Splunk Incident Intelligence

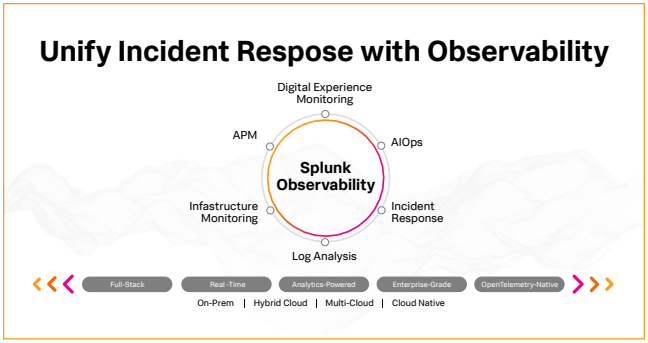
Zap the guesswork around your incidents

What is Splunk Incident Intelligence?

As part of the unified Splunk Observability Cloud experience, Splunk Incident Intelligence is an event management and incident response solution that connects on-call teams with the data they need to:

- Diagnose
- Remediate
- Restore services

Splunk Incident Intelligence has been developed for DevOps engineers, site reliability engineering (SRE) and IT Operations teams.



What benefits can I expect to get from Splunk Incident Intelligence?

Reduce alert noise: Full-context and prioritized alerting aid root cause analysis.

Unify response: Integrated ChatOps and auto-ticketing with ITSM tools help your teams to collaborate and receive proactive notifications on an incident's status.

Improve mean time to acknowledge: Automated on-call scheduling, routing, escalations and notifications — so the right people can quickly acknowledge an incident and get to work.

Accelerate mean time to resolve: Directed troubleshooting, similar incidents and recommended responders help you to fix incidents fast, before your customer's notice impact.

What makes Splunk Incident Intelligence different?

Full-Context Alerting:

When something goes wrong, the last thing you want to do is guess what actually happened. Incident responders and on-call managers need full-context alerting in a unified console. They must get to the bottom of a service-impacting incident fast — without having to hop through multiple tools and systems.

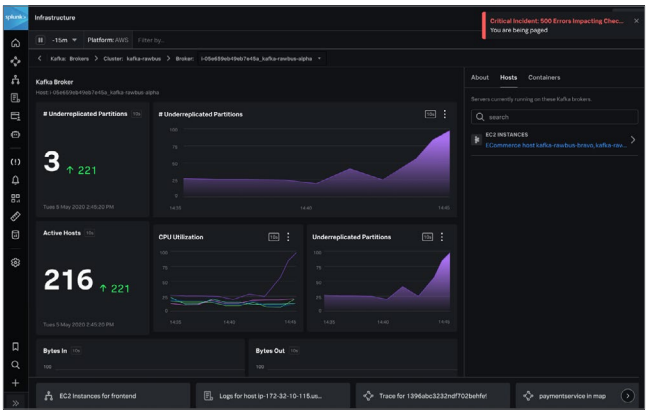


Figure 1: A Splunk Infrastructure Monitoring Alert Details View in Splunk Observability Cloud

As incidents flow into Splunk Incident Intelligence users can drill down into Splunk Infrastructure monitoring in one click for full-context of what transpired. This view includes host and container level details such as: number of under replicated partitions, active hosts, CPU utilization, Bytes In, Bytes Out, etc.

Splunk Incident Intelligence provides full-context alerting from:

- Splunk Enterprise
- Splunk Cloud
- Splunk Observability Cloud products
  - Splunk Infrastructure Monitoring
  - Splunk Application Performance Monitoring
  - Splunk Real User Monitoring
  - Splunk Synthetic Monitoring
- 3rd party monitoring tools like: DataDog, Dynatrace, New Relic, AWS Cloudwatch, Prometheus and many more

