

Speed up ticket handling with automation



Ilkka Tengvall
Solutions Architect
ikke@redhat.com
Matrix: @ikket:hacklab.fi



Tommi Sohlberg
Solutions Architect
suulperi@redhat.com

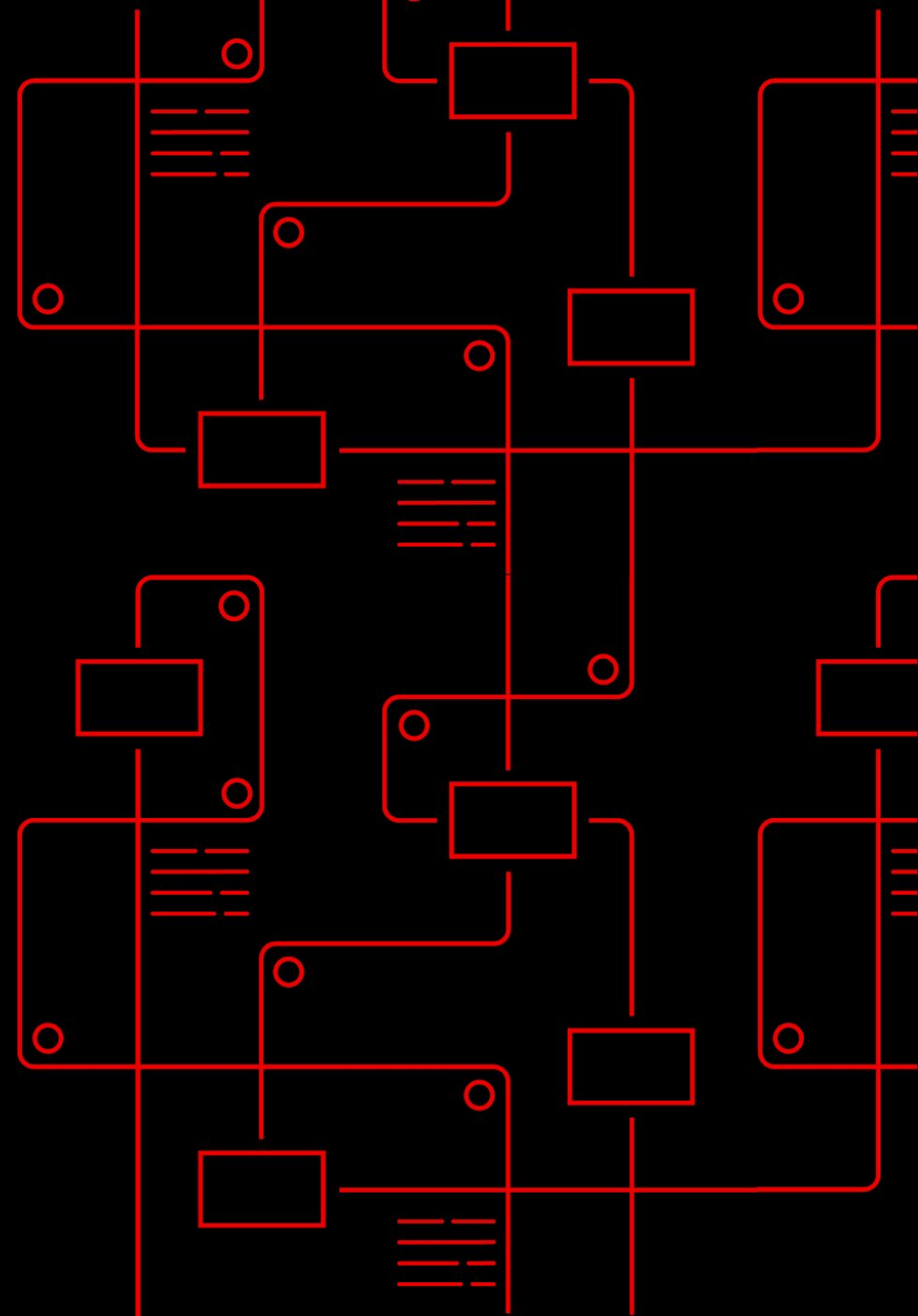
20%
of IT processes will be
“all automated”
in one year

Source: The Impact of Event-Driven Automation on IT Operations,
451 Research, September, 2022.



What is event-driven automation?

The ability to
connect intelligence, analytics and service requests
for an IT solution
to automated actions so that activities
can take place in a single motion.



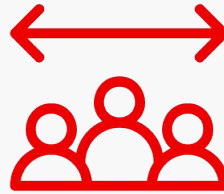
Achieve goals and focus teams with advanced automation techniques



Speed

Reduce the number of manual steps, enable orchestration of multiple tools and accelerate cross-tool interaction

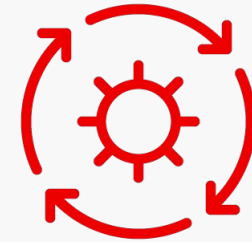
Become more agile



Consistency

Minimize risks with automated workflows, avoid human errors and use auditable and verifiable processes

