PagerDuty

Supercharge your incident resolution

Contents

Introduction

As the world evolves, customer expectations for speed and responsiveness continue to increase. At the same time, operational complexity is also growing, creating a tension that often leads to longer times to solve problems, which may result in delayed flights or service outages. The downtime, along with the associated lost revenue and lost productivity is not just a software problem—it affects all areas of the organization, generating **Incidents.**

According to a 2023 EMA report, Automation, AI, and the Rise of ServiceOps, significant incidents and outages cause unplanned work, with 19% of respondents reporting a high impact (25% or more loss of productivity) and 47% of respondents citing a significant impact (10%-25% productivity loss).

The work resulting from these **incidents** can't always be postponed, and it results in IT and engineering teams getting inundated with vast amounts of signals and alerts on a daily basis. The sheer volume of information can be overwhelming, leaving responders struggling to distinguish the signal from the noise. While human analysis, decision-making, and action are still essential, it is no longer feasible for human teams to manually sift through terabytes of data without some degree of machine assistance. Making the problem worse, are the diminishing returns from more responder labor – As more unplanned work arrives, throwing human hours at it works to a point until it starts compromising other work and stops being a positive ROI.

Once an incident occurs, the process of gathering detailed context to determine the root cause is a time and people intensive process. In fact, our own data shows it can take up to 85% of the duration of an incident to arrive at a diagnosis, and the average incident involves more than 4 responders. Making matters worse, specialists are often spending 25% of their time performing repetitive and relatively boring tasks instead of innovating.

The reason responders need to escalate to other engineers is because responders and engineers have differing levels of experience. Responders need to gather the deeper contextual data (diagnostics) to aid in troubleshooting. They may also lack detailed knowledge of the many different systems (disparate environments) they're in charge of, lack skills (knowledge gap) about how these systems work, or lack access privileges to run tests or execute privileged tasks (security gap).

Process Automation, a component of the **PagerDuty Operations Cloud**, helps overcome these challenges by enabling automated tasks to be executed over disparate environments, narrowing the knowledge gap by democratizing procedures traditionally performed only by specialists. Automation makes the hours you invest in incident response more valuable as you can accomplish more with the same human capital and at the same time mitigate the diminishing return of additional responder engagement.

If you are reading this document it is safe to assume that you are using PagerDuty for Incident resolution and you are also interested in learning about how you can apply automation to further expedite your incident resolution process – this eBook is for you. The first part of this eBook covers how you can take advantage of Automation to reduce Mean Time to Resolution (MTTR). The second part will help you identify your first incident resolution automation candidates. We also cover a few customer examples along with some practical recommendations.

Why does it take your team a long time to close incidents?

There is a knowledge and access gap preventing first line responders from effectively triaging, gathering diagnostics, and remediating incidents. Additionally, production environments at scale are complex, distributed, tightly locked down, and often regulated.

Senior engineers are manually repeating the same diagnostic and remediation steps for too many incidents on a service. Every escalation to senior engineers represents lost focus on innovation time – this averages 25% of their time.

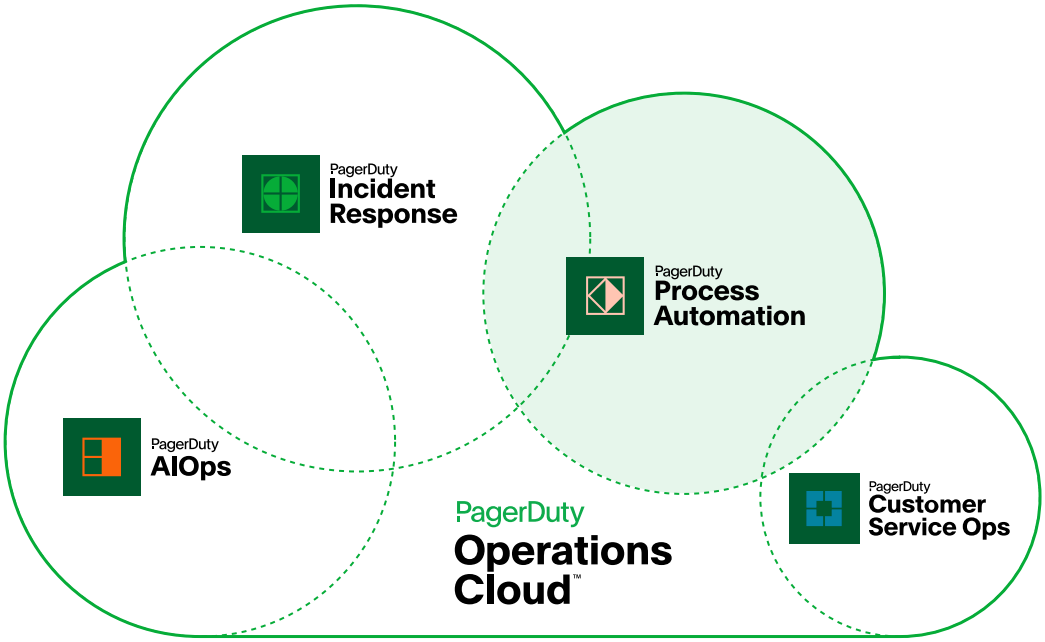
PagerDuty Process Automation empowers responders by harnessing the expertise encapsulated in automation jobs, enabling them to efficiently triage, diagnose, and resolve the majority of incidents independently, without the need for escalation. By leveraging PagerDuty Process Automation, you can effectively translate the knowledge possessed by your most experienced engineers into automation jobs accessible to on-call responders. This powerful tool not only helps reduce MTTR, but also minimizes escalations and support costs, allowing your engineers to maintain their focus on delivering innovative solutions.

