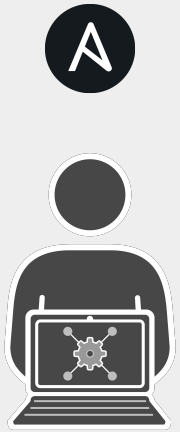
# ANSIBLE LEARNING LOUNGE SECURITY AUTOMATION

Greg Sowell
Senior Specialist Solutions Architect - Ansible

Red Hat



Automation happens when one person meets a problem they never want to solve again

Red Hat

# Ad-hoc Automation is happening in silos

Developers → Ansible used in silo

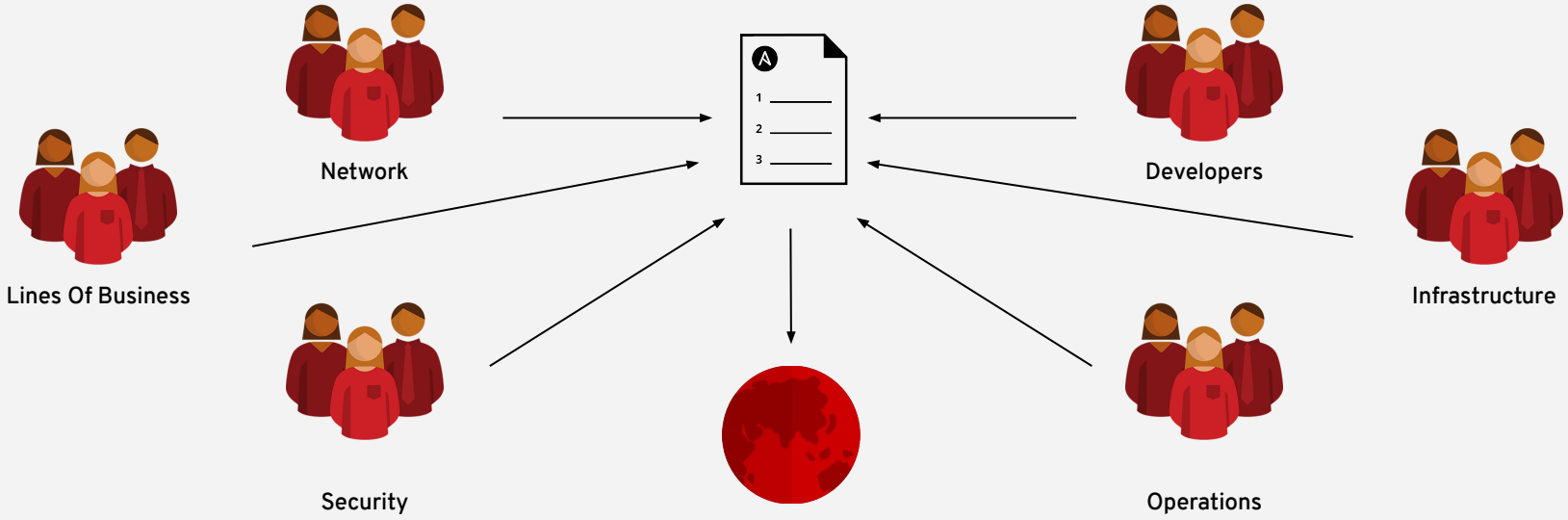
Security → DIY scripting automation

Infrastructure → Open source config management tool

Network → Proprietary vendor supplied automation

Is organic automation enough?

# When automation crosses teams, you need an automation platform



# Why Ansible?

## Simple

Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

**Get productive quickly**

## Powerful

App deployment

Configuration management

Workflow orchestration

Network automation

**Orchestrate the app lifecycle**

## Agentless

Agentless architecture

Uses OpenSSH & WinRM

No agents to exploit or update

Get started immediately

**More efficient & more secure**

Red Hat

# What can I do using Ansible?

Automate the deployment and management of your entire IT footprint.

**Do this...**

| | | | | | |
|---|---|---|---|---|---|
| Orchestration | Configuration Management | Application Deployment | Provisioning | Continuous Delivery | Security and Compliance |

**On these...**

| | | | | |
|---|---|---|---|---|
| Firewalls | Load Balancers | Applications | Containers | Clouds |
| Servers | Infrastructure | Storage | Network Devices | **And more...** |

Red Hat

# Ansible automates technologies you use

Time to automate is measured in minutes, 50+ **certified** platforms

## Cloud

**AWS**
**Azure**
Digital Ocean
**Google**
OpenStack
Rackspace
+more

## Red Hat Products

RHEL
**Satellite**
**Insights**
+more

## Virt & Container

Docker
Kubernetes
OpenStack
OpenShift
VMware
+more

## Storage

**Infinidat**
**Netapp**
**Pure Storage**
+more

## Windows

ACLs
Files
Packages
IIS
Registry
Shares
Services
Configs
Users
Domains
Updates
+more

## Network

**Arista**
**Aruba**
Bigswitch
**Cisco**
Ericsson
**F5**
**FRR**
**Juniper**
Meraki
**OpenvSwitch**
Ruckus
**VyOS**
+more

## Security

**Checkpoint**
**Cisco**
**CyberArk**
**F5**
**Fortinet**
**Juniper**
**IBM**
Palo Alto
Snort
+more

## Monitoring

**Dynatrace**
Datadog
LogicMonitor
**New Relic**
Sensu
+more

## Devops

Jira
GitHub
Vagrant
Jenkins
Slack
+more

# Red Hat Ansible Tower

by the numbers:

