SOLUTION OVERVIEW

Event Driven Automation and Security with F5 and Red Hat

Respond faster to risks and streamline tasks with automation. F5 and Red Hat power proactive operations and improved compliance with F5 content collections for Red Hat Event-Driven Ansible.

KEY BENEFITS

Accelerate mean time to resolution
Enact instant changes with automation to block security threats or avoid outages around the clock.

Improve compliance
Track configuration changes and software versions through a single source of truth for accurate records and audits.

Reduce risk
Prevent incidents and mitigate risk with playbooks and automated responses that enable proactive security.

Alleviate strain on resources
Automate basic tasks to free up limited IT resources for high-value work.

Ensure consistent policies
Deploy policies consistently across all clouds, networks, or devices to prevent misconfigurations.

Increasing Complexity Highlights the Inefficiency of Manual Processes

As IT environments become more advanced, managing network and security operations requires significant resources. However, with an estimated shortage of 3.4 million cybersecurity workers globally[1] and 73% of CIOs worried about IT talent attrition,[2] more resources simply aren't available.

Many current processes for network and security operations are highly manual. Network operators log into individual network components, change configurations, log out, and repeat across other devices. This manual approach slows down configuration changes and raises the risk of overlooking components during the change process.

For security teams, the expanding array of security solutions results in an increasing number of alerts to investigate, transforming the triage process into a time-consuming endeavor. In addition, the growing volume of security threats can easily overwhelm an understaffed team.

Employ Event-Driven Ansible to Streamline Routine Tasks

Automation can speed the mean time to resolution for outages or security incidents by following pre-defined playbooks triggered by specific events discovered via telemetry. Tasks can include applying new configurations quickly and consistently, managing users, or investigating suspicious activity.

However, network and security teams may not have sufficient experience with automation technologies to build, implement, and maintain the scripts needed to operate them. Pre-built, validated packages that include rules, playbooks, roles, and plug-ins to connect solutions make getting started with automation easier. Teams also need to be able to easily write new rules or configure integrations as needed.

F5 content collections for Red Hat® Event-Driven Ansible are certified by Red Hat to ensure reliable automation of F5 networking, application delivery, and security solutions. Together, they help you manage your network, applications, and security operations efficiently.

Automate F5 Solutions with Red Hat Event-Driven Ansible for Proactive Network and Security Operations

The fully supported REST API integrations in F5's Ansible Collections allow you to manage F5 objects imperatively. With event driven automation, you can use Ansible to generate instant actions from F5® BIG-IP® for network operations, policy enforcement, firewall policies, DDoS protection, and more for proactive protection.

KEY FEATURES

Certified content collections
Ensure reliable automation and support with a convenient package of modules, plugins, playbooks, and documentation built by F5 and certified by Red Hat.

Create an Ansible rulebook
Connect event sources with corresponding actions to provide instructions or embed Ansible Playbooks using familiar YAML-like structures.

Achieve broad security coverage
Take action immediately by triggering F5 Advanced WAF workflows, including behavioral DoS protection, bot defense, and API security, to mitigate threats.

Enable agentless automation
Avoid interoperability issues by transferring instructions over existing transport mechanisms, such as APIs and webhooks.

How it Works

Create pre-approved automation workflows that contain a series of actions to take in response to an event. Then monitor your network or applications with a solution like Elasticsearch and Kibana. When a qualifying event is discovered, it will trigger Ansible automation rules for BIG-IP to execute the approved workflow instantly.

For example, if a malicious user is detected trying to access a secure application, the event monitor will trigger Ansible rules, which will in turn automatically instruct F5® BIG-IP® Advanced WAF® to block the malicious user in real time while still allowing access by legitimate users.

