An Introduction to Event Analytics

How ITOps teams can improve system reliability and reduce costs with purpose-built AI/ML

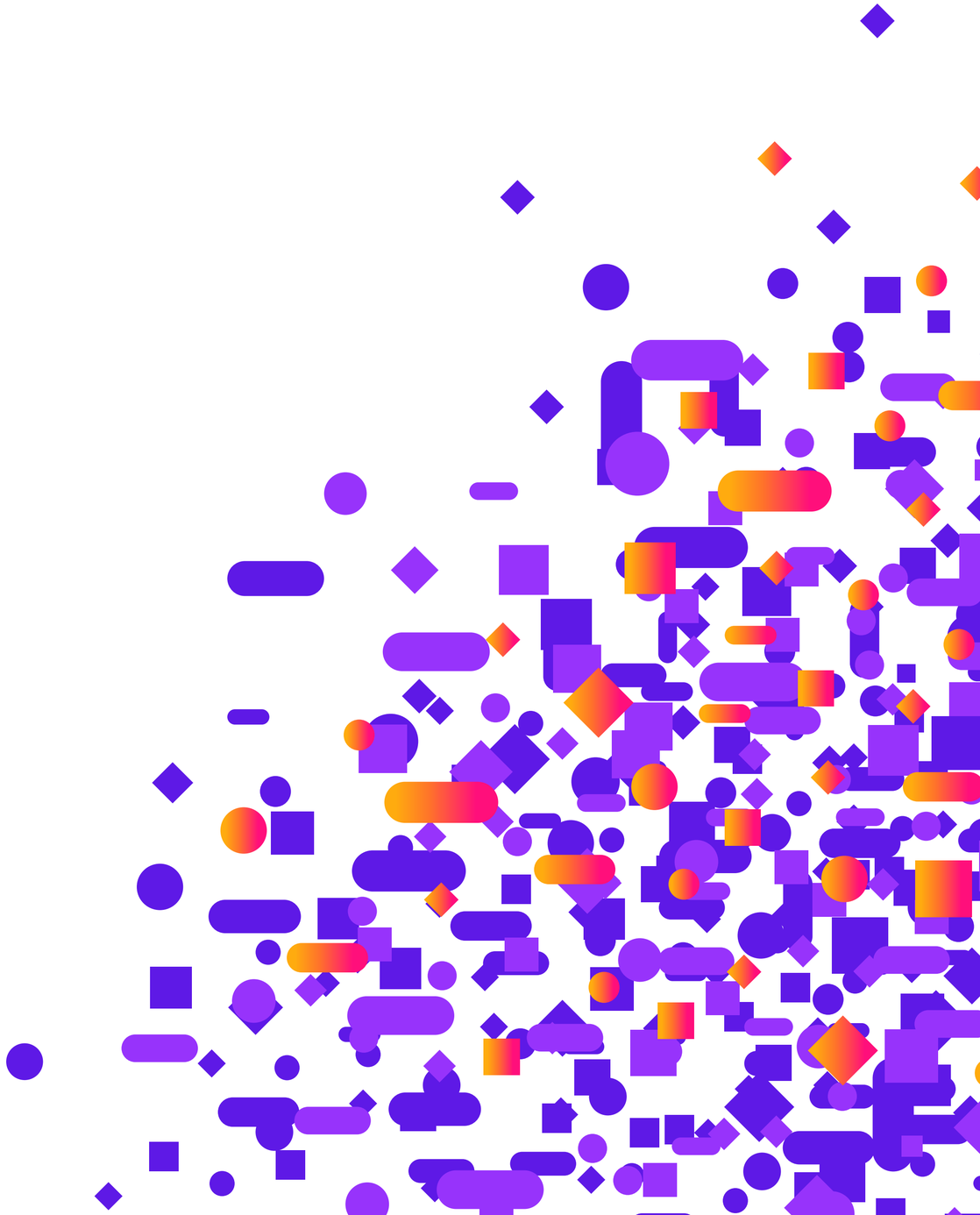
splunk>
a CISCO company

By the time you read this, your IT systems probably generated over a thousand events

… but which ones are worth digging into? It's impossible to make sense of what's happening in your environment, much less find and fix issues, when your team is drowning in alerts. And it gets even worse when you're in the middle of an alert storm. We had a couple of our ITOps friends talk to us about what that feels like. We got stressed just hearing them describe it:

Your kid is screaming and you know they have an ouchie. Based on the yelp, you have a feeling it was probably just a splinter but there's no easy way of knowing. Every time you get close, they pull away and make it impossible to pinpoint the problem.

You're being asked to find something that may or may not even be there — like that proverbial needle in a haystack. You're trying to poke around while constantly being pricked. By the time you found what you're working on, you're exhausted — only for someone to tell you: 'great, but now go back and find the one you missed.'



Now breathe

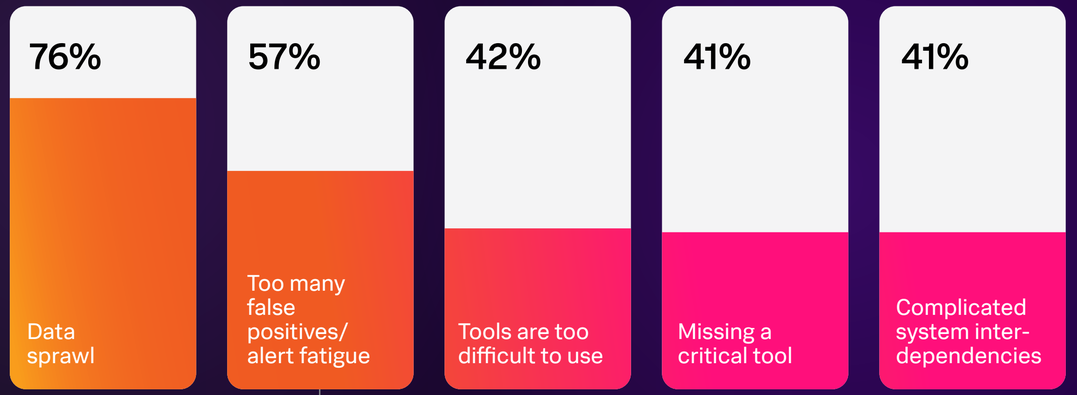
How did you feel after reading those (maybe all-too familiar) anecdotes of what experiencing an alert storm can feel like? Is your heartbeat elevated? Palms sweaty, knees weak, arms heavy? It might have triggered your body's fight or flight response — and that's what leads to burnout.

Burnout is emotional, physical, and mental exhaustion. It happens when you feel overwhelmed, emotionally drained, and unable to meet constant demands. As the stress continues, you can start to lose the interest and motivation that led you to take on a certain role in the first place. Maybe at that point you choose to leave. Maybe your colleague does, or your manager. The result? A team that's already stretched too thin is even more so.

Some teams might have too many alerts all the time because of poor alert hygiene (inaccurate base lines, for example, or poor alert strategy) and are living in a state of constant burnout — even when there are no issues, cascading alerts, or alert storms happening at that current time.

Beyond the real and lasting human impact, staff burnout ripples through the business. It can lead to an organization's inability to identify problems, find root cause, and remediate incidents — meaning longer outages, lost revenue, and a damaged brand reputation.

Technology executives cite their toughest obstacles to managing downtime



57% of technology executives cite their toughest obstacle to managing downtime is too many false positives and alert fatigue.

Source: The Hidden Costs of Downtime

Event analytics, defined

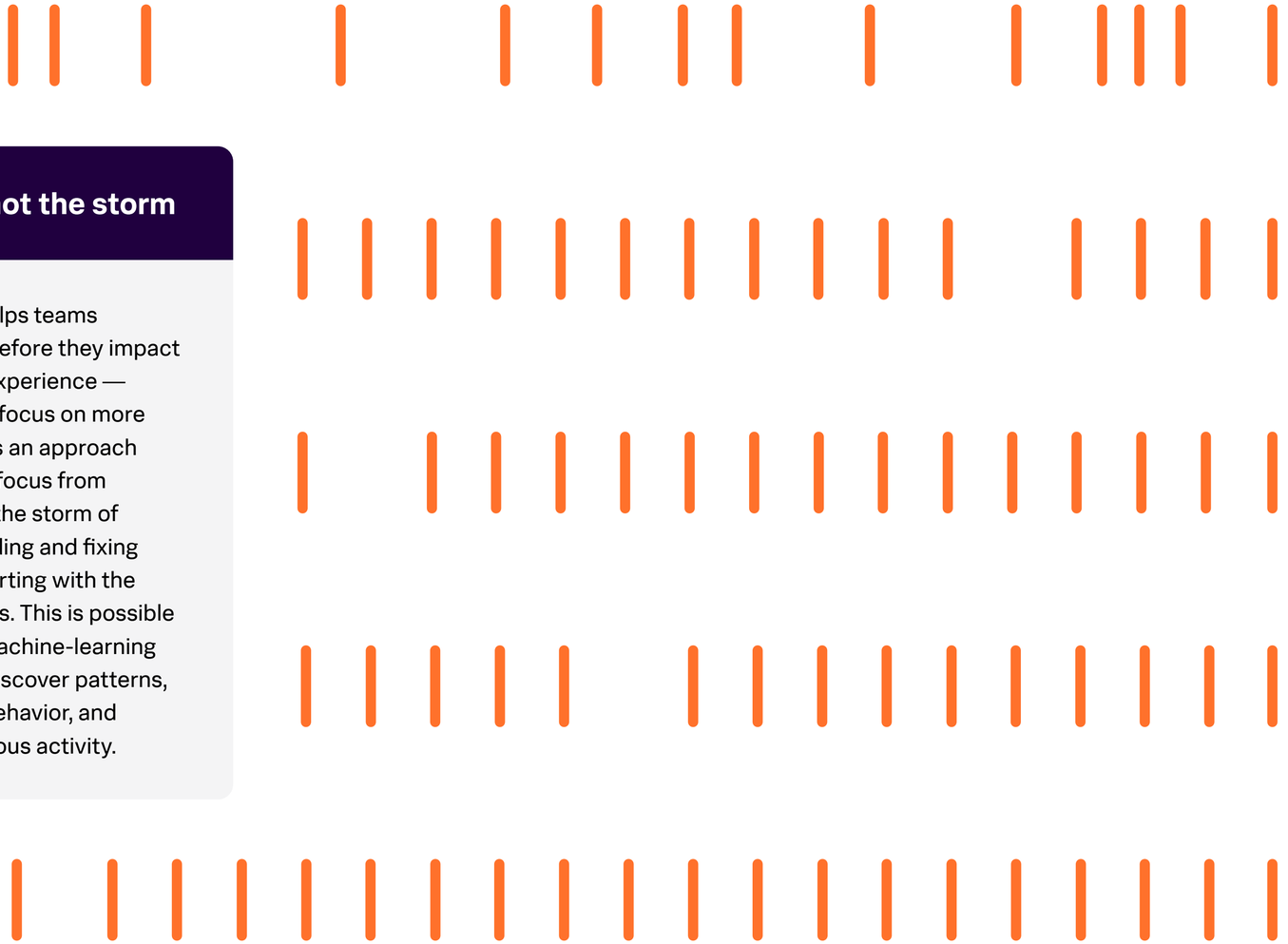
Very simply, event analytics is a way to correlate and analyze telemetry data and alerts from monitoring, event, and incident management tools. Historically, events — and any subsequent event action — had to be managed individually by human analysts, either as the events emerged or by manually searching through log files to look for anomalies and outliers.

When event management systems evolved, they gave ITOps teams a way to sift through the various event alerts and streamline operations. But as networks continued to grow, the number and complexity of alerts in many large enterprises quickly became unwieldy. So, it's common to find multiple tools that manage various events in different segments of the organization.

Event analytics consolidates multiple systems into a centralized platform. This simplifies discovery of the root cause of any given problem.

The calm — not the storm

Event analytics helps teams prevent outages before they impact your customers' experience — freeing up time to focus on more strategic tasks. It's an approach that switches the focus from merely managing the storm of events to truly finding and fixing what's broken, starting with the most critical issues. This is possible with the help of machine-learning capabilities that discover patterns, baseline normal behavior, and recognize anomalous activity.



Managing the problem, not the event

While we were busy breathing into a paper bag after those depictions of alert storms, our ITOps friends told us what they really wanted was pretty straightforward: To see all their alerts in one place. After that, they want to be able to reduce alert noise and correlate related alerts so they'd be able to prioritize what's important and know where to start first. All this, they said to us, would lead to Nirvana in the form of faster incident response and less downtime.

And though the particulars might vary from industry to industry, we imagine event analytics would help ITOps teams across sectors uplevel their troubleshooting capabilities and quality of life demonstrably.

Across sectors, organizations are all wrangling complex architectures, piles of (potentially disjointed) tools and so, so much data to keep their systems up and running. Let's look at some examples.

Finance industry

Banks need to monitor transactions in real time and also need to harness sophisticated event analytics to identify patterns and prevent fraudulent activity.

Healthcare industry

Hospitals need to monitor critical systems and devices in real time to help ensure things like life-support systems function optimally.

Telecommunications industry

Companies need to monitor network status and traffic so they can proactively predict and prevent outages, optimize traffic, and ensure high availability.

How event analytics works

For those completely new to event analytics, here's a Splunk blog that reviews key terms and concepts. We've also included a short glossary of terms in the back of this book. We won't quiz you, though. Don't stress.

The easiest way to understand how event analytics works is to describe the event lifecyle from detection to resolution.

1. Raw data

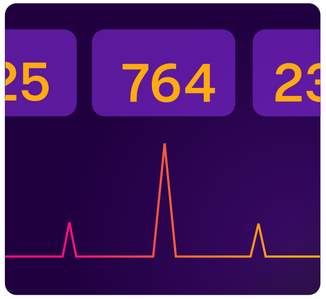
After data is ingested into the event analytics tool from multiple data sources, it's processed through correlation searches to create notable events.

2. Notable event

The tool generates notable events when a correlation search or multi-KPI alert meets specific conditions that your team defines.

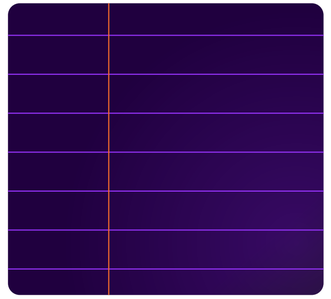
3. Episodes

Notable event aggregation policies group the events into meaningful episodes, a group of events occurring as part of a larger sequence (an incident or period considered in isolation).



4. Identify issues

A dashboard helps you view episode details and identify issues that might impact the performance and availability of your IT services.



5. Take actions

You can then take actions on the episodes, such as running a script, pinging a host, or creating tickets in external systems.

I got 3 big problems and event analytics solves ‘em

Our ITOps friends tell us that there are three main issues getting in the way between them and being able to simplify incident detection so they can get cohesive service insights and reduce time to resolution.

PROBLEM 1

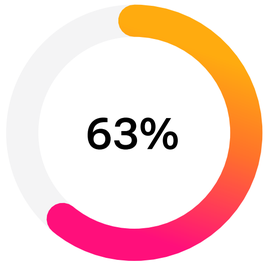
“Making sense of too many alerts is exhausting!”

The issue: Whether that means too many day-to-day alerts or an incident causing cascading alerts, teams are drowning in too many of them — making it impossible to find and fix the important issues.

How event analytics helps: Event analytics tools can help detect and triage incoming alert storms and intelligently group alerts into episodes and prioritize them. This reduces the total number of alerts to actionable episodes and helps teams make sense of the incident. Also, an event analytics tool can help you improve your digital resilience and reduce downtime by giving you insights into historically similar episodes.

Success story: Molina Healthcare needed to ensure uptime for its revenue-generating claims engine while finding a quicker way to identify, respond to, and resolve security and IT incidents. Now with Splunk, the Molina team resolves issues in minutes, slashing IT incidents, boosting claims engine uptime, and eliminating hours spent coordinating with various cross-functional teams and tools.

Read the full story.



reduction in MTTR

“It’s important to get the right visibility so we can be more efficient and drive our costs down. This ties back to that singular vision of taking care of the underserved individuals in the community.”

Ben Gordon, Vice President of Enterprise Infrastructure Services, Molina Healthcare

PROBLEM 2

“I’m tired of false positives! Also, it’s hard to prioritize what’s most important to the business.”

The issue: Isolating, prioritizing, and preventing incidents is hard enough as it is without having to wade through scads of alerts to determine which ones are real and which ones could be false positives.

How event analytics helps: Teams can sort through unwanted noise by grouping and enriching related alerts. With the assistance of machine learning, adaptive thresholding can dynamically adjust baselines based on behavior — leading to more accurate alerting by detecting and excluding outliers from the baselines to quickly help spot unknowns.