**94%** Reduction in recovery time following a security incident

**84%** Savings by deploying workloads to generic systems appliances using Ansible Tower

**67%** Reduction in man hours required for customer deliveries

Financial summary:

**146%**

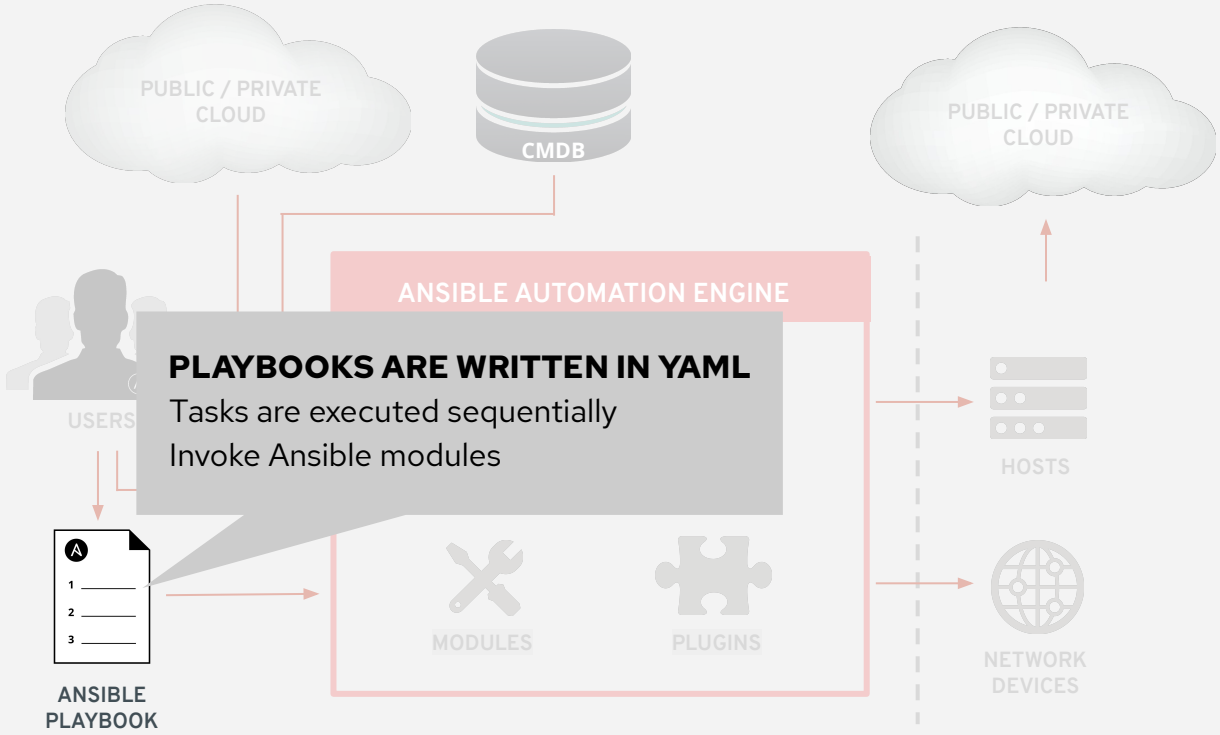
**ROI on Ansible Tower**

**< 3 MONTHS**

**Payback on Ansible Tower**

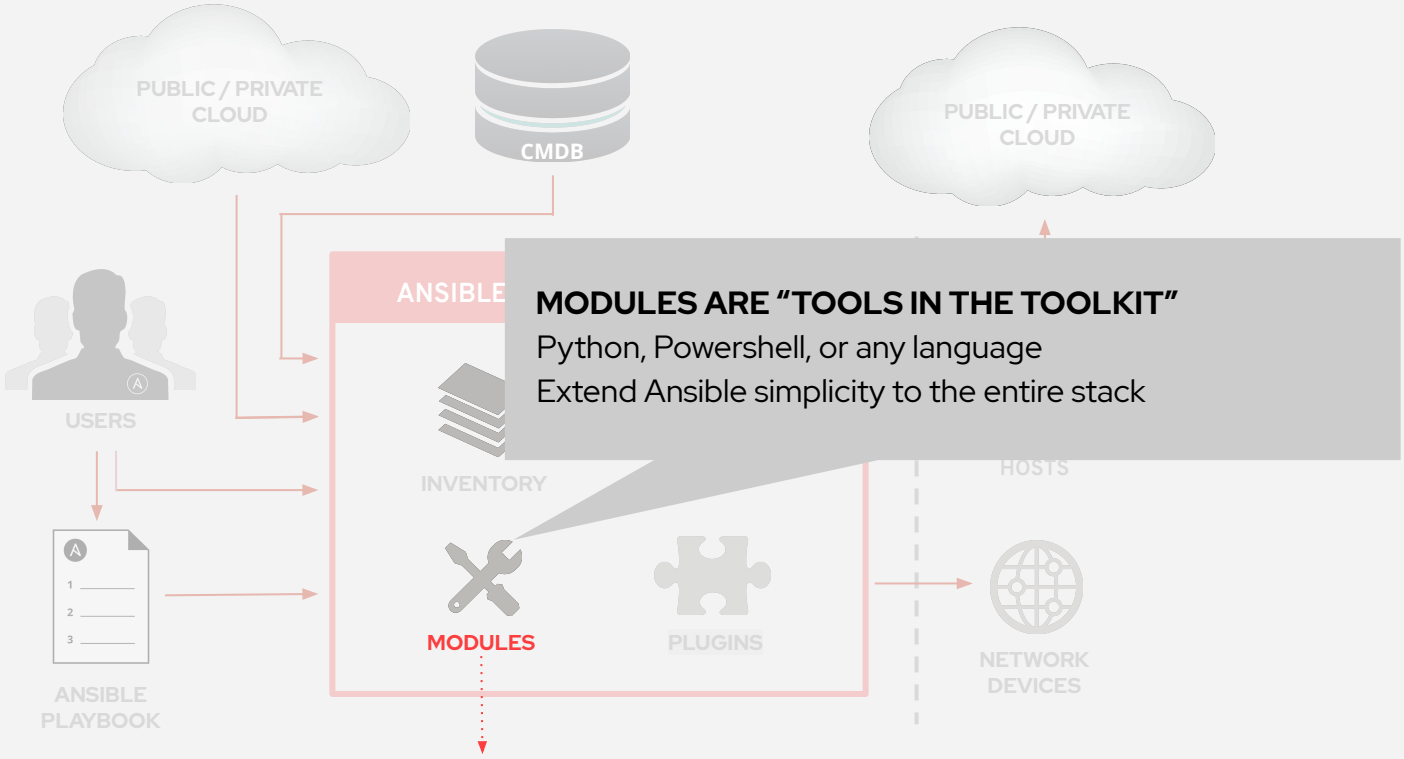
**SOURCE:** *"The Total Economic Impact™ Of Red Hat Ansible Tower, a June 2018 commissioned study conducted by Forrester Consulting on behalf of Red Hat."*
redhat.com/en/engage/total-economic-impact-ansible-tower-20180710

