PagerDuty

The complete guide to end-to-end event-driven automation

Table of contents:

Introduction

In today's macroeconomic environment, IT leaders know that balanced, sustainable growth is the key to moving an organization forward. Yet attaining that is a challenge. Leaders are looking at how to maximize efficiency, preserve their talented teams for value-add work, and provide ever-more-discerning customers with exceptional digital experiences.

One of the best ways to do this is by asking, "Can a machine do this? Or do I need a subject matter expert (SME)?" If automation can complete a task, teams save time so that they can work on more strategic initiatives.

Organizations can use automation in many ways. One that brings high ROI is incident response. Incidents are costly, time consuming, and lower the customers' trust in the business. By reducing mean time to resolution, MTTR, (or even resolving the incident before it becomes customer impacting), organizations see an immediate positive impact. And, so do the customers.

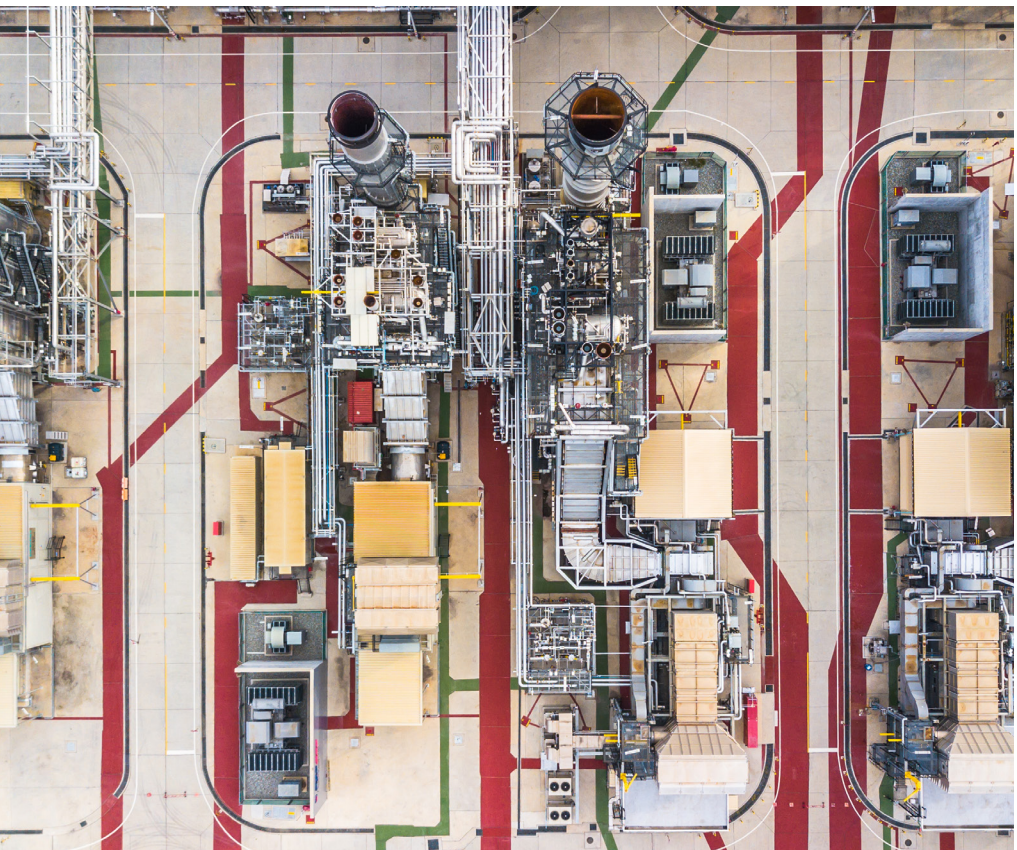
But how can you automate incident response? How early in the incident lifecycle can you start automating things? And is it a pipe dream to have automation throughout your incident response process? You can do so much with end-to-end event-driven automation that the sky is truly the limit. We'll cover how you can adopt and scale automation for better incident response in this eBook.

