SOLUTION BRIEF

# Incydr™ + Logrhythm

**Integrate Incydr with the LogRhythm NextGen SIEM Platform to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence.**

More than half (53%) of security teams are blind to users moving files to untrusted domains – and nearly two-thirds (63%) of security leaders don't know which insider risks to prioritize. On top of that, alert fatigue is real, so having the ability to prioritize the specific events that bring the greatest risk to your organization today has become more crucial than ever.

Incydr integrates with LogRhythm to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence. 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 – all from within LogRhythm.

## Integration Features

- Ingest file telemetry information from Incydr into LogRhythm to visualize top files exposed; top users with exposure events; exposure types by source, file, and file type; removable media activity; and cloud file shares and desktop sync activity
- Create and run saved searches against Incydr data to detect exposure events tied to insider risk use cases, including departing employees or high risk users and contractors
- Deliver file and exposure data into LogRhythm using Common Event Format (CEF)
- Collect and retain Incydr exposure data and audit logs for an extended period of time to meet compliance and audit requirements

### Incydr

- Incydr Watchlists
- File and Application Monitoring
- Untrusted Domains
- File Metadata (name, owner, size, path, MD5 and SHA256)
- Vector and Exposure Metadata (browser uploads, removable media and cloud sync destinations)
- Lifecycle Milestones (Departing, High-Risk User)
- Advanced Alerting Criteria

**Machine Data Intelligence**

Automatically collect and process data from across the distributed environment

### Logrhythm Nextgen Siem Platform

- Single, Unified Platform
- Structured and Unstructured Search
- Machine Data Intelligence Fabric
- Threat Intelligence Service
- Risk-Based Prioritization
- Consolidated Compliance Framework
- Case Management
- Case Playbooks
- Case Metrics

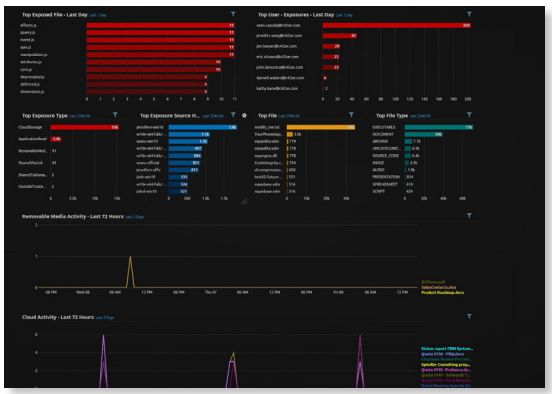
mimecast

## Benefits

- Manage insider risk throughout the employee lifecycle and across users more likely to put data at risk
- Reduce complexity by applying Incydr file telemetry information into LogRhythm dashboards or AI Engine correlation alerts
- Speed response to insider risk incidents with actionable insights to substantiate investigations

## Use Case: ingest file telemetry information from incydr into logrhythm to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence.

**Challenge:** In 2020, data exfiltration was the most common insider risk in the U.S., more than tripling privilege misuse. While most organizations have mechanisms in place to prevent regulated data from leaving corporate systems, proprietary business documents should be protected differently and this is often overlooked.



Incydr data showing top files exposed; top users with file exposure events; top exposure types by source, file and file type; removable media activity; and cloud file shares and sync activity visualized within LogRhythm.

**Solution:** LogRhythm's Machine Data Intelligence (MDI) fabric seamlessly ingests Incydr data to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence. 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 vector, 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 LogRhythm, 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.

**Benefit:** Streamlining alert information and incident triage within LogRhythm reduces complexity by correlating event information to deliver actionable insights that speed insider risk 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.