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
PLAYBOOKS ARE WRITTEN IN YAML
Tasks are executed sequentially
Invoke Ansible modules
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

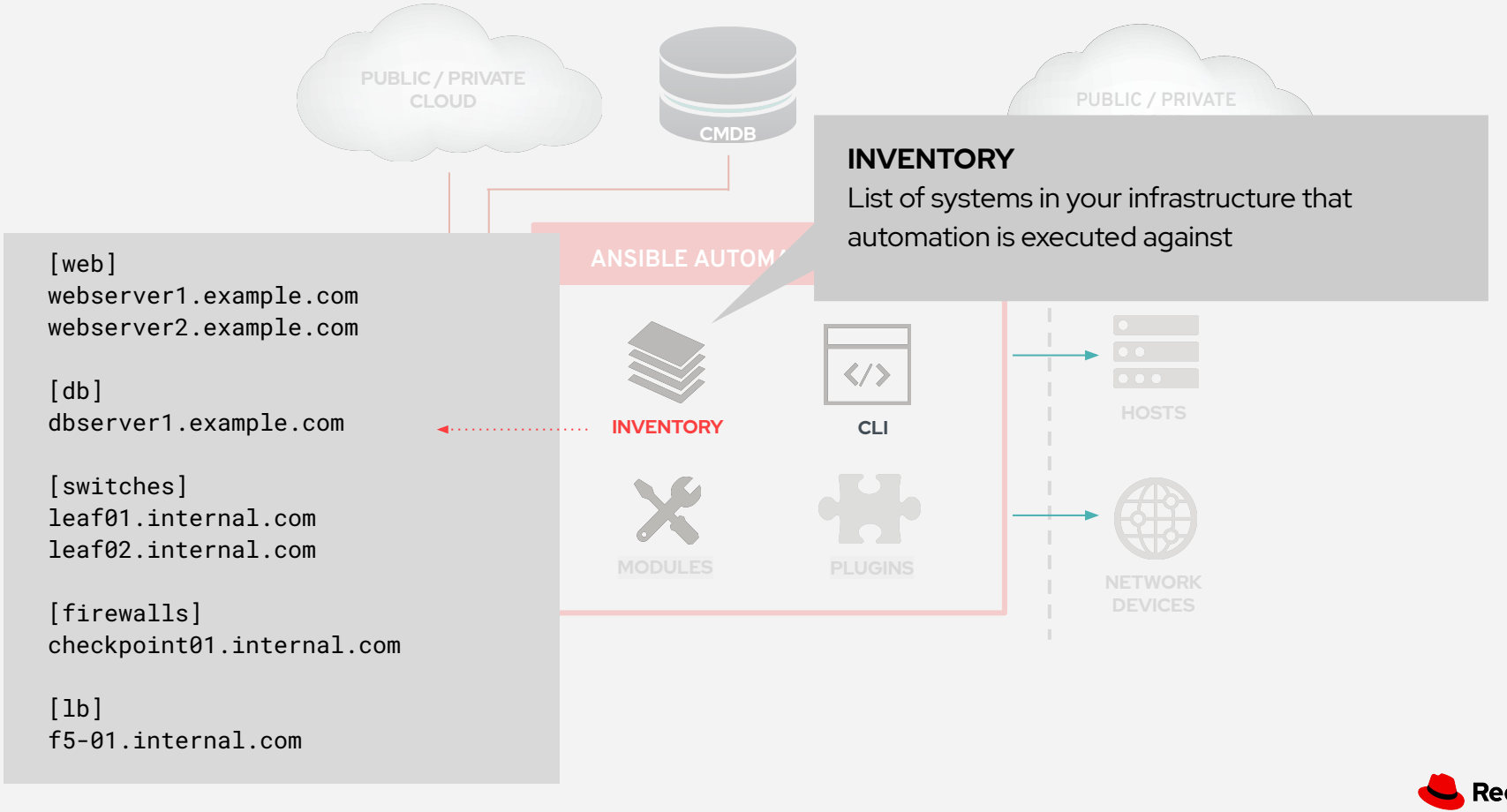
Red Hat

```
---
- name: install and start apache
  hosts: web
  become: yes

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```

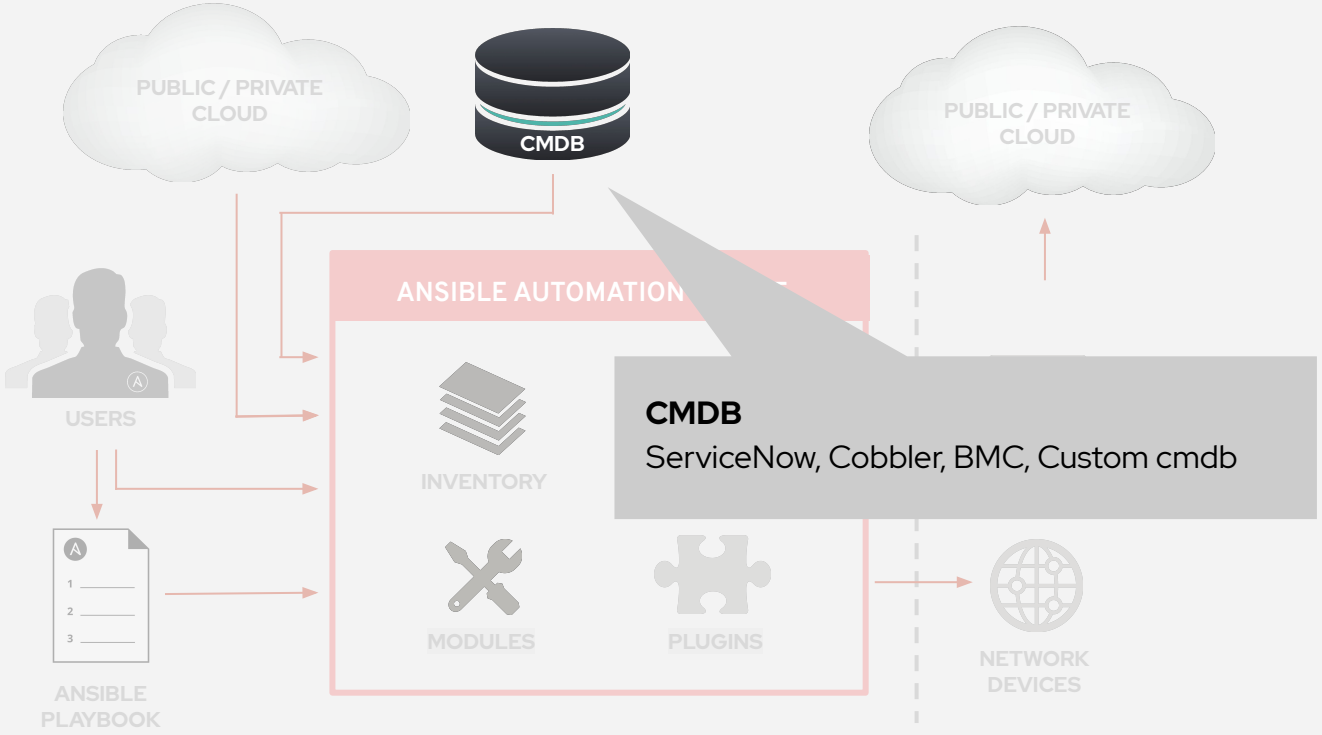