What is end-to-end event-driven automation?

An event is anything that your monitoring tools consider a warning sign of failure. How you configure a monitoring or observability system can vary organization to organization. If you need the information to understand service performance, it should create events to notify your teams.

Event-driven automation is automation that is kick-started at the event level, normalizing and enriching data at ingest. This automation can transform event data to a more understandable format that helps responders get up to speed faster during an incident. It can also jumpstart the incident response process, ensuring that event data is created as an alert and routed to the correct team with added context. For more advanced implementations, this automation kicks off automated diagnostics or even auto-remediation where an issue is resolved before it ever needs to become an incident.

That's where end-to-end comes in. End-to-end means that you can execute automation throughout the entire incident lifecycle if needed. You could even avoid human intervention entirely for well-known issues. End-to-end event-driven automation carries the event from an incoming event stream all the way to a resolved incident.



How can this help my teams?

End-to-end event-driven automation can help a wide variety of teams. Here's how everyone, from the NOC, to support teams, to developers can benefit.

NOC: Depending on how monitoring is set up across the company, your first line of defense may have a hard time making sense of the vastly different alerts pouring in. Without normalized data, the NOC wastes time trying to manually parse what's important from what's not. With end-to-end event-driven automation, NOCs can normalize the incoming event data and set criteria on a global scale for what events are routed where. This helps them prioritize the issues the NOC is responsible for. This L0 automation makes modern NOCs more efficient and capable of resolving issues.

SRE: SRE teams are often the stewards of automation within an organization. They're responsible for crafting, maintaining, and scaling automation. Sometimes they also act as a coach for other teams looking to adopt more efficient ways of working. With end-to-end event-driven automation, SRE teams can set event transformations and routing at ingest and automate the full journey of an event. SRE teams can also build out auto-remediation so that a human is never bothered with an incident that a machine can resolve.

MIM: MIM, or Major Incident Management, teams are responsible for commanding the response effort and coordinating across groups for a unified business response. To do this, they need to have major incidents detected early and routed immediately to them via automation. They also need the incident populated with automated diagnostics and the event data normalized. These small changes are sometimes the difference between an incident costing four figures, or six-plus figures.

Engineering: Engineering teams are necessary for driving innovation in the company. They can't do that if they spend all their time firefighting. With end-to-end event-driven automation, engineering teams can ensure that they only receive notifications for incidents that they need to work on. The incidents intelligently route to the right team every time. And, engineering teams can create auto-remediation for well-understood problems so they can preserve their time for more value-add work.

Support: For support teams, end-to-end event driven automation means faster MTTR and fewer incidents. With auto-remediation, things that might have been customer impacting are resolved immediately without needing to ask an engineering team for help. And, with better data and the correct teams on the incident from the start, support will receive fewer cases from upset customers.

While some organizations use homegrown automation tools, many companies choose to align on one tool for automation that all teams can use. But a tool alone can't make an automation initiative successful. IT leaders need to strategize on how they intend to deploy an initiative and see value while it builds traction.

How can I get started with end-to-end event-driven automation?

For many organizations, it's not reasonable to implement end-to-end event-driven automation all in one go. It would be too much change at once, and would take away from other initiatives that are also crucial. But IT leaders can't afford to skip out on implementing. The happy middle is a crawl, walk, run approach that allows organizations to adopt automation at a pace that fits their needs. It also helps organizations see incremental improvements that drive the initiative on and gather support. Quick wins and simple implementations can lead to drastic improvements in noise levels, MTTR, and more. Here's a crawl, walk, run approach we see customers having success with.

Crawl with suppression and eliminating transient alerts

For organizations looking for quick wins, suppressing alert noise and eliminating transient alerts can reduce the burden of incident response.

