SOLUTION BRIEF

Incydr™ + Splunk

Prioritize real Insider Risk and protect your organization's intellectual property

Mimecast Incydr sends alerts to Splunk and delivers a prioritized view of top exfiltration destinations, most risky users and types of files exposed so that analysts can instantly.

Integration Overview

Through an ongoing partnership, Incydr and Splunk deliver the Insider Risk Management transparency and control security practitioners deserve within the SIEM interface they're used to operating. Incydr and Splunk apply advanced risk prioritization methods and dynamic alerts to give organizations greater focus and the increased context needed to jumpstart an investigation. Additionally, retaining an extended audit log of the Incydr product within Splunk makes it much easier for analysts to keep their organization compliant with relevant industry rules and regulations.

By integrating Incydr with Splunk, you can get all the information you need to investigate, prioritize, manage and respond to Insider Risk incidents.

Features

Alert Triage

Ingest prioritized alerts from Incydr into Splunk

Custom Dashboards

Analyze and report on data exposure to quickly identify untrusted activity and triage the most critical alerts

Device Health Checks

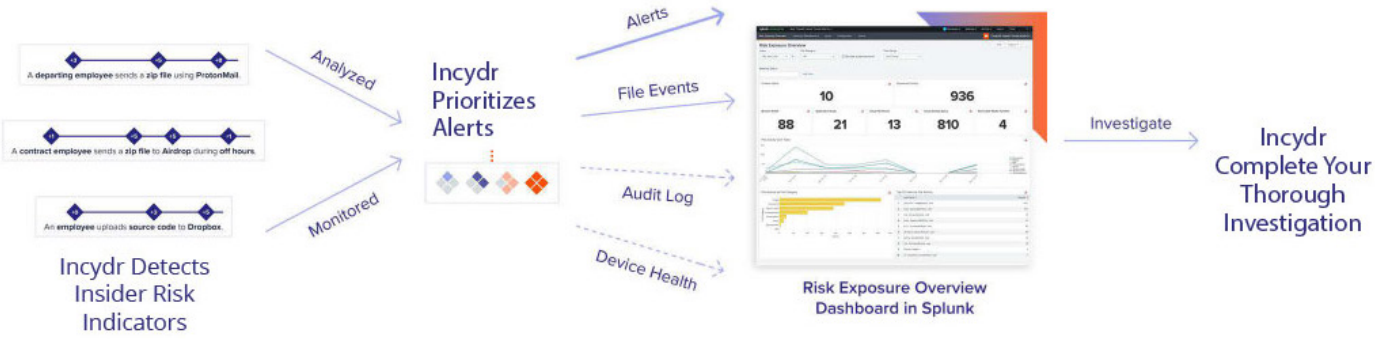
Ensure you're getting accurate, up-to-date information on exfiltration events from all monitored devices

Benefits

Increased visibility: Leverage Incydr's alert prioritization to manage data risk across all employees and gain a company-wide view of exfiltration activity

Alert review efficiency: Streamline workflows by maintaining Splunk as your preferred system for alert review and triage

Data protection: Gain complete visibility into data at risk and protect your company's intellectual property and other high-value data



The Splunk app contains exposure dashboards that provide a quick view of what's happening in Incydr, like detected high-risk employees, insider risk cases, removable media transfers, cloud file shares, cloud desktop syncs, browser and app reads.

The Incydr app for Splunk is an Insider Risk Management analytics and reporting solution that makes it easy to surface, visualize and triage data leak alerts. It leverages Incydr's risk prioritization model to speed up the time to resolve and report the Insider Risk events that matter most.

Incydr sends prioritized alerts, audit log, file exposure, and device health information to Splunk, where it is visualized and can be triaged.