Management (SIEM) system and how to create rules for alert filtering and correlation (ruling). This helps detect threats faster and reduces alert noise.

What You Need Before Starting

- CrowdStrike Falcon account with admin access
- API Client credentials from CrowdStrike
- Access to your SIEM (Splunk, QRadar, ArcSight, etc.)
- Ability to install/configure software (Windows/Linux)
- Basic knowledge of logs and syslog is helpful but not required

Step 1: Create an API Client in CrowdStrike Falcon

1. Log in to the CrowdStrike Falcon Console at https://falcon.crowdstrike.com/login/
2. Go to **Support → API Clients and Keys**
3. Click **Add new API client**
4. Give the client a name like “SIEM Integration”
5. Select the following API scopes/permissions:
   - **Event streams: Read**
   - **Detections: Read**
6. Save the client and note the **Client ID** and **Client Secret** — you’ll need them later

Step 2: Choose Your Integration Method

There are three main ways to forward CrowdStrike data to your SIEM:

- **Falcon SIEM Connector** — easiest for most users, sends logs via syslog
- **Falcon Streaming API** — for custom coding and direct API calls
- **Falcon Data Replicator (FDR)** — for bulk data export, stored in AWS S3

Step 3: Download and Install Falcon SIEM Connector

For Windows

1. Download the SIEM Connector installer from CrowdStrike Support or Falcon Portal
2. Run the installer .exe file

3. Follow the installation wizard to complete setup

For Linux

1. Download the SIEM Connector package(.tar.gz)
2. Extract the package and run install script:
   tar -xzf crowdstrike-siem-connector.tar.gz
   cd crowdstrike-siem-connector
   sudo ./install.sh

```
tar -xzf crowdstrike-siem-connector.tar.gz
cd crowdstrike-siem-connector
sudo ./install.sh
```

Step 4: Configure the SIEM Connector

1. Open the connector configuration file in a text editor:

- Windows:
  C:\Program Files\CrowdStrike\SIEMConnector\config.json
- Linux:
  /etc/crowdstrike-siem/config.json
  2. Add your CrowdStrike API credentials and your SIEM server info. Example config:
  {
  "falcon_api": {
  "client_id": "YOUR_CLIENT_ID",
  "client_secret": "YOUR_CLIENT_SECRET"
  },
  "output": {
  "format": "json",
  "destination": "syslog://your.siem.server:514"
  }
  }

```
{
  "falcon_api": {
    "client_id": "YOUR_CLIENT_ID",
    "client_secret": "YOUR_CLIENT_SECRET"
  },
  "output": {
    "format": "json",
    "destination": "syslog://your.siem.server:514"
  }
}
```

3. Save the file.

Step 5: Start the SIEM Connector Service

Windows:
Open Command Prompt as Administrator and run: "net start CrowdStrikeSIEMConnector"

Linux:
Run the following commands: "sudo systemctl start crowdstrike-siem"
"sudo systemctl enable crowdstrike-siem"

```
sudo systemctl start crowdstrike-siem
sudo systemctl enable crowdstrike-siem
```

Step 6: Verify Data Flow

Check the connector logs to make sure it is running without errors:

- Windows: Logs usually at C:\Program Files\CrowdStrike\SIEMConnector\logs\
- Linux: View logs with: tail -f /var/log/crowdstrike-siem.log

In your SIEM, search for CrowdStrike events to verify logs are being received.

Step 7: Create Alert Rules and Ruling in SIEM

Use your SIEM’s alerting and correlation features to build rules that:

- Filter out low-severity or false-positive alerts
- Combine multiple alerts related to the same incident for context
- Alert on high-severity or confirmed threats only

Example in Splunk: index=crowdstrike severity>=high

```
index=crowdstrike severity>=high
```

Step 8: Best Practices and Tips

- Always **rotate your API credentials** regularly for security
- Use **TCP or TLS syslog forwarding** for reliable and encrypted log delivery
- Limit forwarded logs to relevant event types to avoid SIEM overload
- Monitor the health of the SIEM connector continuously
- Document all configurations and rules clearly for team collaboration

Additional Resources:

Revision #9
Created 18 June 2025 08:44:15
Updated 25 June 2025 07:41:22