Adding a new SIEM connecter

Coro has the ability to integrate with Security Information and Event Management (SIEM) solutions. This means that ticket data is available in real time within your SIEM platform, allowing you to maximize these data benefits.

Coro currently supports the following integrations:

- **Splunk**
- **Microsoft Sentinel**
- **Fluency**
- **Generic webhook integrations**

> **Note**
>
> Additional integrations are planned to be supported in the future.

Splunk

Splunk is a leading platform for collecting, analyzing, and visualizing machine-generated data. It is widely used for log management, SIEM, and operational intelligence. Splunk enables organizations to gain valuable insights from the vast amounts of data generated by their systems, applications, and devices.

Splunk can be integrated with Coro in order to collect information related to an event, for example, detected malware, or a mass download event. This information is used for analytics and reporting.

> **Note**
>
> Coro sends SIEM data to Splunk via HTTP Event Collector REST API endpoints.

Configuring a Splunk connector via the Coro console

To configure a Splunk connector:

1. **Log into the Coro console** and select **Control Panel** from the toolbar: