Building closed-loop AIOps

Create a more resilient operation through observability and automation

Red Hat and Splunk deliver trusted AIOps

Red Hat and Splunk have joined forces to bridge the gap between detecting an issue and resolving it by combining industry-leading observability with enterprise-grade automation. By integrating Red Hat® Ansible® Automation Platform with Splunk Observability and Splunk Enterprise Security, organizations can move from a reactive stance to proactive, closed-loop AIOps. Using AIOps these organizations gain AI-driven insights and trusted automation that takes action in response to those insights.

Using this joint solution, a response to an alert is immediate at any hour of the day, helping critical applications and workloads to remain more resilient. This flexible solution lets teams design the automated actions they need, allowing more responsiveness while staying focused on key priorities.

Take trusted automated action on the right alerts

Alert fatigue is a key issue for site reliability engineers and IT operations teams that must identify the correct alerts and determine the appropriate response to them despite an overload of alerts. Splunk includes AI-driven assistance to correlate or summarize multiple alerts—as well as AI agents that assist with detection, troubleshooting, and remediation—so teams can more quickly understand and respond to issues having an effect on the operation.

Once the issue is understood, automation can make the response immediate and consistent, without the typical churn required in manual resolution steps. Ansible Automation Platform offers several flexible connection options including an application, event or AI interface. Ansible Automation Platform stands out due to its flexibility, broad automation capabilities across IT technologies, its choice of automation modes that can be used for a specific need, and its control and governance of the automation being employed. Post-resolution options are available to close the loop back to Splunk once the action is complete. The joint solution takes teams full circle from intelligent insights or alerts to trusted automated actions to a documented resolution.

Deliver smooth, resilient operations

Organizations need fast, resilient IT operations in a digital and increasingly AI-focused world. Businesses are highly dependent on IT, yet complexity, sprawl and security threats remain concerns. AI applications and infrastructure are critical and are being launched quickly. The Red Hat and Splunk solution acts on the correct alerts with speed and consistency, helping teams to keep pace with the demand for resilient operations.

- **Reduce alert fatigue, mean-time-to-resolution (MTTR) and operational overhead.** Automatically resolve known issues, freeing your teams to focus on strategic work instead of repetitive incident response while decreasing MTTR.

- **Accelerate incident response with governed automation.** Trigger immediate, policy-driven remediation the moment Splunk identifies notable events. Ensure consistent, repeatable response across all incidents with approval options, audit trails and role-based access control (RBAC).
- **Shift from reactive to proactive operations.** Use Splunk machine learning (ML) capabilities to identify patterns and trends. Act on predictive insights using Ansible Automation Platform before incidents can affect business operations.
- **Flexibly design automated responses for specific needs.** Teams choose which Splunk alerts trigger an automated response, define the evaluation rules, and specify which actions to take.
- **Jumpstart automation with trusted content.** Use Splunk integration and automation content to create new automation scenarios more quickly, build closed-loop communication, and manage Splunk itself across enterprise IT environments. Additionally, take advantage of more than 200 Red Hat-approved content collections to automate multivendor technology management across complex environments.

Red Hat and Splunk can offer benefits by solving challenges such as immediately closing down a threat while investigation occurs, restarting a failed service so digital business can resume quickly, and more. The joint solution allows teams to proceed at their own pace and design the exact response processes that meet their needs and policies.

Use case: Fast and automatic service ticket enrichment

For specific alerts, design a response to automate service ticket creation and fact gathering. Eliminate toil and churn when it comes to resolving service tickets by automatically gathering key information to use in resolution. For service teams, this reduces waiting for key information to be added to the service ticket before resolution can even begin. For IT administrators, this reduces the need to interrupt current work—for example to gather configuration data and attach it to a service ticket. When the process is automated, issues can be resolved quickly and IT teams can focus on innovation and key priorities, which improves overall satisfaction across the extended team. Red Hat recommends a "start small, think big" approach to automation adoption, and ticket enrichment is a key use case for getting started.