```
- name: latest index.html file is present
  template:
    src: files/index.html
    dest: /var/www/html/
```

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE
INVENTORY
List of systems in your infrastructure that automation is executed against
[web]
webserver1.example.com
webserver2.example.com
[db]
dbserver1.example.com
[switches]
leaf01.internal.com
leaf02.internal.com
[firewalls]
checkpoint01.internal.com
[lb]
f5-01.internal.com
ANSIBLE AUTOM
INVENTORY
CLI
MODULES
PLUGINS
HOSTS
NETWORK DEVICES

Red Hat

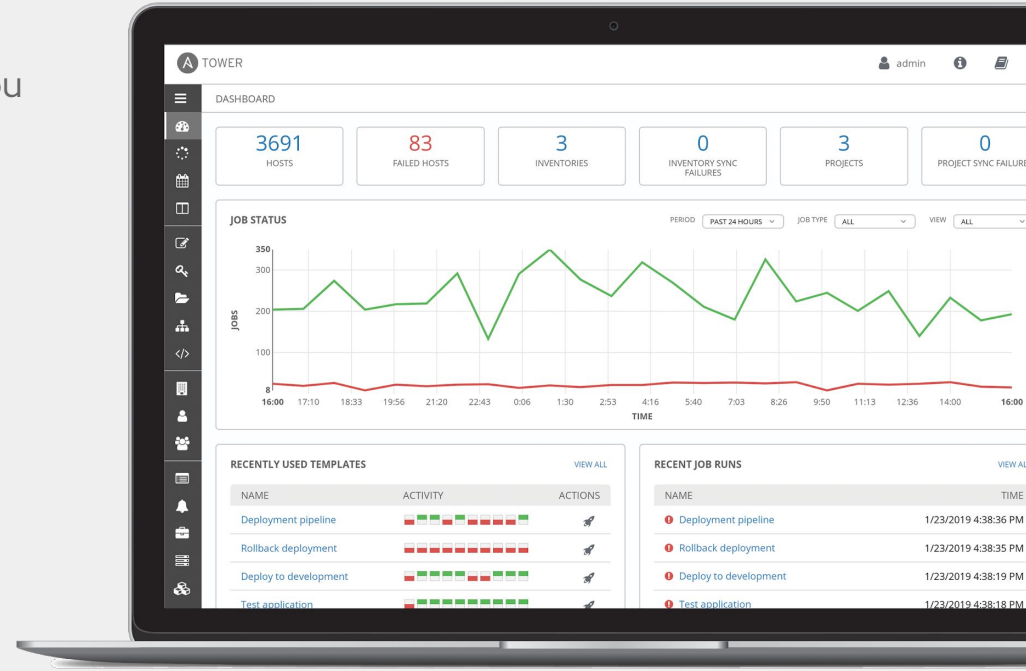

PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION
USERS
INVENTORY
CMDB
ServiceNow, Cobbler, BMC, Custom cmdb
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat

# What is Ansible Tower?

Ansible Tower is a UI and RESTful API allowing you to scale IT automation, manage complex deployments and speed productivity.

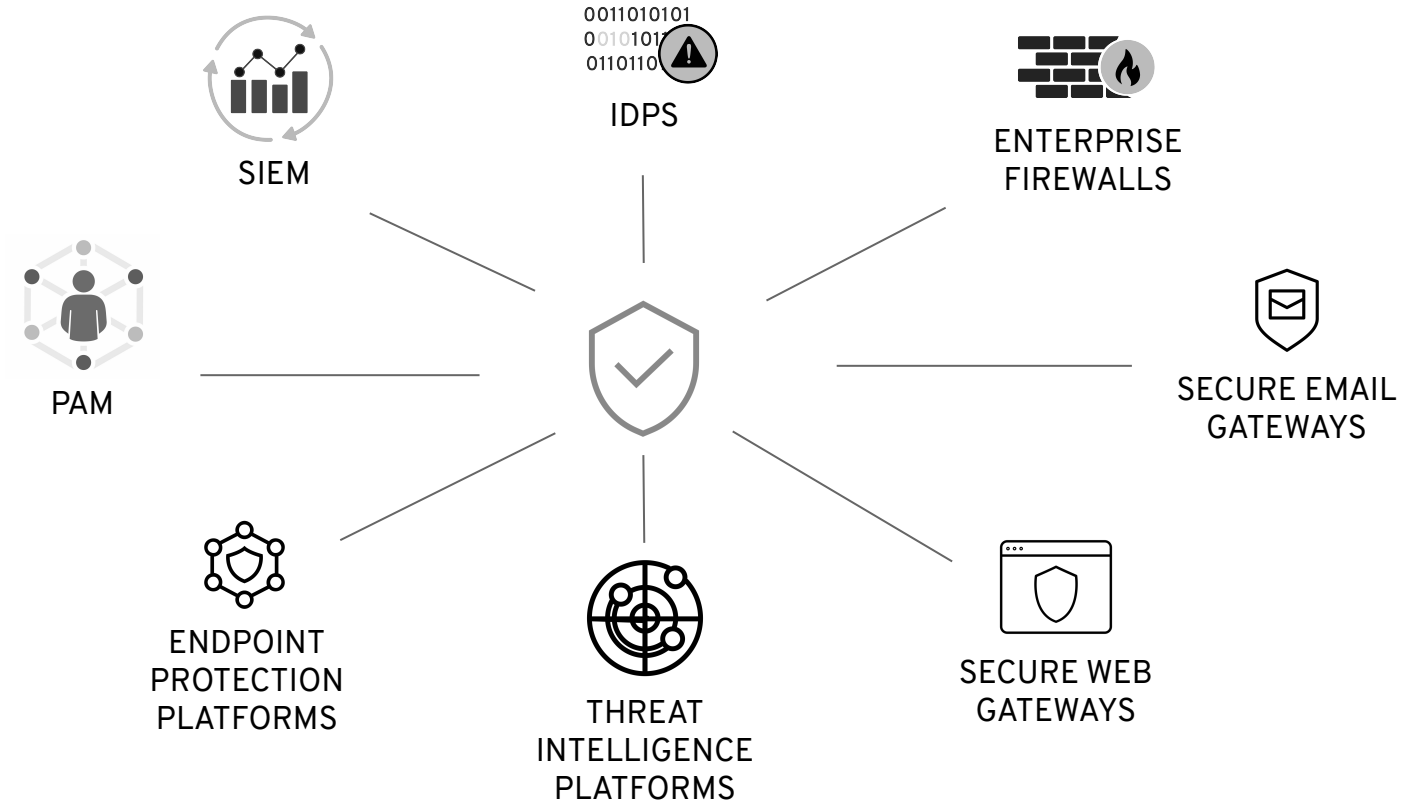
- Role-based access control
- Deploy entire applications with push-button deployment access
- All automations are centrally logged
- Powerful workflows match your IT processes




Red Hat

# Introducing Ansible security automation

Red Hat
Ansible Automation
Platform


SIEM
0011010101
0010101
0110110
IDPS
ENTERPRISE FIREWALLS
PAM
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

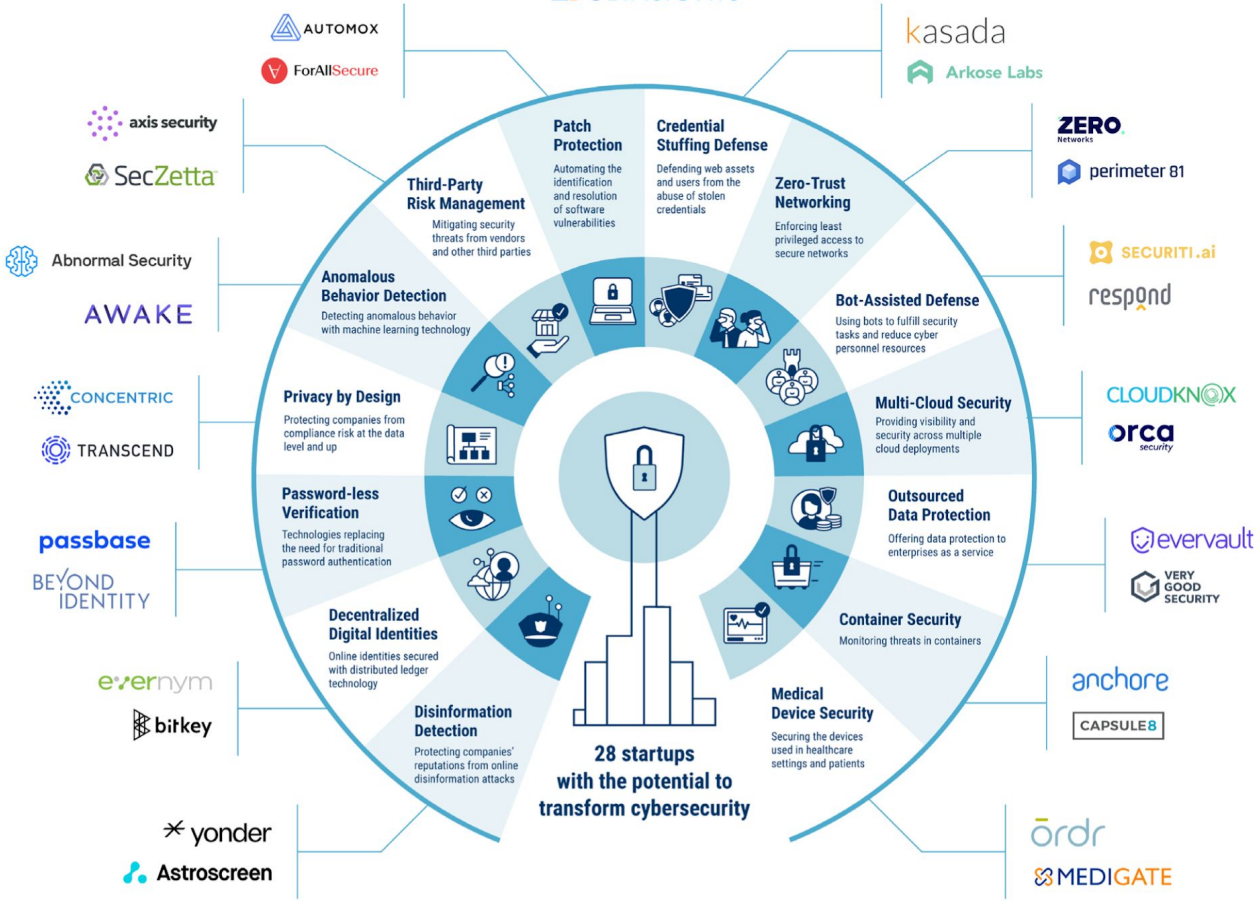


Red Hat


Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum Cyber
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Infrastructure