Organizations typically adhere to a standardized incident resolution process. The following diagram illustrates this standard process. With this structured approach, organizations can streamline their incident resolution practices and identify areas where automation can significantly enhance efficiency.

Automating Incident Resolution with PagerDuty Operations Cloud

The **PagerDuty Operations Cloud** is the platform that enables our customers to manage the full incident lifecycle. When alerting data comes in, the first task is to help our customers identify the signal in the noise and find the critical issues to address leveraging the AIOps component. Once we find that signal, it becomes the starting point for the Incident Response component of the operations cloud, where we mobilize the right people at the right time to solve the problem.

As we move forward, we strive to augment your team members with **Process Automation** to enhance their abilities to triage, diagnose, and resolve incidents. Organizations use Process Automation in their incident resolution process to take action on urgent incidents, resolve them faster, reduce IT support costs, and eliminate interruptions.

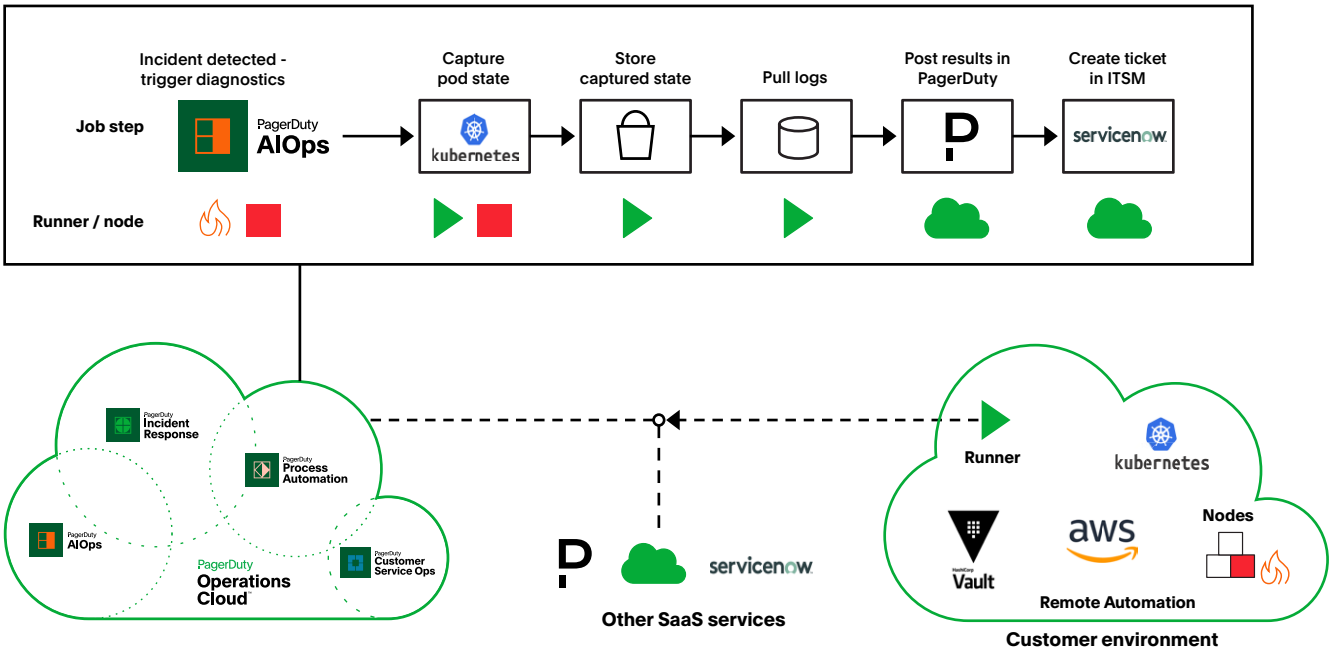


Automated Incident Resolution for PagerDuty Operations Cloud is an end-to-end solution that democratizes expert knowledge and access to enable first responders to triage, diagnose and remediate incidents.

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.

The information returned by these jobs is then presented in PagerDuty in a format that is consumable by first-responders. This allows them to make more informed decisions on the next steps, as well as determine the right individuals to involve for assistance.

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.



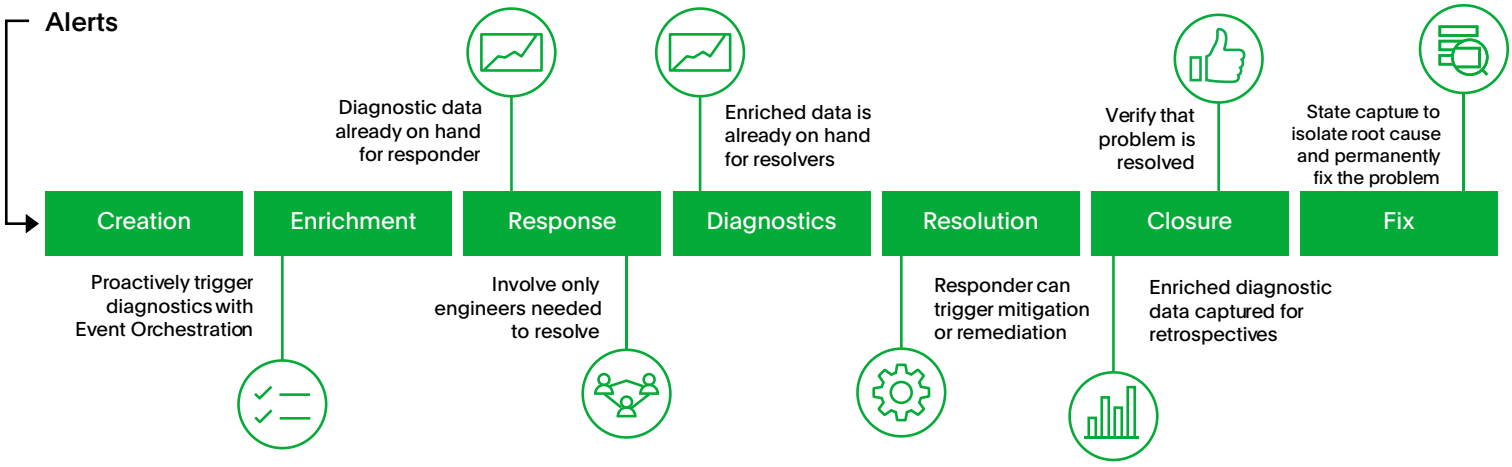
The Automated Incident Resolution solution for PagerDuty Operations Cloud includes:

