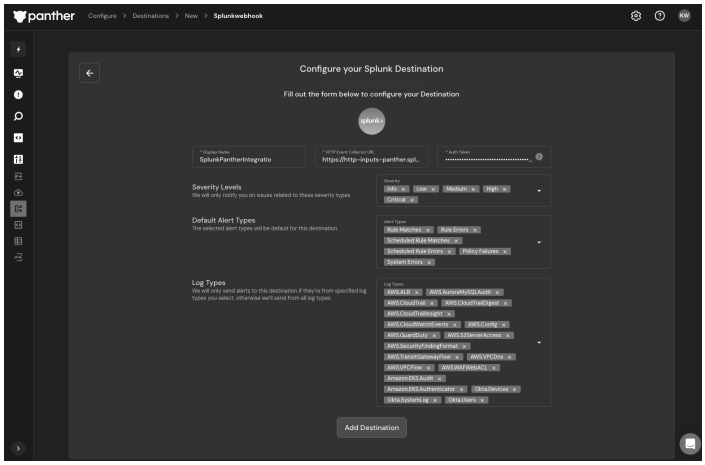
panther | splunk>

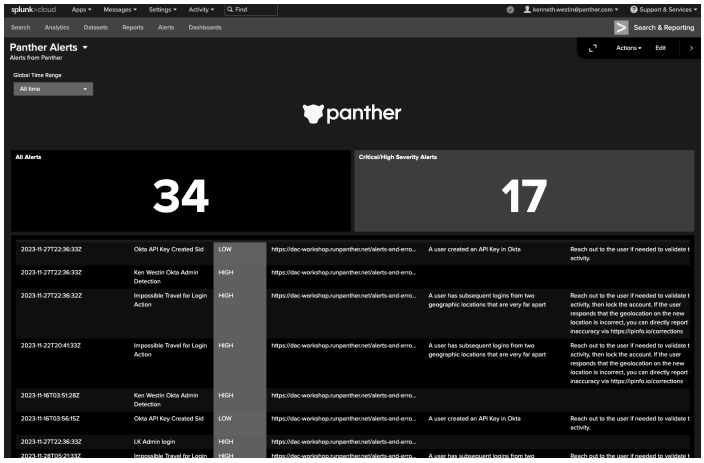
Unlock Detection Engineering in Splunk with Panther

Splunk has long been a powerful tool for security teams for analytics, security workflows, and rich dashboarding capabilities. Panther is a modern SIEM designed to operate at cloud scale, leveraging detection-as-code for real-time detections paired with a cost-effective, high-performance security data lake. Panther's new Splunk alert destination empowers security teams to leverage the power of both platforms. Combining Panther's Detection-as-Code, real-time detections, and efficient cloud ingestion with Splunk's ticketing and dashboarding unlocks cloud-scale detection and response workflows.

Panther's Alert Destination capability provides flexibility to direct Panther's real-time alerts to the destination of their choice based on log type, severity, or other parameters. The new Splunk integration is added to a list of other alert destinations such as Slack, Jira, PagerDuty, and others, as well as our Custom Webhook feature to send alerts to any destination.

panther | splunk>





Panther Detections & Alerts

The new Panther Splunk Alert Destination leverages Splunk's HTTP Event Collector, and works with Splunk Cloud, Spunk Enterprise as well as Splunk Enterprise Security to send alerts to common Splunk security workflows.

The alerts from Panther into Splunk provide rich context, giving responders the information they need to triage and respond to threats. Leveraging Panther enables organizations to run high-volume, high-velocity log sources that may not be run through other SIEMs due to cost and technical constraints. Panther's real-time detection engine provides increased visibility and threat mitigation without breaking the bank. In addition, the logs from these high-volume sources are stored in Panther's cost-effective, high-performance security data lake for deeper investigations. One year of searchable data retention helps support other key use cases like in-depth threat hunting and saved search.

Splunk Dashboarding

Splunk users love to create custom dashboards on the fly. By sending Panther alerts to Splunk, security teams can quickly build new dashboards that seamlessly incorporate Panther alert data into existing security workflows. With added context from Panther, Splunk users can conduct in-depth investigations, identify trends, and quickly mitigate potential threats.

If you would like to learn more, please visit the Panther Splunk Integration solution page, where you can watch videos of the integration, sign up for a personal demo, or register to attend live, hands-on workshops, where the integration will be featured.

SEE PANTHER + SPLUNK IN ACTION

Request a Demo