Ensure resilience



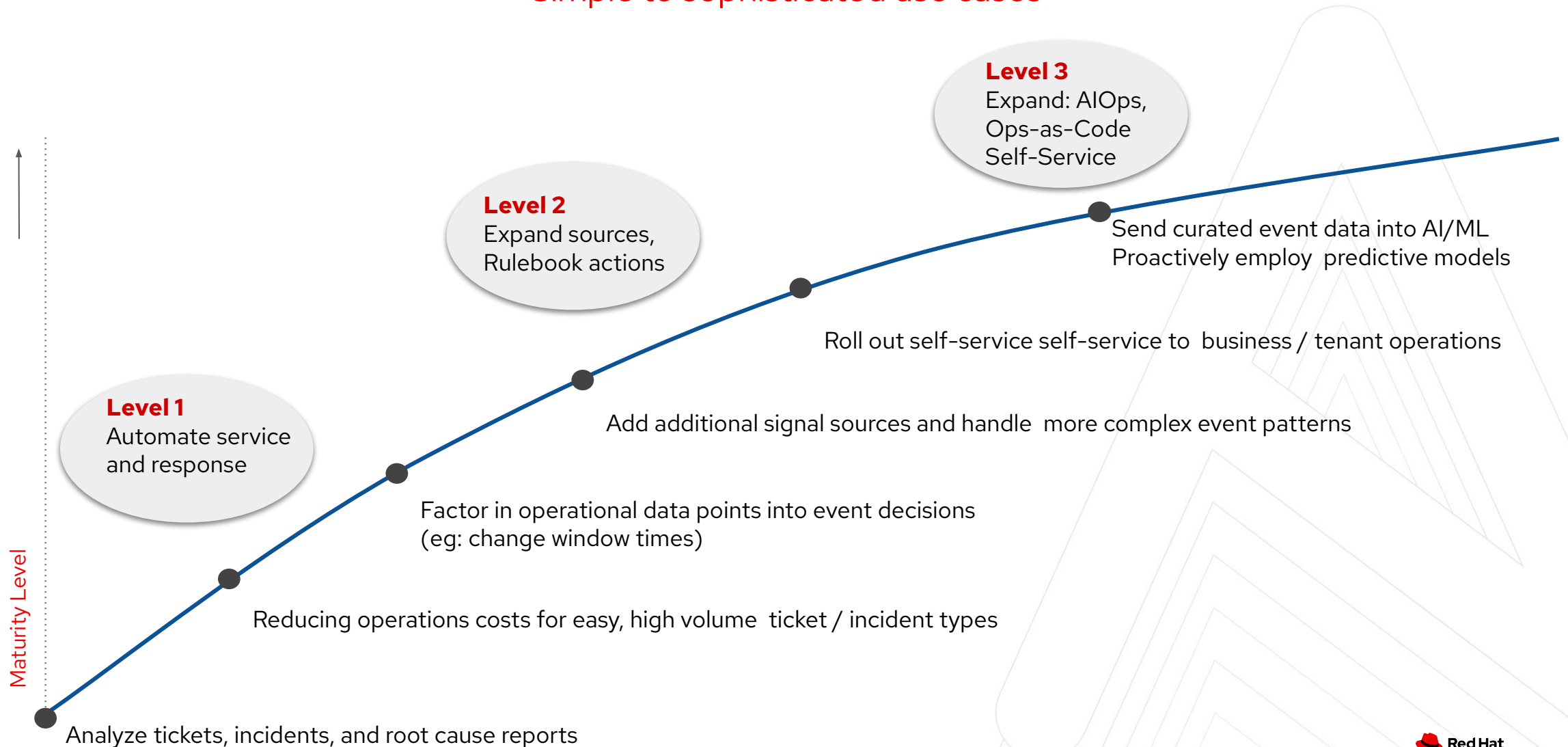
Innovation

Innovate to more advanced levels of automation and free productivity for innovation and higher level projects

Transform IT

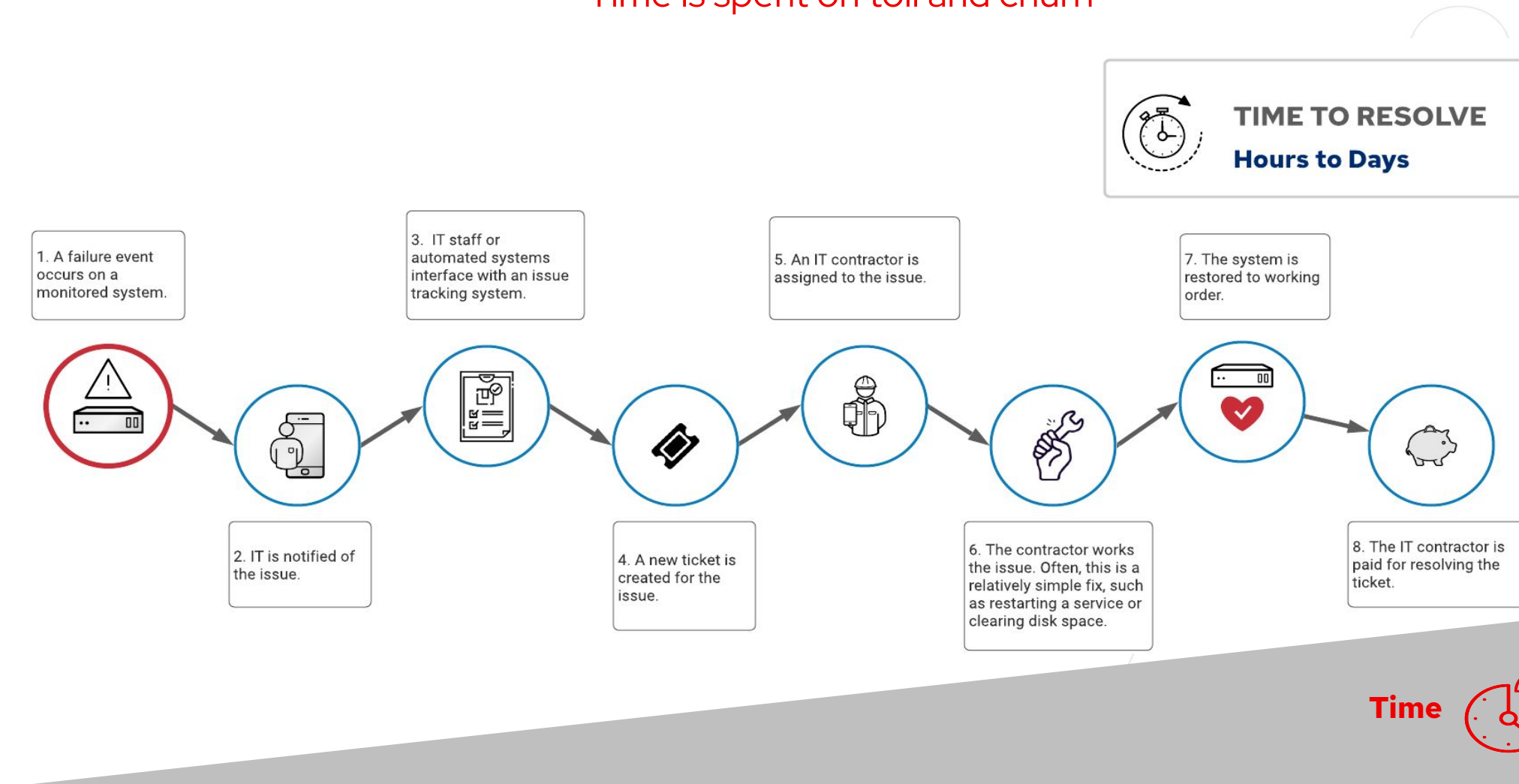
Suggested path to event-driven automation maturity

Simple to sophisticated use cases



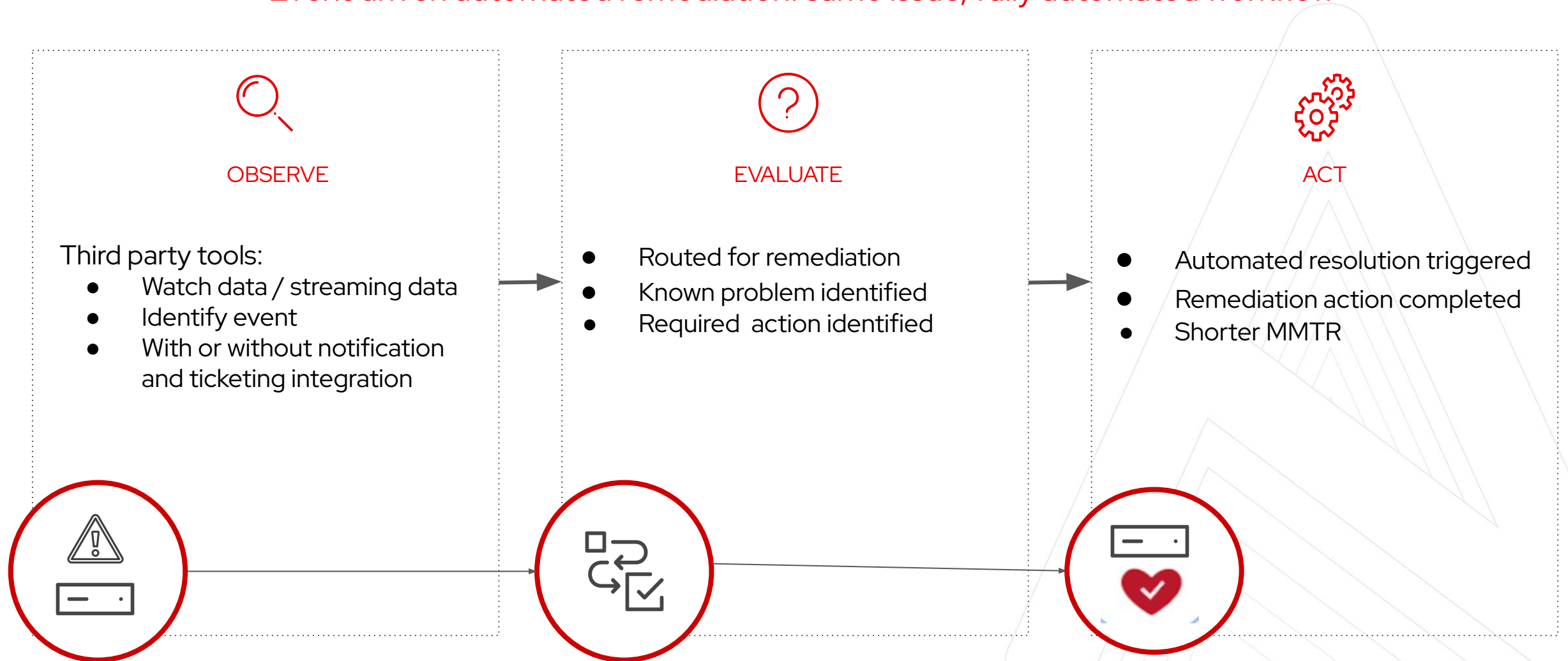
Example manual workflow: remediating issue on managed system

Time is spent on toil and churn



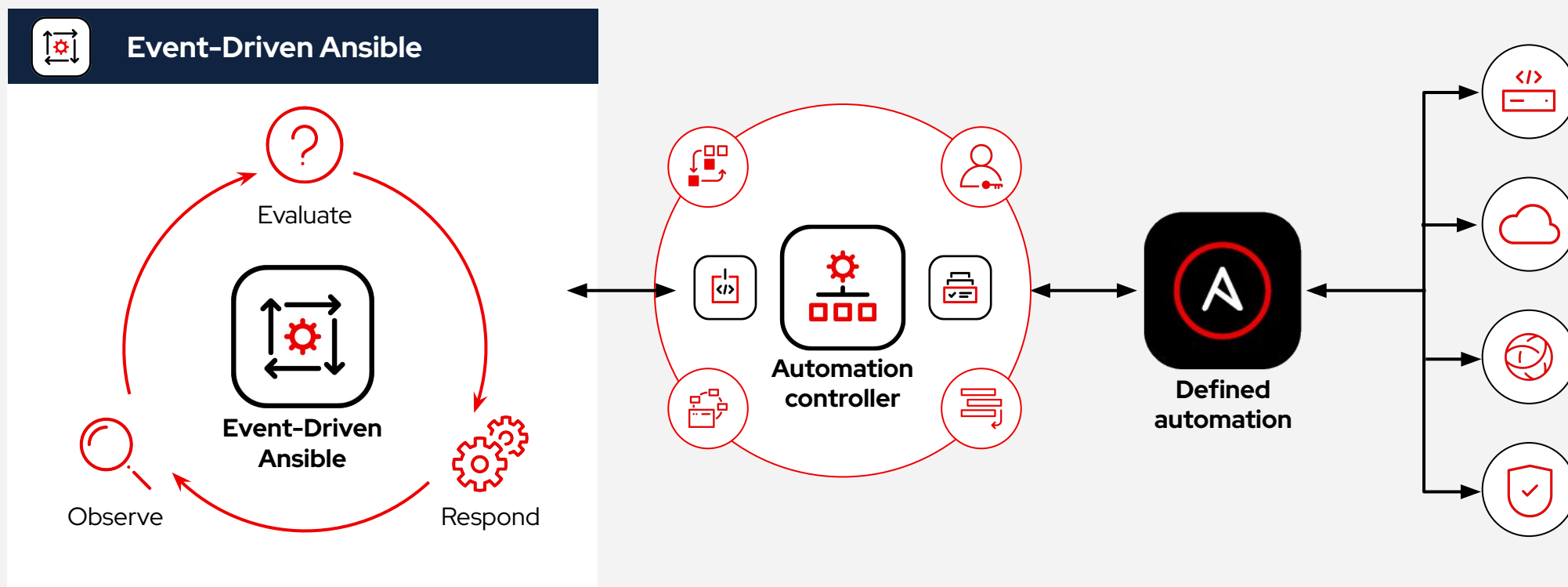
Example event-driven workflow: Speed and shorter MTTR