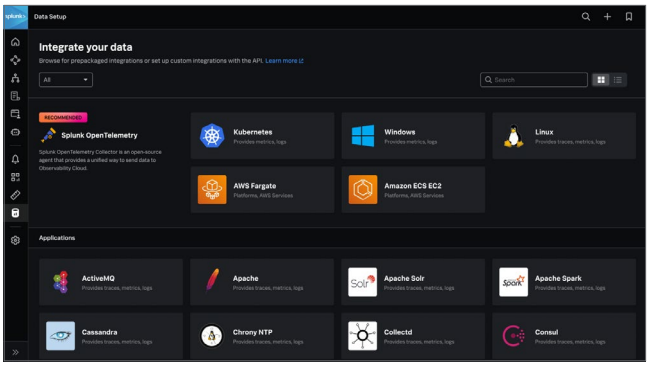


Figure 2: Data Setup View in Splunk Observability Cloud

Incident Intelligence provides the ability to integrate a variety of 3rd party alert data sources with prepackaged integrations or by setting up custom integrations via APIs.

Point being, you never miss an alert. They are in one place, and you get the full context of what happened. With Splunk you can easily integrate alerts from 3rd party tools Splunk Observability Cloud provides the entire detect to correct experience in one integrated solution — helping you to reduce:

- Tool sprawl and costs
- Data silos
- Time-consuming war rooms

Directed troubleshooting:

We hear it all the time, "We want the system to point us to where the problem spots are."

With Splunk Observability and Incident Intelligence you can take advantage of intuitive, directed troubleshooting guidance. See exactly where and when problems started to unfold, and how big the blast impact is — all without having to swivel between tools and screens.

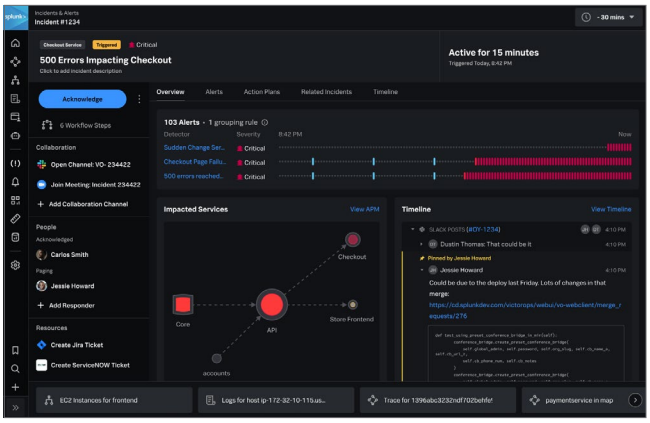


Figure 3: Within the Incident Details window users can see all the granular information that pertains to each incident.

This includes: incident status (trigger, acknowledge, reject resolve or re-route) incident overview, alerts, action plans, related incidents, timeline, as well as workflow steps, collaboration channels (Slack, Zoom), who has acknowledged the incident, who is being paged, and the ability to create a ticket in Jira or ServiceNow.

Similar incidents, recommended actions and responders:

A big part of removing guesswork in your incident response practice is notifying the right people at the right time, with the right amount of context behind an incident. Splunk Incident Intelligence uses machine learning and historical data to surface the similarity of current incidents to previously resolved ones, and automatically recommends the best person to start investigating and fixing that issue.

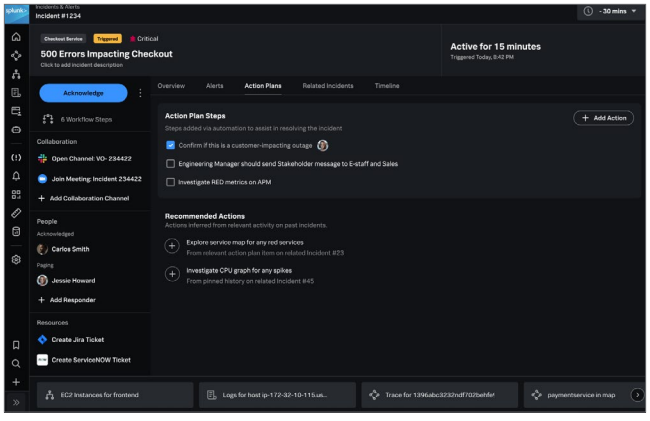


Figure 4: An Action Plans view in Splunk Incident Intelligence outlines next steps an incident responder should take as automated by an administrator, as well as recommended actions based on past incidents.

Automated actions from shift scheduling to incident resolution.