Success story: Leidos’ 48-year history spans everything from supporting the U.S. space shuttle program to helping design an America’s Cup yacht race winner. To continue solving global challenges in defense, intelligence, health and other markets, Leidos needed to pare down the thousands of alerts and events that the team was fielding. With Splunk, Leidos now has real-time correlation to automate event handling and customizable dashboards for business process views.

Read the full story.

3,500-5,000 daily alerts boiled down to roughly 50 tickets for network and datacenter operations to act on.

“We have so much information at our fingertips thanks to Splunk … we’re constantly solving business problems in creative ways.”

Don Mahler, Director of Performance Management, Leidos

PROBLEM 3

“I wish I had more context to solve these issues — fast — without all the manual work.”

The issue: A lot of manual labor and time can go into enriching your data so you have the context you need to solve issues quickly. Click this field here, enter in an IP address. Click another field, and enter a location. This takes valuable time away from fixing issues and being more proactive about avoiding certain issues to begin with.

How event analytics helps: Teams can set up automated actions to use for not only alerts but also scenarios — helping save valuable time. Also, enriching your data by adding information from other sources to your events can help you speed mean time to respond.

Success story: Providing landline, broadband, fiber, TV, and mobile services to UK consumers and businesses, TalkTalk aims to use data and automation to become the country’s most recommended communications provider. Legacy systems made it difficult to gain sufficient data on network performance and service outages, resulting in limited ability to identify problems quickly and effectively. With a more complete picture of network and performance metrics, TalkTalk has drastically reduced cases of underperformance across more than 5,000 exchanges while strengthening its brand reputation.

Read the full story.

Reduced the weekly number of critical “red exchange” incidents from several thousand to 10 or fewer.

“It’s about spotting where we have a flawed process, then using the Splunk platform to provide us with a list of affected customers so we can fix the problems using robotic process automation (RPA). Splunk gives us access to the data to tactically fix processes.”

Paul Emmett, Head of Network Operations

Eight implementation tips

Our ITOps friends helped us narrow down some best practices once you decide to implement event analytics.

1

Start big and whittle down to small. You don't want to have to backtrack when it comes to setting up rules for grouping and alerting, so think big to start.

2

Make sure you're receiving all the alarms from any 3rd party tooling. It's pretty simple, but you don't want to miss anything important.

3

Create generic correlation searches. More correlation searches doesn't equate to better outcomes. Make your correlation searches as generic as possible to make them easier to manage.

4

Enrich your data. There is so much you can do in the correlation search to drive later processes, such as utilizing lookups to correctly target service owners.

5

Work backwards. Think of how you want to end incidents. When you do create episodes or incidents, think about how you want to end them. Ask yourself what's your indicator that things are healthy or if a new incident should be created.

6

Opt for cloud-based tools when possible. Cloud-based analytics tools are simpler to install, require much less in the way of infrastructure, and are just as configurable and customizable as on-prem tools.

7

To avoid duplicate events, use the same frequency and time range in correlation searches. When configuring a correlation search, consider using the same value for the search frequency and time range to avoid duplicate events. For example, a search might run every five minutes and also look back every five minutes.

8

Don't create too many aggregation policies. Too many policies create too many groups, which produces an overly granular view of your IT environment. By limiting the number of policies, you create more end-to-end visibility and avoid creating silos of collaboration between groups in your organization.

Here’s that glossary we promised you

The following terminology list will hopefully make it a little easier for you to understand event analytics and start waxing poetic about its potential to your managers and your team.

Plus, we have some parting words for you. Look: We’ve only been gifted so many hours each day to do the things we need to do, plus the things we love. Are we getting a little philosophical and a tad out of scope for an e-book about an ML-assisted prediction, detection, and resolution tool? Maybe.

But — could event analytics help you and your team better manage alert storms and give you the ability to be more proactive and strategic? Yes. And if that means less stress and burnout and more time lingering over your morning coffee or deciding to take on fly fishing with some of your new-found leisure time, then we’re all for it.

We want to help you simplify your IT strategy. Contact sales and let our experts help you find the perfect scalable solution to meet your needs.

Event analytics terminology for beginners

Event: In analytics, an event is a record that refers to a change in the state of a device on the network.