Event driven automated remediation: same issue, fully automated workflow

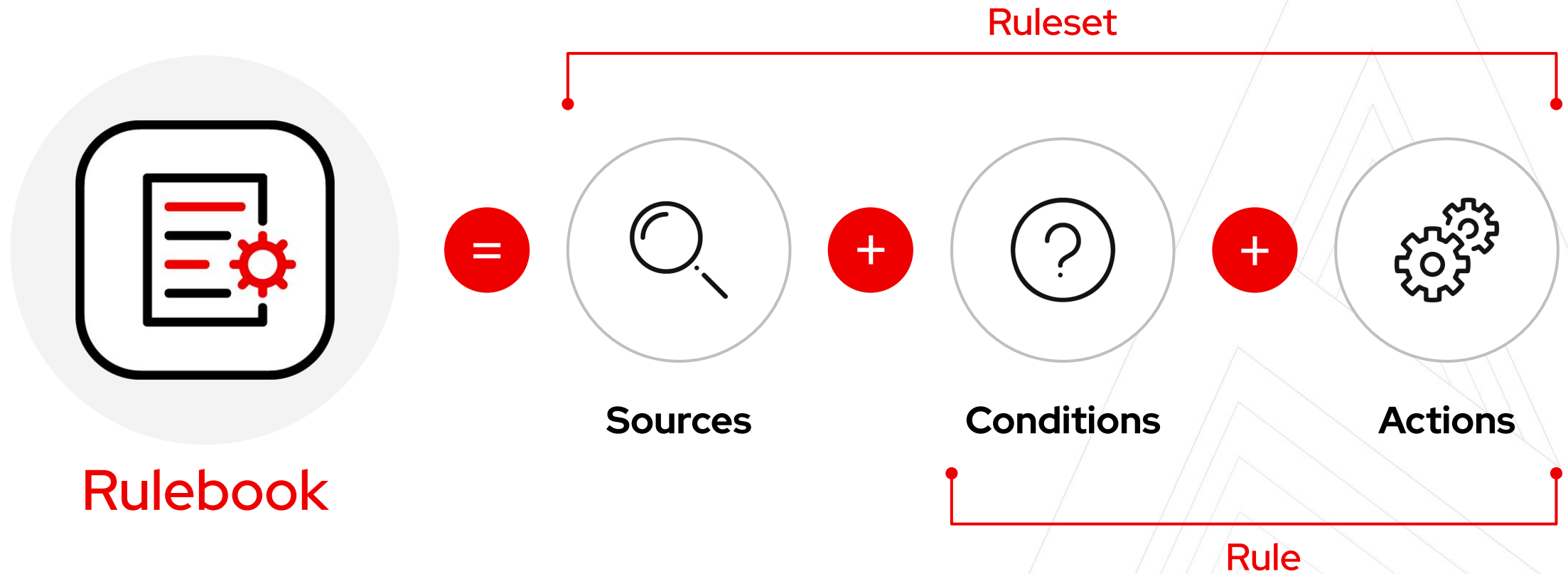


Event-Driven Ansible overview

Event-Driven Ansible. **Observe, evaluate, respond.**



What makes up an Ansible Rulebook?



Ansible Rulebooks

```
---
- name: Capture alertmanager alerts
  hosts: all
  sources:
    - ansible.eda.alertmanager:
        host: 0.0.0.0
        port: 5050
        data_alerts_path: alerts
        data_host_path: labels.instance
        data_path_separator: .
        skip_original_data: true

  rules:
    - name: SELinux was disabled
      condition: event.alert.labels.alertname == "selinux disabled" and
                event.alert.status == "firing"
      action:
        run_job_template:
          name: Apply baseline
          organization: Default
          job_args:
            limit: "{{ event.meta.hosts }}"
```



Event-Driven Ansible rulesets. **Event sources and rules.**

What are they?

- ▶ Top level specification that defines event sources and rules.
- ▶ Defines properties such as Ansible inventory target hosts, gathering facts, and more.

Building blocks for Rulebooks

- ▶ Multiple rulesets can exist within an Ansible Rulebook.

```
---  
- name: Capture alertmanager alerts  
  hosts: all
```

Event-Driven Ansible sources. How are events gathered?



What are they?

- ▶ Event data is gathered from multiple sources using source plugins.
- ▶ One or multiple event source plugins can be configured in a ruleset.

Source plugins

- ▶ Puts events in the queue to be passed to rules engine.

Event filters

- ▶ Enables data transformation and clean-up before being passed to rules engine.

```
---
- name: Capture alertmanager alerts
  hosts: all
  sources:
    - ansible.eda.alertmanager:
        host: 0.0.0.0
        port: 5050
        data_alerts_path: alerts
        filters:
          - ansible.eda.json_filter:
              include_keys: ['alert']
```



Event-Driven Ansible rules. Evaluate and automate.

What are they?

- ▶ Rules determine actions taken on events based on conditions using simple YAML structure.

Conditions

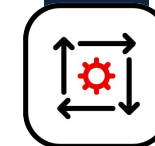
- ▶ Evaluates event data using "If-Then-Else" structure.
- ▶ Single condition or multiple conditions supported.