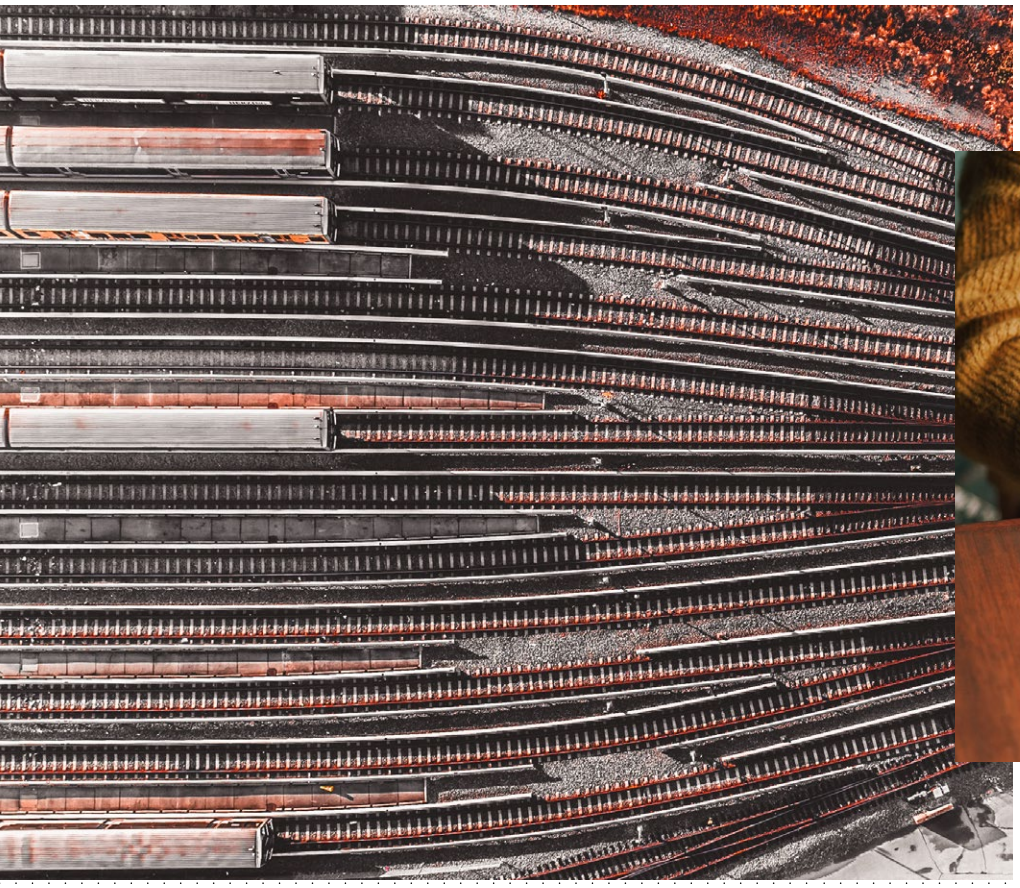
- **PagerDuty Automation Actions** which securely connects PagerDuty end users with remotely executed automation. PagerDuty Automation Actions is a vehicle for invoking jobs that are staged in PagerDuty Process Automation from PagerDuty Incident Response. By associating Automation Actions with a PagerDuty service, responders get push-button access to a library of defined diagnostic and remediation actions, resulting in shorter resolution times and fewer disruptive escalations. PagerDuty Automation Actions can be invoked from any PagerDuty surface: Web UI, Slack, Microsoft Teams, Mobile, Customer Service Ops (CSOps), and PagerDuty AIOps Event Orchestration.
- **PagerDuty Process Automation** is the automation orchestration component of PagerDuty Operations Cloud. It enables automation and orchestration of the most common IT processes, allowing customers to meet SLAs and lower operating costs. It enhances growth and innovation by eliminating old human-ticket concierge services and replacing them with automated systems that bridge departmental and technological islands. PagerDuty Process Automation provides a design-time environment where developers can define jobs that incorporate executing commands, running scripts, and calling APIs for infrastructure, services, and systems owned by customers.
- **Plugin integrations** that expedite secure API integration into automated workflows. It offers integration to common infrastructure and systems where automation is executed.
- **Predefined jobs** providing common diagnostics for OS and infrastructure tools. For example: Amazon Cloudwatch - Surface specific application and VPC logs; Amazon ECS – View stopped ECS task errors; AWS ELB – Debug unavailable target-group instances; Kubernetes - Retrieve logs from pods by selector label; Linux – Retrieve service status; Nginx – Retrieve error logs; Redis – Slow log entries.
- **Implementation & customization quickstart services**

The Process Automation Component is seamlessly connected with the rest of PagerDuty Operations Cloud, so that:

- **PagerDuty AIOps** can trigger diagnostics when incidents are detected
- Responders can invoke runbook remediations with **PagerDuty Incident Response**
- Customer Support engineers can validate customer issues within **PagerDuty CSOps**

The diagram below is the same incident response process we introduced at the beginning of this section but it now highlights the opportunities for automation in the different steps of the incident lifecycle.

