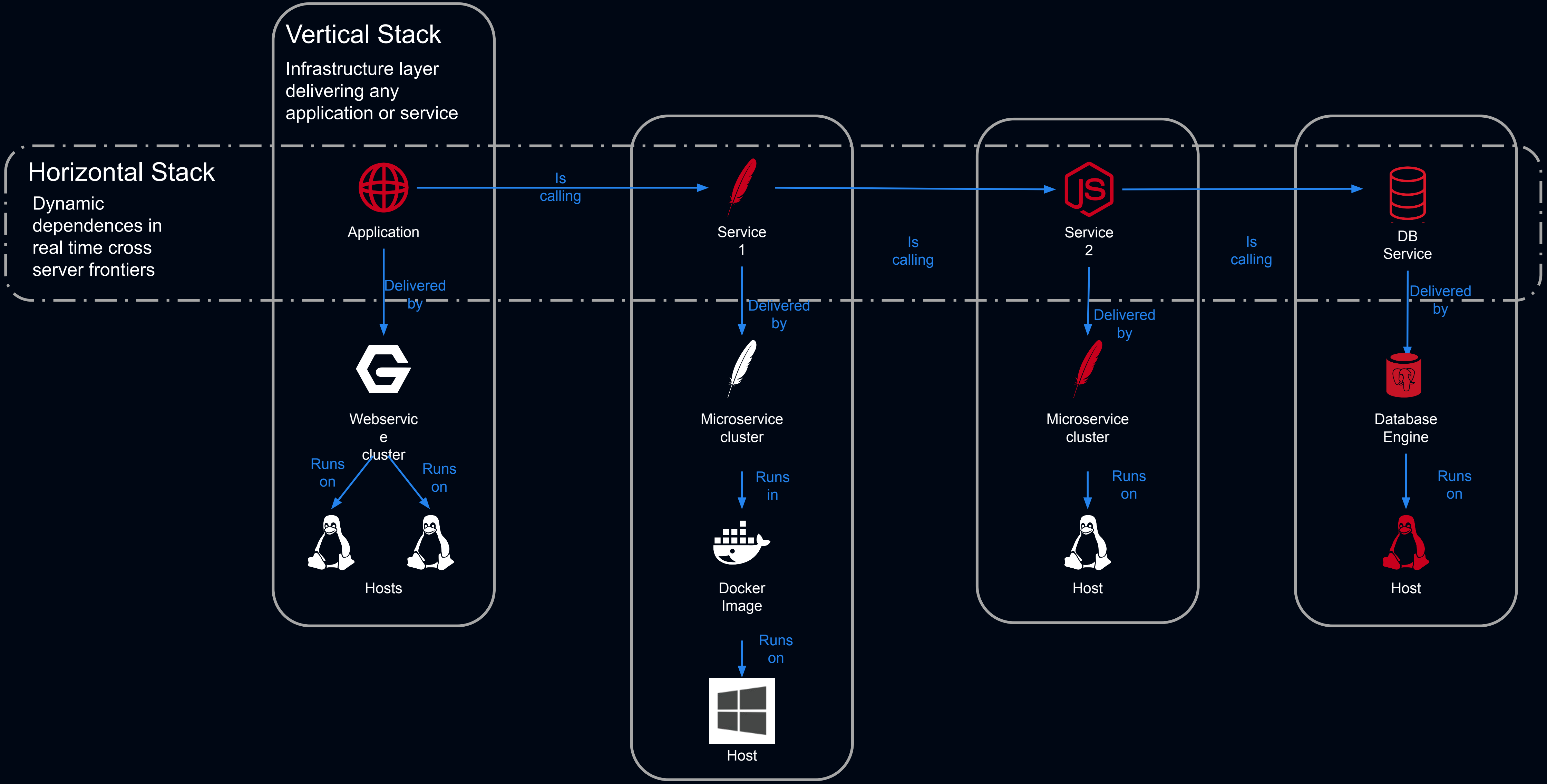
AUTO-REMEDIATION

“Intelligent Operations“ to automate the processes of problem remediation with the Dynatrace AI and Red Hat Ansible