Actions

- ▶ Triggered once rule conditions are met
- ▶ Processed sequentially once conditions are met.

```
rules:
  - name: SELinux was disabled
    condition: event.alert.labels.alertname == "selinux disabled"
    action:
      run_job_template:
        name: Apply baseline
        organization: Default
        job_args:
          limit: "{{ event.meta.hosts }}"
```

Event-Driven Ansible controller. **Define and manage.**

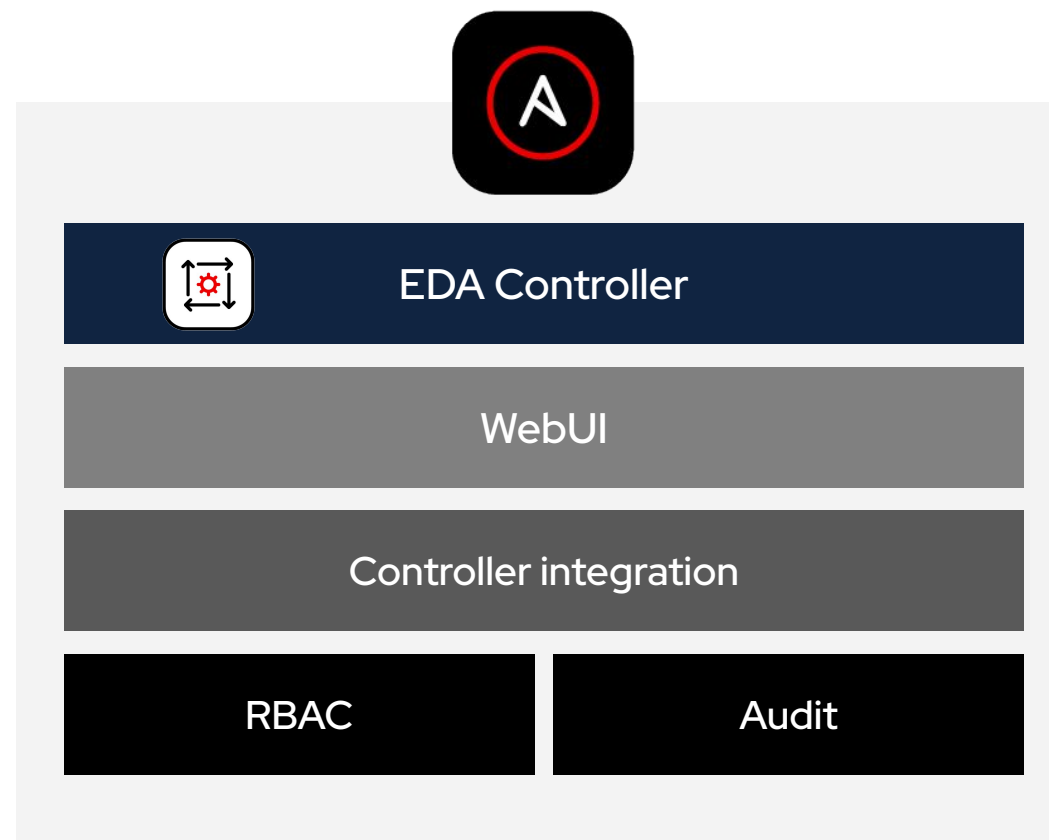


What is it?

- ▶ EDA Controller enables users to centrally manage Event-Driven Ansible across the enterprise.

EDA controller provides:

- ▶ WebUI.
- ▶ Rulebook activation.
- ▶ Role-based access control.
- ▶ Auditing trail.
- ▶ Secure automation controller integration.



Key building blocks in Event Driven Ansible

Flexible and interoperable from source to rule to action to automate IT



Certified Sources

- ▶ Define where events come from, consume events and pass to the rules engine.
- ▶ Source support includes Prometheus, Sensu, Red Hat, as well as webhooks and Kafka.
- ▶ "Custom source" plugin support.



Rules

- ▶ Conditional structure for describing when actions should occur, based on information matching source file data.
- ▶ Ansible Rulebooks



Actions

- ▶ Familiar Ansible actions such as playbooks, and "ad-hoc" tasks
- ▶ "Create Event" function allows system to still act on data not contained in a source file
- ▶ Automate any IT use case

Get started with Event-Driven Ansible

Quick wins: solve these use cases fast, simply and cost-effectively



SERVICE TICKET AUGMENTATION

- ▶ Automate fact gathering
- ▶ Network administration, e.g. Update infrastructure awareness on network events
- ▶ Edge device management, e.g. Compliance & drift are managed post event



REMEDIATION

- ▶ Address drift issues
- ▶ Slow performance issues, e.g. Automate common port troubleshooting and shut/no shut the port
- ▶ Outage issue



USER MANAGEMENT

- ▶ User authentication + access, e.g., providing and troubleshooting access
- ▶ Login issues, e.g., reset password
- ▶ Group/role access, e.g., configuring access to network resources

Event-Driven Ansible is Use Case-Friendly

Apply to any of your IT domains for full automation of key tasks

Networking

- Basic network troubleshooting tasks
- Remediate configuration issues based on port events
- Infrastructure awareness based on routing events

Edge

- Remediate application deployment issues
- Trigger edge app redeployments
- Automate application scaling

Cloud

- Trigger cloud estate check from instance creation events
- Automate remediation tasks from service bus events

Infrastructure

- Escalate Infrastructure issues for improved observability
- Ensure compliance post change events

Security

- Automate log enrichment from a security event.
- Automate security responses from incidents.
- Escalate events for human intervention

Applications

- Allow applications to trigger remediation of issues from patterns
- Enrich healing capabilities of applications and their dependencies.

