Bridging IT and SecOps: Supercharging Zabbix with XSOAR Playbooks

Harri Ruuttila

Sr. Consulting Engineer - Cortex - EMEA

Palo Alto Networks

Common issues customers face with IT infrastructure monitoring tools.

1. Alert Fatigue

Teams get overwhelmed by notifications that don't provide clear guidance on what to do next, leading to important alerts being ignored or delayed responses.

2. Limitations of Automated Response

Lack of self-healing capabilities for routine issues and human-dependent incident escalation processes.

3. Skill and Tooling Deficiencies

Building reliable automation requires specific skills (e.g., scripting with Python, PowerShell, or Ansible) and tools that can integrate with the monitoring system.

Cortex XSOAR

ZABBIX 20 YEARS

Cortex® XSOAR

1. Automate

Automate manual tasks so your staff can focus on what's important.

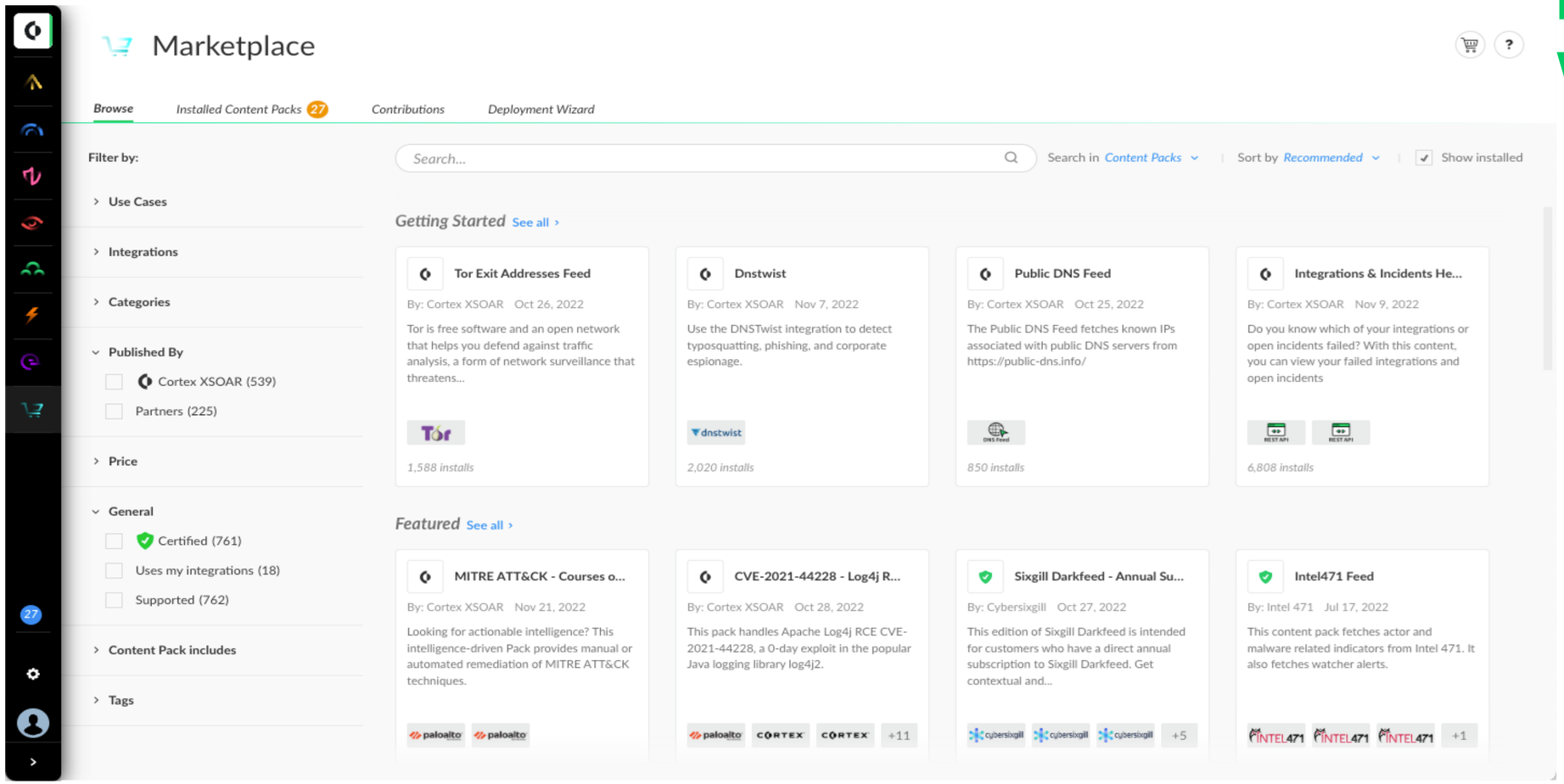
2. Orchestrate

Orchestrate responses across **ALL** your tools.

