splunk>

TECH BRIEF

USING SPLUNK ITSI FOR EVENT ANALYTICS

Simplify incident detection, reduce time-to-resolution and gain cohesive service insights

- **Catch issues** before they impact your business
- **Reduce event clutter** and prioritize incident investigation
- **Streamline incident management** and automate incident resolution
- **Reduce manual and repetitive tasks** with artificial intelligence
- **Simplify operations** with unified insights on a scalable platform

When IT events are buried among thousands of others, it's impossible to find and fix the important issues. Instead you're stuck manually filtering out the noise to find the one meaningful event that requires action. The real focus should be on managing the problem, not the event.

Splunk IT Service Intelligence (ITSI) for event analytics provides relief from the suffering of manual parsing of events and enables you to quickly isolate problem incidents that require immediate action. The solution uses artificial intelligence powered by machine learning to provide service context on relevant events, so you can investigate the highest-impacting incidents immediately.

Why Splunk ITSI for Event Analytics?

Splunk ITSI applies machine learning against the large scale of machine data, including logs, events, metrics, wire data and more, and delivers context to understand what components support which high-visibility and critical services. In applying that context, Splunk ITSI helps catch emerging issues, accelerate investigations and ensures speedy recovery of business critical services.

Streamlined Operations

Build on the business-critical service insights you get with Splunk ITSI and deliver the same context to your event data. This empowers you with unified insights to proactively fix problems and also reduce downtime through accelerated root-cause analysis, automated remediation and streamlined incident workflows.

Service Context on Events

With insights that help prioritize IT events, align the business across silos and ensure your staff focuses on the right tasks at the right time. Deliver service context without extensive customizations—initiating incident responses based on business impact. The result? Rapid incident investigation and reduced time-to-resolution.

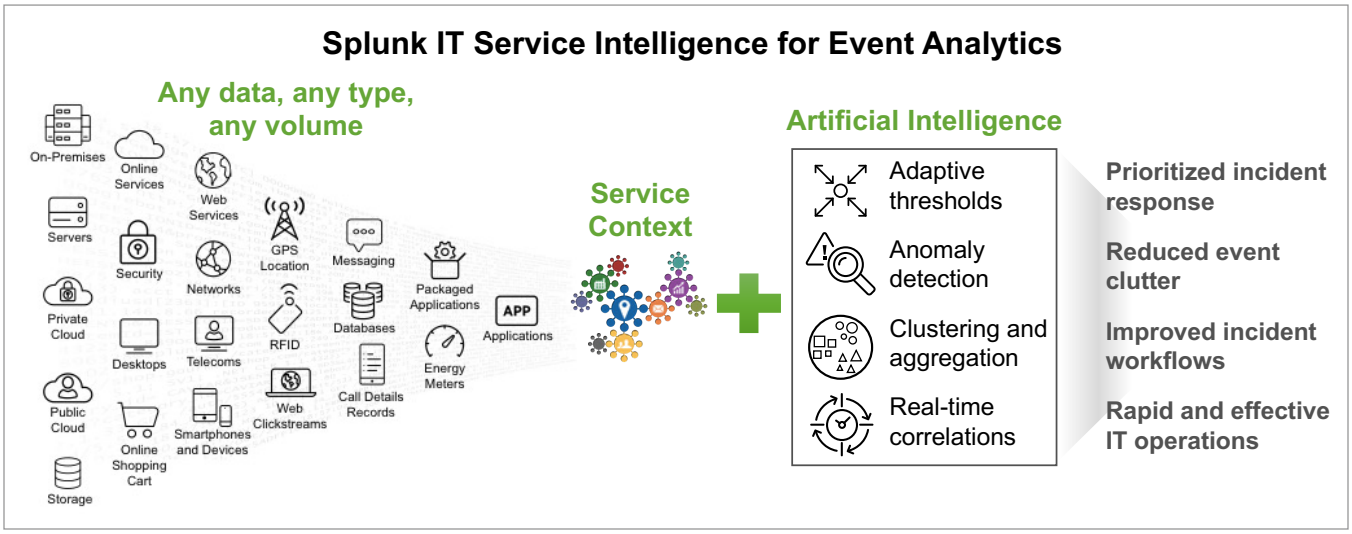

Figure 1: Splunk ITSI helps you move from reactive to proactive operations with service-relevant events and artificial intelligence.