Event-Driven Ansible

technical overview

Ansible Rulebooks

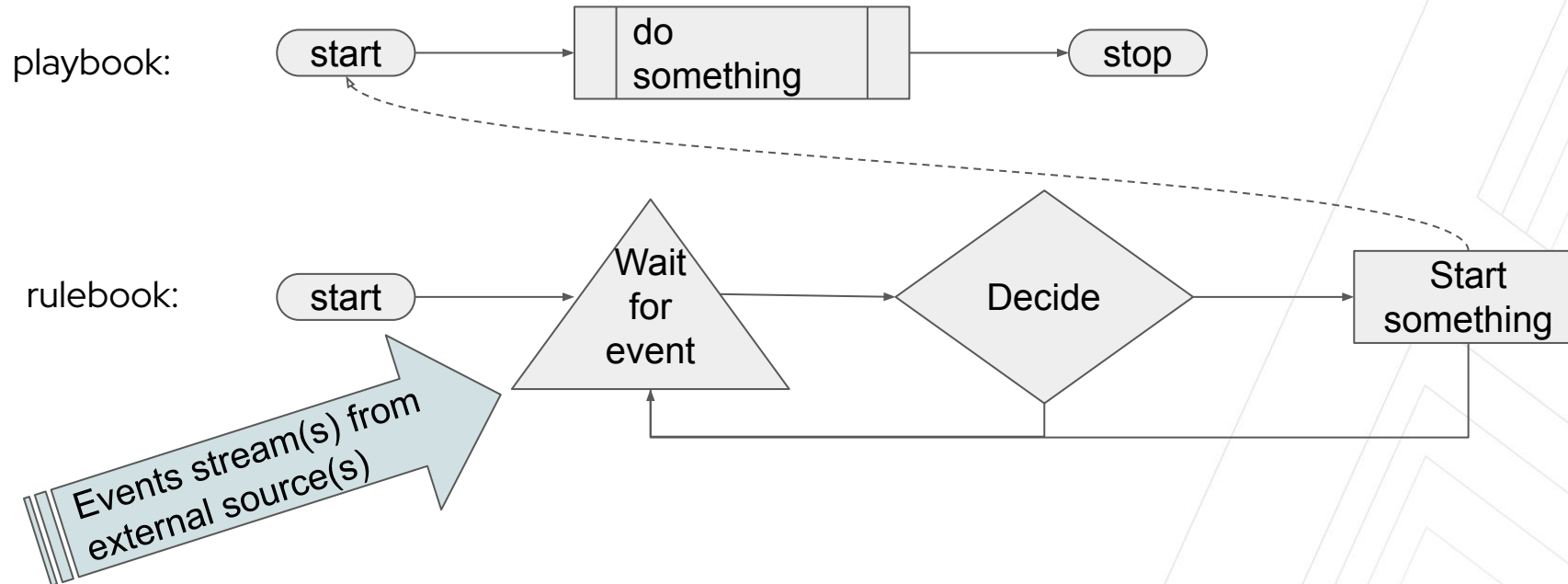
Simple declarative decisions through rules

- ▶ **Events are processed by a rules engine**
 - ▷ Rules trigger based on conditions and actions can be carried out by the rules engine
 - ▷ Rules are organized into Ansible Rulebooks
 - ▷ Ansible rules can apply to events occurring on specific hosts or groups
- ▶ **Conditional management of actions to events**
 - ▷ Simple YAML structure for logical conditions
 - ▷ Events can trigger different types of actions:
 - Run Ansible Playbooks
 - Run Modules
 - Post new events to the event handler
- ▶ **YAML-like format familiarity**
 - ▷ Current Ansible users quickly learn and use Rulebook writing

```
- name: Automatic Remediation of a web server
  hosts: all
  sources:
    - name: listen for alerts
      ansible.eda.alertmanager:
        host: 0.0.0.0
        port: 8000
  rules:
    - name: restart web server
      condition: event.alert.labels.job == "fastapi" and
        event.alert.status == "firing"
      action:
        run_playbook:
          name: ansible.eda.start_app
```