Suppression

Suppression stops an incident from sending a notification. Within PagerDuty, the incident turns into an alert with a status of "suppressed." According to AIOps customer data, **50% of noise compression comes from suppression.** Suppression can reduce incident volumes via broad rules targeting swaths of events that provide no value.

For example, the Event Orchestration team suppresses events until a certain number of them arrive. At that point, the team turns suppression off and allows Event Orchestration to start creating incidents.

Eliminating transient alerts

Pausing notifications for transient alerts allows users to suspend the creation of an incident for a predefined period of time. Once that period lapses, the incident is created as per usual. This orchestration is best used for flapping incidents with well-defined conditions. It pairs well with threshold and schedule conditions where incidents are suspended over a period of time.

For example, one of our customers pauses certain high CPU usage incidents for five minutes. The organization only creates an incident if high CPU usage turns out to be long lasting.

Walk with event, alert, and incident enrichment

Once you've reduced your noise and eliminated transient alerts, the next stage is to make sure that the events, alerts, and incidents your teams do interact with are as informative as possible. This is where enrichment comes in.

Event enrichment

Event enrichment allows you to re-write common event format (CEF) fields upon event ingestion, or create new fields for an event that will live in the event's custom details. This speeds up triage by ensuring responders have incidents populated with relevant contextual information. It also normalizes event data so incidents look the same across teams.

For example, a company could create a custom detail with the results of diagnostic monitoring. The organization could then call the field results and load it with the result of scripting.

Alert enrichment

Once an event becomes an alert, users can define the severity that an alert should be created with. As severity drives how an escalation policy is used, triggering an incident with the correct severity can mean the difference between routing notifications to the right or wrong escalation policy.

For example, you could say that alerts for a particular service, like check out, that's customer-facing and revenue-impacting should be listed as a Sev1. Or, for a lower-priority service, you could mark that all alerts are considered a Sev3 or Sev4.

Incident enrichment

Incident enrichment allows users to define the priority and notes that an incident has when it is created. Notes are particularly useful for telling responders potential root cause of an incident. They can also populate knowledge base articles, internal wikis, or provide information on how a responder should proceed.

One of our customers leverages incident enrichment to populate incidents with instructions indicating an incident will not be auto-resolved, and further provides standard operating procedures (SOP) and knowledge base links to responders so they can get production online faster.