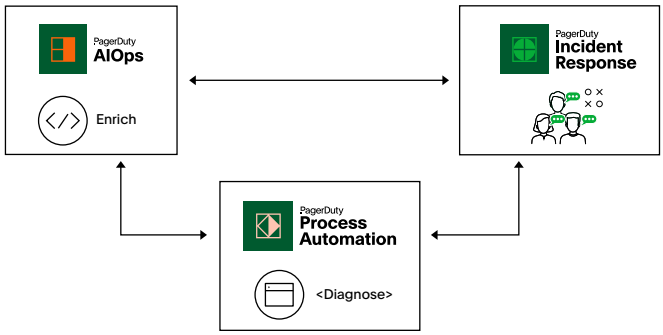




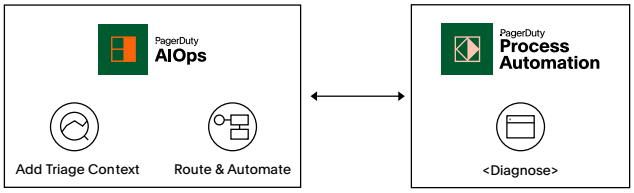
Utilizing Process Automation to build and run these automations, incorporates platform capabilities that meet security and compliance including authentication, access control, audit logging, and encrypted connectivity to mitigate risk and expedite task completion. Automated Incident Resolution provides the means to supercharge your incident response process by creating and connecting different automations as shown in the following table.

Noise Suppression. PagerDuty AIOps reduces alert fatigue and cuts down on system noise. PagerDuty AIOps eliminates 87% of unnecessary incidents by grouping together alerts that correspond to the same issue. Additionally, with Auto-Pause Incident Notifications, transient alerts are also suppressed to eliminate distractions. This helps responders focus on what's important and surfaces the signal from the noise.

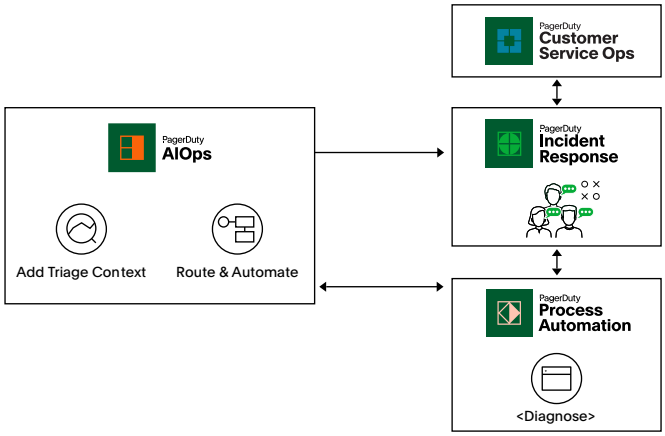
End-to-end event driven automation – Automated Diagnostics can be triggered by **PagerDuty AIOps** either across services via **Global Event Orchestration** or for a single service with Service Event Orchestration. This ensures that a diagnostic script is already run by the time the right responders are called. And, teams can even leverage these capabilities to create auto-remediation so incidents are resolved without any responder intervention.



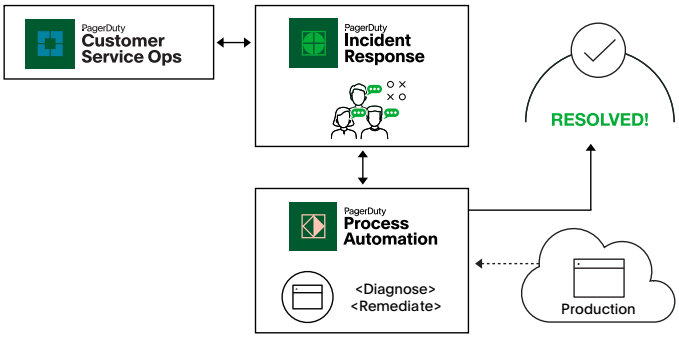
Accelerated triage – PagerDuty AIOps helps teams triage efficiently to drive the right actions towards resolution using both historical event data, human incident response data, and Machine Learning to consolidate the data into actionable information. This provides the Automated Classification and Prioritization information which **triggers the right response and autorouting** – which means the right specialists are called, and the diagnostic information is already available to them.



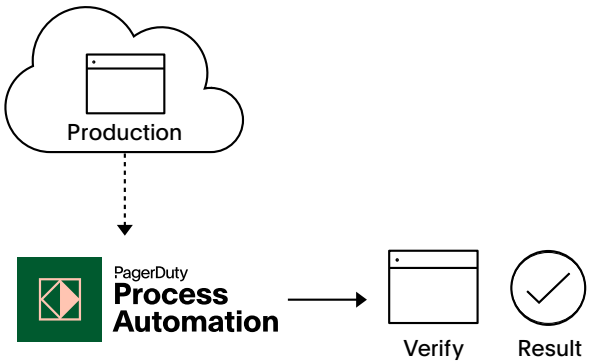
Automation-Assisted Triage – When human intervention is required in the **PagerDuty Incident Response** process, first line responders also have the ability to start **Automated Diagnostics** (if not already initiated by PagerDuty AIOps) via Automation Actions. With the diagnostics results, responders only involve the correct specialist who can solve the problem faster by not having to wait for the diagnosis. **PagerDuty CSOps** users are also empowered to validate customer impacting issues, initiating diagnostics directly from Zendesk and Salesforce Service Cloud.