Mert Mantarci
Solutions Engineer, Dynatrace

THE DIAGNOSTICS OF THE UNKNOWNS

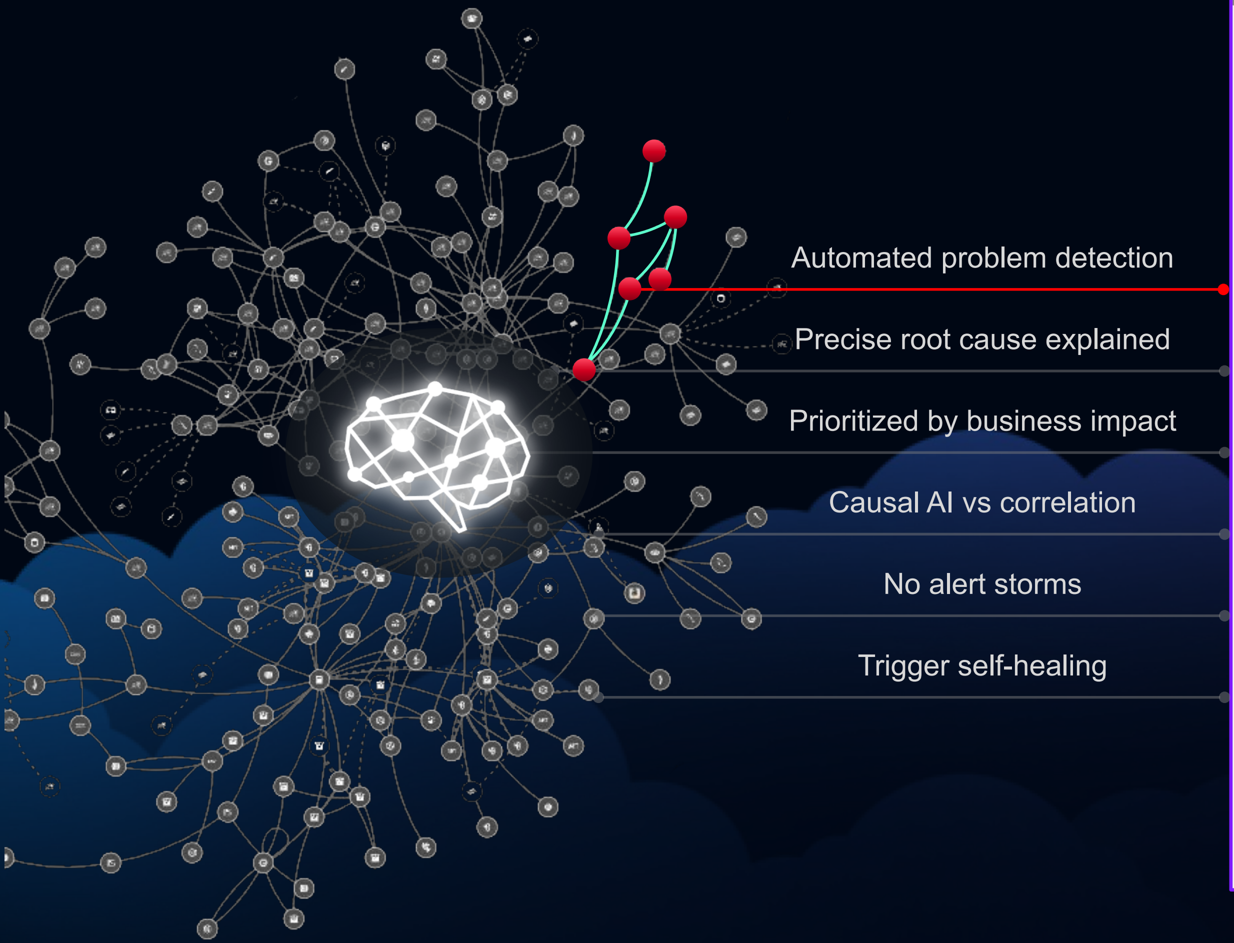


GO BEYOND DASHBOARDS AND GET PROACTIVE ANSWERS

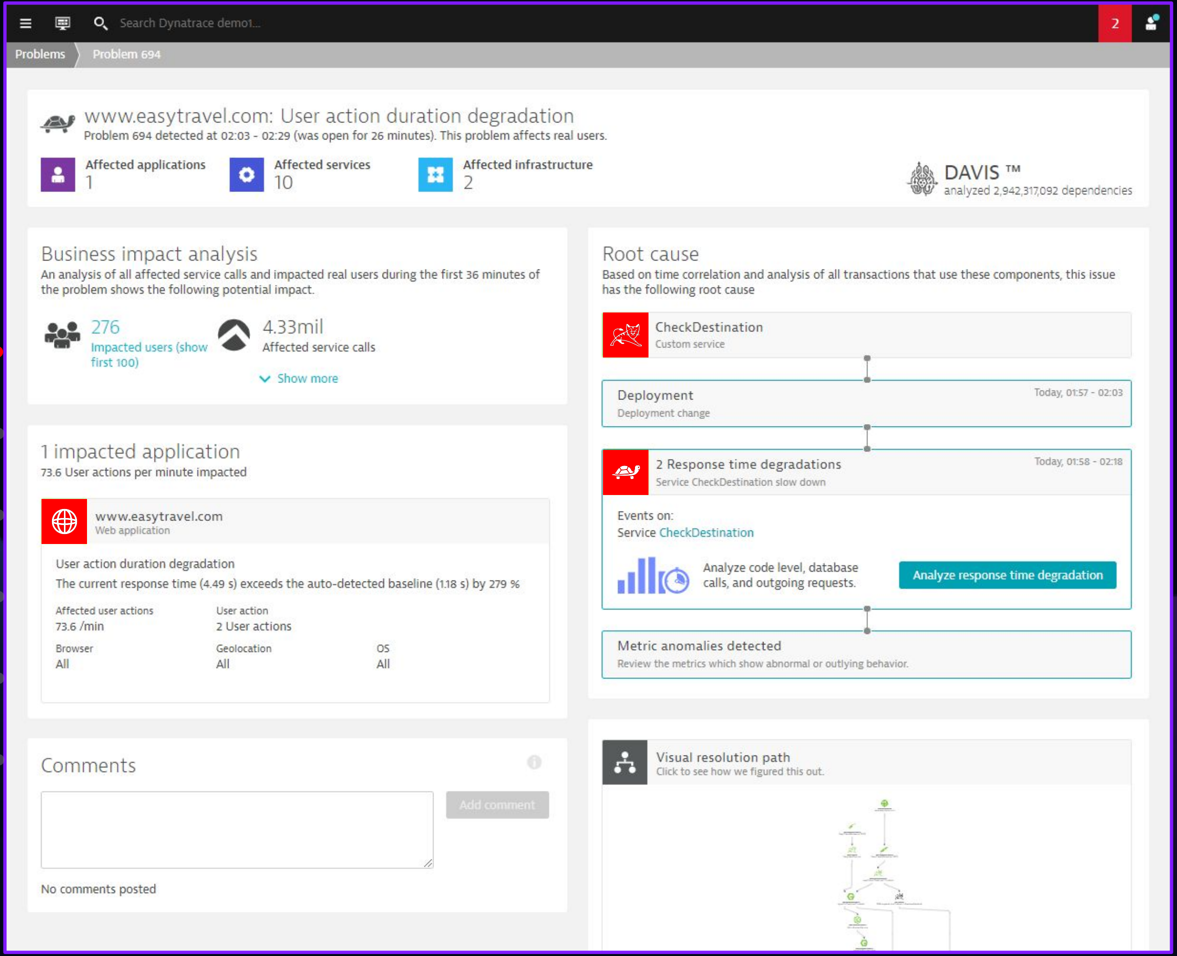
Dynatrace continuously observes, learns and auto-adapts to changes in real-time to detect problems automatically (even the ones you never thought of.)

“Dynatrace’s AI-driven answers are helping the business to remediate problems quicker, meaning we’re able to spend more time innovating and less time solving problems.”

— Anish Patel, Principal Systems Engineer CENGAGE



Automated problem detection
Precise root cause explained
Prioritized by business impact
Causal AI vs correlation
No alert storms
Trigger self-healing



www.easytravel.com: User action duration degradation

Problem 694 detected at 02:03 - 02:29 (was open for 26 minutes). This problem affects real users.

Affected applications 1 | Affected services 10 | Affected infrastructure 2

DAVIS ™ analyzed 2,942,317,092 dependencies

Business impact analysis

An analysis of all affected service calls and impacted real users during the first 36 minutes of the problem shows the following potential impact.

276 Impacted users (show first 100)

4.33mil Affected service calls

Show more

1 impacted application

73.6 User actions per minute impacted

www.easytravel.com
Web application

User action duration degradation

The current response time (4.49 s) exceeds the auto-detected baseline (1.18 s) by 279 %

Affected user actions	User action	
73.6 /min	2 User actions	
Browser	Geolocation	OS
All	All	All

Comments

Add comment

No comments posted

Root cause

Based on time correlation and analysis of all transactions that use these components, this issue has the following root cause

CheckDestination
Custom service

Deployment — Today, 01:57 - 02:03
Deployment change

2 Response time degradations — Today, 01:58 - 02:18
Service CheckDestination slow down

Events on:
Service CheckDestination

Analyze code level, database calls, and outgoing requests.

Analyze response time degradation

Metric anomalies detected
Review the metrics which show abnormal or outlying behavior.

Visual resolution path
Click to see how we figured this out.

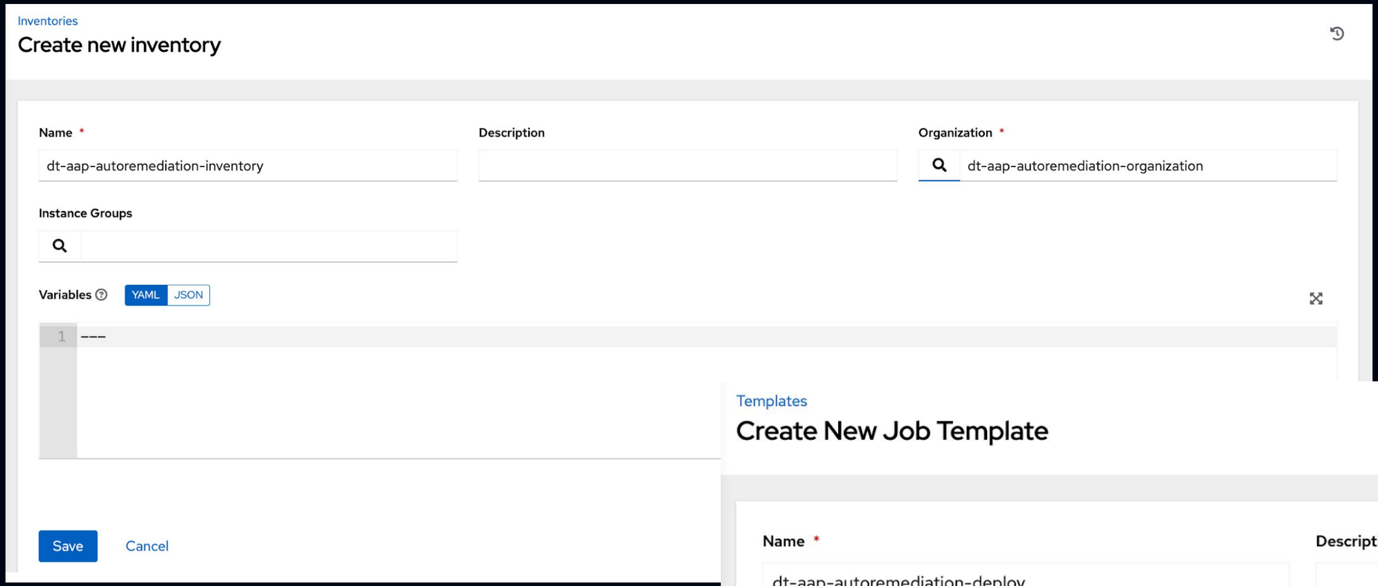
WHAT IS AUTO-REMEDIATION?

Auto-remediation, or **self-healing**, is a workflow that triggers and responds to alerts or events by executing actions that can prevent or fix an issue.

Auto-remediation significantly **reduces MTTR**.

Types:

1. Automated remediation of a **know problem** or **frequent issue (proactive)**
2. Automated rollback of a **problematic change (reactive)**



Inventories

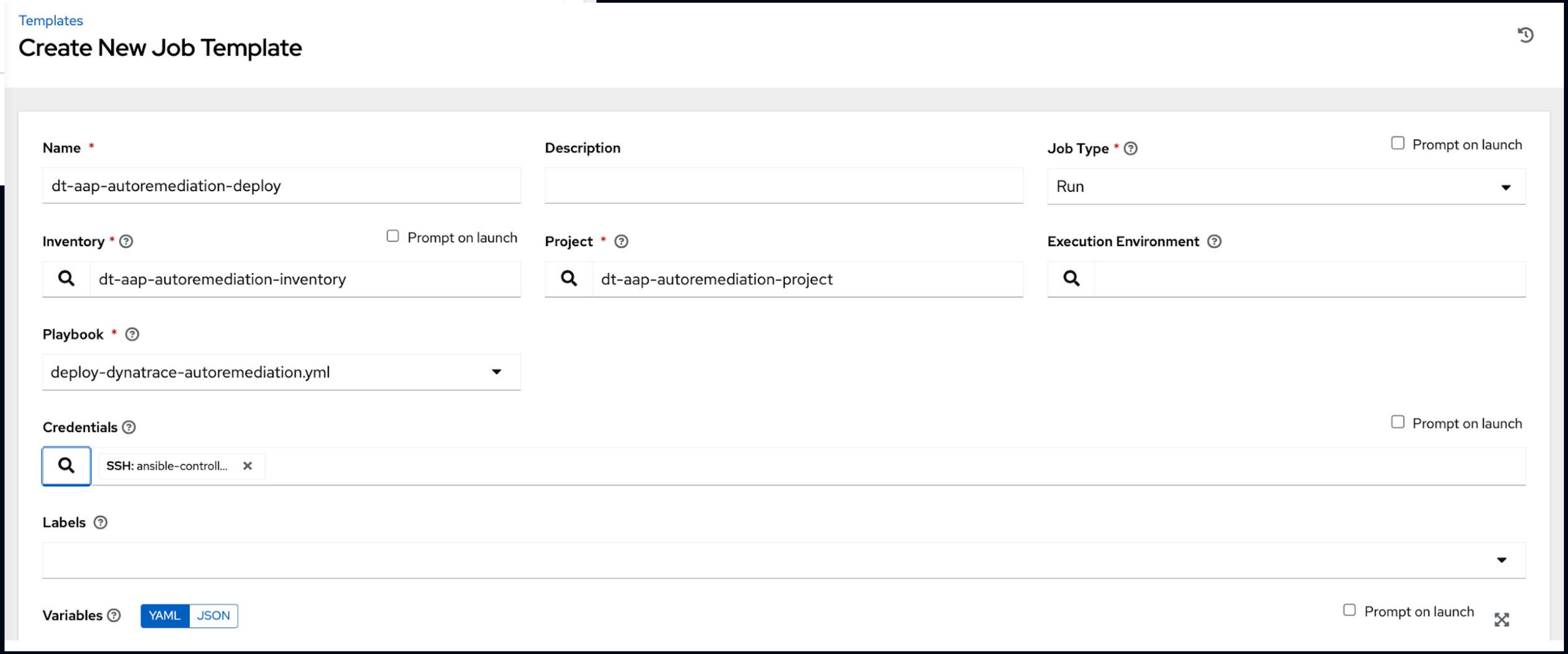
Create new inventory

Name *	Description	Organization *
dt-aap-autoremediation-inventory		dt-aap-autoremediation-organization
Instance Groups		