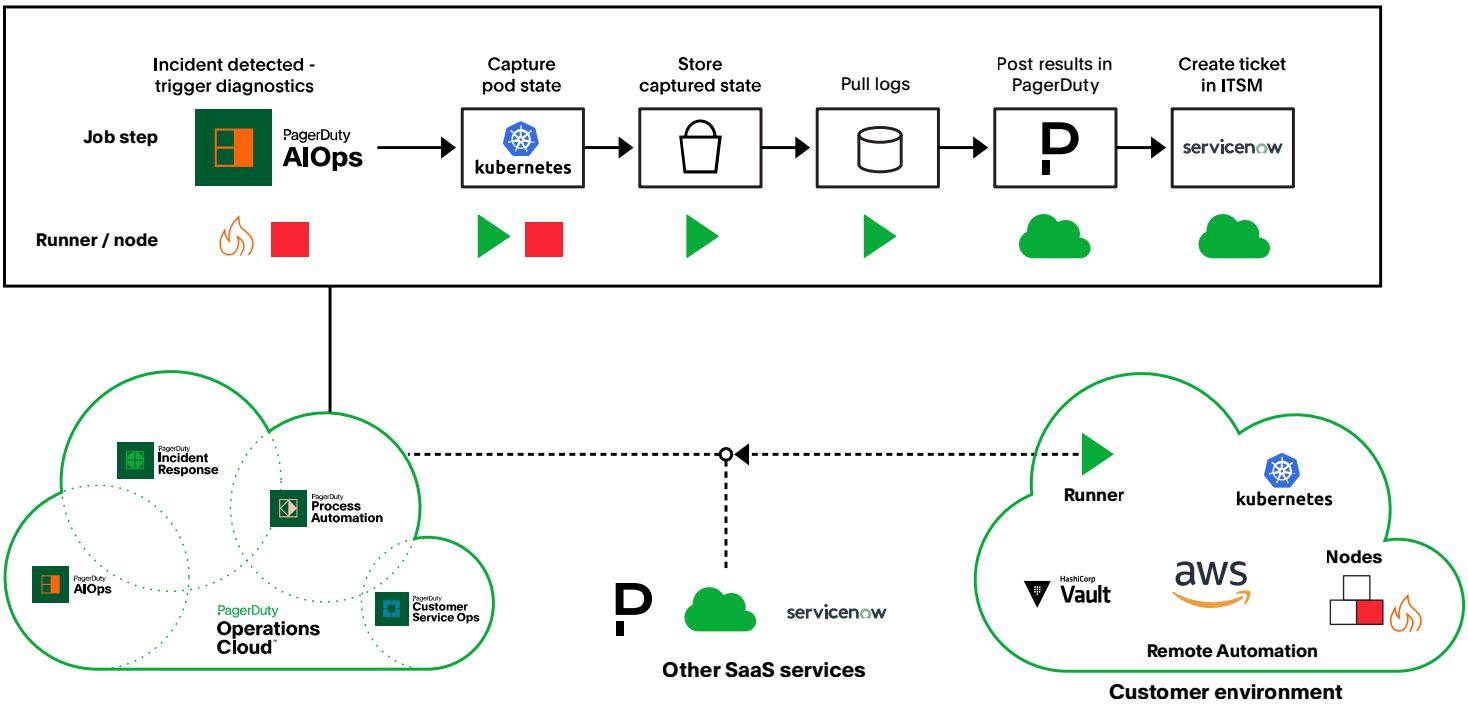
Run with end-to-end automation and auto-remediation

After you've reduced noise, eliminated transient alerts, and ensured that events, data, and incidents are all as informative as possible, what's next? You can begin employing automation to gather diagnostics or resolve incidents with well-understood fixes.

One way to do this is via webhooks. Webhooks allows the user to define custom headers and payload body fields that trigger upon incident creation. For diagnostic purposes, this helps responders gather more key information about an incident without having to run manual processes. For auto-remediation purposes, this can mean webhooks triggering an action that resolves the incident before a human is ever involved. Both can improve MTTR and make incidents less painful for both the teams responding to them and the end customer waiting for service to resume.

Another way to do it is via **Automated Incident Resolution.** Automated Incident Resolution is part of PagerDuty Process Automation. It democratizes expert knowledge and access to enable first responders to triage, diagnose and remediate incidents. When an incident is created in PagerDuty, automation jobs can be invoked either automatically or by responders with the click of a button. With pre-built job templates and plugin integrations, you can empower your first responders with the expertise to modify and add new automation that previously only subject matter experts could do before.

Automated Incident Resolution connects to production infrastructure through a Runner (depicted as green triangle in the diagram below) that is deployed behind a firewall or within a VPC. The Runner executes local automation steps and provides an encrypted connection back to the central automation environment.



How do I provide a metric for success?

You may not want to wait until you've reached the "run" stage before showing success, though. And small signs of success will be apparent throughout the journey. To keep an end-to-end event-driven automation initiative gathering steam, you'll need to show value to the organization. You can do this both qualitatively and quantitatively.

Qualitative value

Qualitative value is tougher to understand because it's squishy. It's not usually tied to a number, KPIs are difficult to identify, but yet it exists. And, it's one of the first signs of success in automation. Why? Teams are excited about improving their workloads. They want better work-life balance, fewer interruptions, more time for deep work and value-add initiatives. This makes their work experience better. And that's difficult to measure. Here are a few ways you can consider measuring success:

- **Attrition:** Compare attrition rates to teams with more automation initiatives completed vs those without. Especially for incident-heavy teams, this can be quite illuminating. Even a 5-10% difference in attrition means lower costs to the business for time and resources spent towards recruiting and training replacements.