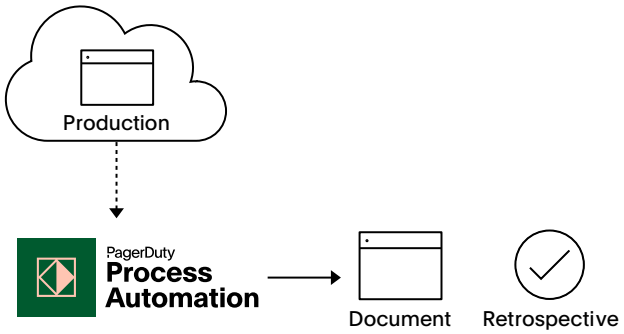
Automated Remediation. Automation Actions also allow first line responders to run **automated remediation** directly from **PagerDuty Incident Response** or **CSOps**. PagerDuty Automation Actions and Process Automation provide all the necessary features and functionality to allow you to implement automation for safe, known fixes as part of your incident resolution process. Here are a few common categories of auto-remediation: Restarting a service running on a Windows or Linux operating system; Rebooting a virtual-machine; Redeploying a Kubernetes pod; Adding infrastructure resources – such as CPU cores or expanding disk-drive space; Performing a "fail-over," or rerouting traffic from unhealthy endpoints to healthy endpoints; Executing a rollback from an unhealthy deployment to the last known healthy deployment; Rotating an unhealthy virtual-machine out of a load-balancer-group.



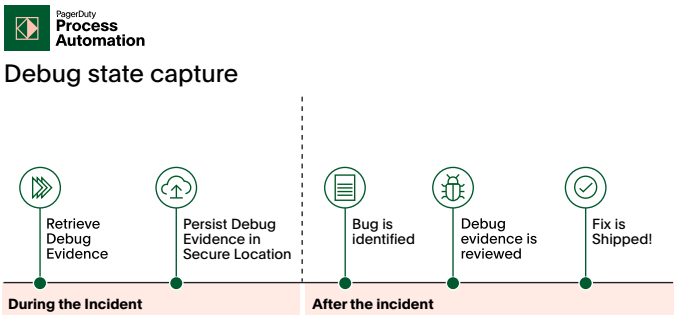
Automated Verification. Allows you to verify that a fix happened and that it worked as intended. In its simplest form, Automated Verification is a special case of Automated Diagnostics. It consists of running (or re-running) a diagnostic script with the expectation of having it come back with no red (or orange) flags. Automated Verification is often a required step in a regulated environment (e.g. financial services and healthcare). It offers a number of benefits: the elimination of human error, immediately available reporting, and documents that the proposed changes were applied with an expected outcome.

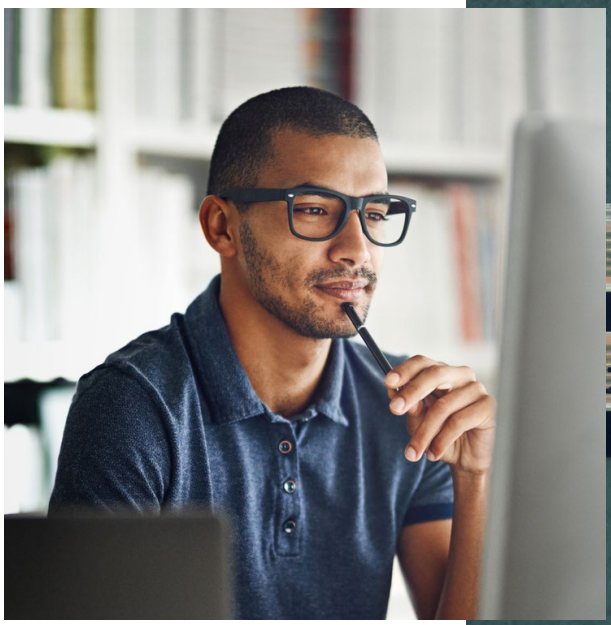


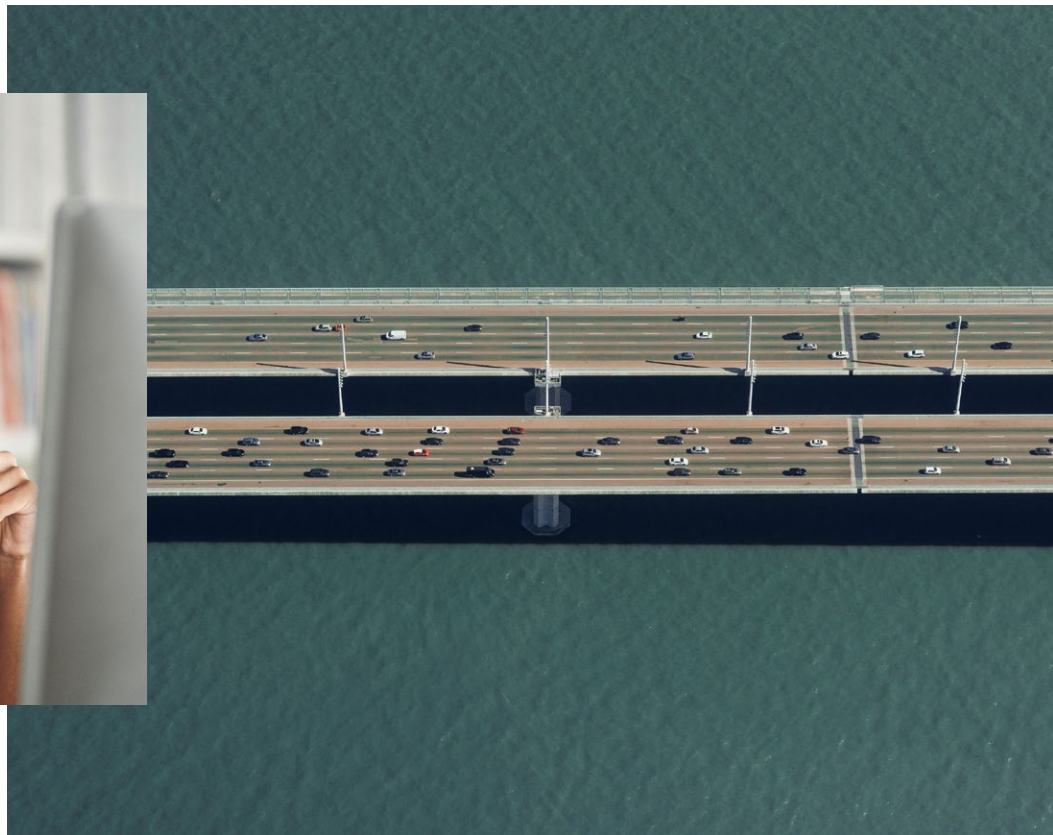
Automated Retrospectives. Retrospectives provide a streamlined learning process so your organization can get better at resolving and preventing incidents. The information returned from the automation jobs becomes part of the incident record and it is available for retrospectives and ticketing systems such as Jira and ServiceNow. These automated retrospectives save a significant amount of manual labor which allows you to invest more time in understanding the root cause and determining the most important follow-up actions.