Automating your incident response practices is one of the best ways to effectively reduce mean time to acknowledge (MTTA) and accelerate your mean time to resolve (MTTR). Splunk Incident Intelligence provides automated actions ranging from: on-call scheduling, incident routing, escalations, and mobile and desktop notifications, to ChatOps integrations with Slack and Microsoft Teams, and automated ticketing with ServiceNow and Jira. Save critical time in your incident response process and keep your services running and customers happy.

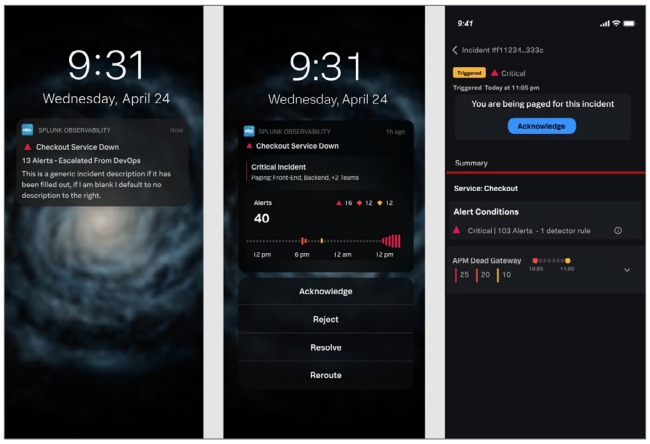


Figure 6: Splunk Incident Intelligence users can set up automated mobile push notifications, so that as alerts and incidents are triggered they can see what transpired, and take action to acknowledge, reject, resolve or re-route each instance appropriately.

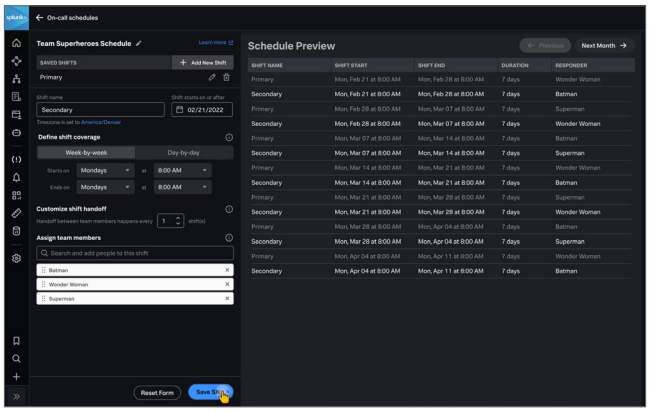


Figure 5: As part of the set up process, administrators of Splunk Incident Intelligence can create and manage on-call schedules for their organization. Here they can name shifts, define shift start dates, timezone, shift coverage on a week-by-week or day-by-day basis, customize shift handoffs between team members, and assign team members to a shift.

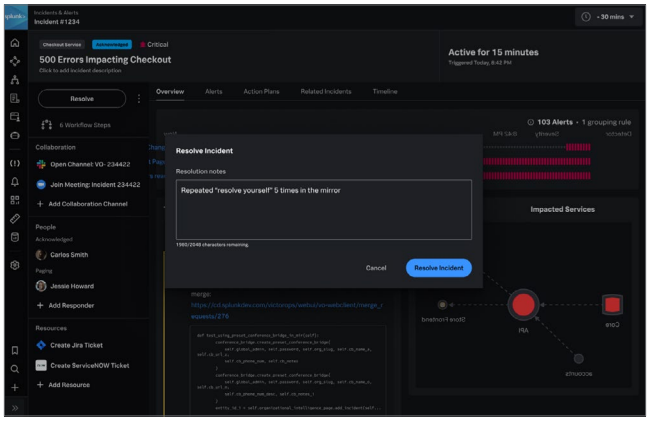


Figure 7: After the appropriate incident responders have acknowledged an incident, they need to resolve the incident. While still within the incident details view they can click the tic tac in the top left of the UI to move the incident from "acknowledged" to "resolve" and add and store resolution notes and chat collaboration artifacts.

Ready to get started? Contact your Splunk representative or start a free trial of Splunk Observability Cloud to experience Splunk Incident Intelligence as part of our unified experience.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com