Variables YAML JSON

```
---
```

Save Cancel



Templates

Create New Job Template

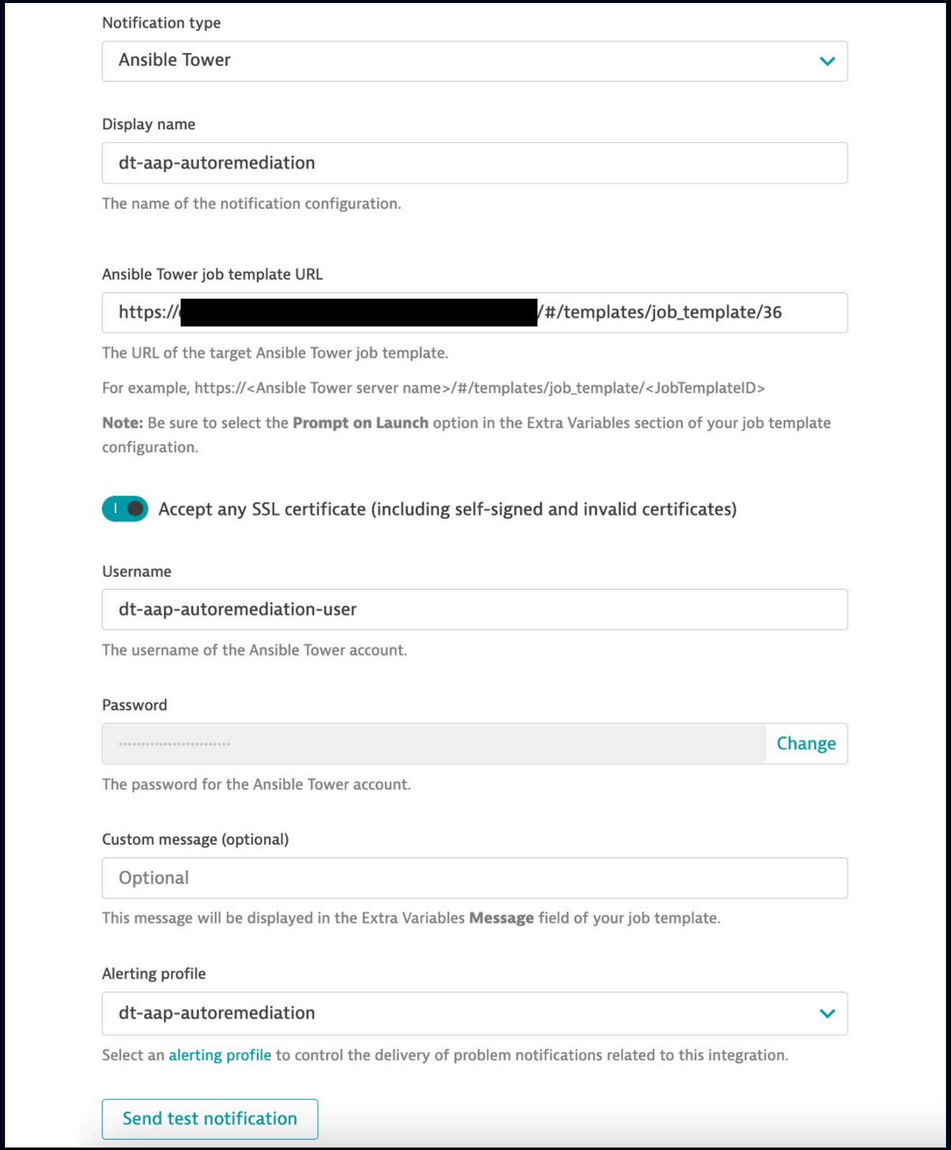
Name *	Description	Job Type * ☐ Prompt on launch
dt-aap-autoremediation-deploy		Run
Inventory * ☐ Prompt on launch	Project *	Execution Environment
dt-aap-autoremediation-inventory	dt-aap-autoremediation-project	
Playbook *		
deploy-dynatrace-autoremediation.yml		

Credentials ☐ Prompt on launch

SSH: ansible-controll...

Labels

Variables YAML JSON ☐ Prompt on launch



Notification type

Ansible Tower

Display name

dt-aap-autoremediation

The name of the notification configuration.

Ansible Tower job template URL

https://[redacted]/#/templates/job_template/36

The URL of the target Ansible Tower job template.

For example, https://<Ansible Tower server name>/#/templates/job_template/<JobTemplateID>

Note: Be sure to select the **Prompt on Launch** option in the Extra Variables section of your job template configuration.

Accept any SSL certificate (including self-signed and invalid certificates)

Username

dt-aap-autoremediation-user

The username of the Ansible Tower account.

Password

••••••••••••••••••••••••••• Change

The password for the Ansible Tower account.

Custom message (optional)

Optional

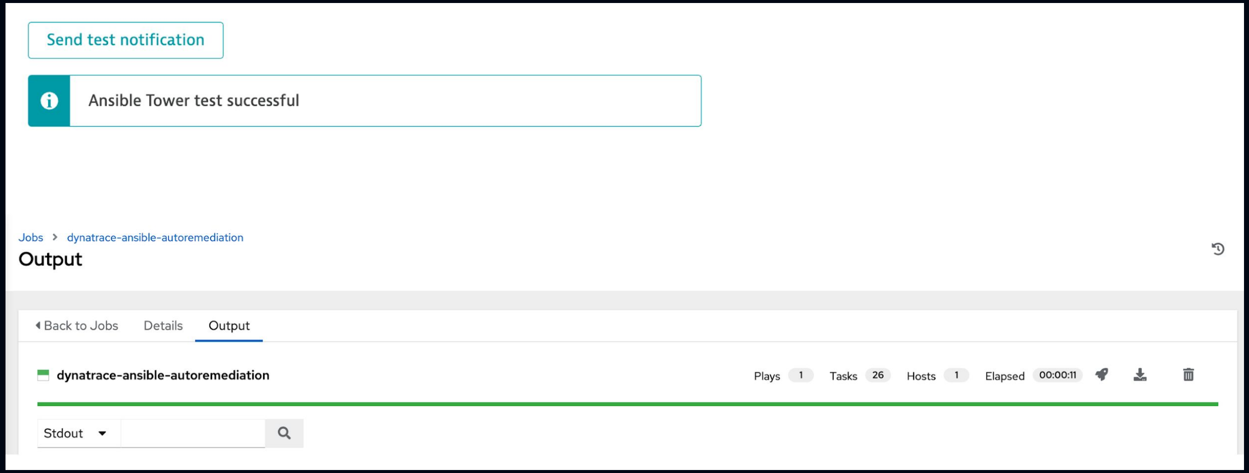
This message will be displayed in the Extra Variables **Message** field of your job template.

Alerting profile

dt-aap-autoremediation

Select an alerting profile to control the delivery of problem notifications related to this integration.

Send test notification



Send test notification

Ansible Tower test successful

Jobs > dynatrace-ansible-autoremediation

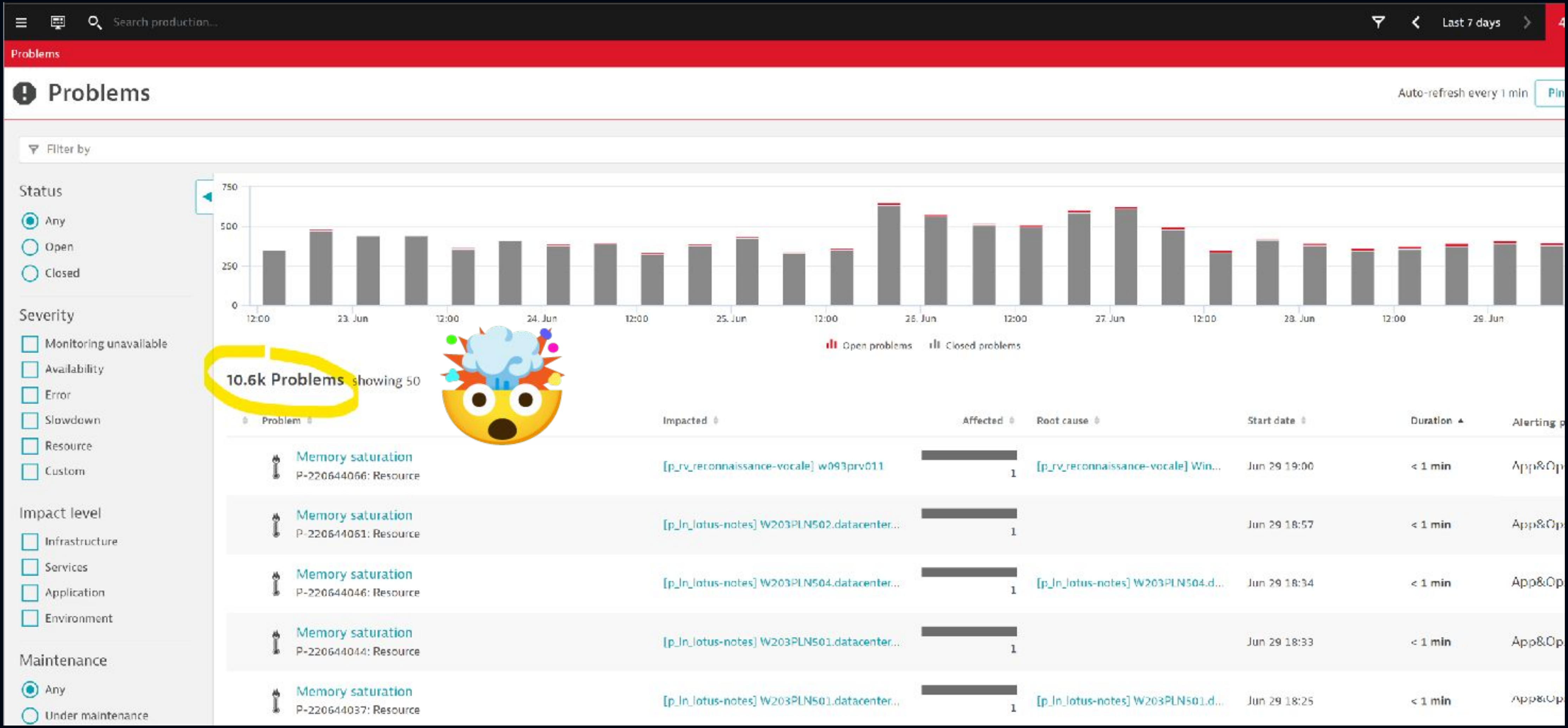
Output

Back to Jobs Details Output

dynatrace-ansible-autoremediation Plays 1 Tasks 26 Hosts 1 Elapsed 00:00:11

Stdout

SENSORY OVERLOAD!