Debug State Capture. There are several instances where implementing a "quick fix" such as a service restart will erase vital evidence (logs, environment variables, and so on) that would help engineers replicate the issue or provide the root cause of the problem. In order to accommodate these two opposing forces, a solution is needed that can take action at "instant speed" such that evidence is captured and persisted—while also immediately restoring service thereafter. PagerDuty's Operations Cloud harnesses runbooks that are instantly triggered when an issue is detected, debug-level evidence can be captured and sent to a persistent storage service – such as AWS S3 – and services can be restored using known fixes.







Supercharge your Incident Resolution Process with Automation

The preceding pages provide insights into applying Process Automation for faster incident resolution. This section will help you identify the low hanging fruit, ripe for automation in your incident resolution process. It provides best practices, along with important considerations relevant for secure and regulated environments. The final section offers guidance on initiating your journey towards automating your incident resolution process.

Where should you start?

When determining the priority for applying automation to incidents, your team should consider the following factors:

- **Frequency of the problem:** Focus on addressing the most frequently occurring problems to achieve the maximum impact. Additionally, give consideration to **frequently escalated** issues within this category.
- **Maturity of resolution steps:** Assess how well the resolution steps are understood and documented for effectively resolving the incidents.
- **Repetitiveness of resolution steps:** Evaluate how frequently similar diagnostic or remediation steps are performed, not only for recurring incidents but also for any problems related to the same service.
- **Incident length:** Take into account the manual effort required to resolve the issue when the incident occurs. Consider incidents with longer resolution times as potential candidates for automation.

For your initial automation efforts, you can start with alerts specific to a single technology domain, such as disk space warnings, or alerts that already have a manual runbook that can be automated. As you gain confidence and experience with automation, you can gradually expand to tasks with longer execution times and those spanning multiple technologies and areas.

Best practices

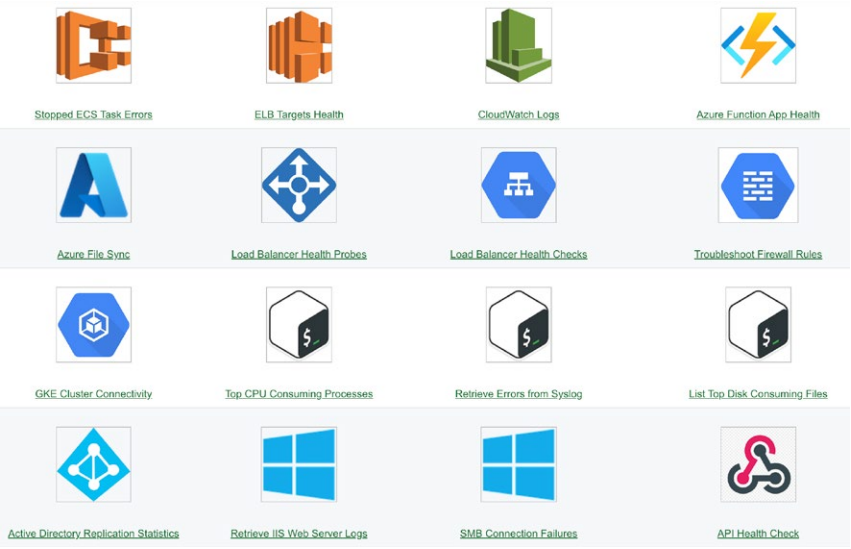
Automation can be applied to many facets of a technical project, from building and testing software, to creating the runtime environments, to responding to error conditions and incidents. Various stages of the Incident Response lifecycle include tasks that are candidates for automation, as well as tasks that are done repeatedly that require little or no input from humans and have consistent end states. Creating and maintaining automation, whether in the form of scripts or libraries or other components, comes with a cost, so you want to find the tasks that will have the most impact on team resources when performed by automation. In general your automation practice should follow these **design principles**:

1. Align with existing workflows: Automation should be developed to support the existing work processes and not create conflicts or disruptions.
2. Deliver meaningful results: The automation workflows should provide outputs that make sense to end users, enabling them to derive immediate value from the automation results.
3. Promote consistency: Standardize code style, input parameters, and catalog presentation to ensure a consistent and simplified experience for users.
4. Document the process: Establish standardized methods and tools for documenting the automation implementation to improve understanding and maintainability.

In addition to these design principles, **implementing guardrails** is essential to build trust and keep stakeholders informed about the operation of automated tasks. Here are some recommended guardrails:

- Send notifications (via email, Slack, Teams, etc.) when starting or stopping an automation job.
- Trigger alerts if any unexpected events occur during automation execution.
- Align credentials with risk levels, ensuring that read-only access is utilized for most tasks.
- Avoid the use of loops (e.g., while, case, goto statements) in automation scripts, gradually adopting more sophisticated techniques.
- Minimize decision making within the automation script, avoiding if/else if, else statements.