Use Cases

Automation with Red Hat Event-Driven Ansible and BIG-IP is designed for both network and security operations. NetOps uses include:

- Consistent network configurations to standardize and enforce best practices
- Operational state management to determine preventive maintenance needs and reduce outage risks
- Compliance and traceability of configuration changes for accurate audits

SecOps automation use cases include:

- Investigation enrichment by gathering additional information from logs to reduce triage times
- Threat hunting to identify threats faster through data correlation
- Incident response that takes immediate action to update security policies or block access

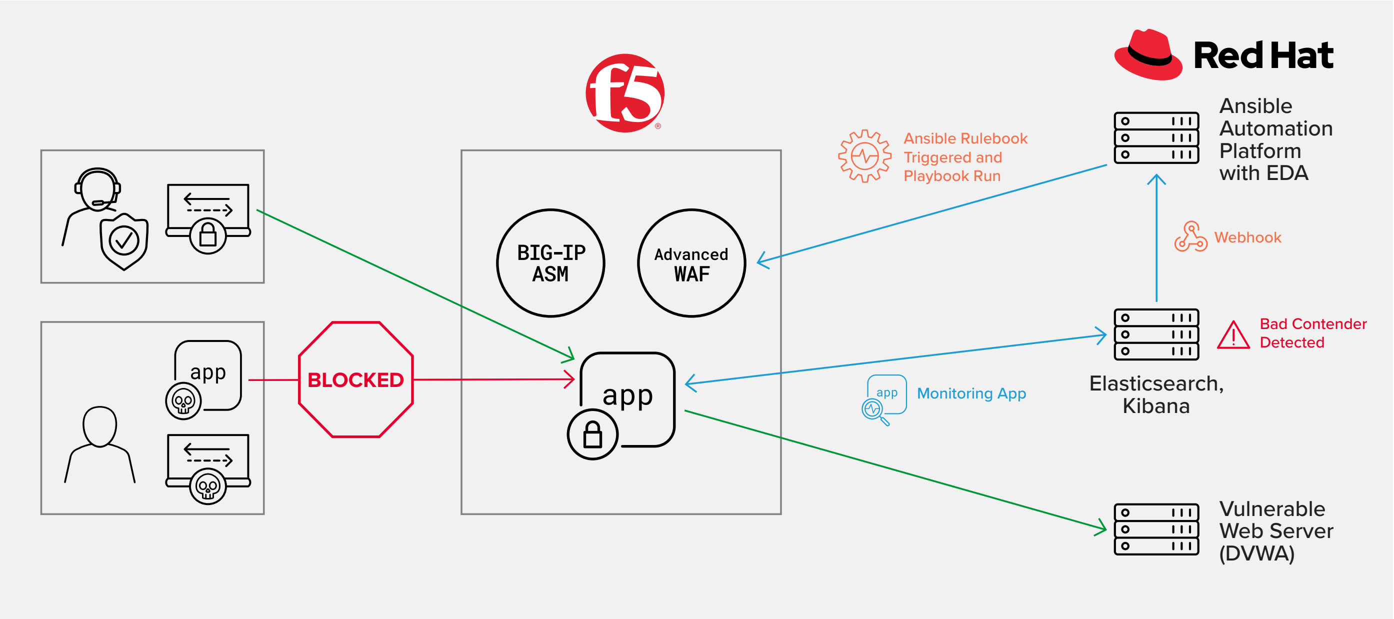

Figure 1: When suspicious activity is detected by Elasticsearch and Kibana, an Ansible Rulebook is triggered to take immediate action using BIG-IP Advanced WAF to block the malicious user.

Benefits of F5 BIG-IP and Red Hat Event-Driven Ansible

Together, F5 and Red Hat can better protect your environment through fast, automated action that improves operational efficiency and compliance while reducing security risk. In turn, this lessens the workload for busy IT teams, allowing them to focus on high-value tasks. As hybrid environments become more complex, the need for reliable automation will only increase to efficiently scale, optimize, and protect your business.

Learn more about F5 and Red Hat's partnership at f5.com/redhat

[1] (ISC)², 2022 Cybersecurity Workforce Study, June 2022.
[2] Gartner, Do Recent Layoffs Mean the Tech Talent Crunch Is Over?, March 2023.