# Next-Gen SIEM Event Investigation

*Last updated: Apr. 21, 2025*

## Overview

Search against cross-domain data to hunt for suspicious activity or further investigate detections and incidents.

- **Events**: Events represent an occurrence, object, or process in the Falcon platform. Event fields represent data in many different formats. For more info, see Events [/documentation/category/j282ed2d/event-investigation/events].
- **Advanced Event Search**: Analyze, explore, and hunt for suspicious or malicious activity in your environment using the CrowdStrike Query Language (CQL). For more info, see Advanced Event Search [/documentation/page/ic5d7b7d/event-search-advanced].
- **Dashboards:** Create your own customized dashboard widgets from a search query. For more info, see Dashboards [/documentation/page/ic5d7b7d/event-search-advanced#r48010d4].
- **Event investigation**: Hunt for adversaries, suspicious activities, suspicious processes, and vulnerabilities. For more info, see Event Investigation [/documentation/category/feb7faf0/event-investigation].

‹ Correlation Rules[/documentation/page/n1eb89fd/correlation-rules-and-custom-incidents] Fusion SOAR › [/documentation/page/v430f1d6/soar-falcon]