Search production...

Last 7 days

Problems

Problems

Auto-refresh every 1 min

Filter by

Status
- [✓ Any]
- Open
- Closed

Severity
- Monitoring unavailable
- Availability
- Error
- Slowdown
- Resource
- Custom

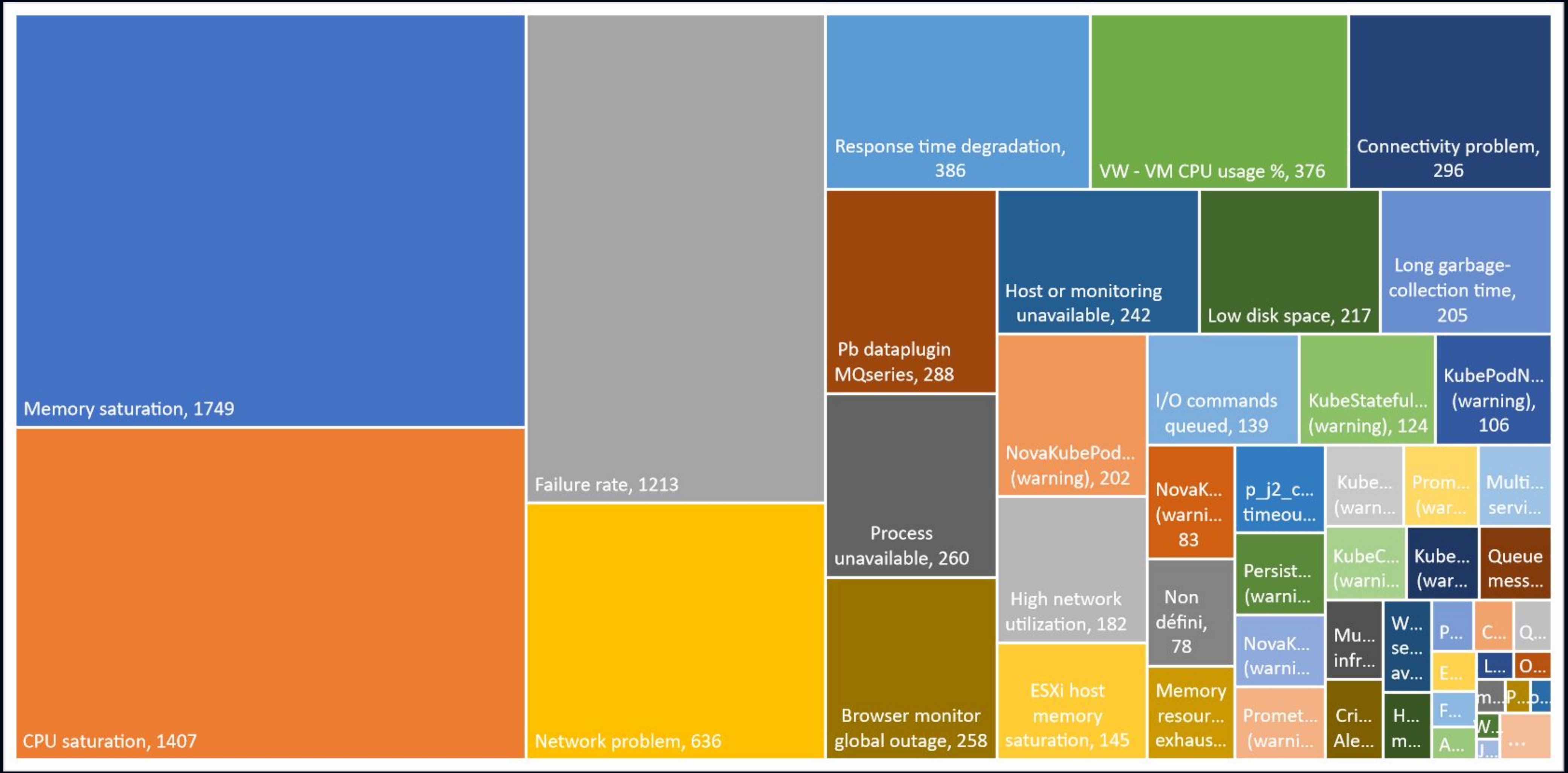
Impact level
- Infrastructure
- Services
- Application
- Environment

Maintenance
- [✓ Any]
- Under maintenance

10.6k Problems showing 50

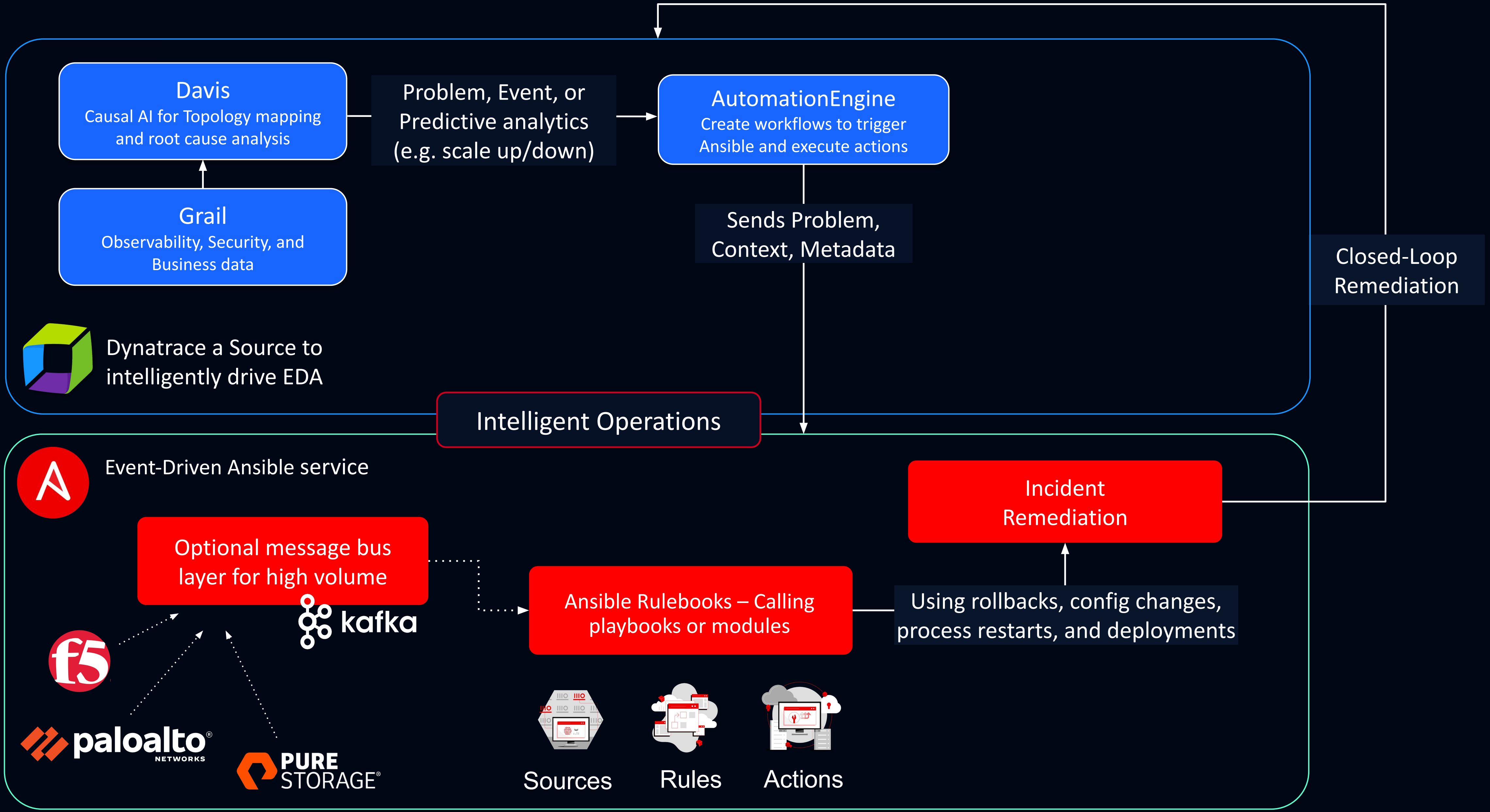
Problem	Impacted	Affected	Root cause	Start date	Duration	Alerting p
Memory saturation P-220644066: Resource	[p_rv_reconnaissance-vocale] w093prv011	1	[p_rv_reconnaissance-vocale] Win...	Jun 29 19:00	< 1 min	App&Op
Memory saturation P-220644061: Resource	[p_ln_lotus-notes] W203PLN502.datacenter...	1		Jun 29 18:57	< 1 min	App&Op
Memory saturation P-220644046: Resource	[p_ln_lotus-notes] W203PLN504.datacenter...	1	[p_ln_lotus-notes] W203PLN504.d...	Jun 29 18:34	< 1 min	App&Op
Memory saturation P-220644044: Resource	[p_ln_lotus-notes] W203PLN501.datacenter...	1		Jun 29 18:33	< 1 min	App&Op
Memory saturation P-220644037: Resource	[p_ln_lotus-notes] W203PLN501.datacenter...	1	[p_ln_lotus-notes] W203PLN501.d...	Jun 29 18:25	< 1 min	App&Op