EDA – Playbook vs. Rulebook

Event Driven Ansible



Event-Driven Ansible Integration Technologies

Event source plugins

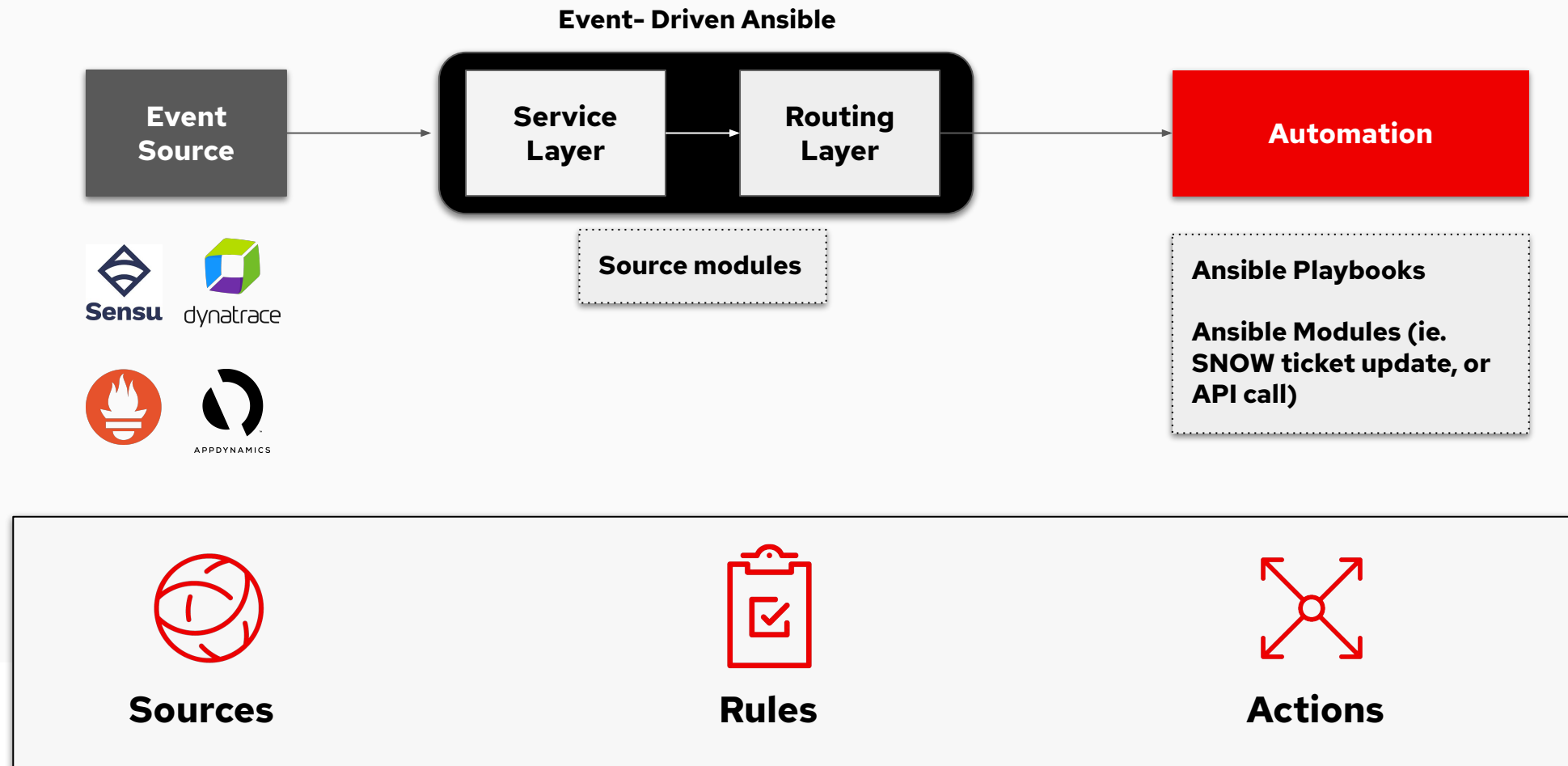
CERTIFIED SOURCE PLUGINS

- Prometheus/Alertmanager
- AppDynamics
- Sensu
- Dynatrace
- Kafka (event streams)
- webhooks
- watchdog (file system watcher)
- url_check (url status check)
- range (event generation plugin_
- file (loading facts from yaml)

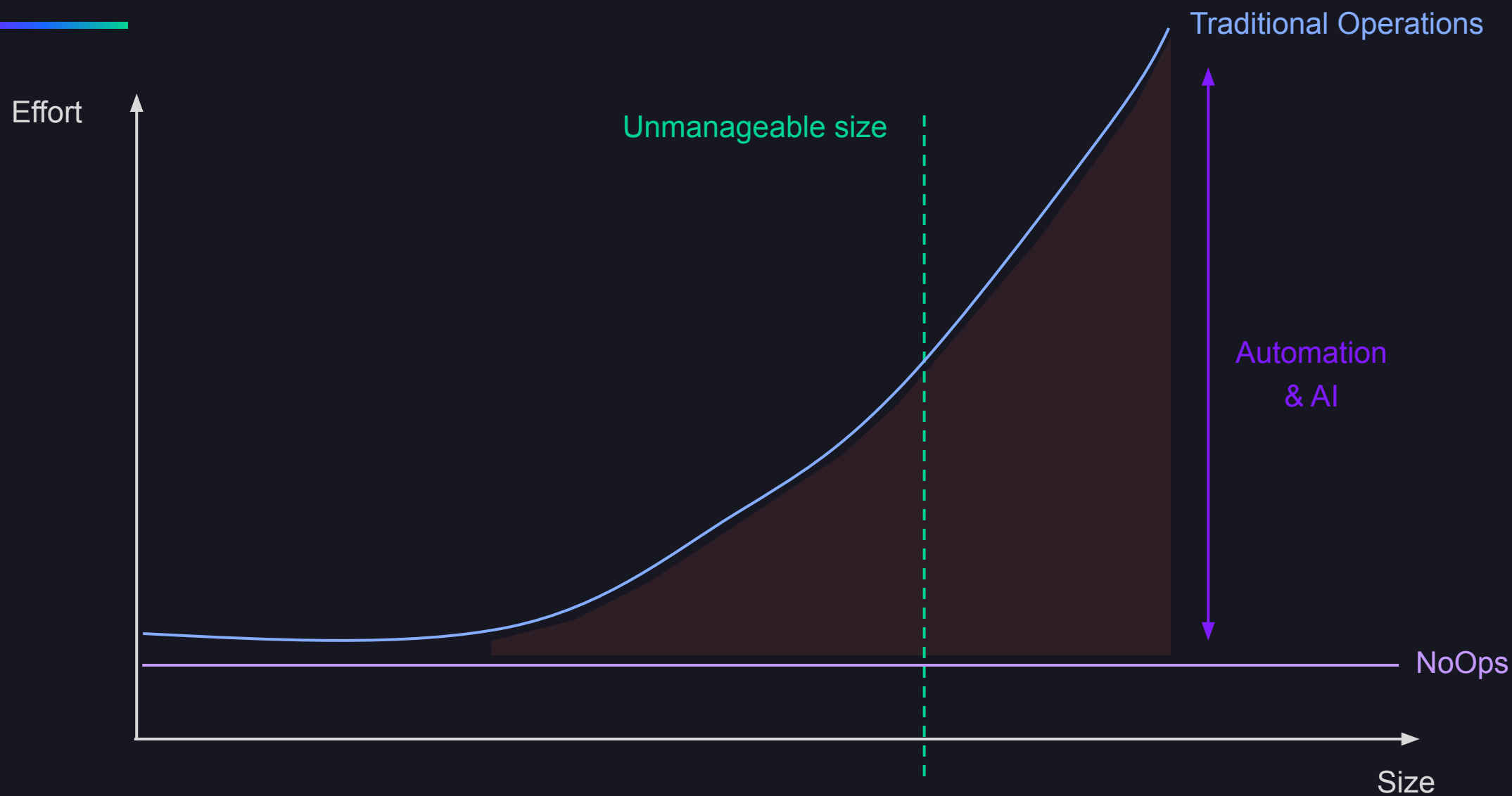
ROADMAP FOR INTEGRATIONS

- Azure Service Bus
- AWS EventBridge

Execution layers of Event Driven Automation



How Many Apps Can You Manage?