Container
CASB

# CYBER DEFENDERS 2020

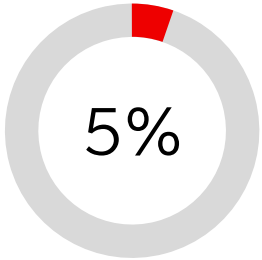
CBINSIGHTS



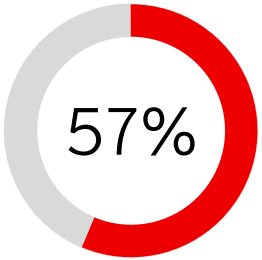



Red Hat

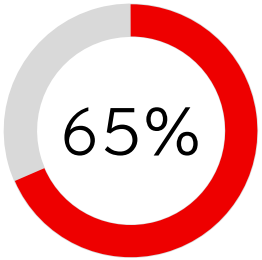
# Why Ansible security automation?



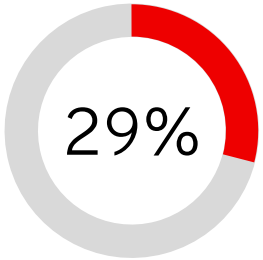

Portion of alerts coming in that the average security team examines every day




Said the time to resolve an incident has grown




Reported increased Severity of attacks




Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience

Source:

1 The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)

2 https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/

Red Hat

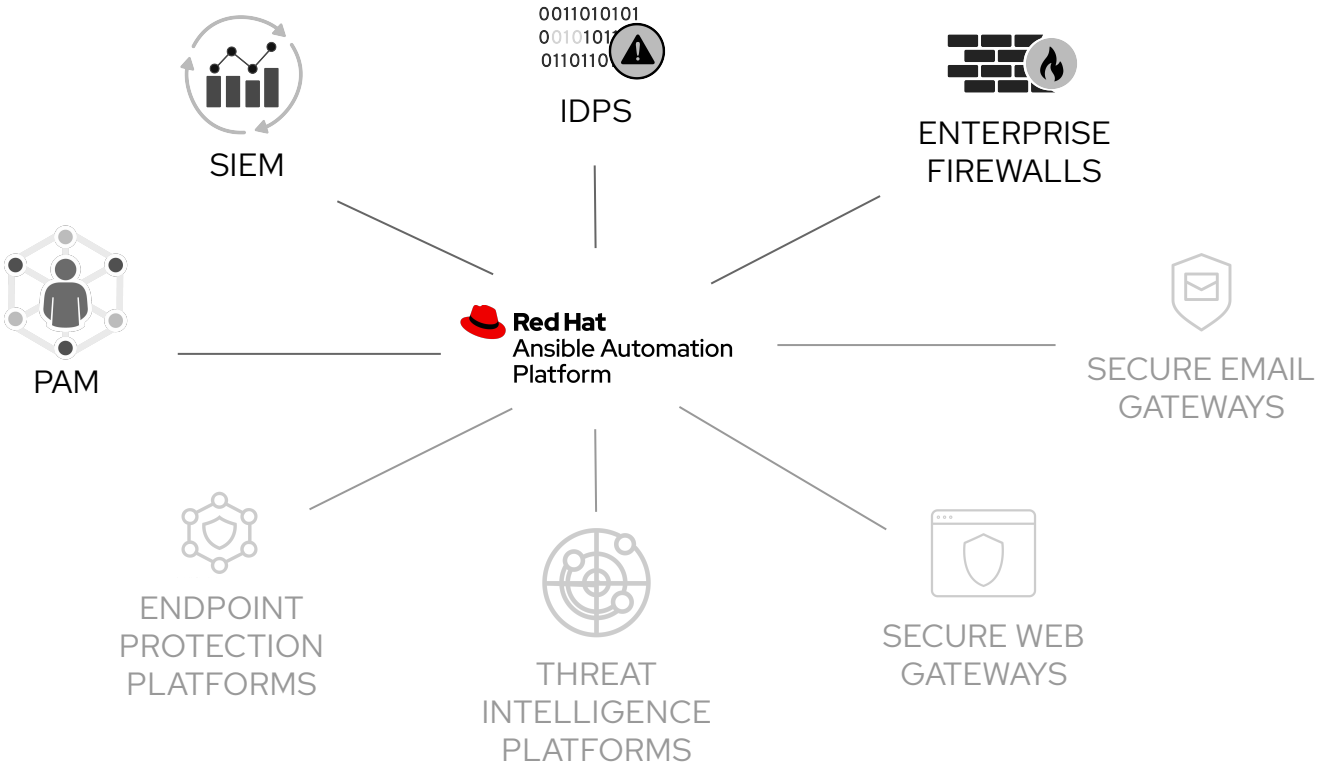
**‘Lack of automation and orchestration’** ranked second and **‘Too many tools that are not integrated’** ranked third on the list of SOC challenges.

SANS Institute

Source:
The Definition of SOC-cess? SANS 2018 Security Operations Center Survey

Red Hat

# What Is Ansible security automation?






Red Hat

# What Is Ansible security automation?

Ansible security automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events. This is more complex and higher-value than the application of a security baseline (PCI, STIG, CIS) to a server.

Ansible security automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks.

# Is It A Security Solution?

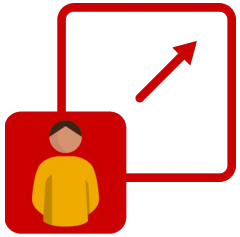
No. Ansible can help Security teams “stitch together” the numerous security solutions and tools already in their IT environment for a more effective cyber defense.