SAME PROBLEMS SEEM TO REPEAT THEMSELVES

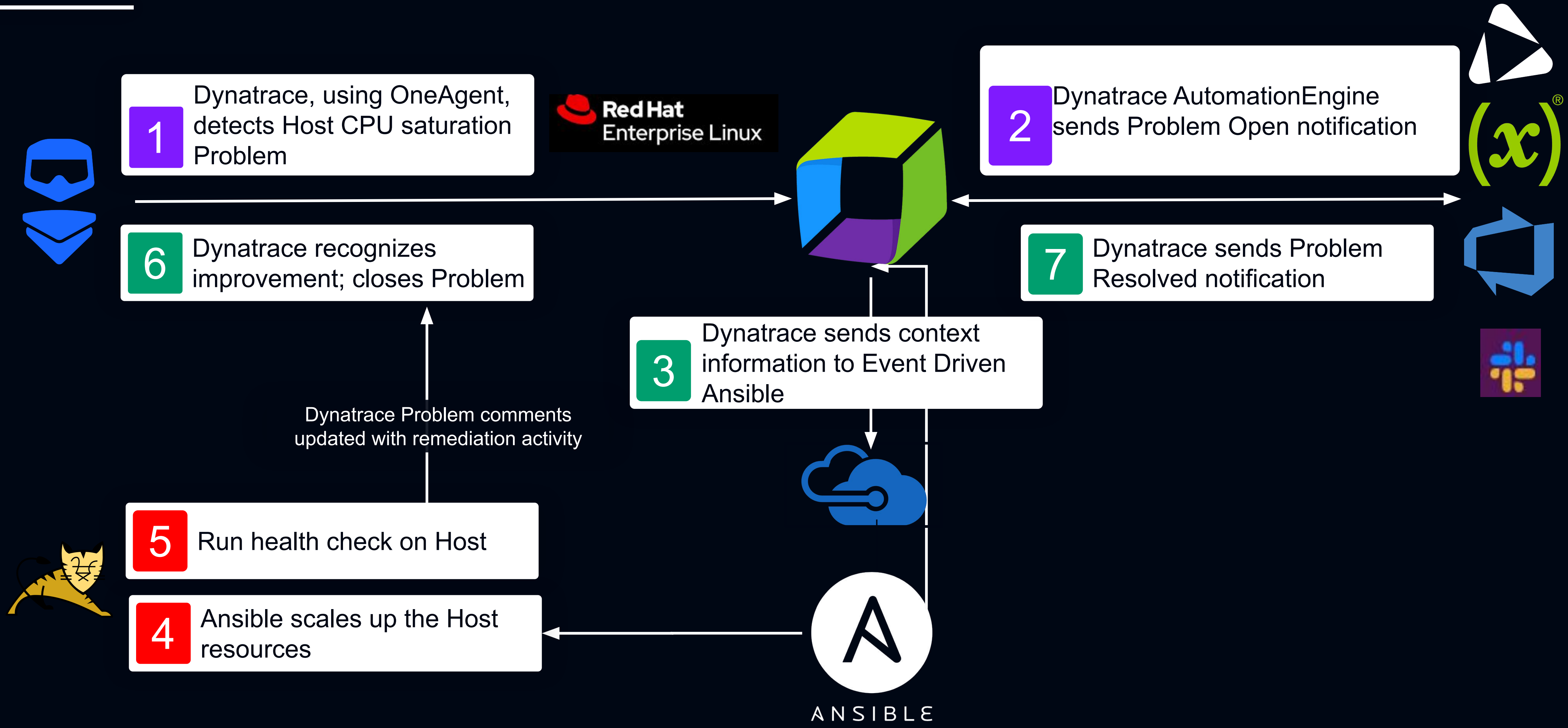


CANT WE
AUTOMATE THIS?
memegenerator.net

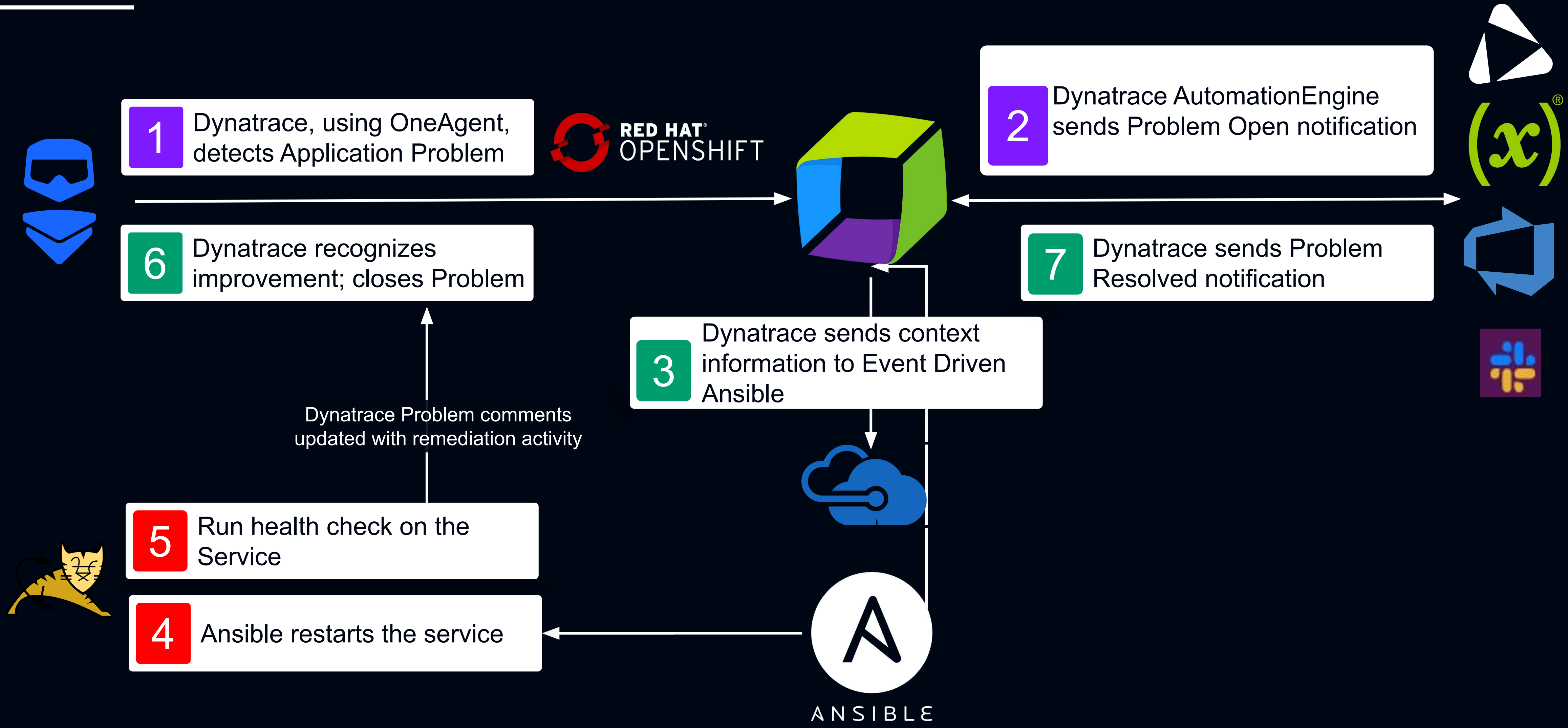
RED HAT ANSIBLE & DYNATRACE 'INTELLIGENT OPERATIONS' ARCHITECTURE