3. No code deployment

Visual playbook editor for code-free control of your automation and orchestration flow.

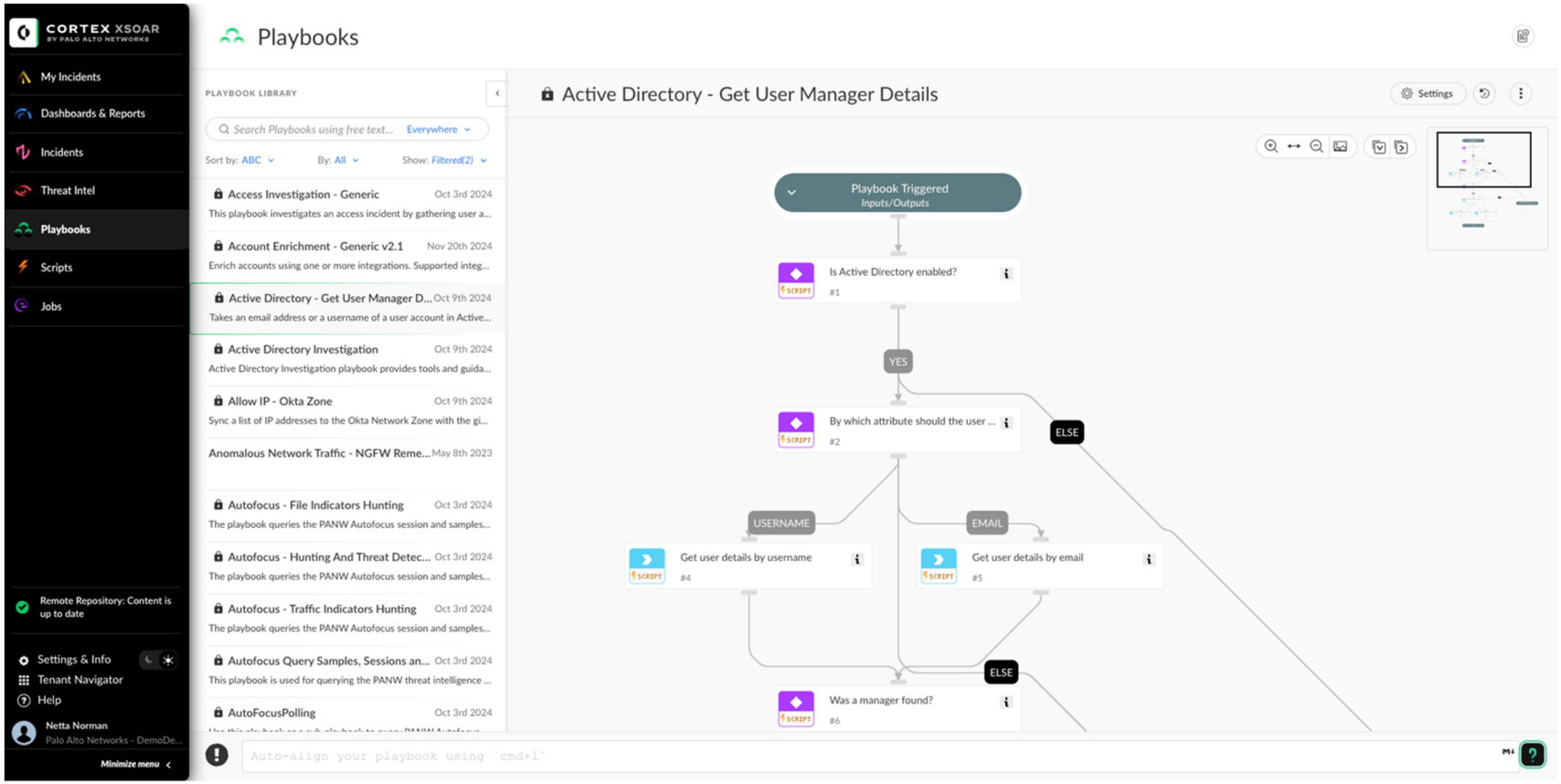
Cortex XSOAR Makes it Simple to Deploy Automation