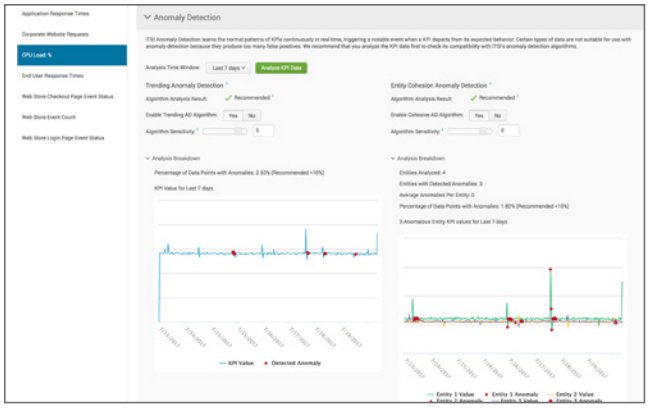

Figure 2: Anomaly Detection

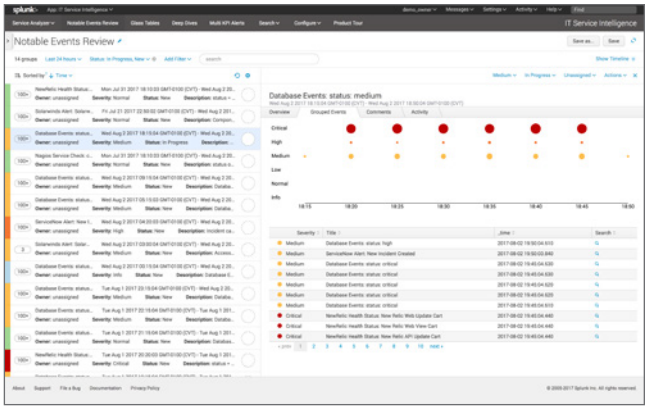

Figure 3: Notable Events Review

Anomaly Detection

Find abnormalities quickly in your KPIs based on an infinite amount of historical data. This enables you to detect subtle pattern changes in the behavior of a single KPI or multiple entities, using trending and entity cohesion algorithms. Instantly apply sophisticated algorithms to the KPIs for meaningful alerts and reduced event traffic.

Adaptive and Time-Variant Thresholds

Employ machine learning to baseline normal operational patterns. Use statistical measurements to determine threshold variability patterns and use built-in templates or custom configurations to account for seasonal trends and expected variance. Dynamically adapt thresholds to this changing behavior in real time to accurately represent the health of KPIs and services to reduce your event clutter.

Event Correlation and Aggregation

Use Smart Mode and Intelligent Correlation to employ built-in artificial intelligence algorithms to automatically group notable events based on their similarity. This reduces the burden to manage events continuously and reduces unnecessary event traffic. Decrease your event noise by grouping related events using aggregation policies. Focus on key event groups and perform actions based on trigger conditions and rules, such as consolidating duplicate events, suppressing alerts or closing notable events when a clearing event is received.

Notable Events

Ingest events from across the IT landscape, other monitoring silos, Splunk ITSI's multi KPI alerts and anomalies to gain an unified operational console of all your events and service-impacting incidents. Make it easier to sift through these events through filtering, tagging and sorting events based on priority. Tag, enrich, review, assign and comment on events to make them informative and actionable.

Multi KPI Alerts

Decrease insignificant alerts by combining KPIs that repeatedly contribute to an outage across multiple services to generate a single notable event. Define severity levels and trigger conditions, or assign weights to KPIs to attribute relative importance. Gain access to the few most important alerts, giving you lead time to address an issue prior to service degradation.

Integrations to Improve Workflows

Integrate with incident management tools and helpdesk applications to accelerate incident investigation and automate remedial actions. Splunk ITSI ships with built-in integrations with incident management tools such as ServiceNow, BMC Remedy, PagerDuty and xMatters. Build custom integrations into other incident management tools to accelerate your incident investigation and streamline incident resolution with automated actions—by running scripts and custom integrations into incident management and automation using Splunk ITSI SDKs.

Next Steps

Gain access to a 7-day personal Splunk ITSI sandbox in the cloud, where you can experience the power of Splunk ITSI for free. Learn more at splunk.com/ITSI-Sandbox.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com