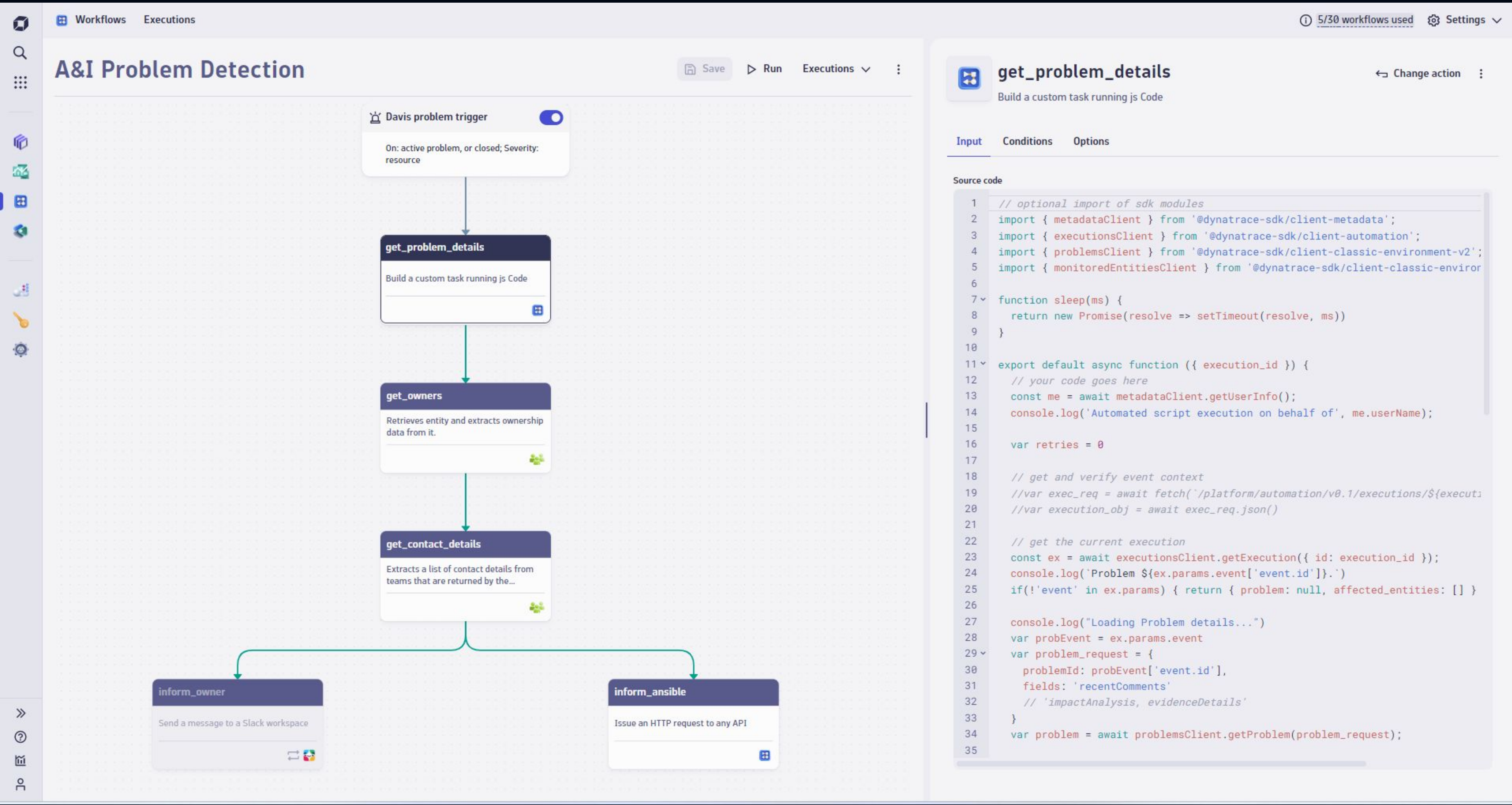

Davis
Causal AI for Topology mapping and root cause analysis
Grail
Observability, Security, and Business data
Problem, Event, or Predictive analytics (e.g. scale up/down)
AutomationEngine
Create workflows to trigger Ansible and execute actions
Sends Problem, Context, Metadata
Closed-Loop Remediation
Dynatrace a Source to intelligently drive EDA
Intelligent Operations
Event-Driven Ansible service
Optional message bus layer for high volume
kafka
Ansible Rulebooks – Calling playbooks or modules
Incident Remediation
Using rollbacks, config changes, process restarts, and deployments
f5
paloalto NETWORKS
PURE STORAGE
Sources
Rules
Actions

SOLUTION ARCHITECTURE FOR CPU SATURATION


1 Dynatrace, using OneAgent, detects Host CPU saturation Problem
Red Hat Enterprise Linux
2 Dynatrace AutomationEngine sends Problem Open notification
6 Dynatrace recognizes improvement; closes Problem
7 Dynatrace sends Problem Resolved notification
3 Dynatrace sends context information to Event Driven Ansible
Dynatrace Problem comments updated with remediation activity
5 Run health check on Host
4 Ansible scales up the Host resources
ANSIBLE

SOLUTION ARCHITECTURE FOR APP HEALING


1 Dynatrace, using OneAgent, detects Application Problem
RED HAT OPENSHIFT
2 Dynatrace AutomationEngine sends Problem Open notification
6 Dynatrace recognizes improvement; closes Problem
7 Dynatrace sends Problem Resolved notification
3 Dynatrace sends context information to Event Driven Ansible
Dynatrace Problem comments updated with remediation activity
5 Run health check on the Service
4 Ansible restarts the service
ANSIBLE



A&I Problem Detection

Davis problem trigger

On: active problem, or closed; Severity: resource

get_problem_details

Build a custom task running js Code

get_owners

Retrieves entity and extracts ownership data from it.

get_contact_details

Extracts a list of contact details from teams that are returned by the...

inform_owner

Send a message to a Slack workspace

inform_ansible

Issue an HTTP request to any API

get_problem_details

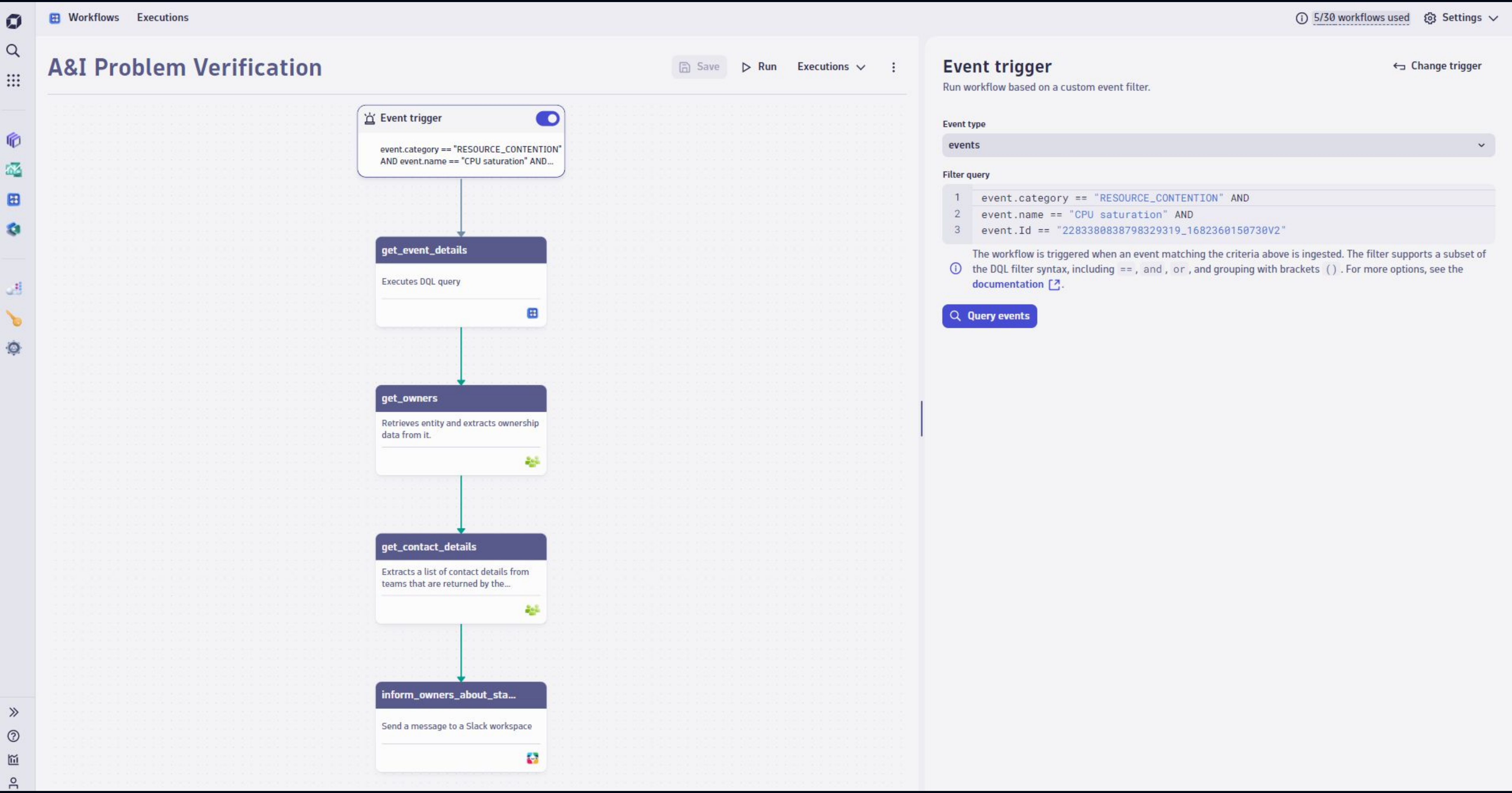
Build a custom task running js Code

Source code

```
// optional import of sdk modules
import { metadataClient } from '@dynatrace-sdk/client-metadata';
import { executionsClient } from '@dynatrace-sdk/client-automation';
import { problemsClient } from '@dynatrace-sdk/client-classic-environment-v2';
import { monitoredEntitiesClient } from '@dynatrace-sdk/client-classic-environ

function sleep(ms) {
  return new Promise(resolve => setTimeout(resolve, ms))
}

export default async function ({ execution_id }) {
  // your code goes here
  const me = await metadataClient.getUserInfo();
  console.log('Automated script execution on behalf of', me.userName);

  var retries = 0

  // get and verify event context
  //var exec_req = await fetch(`/platform/automation/v0.1/executions/${executi
  //var execution_obj = await exec_req.json()

  // get the current execution
  const ex = await executionsClient.getExecution({ id: execution_id });
  console.log(`Problem ${ex.params.event['event.id']}.`)
  if(!'event' in ex.params) { return { problem: null, affected_entities: [] }

  console.log("Loading Problem details...")
  var probEvent = ex.params.event
  var problem_request = {
    problemId: probEvent['event.id'],
    fields: 'recentComments'
    // 'impactAnalysis, evidenceDetails'
  }
  var problem = await problemsClient.getProblem(problem_request);

```

Dynatrace Events Rulebook - Webhook

```yaml
- name: Listen for events on a webhook
  hosts: all
  sources:
    - ansible.eda.webhook:
        host: 0.0.0.0
        port: 5000

  rules:
    - name: Problem payload Dynatrace for CPU issue
      condition: event.payload.problemTitle contains "CPU saturation"
      action:
        run_job_template:
          name: "Remediate CPU saturation issue"
          organization: "Default"
    - name: Problem payload Dynatrace for App Failure rate increase issue
      condition: event.payload.problemTitle contains "Failure rate increase"
      action:
        run_job_template:
          name: "Remediate Application issue"
          organization: "Default"
```



A&I Problem Verification

Event trigger

event.category == "RESOURCE_CONTENTION" AND event.name == "CPU saturation" AND...

get_event_details

Executes DQL query

get_owners

Retrieves entity and extracts ownership data from it.

get_contact_details

Extracts a list of contact details from teams that are returned by the...

inform_owners_about_sta...