Enterprise-ready workflow automation

- **Turnkey** automation packs for **end-to-end** workflow automation
  - Integrations
  - Playbooks
  - Layouts
  - Reports
- **Guided DIY** for downloads & custom integrations
- Currently over **1000** packs available

Cortex XSOAR Automates Your Manual Workflows

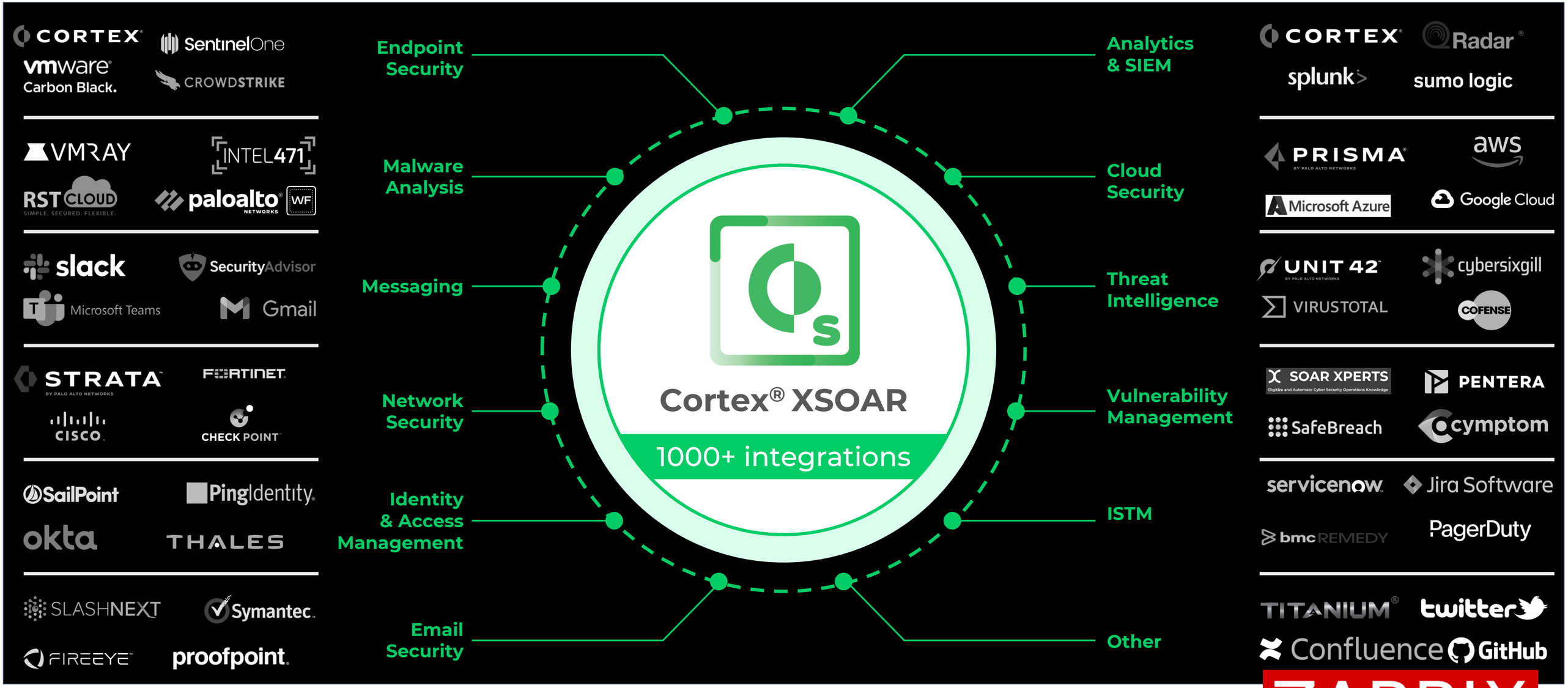


Easy to deploy as is or customize to your needs

- **1000+** integrations for easy deployment of tools you use daily
- **1000s** of security actions for DIY playbooks
- Drag & drop, **visual playbook editor** for **code-free** editing

The Industry's Most Comprehensive SOAR Ecosystem

ZABBIX 20 YEARS



ZABBIX

Cortex XSOAR + Zabbix Integration

Pull Zabbix problems as incidents in XSOAR over API integration

Issue **ANY** commands to Zabbix over API.