By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

# How Automation solves today's security operations challenges

### Speed

Reduce the number of manual steps and GUI-clicking, enable the orchestration of security tools and accelerate their interaction with each other



### Reduce Human Errors

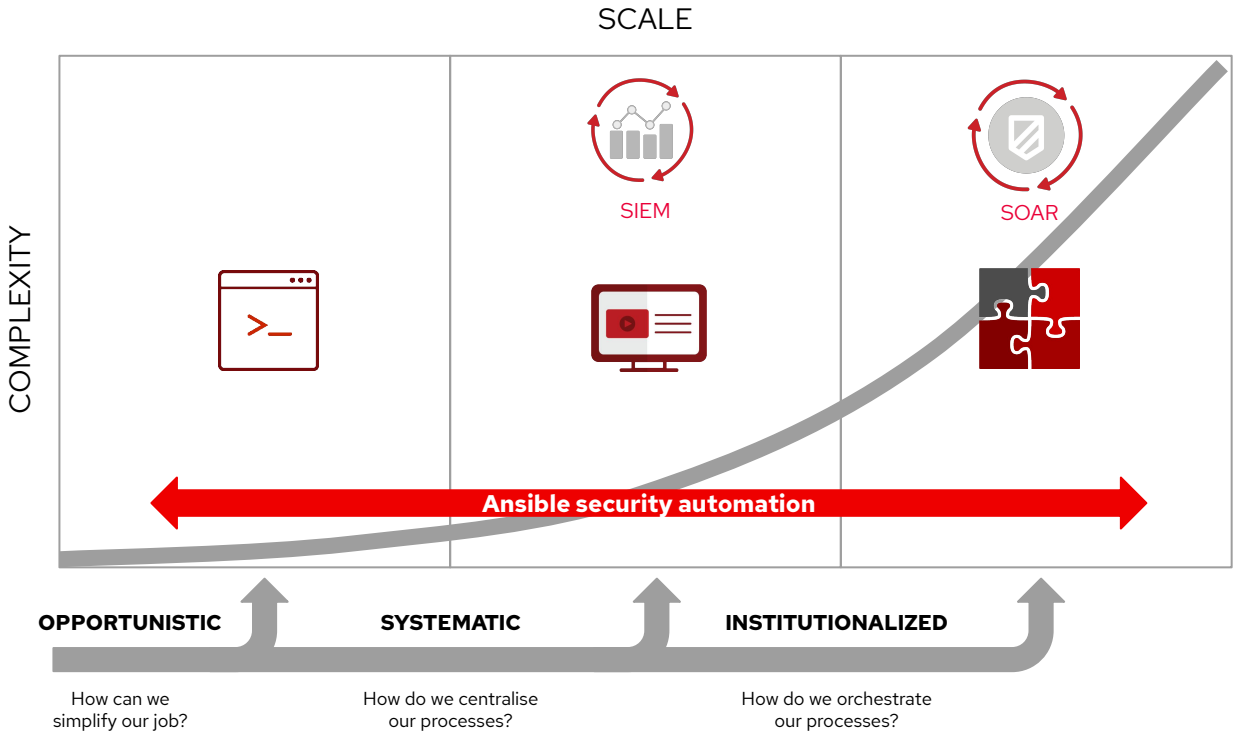
Minimize risks with automated workflows, avoid human operator errors in time-sensitive, stressful situations

### Consistency

Enable auditable and verifiable security processes by using a single tool and common language covering multiple security tools

Red Hat

# How customers adopt security automation?




https://www.ansible.com/blog/the-journey-to-security-automation

Red Hat

# Investigation Enrichment: Mimecast to Virustotal

Perform deeper email link and attachment investigation.


User submits email to potential phishing account.

Alert sent to Qradar.

Ansible takes original links/attachments from Mimecast API and submits to Virustotal.

If reputation score for any is above 1 then the email is pulled from any other receiving mailboxes.

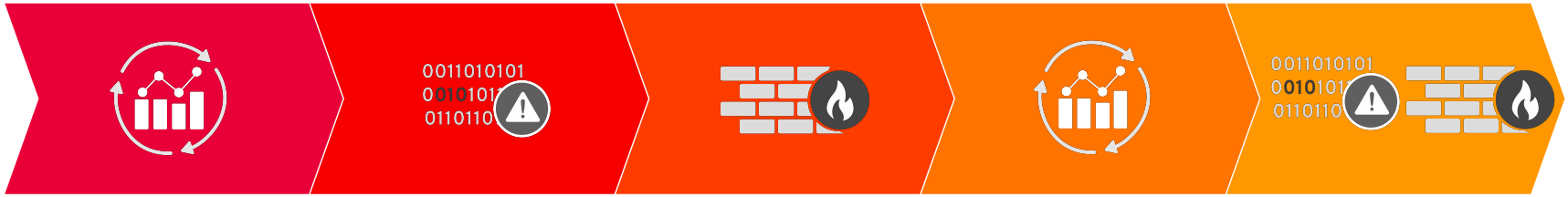
Incident updated in QRadar.



Red Hat

# Investigation Enrichment: Application Behaviour

The Assessment Of Abnormal Behaviours Involves Multiple Steps Like Validating An Ip Address Against Multiple Sources, Searching The Environment For Signs Of Infiltration, Etc. And Then Process And Present The Information To The Security Analyst.