Send a message to a Slack workspace

Event trigger

Run workflow based on a custom event filter.

Event type: events

Filter query

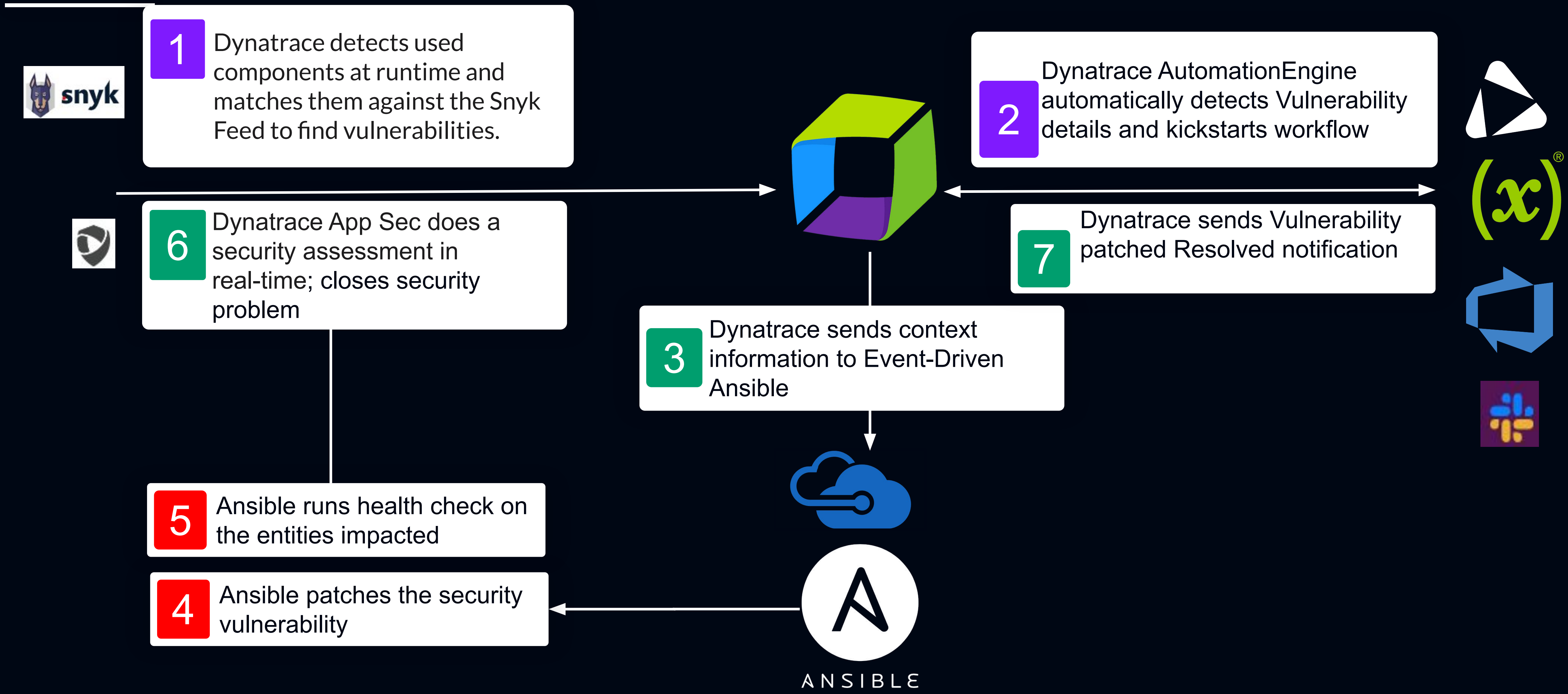
```
event.category == "RESOURCE_CONTENTION" AND
event.name == "CPU saturation" AND
event.Id == "2283380838798329319_1682360150730V2"
```

The workflow is triggered when an event matching the criteria above is ingested. The filter supports a subset of the DQL filter syntax, including `==`, `and`, `or`, and grouping with brackets `()`. For more options, see the documentation.

Dynatrace Events Rulebook - API

```
hosts: all
  ## Define Dynatrace source for events
  sources:
    - dynatrace.eda.dt_esa:
        dt_api_host: "https://xxxx.live.dynatrace.com"
        dt_api_token: "xxxxx"
        dt_entity_tags: "entityTags(\"EDA Priority:High\",\"key1:value1\")"

  ## Define the conditions we are looking for
  rules:
    - name: Problem payload Dynatrace for App Healing
      condition: event.title == "Failure rate increase" and event.rootCauseEntity
is defined
      ## Define the action we should take should the condition be met
      actions:
        - run_playbook:
            name: playbooks/remediate-dynatrace-securitychange.yml
        - run_playbook:
            name: playbooks/dynatrace-update-problem-comments.yml
```

SOLUTION ARCHITECTURE FOR APPLICATION SECURITY REMEDIATION



1 Dynatrace detects used components at runtime and matches them against the Snyk Feed to find vulnerabilities.

2 Dynatrace AutomationEngine automatically detects Vulnerability details and kickstarts workflow

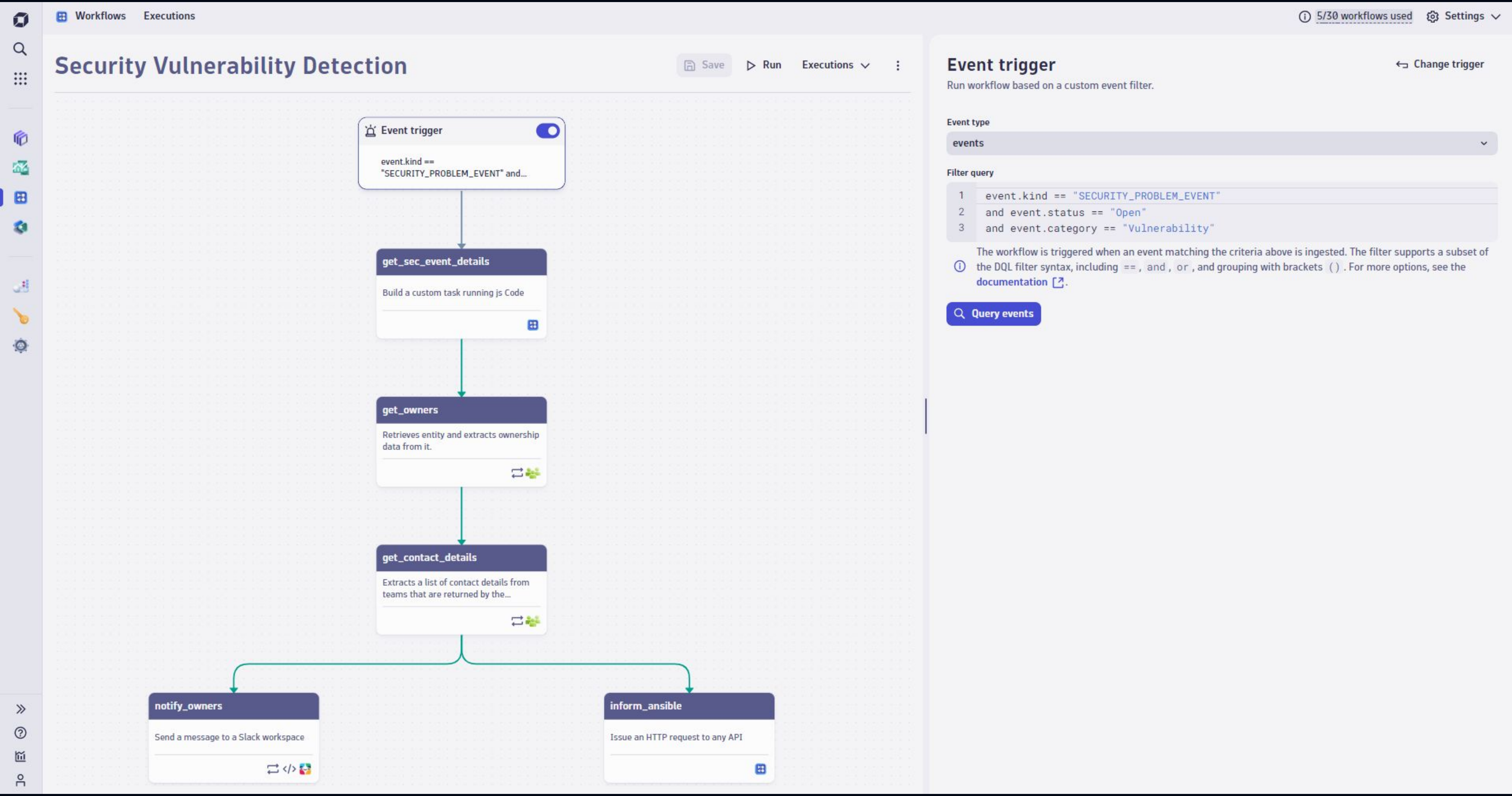
3 Dynatrace sends context information to Event-Driven Ansible

4 Ansible patches the security vulnerability

5 Ansible runs health check on the entities impacted

6 Dynatrace App Sec does a security assessment in real-time; closes security problem

7 Dynatrace sends Vulnerability patched Resolved notification



Security Vulnerability Detection

Event trigger

event.kind == "SECURITY_PROBLEM_EVENT" and...

get_sec_event_details

Build a custom task running js Code

get_owners

Retrieves entity and extracts ownership data from it.

get_contact_details

Extracts a list of contact details from teams that are returned by the...