Furthermore, to expedite your work, take advantage of the **Examples & Templates** we provide. We have a wide range of pre-built templates and examples available, designed to facilitate your automation efforts. While the provided list offers a small sample, please refer to our documentation for a more extensive collection of resources.

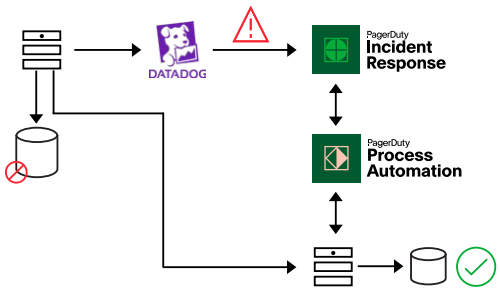


> "Building an automation practice is not easy but when you build it with care and deliberate focus on building value within the constraints of good practices you will see a significant return on investment."
>
> – **Robert Powers**, IT Automation Manager, Brinks

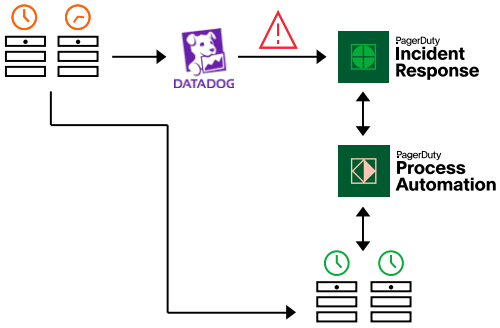
Customer examples

The following table showcases instances where our customers have chosen to automate their incident response. In each of these cases, monitoring tools send an alert to PagerDuty Incident Response, triggering automated diagnostics and remediation.

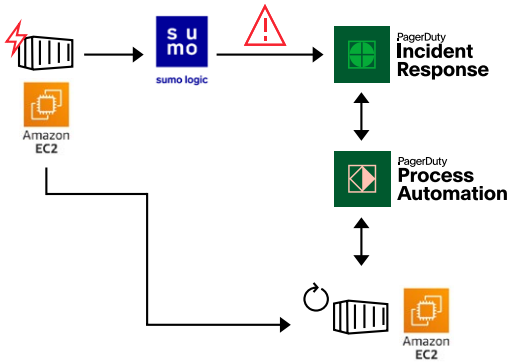
Low Storage Alerts from a monitoring tool. PagerDuty Process Automation frees up disk space.



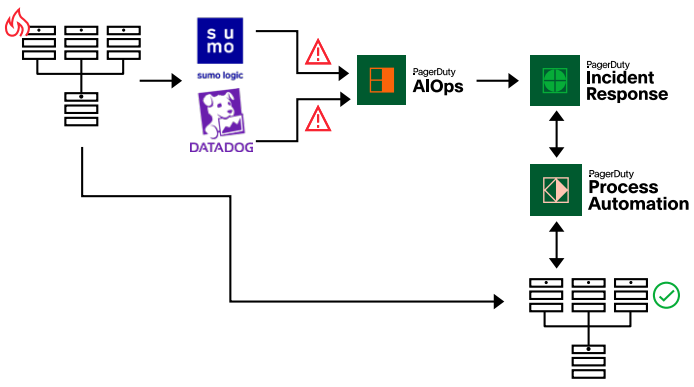
An alert indicates clocks on a server pod are drifting out of sync. PagerDuty Process Automation re-syncs the clocks.



Efficiently restart problematic containers in a public cloud environment.



Diagnosing, rebooting, and reattaching problematic nodes in a cluster.



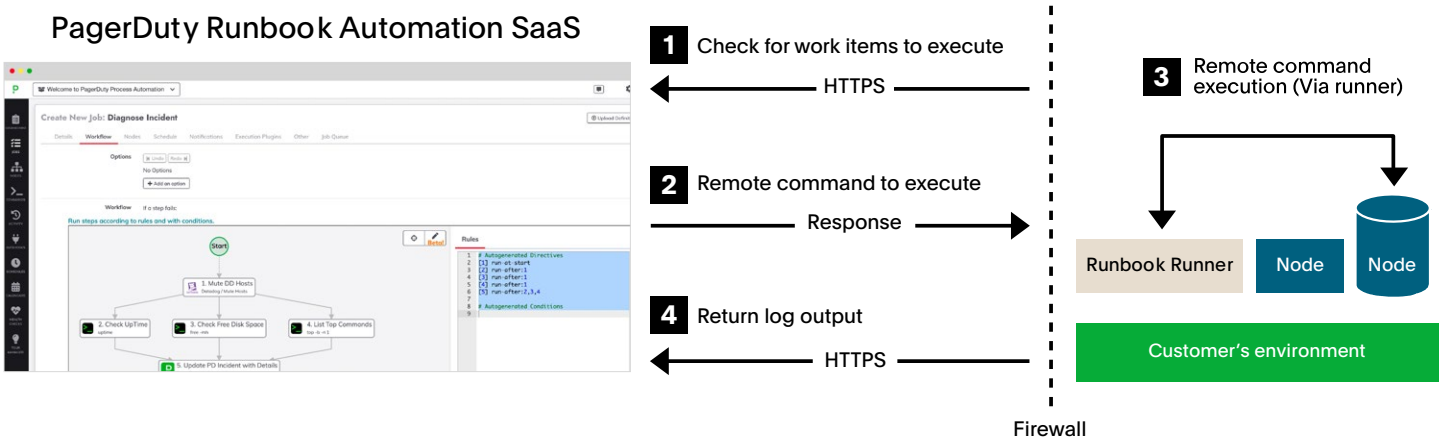
Dealing with complex and secure environments

A common challenge faced by our customers is the efficient management and execution of automation in highly secure and compliant environments. Engineers often find themselves manually handling multiple isolated environments due to the intricate security requirements and process dependencies within each zone. PagerDuty's Runbook Automation addresses these challenges by serving as a conduit for distributed operations, helping you deal with:

Disparate environments. Runbook Automation and Process Automation enables the authorization and orchestration of automation steps in remote environments as if they were local. It enables the incorporation of many environments in the same job definition. This eliminates network silos that typically compromise automation and require manual authentication. Runbook Automation provides zero trust connectivity into remote environments allowing that infrastructure to be incorporated into centrally orchestrated automated jobs.