- **Exit interviews:** All attrition isn't possible to mitigate. Sometimes, the right opportunity comes up. But, exit interviews can be a key way to understand why someone is leaving. Ask your HR team about the exit interview process. Is there a way to ask a question about processes, including automation? Can they consolidate feedback and share it with you without exposing employee details?

- **Employee surveys:** Waiting to understand whether an initiative is driving towards better employee experience until they leave is costly. It's better to take your team's pulse frequently. Review your employee survey cadence and incorporate questions about the automation initiatives to understand how your team is feeling. Comparing sentiment even across a quarter can show success.

Quantative value

Some metrics are less difficult to measure than employee satisfaction, and gathering the data is easier. These quantitative measures can show how much end-to-end event-driven automation helps teams within a few weeks, making it much faster than most of the qualitative metrics above. Let's take a look:

- **MTTR:** Look at the MTTR for services that are undergoing an end-to-end event-driven automation initiative. Compare the MTTR to previous months' MTTR to see a reduction. Take into account seasonality as well as any outlier major incidents that can skew the data. You can compare that improvement against similar services that are not currently working on automation. Is there an improvement in MTTR between the two?

- **Binary per service:** This is the most crude metric, but perhaps the easiest to attain. You can examine how many services have automation applied now vs prior to beginning this initiative. Are you scaling automation across your organization faster than before?

- **SLA penalties:** Review SLA penalties for past incidents. As you adopt more automation, is there a correlation between fewer SLA penalties and more end-to-end event-driven automation?

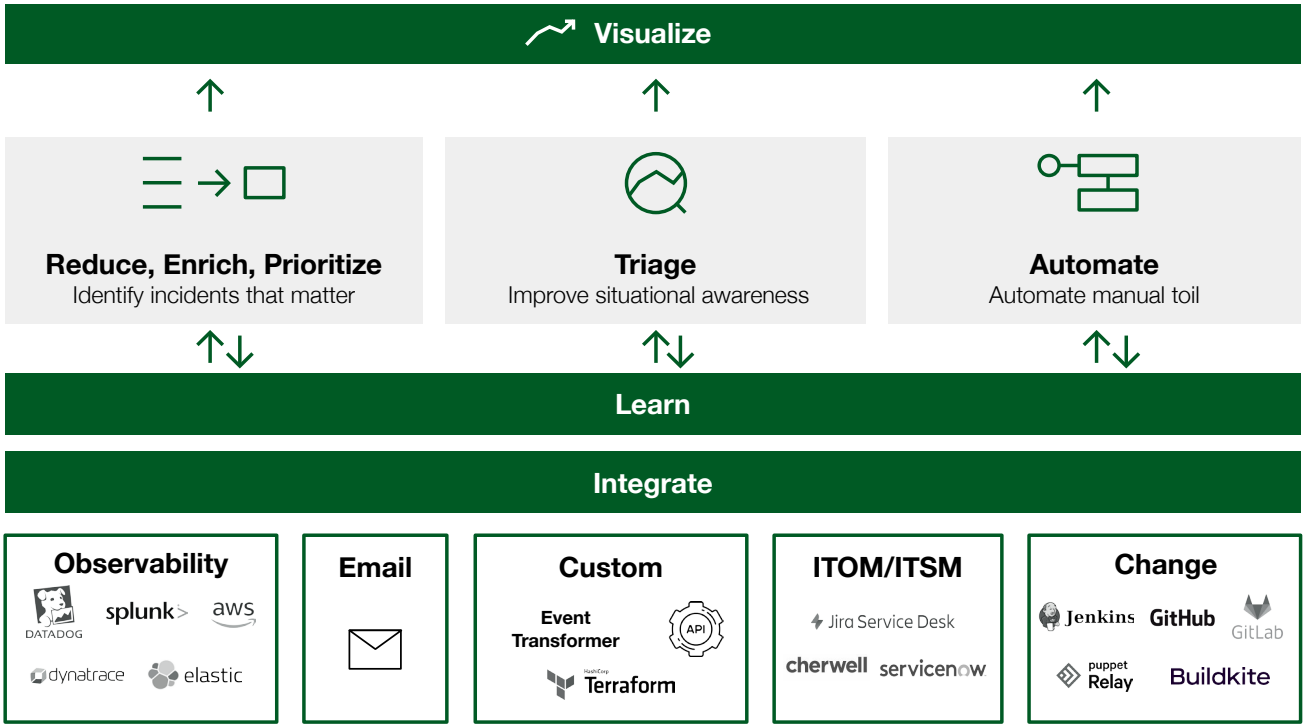
As you gather data, ensure you share it with teams involved and stakeholders to keep the momentum going. The more support you have internally, the more ROI you can expect. You may also want to consider looking at external support from a vendor to help your organization double down on automation investments and scale them safely across the ecosystem.