notify_owners

Send a message to a Slack workspace

inform_ansible

Issue an HTTP request to any API

Event trigger

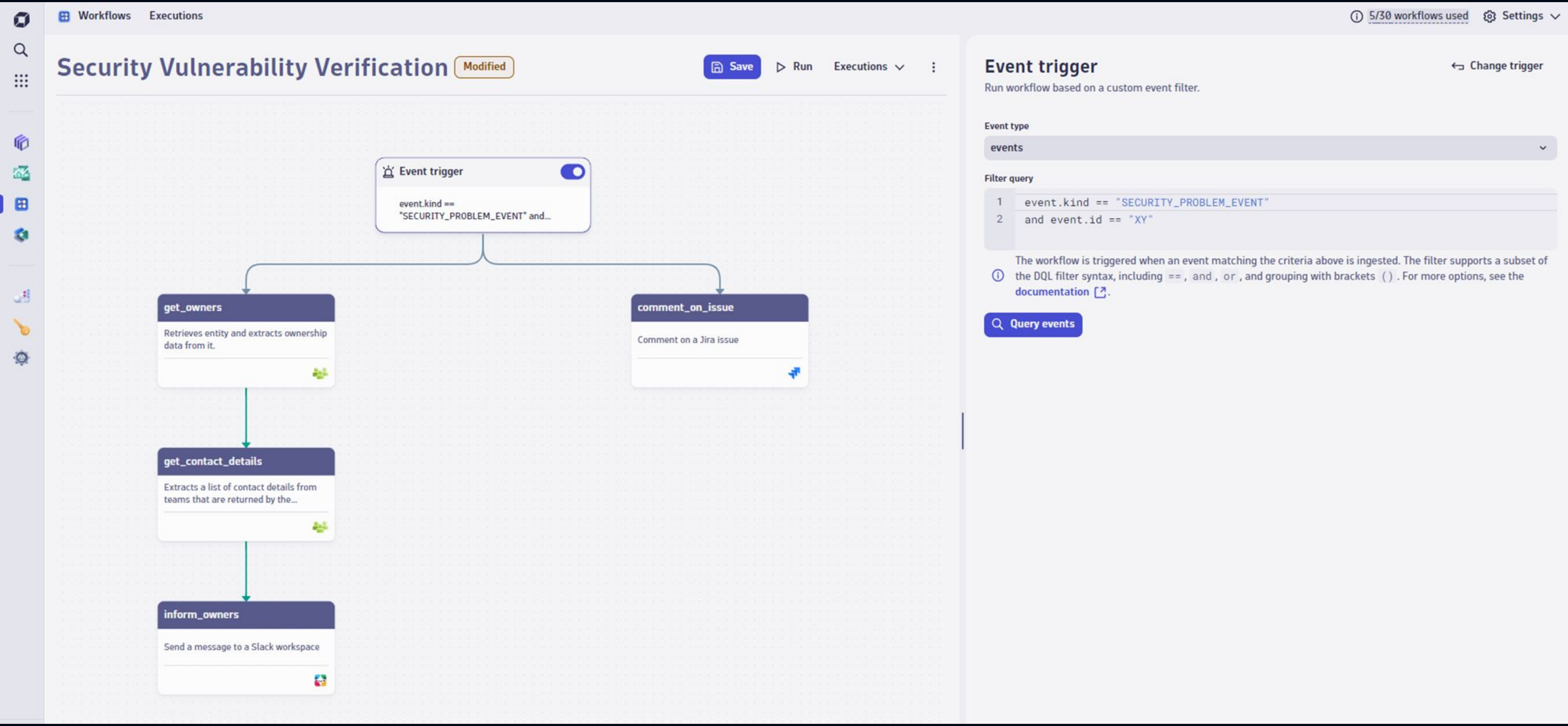
Run workflow based on a custom event filter.

Event type: events

Filter query

```
event.kind == "SECURITY_PROBLEM_EVENT"
and event.status == "Open"
and event.category == "Vulnerability"
```

The workflow is triggered when an event matching the criteria above is ingested. The filter supports a subset of the DQL filter syntax, including `==`, `and`, `or`, and grouping with brackets `()`. For more options, see the documentation.



Security Vulnerability Verification

Event trigger

event.kind == "SECURITY_PROBLEM_EVENT" and...

get_owners

Retrieves entity and extracts ownership data from it.

comment_on_issue

Comment on a Jira issue

get_contact_details

Extracts a list of contact details from teams that are returned by the...

inform_owners

Send a message to a Slack workspace

Event trigger

Run workflow based on a custom event filter.

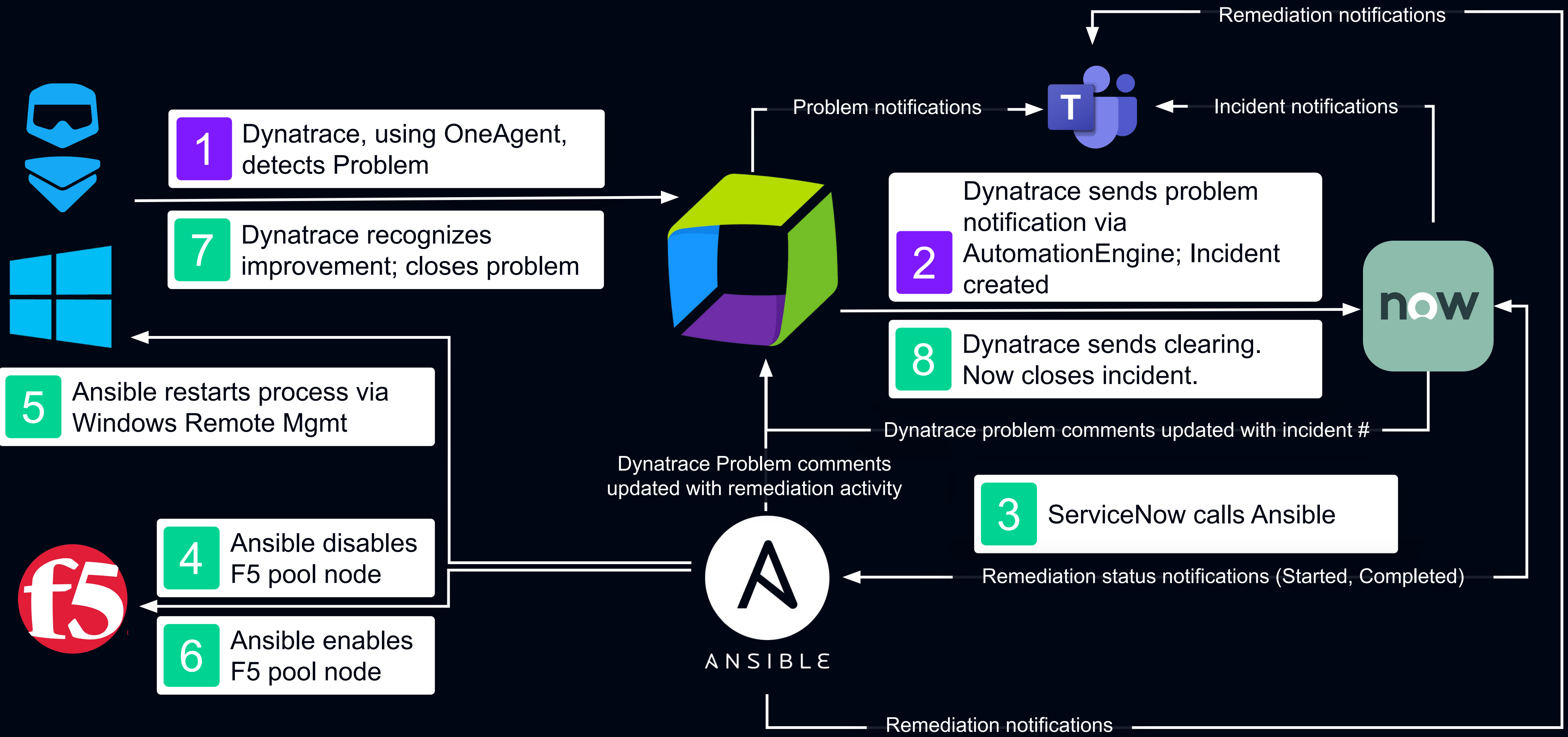
Event type: events

Filter query

```
event.kind == "SECURITY_PROBLEM_EVENT"
and event.id == "XY"
```

The workflow is triggered when an event matching the criteria above is ingested. The filter supports a subset of the DQL filter syntax, including `==`, `and`, `or`, and grouping with brackets `()`. For more options, see the documentation.

SOLUTION ARCHITECTURE FOR APP HEALING FOR A CUSTOMER



Remediation notifications
Problem notifications
Incident notifications
1 Dynatrace, using OneAgent, detects Problem
7 Dynatrace recognizes improvement; closes problem
2 Dynatrace sends problem notification via AutomationEngine; Incident created
8 Dynatrace sends clearing. Now closes incident.
5 Ansible restarts process via Windows Remote Mgmt
Dynatrace problem comments updated with incident #
Dynatrace Problem comments updated with remediation activity
3 ServiceNow calls Ansible
4 Ansible disables F5 pool node
6 Ansible enables F5 pool node
Remediation status notifications (Started, Completed)
ANSIBLE
Remediation notifications

5 STEPS TO START YOUR AUTO-REMEDIATION SUCCESS WITH ANSIBLE

Increasing confidence

5 **Automate**
Fully automate the remediation actions with a proven track record end-to-end.

4 **Integrate**
Create approval-based triggering of remediation with Change Management.

3 **Trigger**
Trigger the playbooks manually when a Problem is detected by Dynatrace, learn and repeat.

2 **Create**
Determine current rulebooks and playbooks on Red Hat Ansible that can be manually triggered.

1 **Analyze**
Evaluate your problems for repetitive patterns to identify automation opportunities.