- Events are classified based on severity levels and the impact of these levels on response strategies: An event is not necessarily negative — event categories are divided into three types: informational, warning, or exception.
- There are also different sources of events, for example, servers, apps, and network devices.

Event data: This is extra data added to specific events in an analytics index. Event data, which commonly includes information like character set encoding, time stamping, and user-defined metadata, makes it easier to do analysis and conduct quicker searches. As the event data index grows, anomalies can get easier to spot with event tracking that illuminates long-term trends.

Incident: An incident is triggered when there is a security breach or an interruption of service. In an event analytics tool, an incident dashboard will display all notable events and episodes.

Correlation search: A correlation search is a type of scheduled or recurring search of analytics event logs that monitors for suspicious events or patterns. Users can configure a correlation search, which is used to generate a notable event when certain conditions are met. Correlation searches can span across multiple types of data, helping teams more accurately identify suspicious attack patterns.

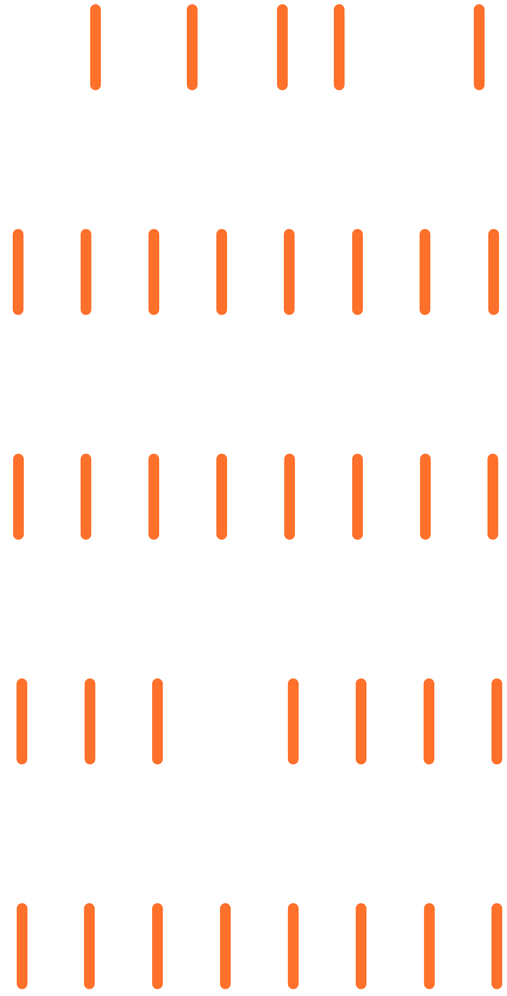
Notable events: A notable event, or top event, is a specific event record that is generated by a correlation search. Typically this takes the form of an alert or the creation of an incident, delivered to the analyst after certain criteria have been met. Essentially, notable events are the ones you need to worry about.

Notable event aggregation policy: A notable event aggregation policy is used to group together and organize notable events. These policies can be set by a human analyst or a machine learning algorithm that automates their implementation. During this process, duplicate entries are removed, and an episode is created once the events are appropriately grouped. The notable aggregation policy contains both the notable events and the rules that automate the actions in response to an episode. In other words, the policy contains both the problem and the solution.

Grouped alerts/Episode: A group of notable events that have been identified and clustered together in an event category by an event analytics system. Episodes typically describe potentially serious events that have an adverse effect on service, like an application that is no longer running, for example. An episode is generally a subset of an incident, which describes a longer and more sustained sequence of events.

Alert triggers: Analysts can configure alert trigger conditions, which can be triggered in real time or on a schedule. When an analyst creates a set of alert trigger conditions, correlation search results are checked to see if they match the conditions. For example, an alert trigger condition may be set to monitor the bounce rate of a web page that would be triggered if the bounce rate exceeded a prescribed threshold.

Types of alerts: There are two kinds of alerts: real-time alerts and scheduled alerts. Real-time alerts monitor for qualifying events and are useful in cases where an emergency exception situation has been created, such as a crashed server or a network outage. In contrast, scheduled alerts are not run in real-time but are run periodically. Typically alerts are run during slower times of the day (such as late at night) or at the end of a given time period.



Simplify your IT strategy. Contact sales and let our experts help you find the perfect scalable solution to meet your needs.

splunk> a cisco company

24_CMP_ebook_an-introduction-to-event-analytics_v9