Logging for auditability. Runbook Automation and Process Automation simplify compliance by embedding access control and logging into the automation process. These capabilities extend into remote environments—all from a centralized control plane.

The diagram below illustrates that communication between the Runner and Automation Server occurs over HTTPS and is initiated from the Runner's end. This approach enhances firewall security by eliminating the need to open sensitive ports on the Automation Server for communication with the Runners. (e.g. SSH/22)



By leveraging PagerDuty's Runbook Automation, our customers can overcome the challenges associated with managing automation in secure and compliant environments, streamlining operations and ensuring auditability while maintaining the highest standards of security.

> "For cybersecurity, runbooks significantly reduce the risk of misconfiguration of existing controls, and subsequently reduce the risk of new vulnerabilities based on human mistakes or completely unintentional actions."
>
> – **Rusty Boguslavsky**, ChangeHealth

Ready to start automating your incident response process?

Deploying automation reduces toil and frees up space for innovation instead of being occupied by unplanned work. Applying automation to incident response improves overall consistency, predictability, and reliability.

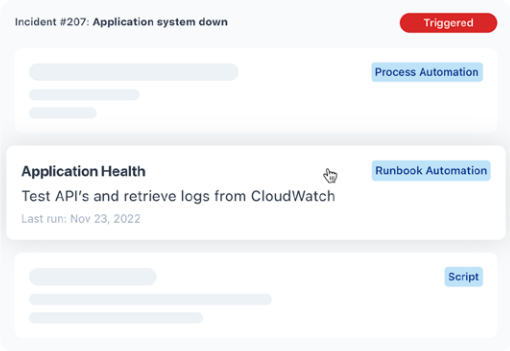
If your team hasn't started automating the incident response processes, we hope this eBook has helped you think through the Automation opportunities and rewards. The crucial next step is to implement automation. Existing PagerDuty Incident Response customers can sign up for a trial of Runbook Automation for Incident Response from the Automation tab using the web UI:

Reduce escalations and accelerate resolution with Automation Actions

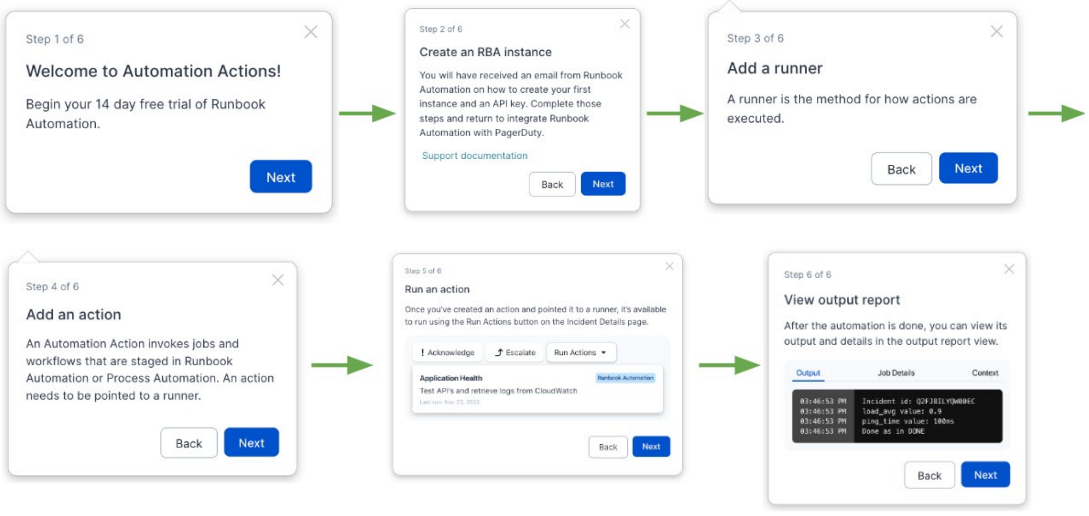
PagerDuty Automation Actions can help your teams:

- Connect PagerDuty to existing automation inside your own production environment(s) through PagerDuty Process Automation
- Reduce escalations by up to 40% and keep your engineers free from interruption
- Shave ~25 minutes off MTTR by automating diagnostic and mitigation actions
- Eliminate toil and increase engineering capacity for high-value work

Contact Sales



Your PagerDuty Account Owner or Administrator will receive an email and they will need to approve the trial. Once approved, users will see a visual guide to help them get started authoring automation, including: Creaing a Runbook Automation (RBA) Instance, Adding a Runner (a program that allows you to execute automation jobs in your environment), Adding Automation Actions (which allows you to invoke automation jobs and workflows from PagerDuty), Running Actions (from the PagerDuty incident details page), and viewing the output from the automation.



If you are new to PagerDuty, please sign up for a trial **here.** We look forward to hearing about your automation success stories.

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, Genentech, Electronic Arts, Cox Automotive, Shopify, Zoom, DoorDash, Lululemon and more.

To learn more and try PagerDuty for free, visit www.pagerduty.com. Follow our blog and connect with us on Twitter, LinkedIn, YouTube and Facebook.

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

PagerDuty