splunk>

Detects an anomaly from the behaviour of an application.
Asks Snort & Check Point for more information.

SNORT

Implements a new rule to collect more information in the affected perimeter.

Check Point SOFTWARE TECHNOLOGIES LTD.

Raises the level of logging on low level networking perimeter.

splunk>

Consolidates information for the triage.

SNORT Check Point SOFTWARE TECHNOLOGIES LTD.

Restore original configurations.



Red Hat

# Threat Hunting: Firewall Rule Violation

A Threat Intelligence Or Incident Responder Could Investigate An Incident And End Up With Hundreds Of Ips, File Hashes, And Domains.


CISCO

Registers a continuous rule violation. Sends alerts to IBM QRadar.

IBM

Creates an offense, requests additional information to Fortinet IPS.

FORTINET

Creates a new rule to investigate the origin of the violation.

IBM

Confirms the rule violation is caused by a misconfigured IP address.

CISCO

Whitelists the IP address.



Red Hat

# Incident Response: Sql Injection Attack

Sql Injections Mitigation Requires Up To 10 Manual Steps Between Identification And Remediation.

Check Point IPS detects a SQL Injection attack & alerts IBM QRadar.

Validates the threat, creates an Offense & triggers remediation.

Fortinet NGFW creates a new rule to blacklist the IP source of the attack.

Confirms the end of the attack & updates IBM QRadar.

Double checks the end of the attack and closes the incident.

# Thank You, any Questions?