SOLUTION BRIEF

Incydr™ + Sumo Logic

Analyze Incydr Risk Indicators with additional data sources for enhanced risk intelligence

Integration Overview

The Mimecast Incydr app for Sumo Logic allows security teams to analyze Incydr Risk Indicators surfaced within Incydr with additional data sources within the Sumo Logic Continuous Intelligence Platform™ for enhanced risk intelligence. Security teams can configure Incydr's file exposure and exfiltration events into existing Sumo Logic dashboards or create custom dashboards within Sumo Logic to easily visualize:

- Cloud and endpoint data exposure events
- Removable media exposure by user
- Exposure by filename
- Top files exposed
- Top endpoint and cloud users by exposure type
- Exposure events by location

Features

Alert Triage

Ingest prioritized alerts from Incydr into Sumo Logic

Custom Dashboards

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

Device Health Checks

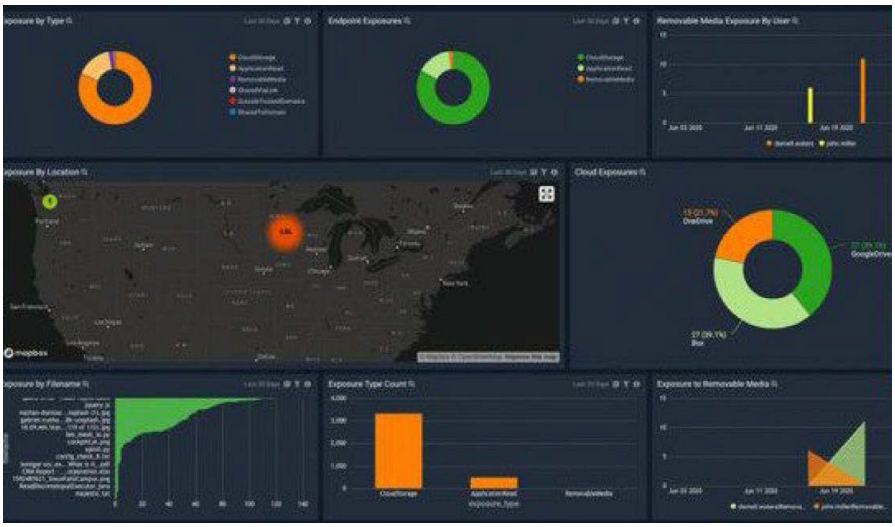
Ensure you're getting accurate, up-to-date information on exfiltration events from all monitored devices

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



Incydr records all employee file activity, and makes it searchable for investigation, but only alerts you to the events that indicate Insider Risk. Incydr enriches detected activities with context on the source, destination, file and user, including the type of files involved, whether the activity took place remotely, was performed during hours when the user is not typically active on their device, and even the ability to review full file contents. Within Sumo Logic, security teams can configure rules to alert on Incydr-specific file exposure and exfiltration events, create customized dashboards using Incydr data, and run saved searches against Incydr data to detect exposure events to support investigations and speed response.

About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.