Use case: Automated remediation on any part of your IT landscape

This joint solution connects Splunk alerts to Red Hat actions across networks, on-premise infrastructure, clouds and more. It allows alerts to come from Splunk into Ansible Automation Platform, which then triggers automated actions in response. For example, when Splunk detects a vulnerability affecting servers across the infrastructure, it can automatically trigger an Ansible Automation Platform action to evaluate patch eligibility and execute at-scale remediation. Integrations can also identify existing, trusted automation for a suggested use, create an inventory of affected systems, generate the required automation for evaluation and testing, or supply post-remediation information back to Splunk. When teams can resolve issues immediately and consistently, operations are more resilient.

Use case: Automated predictive maintenance and certificate management

When applications and infrastructure hit thresholds, users will experience latency or even outages. A degradation in 1 area can also have a cascading effect. In addition to user impacts, an influx of alerts can result. Predictive maintenance helps avoid this. Splunk can create alerts for anomalies and near-threshold limits so that Ansible Automation Platform's remediation is proactive—before there is an outage or degradation.

Using AI, Splunk includes capabilities for ML so future decisions are based on trends, past experience, and predictions as to when limits may be reached. Ansible Automation Platform can perform the desired action including human approvals if desired.

Because an expired certificate can cause similar interruptions and outages, the same predictive maintenance model can be applied to identify certificates close to expiration and rotate them. This can help avoid outages and interruptions caused by expired certificates at any hour of the day, improving team workloads and keeping operations smooth.

Use case: Infrastructure drift management

Remediation efforts to correct drift issues often require extensive resources and staff hours. Managing drift is important because it can cause outages and impact the security and compliance posture of the organization. While drift is being managed, IT teams are diverted from key innovations and priorities.

Ansible Automation Platform responds to Splunk alerts with desired actions, including reapplying baselines and source of truth (SoT) configurations, identifying existing remediation playbooks, creating service tickets or notifications, shutting down services affected by severe drift issues, and capturing audit trails of the automated actions. Closed-loop communication of automated actions taken can be communicated back to Splunk. For Red Hat Enterprise Linux® and Microsoft Windows servers, as well as cloud instances, all of this means that systems are more consistent and predictable because they are closely aligned to security and other policies.

Use case: Threat containment

When there is an active security threat in process, time-to-containment is a key metric to limit effects such as loss of sensitive data, ransomware attacks, malware propagation, and unauthorized access to critical systems. When Splunk detects a security anomaly, Ansible Automation Platform can respond across the diverse infrastructure, including execution of full automated workflows and orchestration. For example, resources and users can be disabled, network traffic can be blocked or redirected, backup and restore processes can be initiated, or at-scale scans for specific malware or vulnerabilities can be conducted.

When time-to-containment is important, the Model Context Protocol (MCP) server and generative AI capabilities provided by Ansible Automation Platform can help to create the correct automated response with options for approvals, testing prior to use, fact and forensics gathering, or automated rollback as needed. Audit trails of all actions and closed loop communication with Splunk are also possible.

Splunk and Red Hat: the solution for resilient operations

Splunk and Ansible Automation Platform can help address issues quickly, reducing MTTR and the cost of downtime. One Splunk-sponsored study showed the cost of downtime to be $200M on average per year per company.[1] When every minute matters, the joint solution helps teams respond with speed. Beyond addressing an outage, the solution also delivers predictive capabilities and consistent, accurate actions so teams can avoid downtime from the outset.

If you are ready to put the power of this solution to work for your operation, these resources can help you expand your knowledge and see how to get started:

- Observe and automate your tech stack with Red Hat and Splunk webinar
- AIOps with Splunk and Event-Driven Ansible solution guide
- AIOps: Turning intelligence into trusted automation
- Closing the AIOps gap: Why AI insights need trusted action
- Integration assets: Splunkbase and Red Hat Content Collections

1 "The Hidden Costs of Downtime." Splunk. 1 Oct. 2024.

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

facebook.com/Redhat
x.com/RedHat
linkedin.com/company/red-hat

redhat.com