How can PagerDuty help?

The PagerDuty® Operations Cloud™ helps organizations resolve urgent, unplanned, high-impact work faster and with less expense to the business. As part of the PagerDuty Operations Cloud, PagerDuty AIOps helps teams reduce noise, triage efficiently to drive the right actions towards resolution, and remove manual, repetitive work from the incident response process.

PagerDuty AIOps

How we do it



PagerDuty AIOps works out of the box without requiring long implementations or heavy ongoing maintenance. Organizations continue to see best-in-class results (including a 400+% ROI).

PagerDuty's AIOps solution leverages machine learning and automation to empower our customers to remove manual processes and drive to the next best action. And, with the PagerDuty Operations Cloud, AIOps becomes a supercharger for incident response, plugging into all your critical systems to accelerate urgent work.

But don't take our word for it. Hear what our customers have to say:

"Leveraging PagerDuty's Global Event Orchestration has been critical to ensure that our event routing processes are efficient and scalable to optimize IT operations and spend," said Brian Long, Cloud Infrastructure Engineer at Hyland. "With Global Event Orchestration, our organization is able to detect the "resolved" condition from our notifications to execute as a resolve and reduce the number of places these conditions need to be configured by at least a factor of three. This frees up our time to focus on innovation, not configuration."

You can also look to analyst firm Forrester for more information on how PagerDuty excels. In fact, PagerDuty is named a Leader in The Forrester Wave™: Process-Centric AI for IT Operations (AIOps), 2023.

"Reference customers praised PagerDuty's event noise reduction, with one calling its Event Intelligence "very powerful." PagerDuty is a good fit for enterprises with diverse technologies that will remain in place or must integrate into a common platform that can drive automation and eliminate low-value work."

If you're looking for similar results, reach out to us today and book a custom demo from our team. Or, check out our Modern Approach to Buying AIOps Key Principles and Paths for Success eBook.

PagerDuty AIOps customers tout:

87% fewer incidents

14% faster MTTR

9X faster adoption of automation, and more

About PagerDuty

PagerDuty, Inc. (NYSE:PD) is a leader in digital operations management. In an always-on world, organizations of all sizes trust PagerDuty to help them deliver a better digital experience to their customers, every time. Teams use PagerDuty to identify issues and opportunities in real time and bring together the right people to fix problems faster and prevent them in the future. Notable customers include Cisco, Cox Automotive, DoorDash, Electronic Arts, Genentech, Shopify, Zoom and more. To learn more and try PagerDuty for free, visit pagerduty.com. Follow our blog and connect with us on Twitter, LinkedIn, YouTube and Facebook. We're also hiring, visit pagerduty.com/careers to learn more.

Learn more about PagerDuty and start a free trial at pagerduty.com/freetrial.