Cortex XSOAR + Zabbix Integration - Example #1

ZABBIX 20 YEARS

#3 Zabbix: Linux: Zabbix agent is not available (for 3m) - Zabbix i... | Source | Zabbix_instance_1 | < 7/8 > | Actions | Side panels | Search in Incidents

Zabbix info | War Room | Work Plan | Show empty fields

ZABBIX REPORTED INFO

Details

Linux: Zabbix agent is not available (for 3m)

Zabbix Acknowlegement

false

ZabbixID

209

External Status

Active

Host Name

XSOAR server

Source IP

192.168.1.240

RESPONSE ACTIONS

- Create a helpdesk ticket
- Send an email to the asset owner
- Set up a virtual war room in MS Teams and send the details
- Mark problem as acknowledged

AI EXPLANATION (1)

DBot

Sep 19th 2025 09:17:54

Task Result #3: ask AI for the explanation

Command: *!claude-send-message message="What does this Zabbix problem mean: Linux: Zabbix agent i...* (Anthropic Claude)

This Zabbix problem means that the Zabbix server cannot communicate with the Zabbix agent running on a Linux host for at least 3 minutes.

What it indicates:

- The Zabbix agent service on the monitored Linux system is either:
  - **Stopped/crashed** - The agent process is not running
  - **Unreachable** - Network connectivity issues between server and agent
  - **Overloaded** - The agent is running but not responding due to high system load
  - **Misconfigured** - Firewall, authentication, or configuration problems

Common causes and solutions:

1. Agent Service Issues

```
# Check if agent is running
sudo systemctl status zabbix-agent
# or
sudo service zabbix-agent status

# Restart the agent
sudo systemctl restart zabbix-agent
```

2. Network/Firewall Problems

- Check if port 10050 (default) is open
- Verify network connectivity between Zabbix server and agent
- Check firewall rules on the monitored host

3. Configuration Issues

- Verify `Server` parameter in `/etc/zabbix/zabbix_agentd.conf` matches your Zabbix server IP
- Check agent logs: `/var/log/zabbix/zabbix_agentd.log` …

Partial View: Too many rows. View full artifact in a new tab.

Show in War room

Cortex XSOAR + Zabbix Integration - example #2

ZABBIX 20 YEARS

#4 Zabbix: Linux: High CPU utilization (over 90% for 5m) - Zabbi... | Source | Zabbix_instance_1 | < 6/8 > | Actions | Side panels | Search in Incidents

Zabbix info | War Room | Work Plan

Show empty fields

ZABBIX REPORTED INFO

Details

Linux: High CPU utilization (over 90% for 5m)

Zabbix Acknowlegement

false

ZabbixID

219

External Status

Active

Host Name

XSOAR server

Source IP

192.168.1.240

RESPONSE ACTIONS

- Create a helpdesk ticket
- Send an email to the asset owner
- Set up a virtual war room in MS Teams and send the details
- Mark problem as acknowledged

AI EXPLANATION (1)

DBot

Sep 19th 2025 09:52:51

Task Result #3: ask AI for the explanation

Command: *!claude-send-message message="What does this Zabbix problem mean: Linux: High CPU utili...* (Anthropic Claude)

This Zabbix problem alert means that your Linux server has been experiencing consistently high CPU usage - specifically, the CPU utilization has exceeded 90% for a continuous period of 5 minutes.

What this indicates:

Severity: This is typically a **warning or high-priority alert** indicating potential performance issues.

Impact: When CPU usage stays above 90% for extended periods, it can cause:

- Slow system response times
- Application delays or timeouts
- Poor user experience
- Potential system instability

Immediate steps to investigate:

1. **Check current CPU usage:**

```
top
htop
vmstat 1 5
```

2. **Identify resource-heavy processes:**

```
ps aux --sort=-%cpu | head -10
```

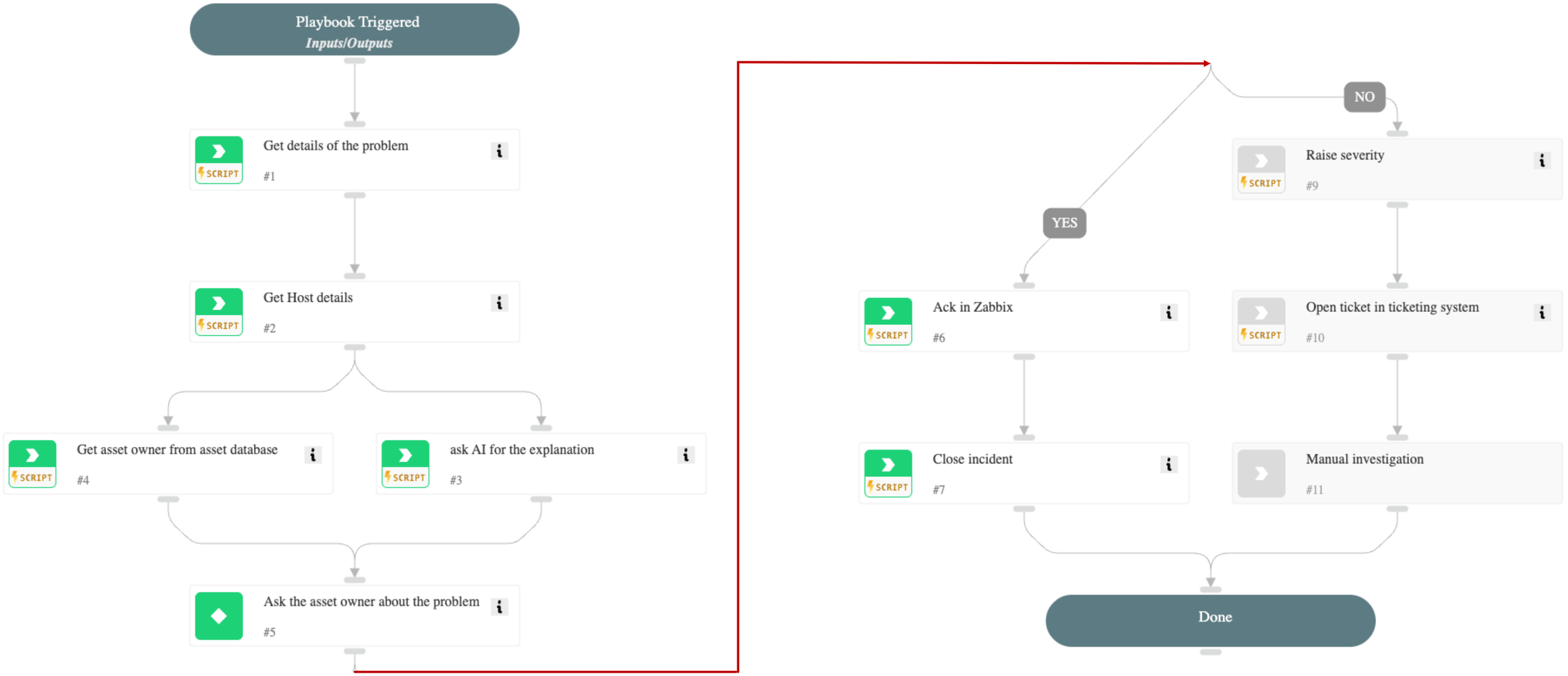
3. **Check system load:**

```
uptime
cat /proc/loadavg ...
```

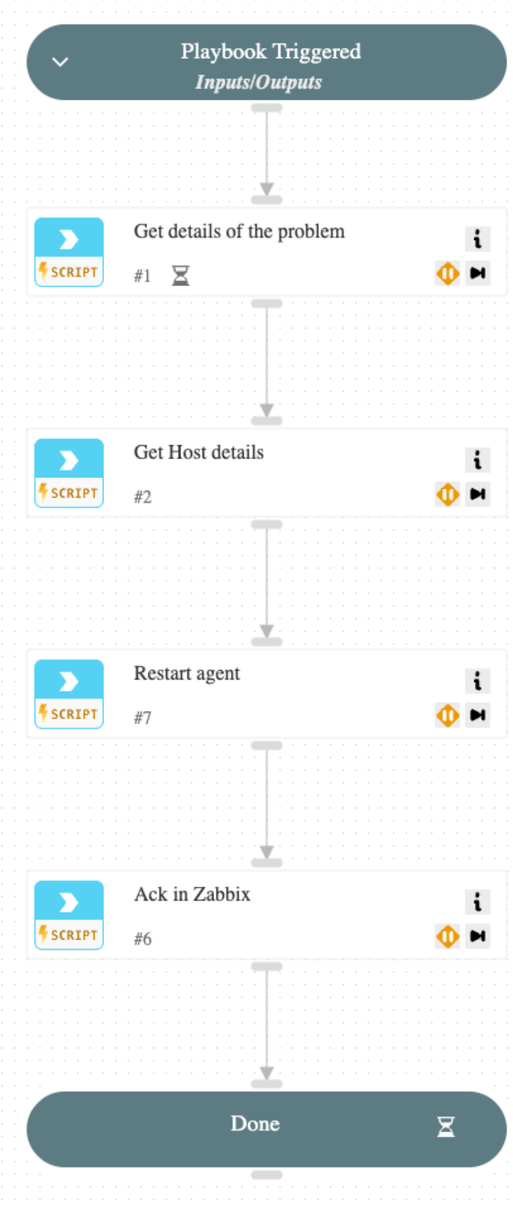
Partial View: Too many rows. View full artifact in a new tab.

Show in War room

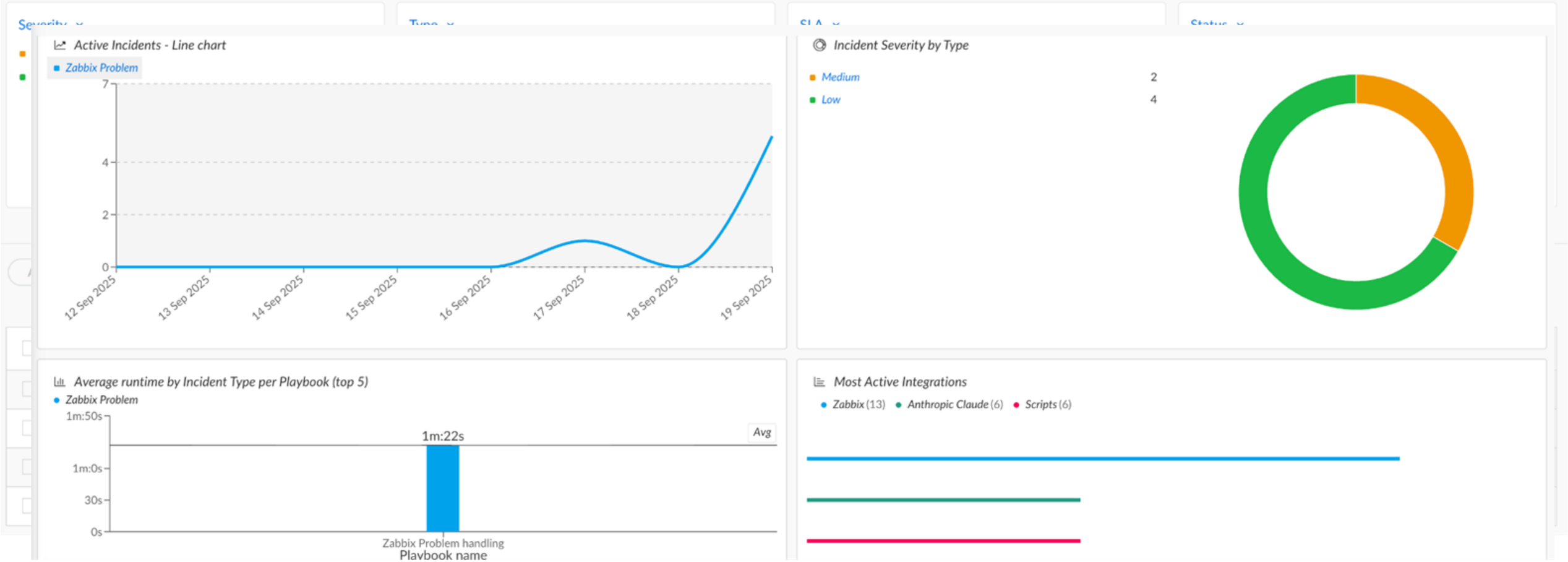
Cortex XSOAR + Zabbix Integration



Cortex XSOAR + Zabbix Integration



Cortex XSOAR - Track Metrics



Cortex XSOAR + Zabbix Integration - Summary

1. Automate Response

Automate enrichment and response to and from Zabbix.

2. Orchestrate

Orchestrate a response across **all** your tools to respond to problems reported by Zabbix.

3. Monitor Progress & SLAs

Ensure all issues are resolved within SLA limits and monitor custom timing metrics.