Example with Dynatrace

Dynatrace

- Observability
- Event detection
- Enterprise cloud, container & infrastructure monitoring
- Installation and configuration



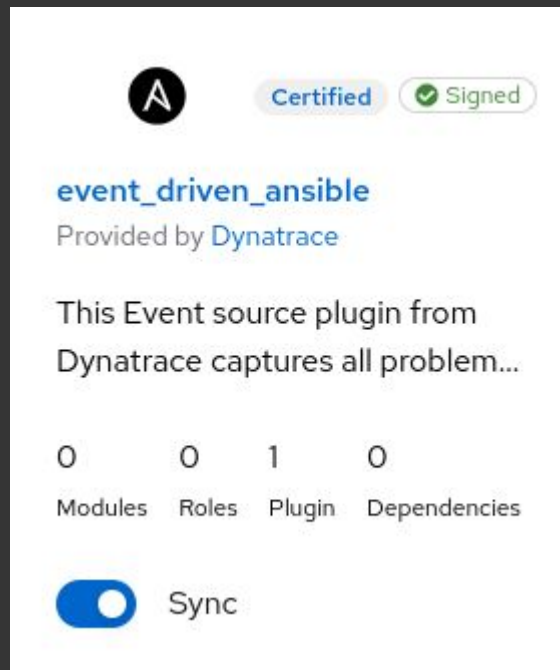
Ansible Automation Platform

- Event-Driven Automation capabilities
- Integrations and Partners
- Certified content collections
- Scalability



Red Hat
Ansible Automation
Platform

Integration

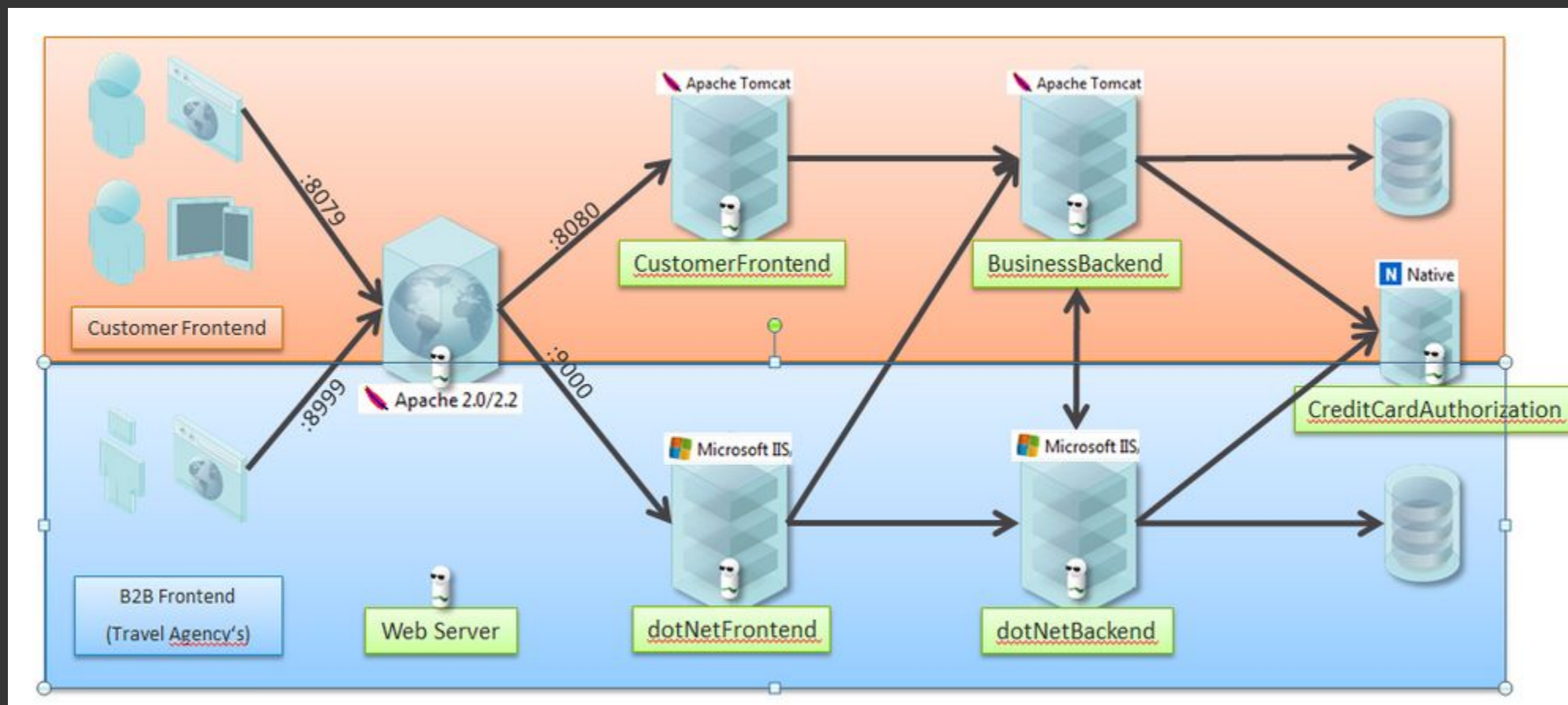


```
---
- name: Waiting for Dynatrace problems
  hosts: all

  sources:
    - name: Dynatrace source
      dynatrace.event_driven_ansible.dt_esapi:
        dt_api_host: {{ dynatrace_instance_host }}
        dt_api_token: {{ dynatrace_eda_token }}
        delay: 60

  rules:
    - name: Remediate Watches-eShop application
      condition: event.title == "Watches-eShop Error" and
event.status == "OPEN"
      action:
        run_job_template:
          name: "[JT] Remediate Watches-eShop application"
          organization: "Default"
```

DEMO



Books > Computers & Technology > Programming



Roll over image to zoom in



Read sample

Strategy Guide for Automation: Scale your business with IT automation (English Edition)

by Magnus Glantz (Author)

5.0 ★★★★★ 3 ratings

[See all formats and editions](#)

Kindle
\$19.95
[Read with our Free App](#)



Paperback
\$29.95
3 Used from \$61.96
3 New from \$29.95

Learn how to develop and implement a sustainable and scalable automation strategy

Key Features

- Get familiar with the essential elements of a successful automation strategy.
- Understand how to incorporate emerging technologies into your automation strategy to improve efficiency and productivity.

[Read more](#)

ISBN-10	ISBN-13	Publication date	Language
 9355515650	 978-9355515650	 August 11, 2023	 English

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat