How to introduce automation to your colleagues in IT Security

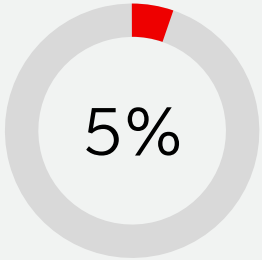
(and what's in for you)

Massimo Ferrari
Consulting Product Manager,
Ansible Automation Platform
@crosslogic

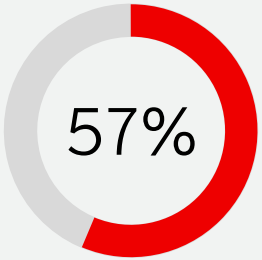
AnsibleFest

The State of Cybersecurity

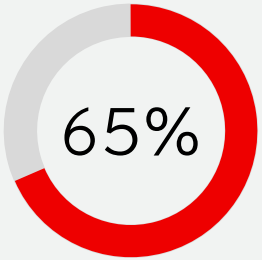
Threats are evolving faster than ever and becoming increasingly sophisticated



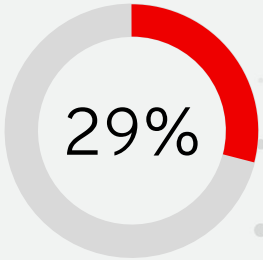
Portion of alerts coming in that the average security team examines every day



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:

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

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

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

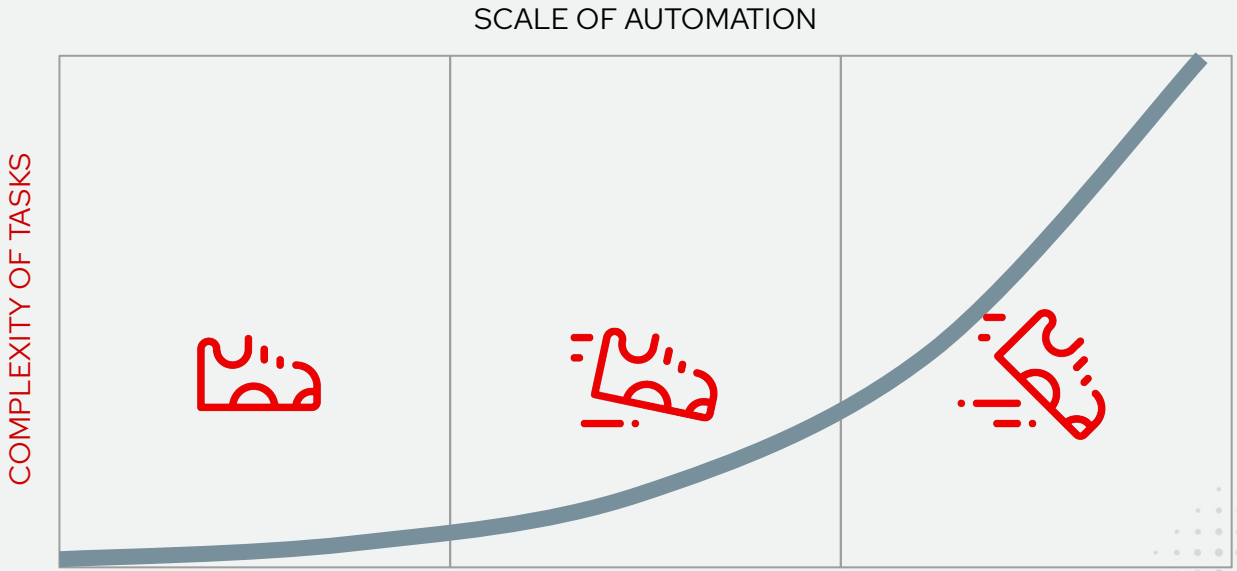
SANS Institute

AnsibleFest

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

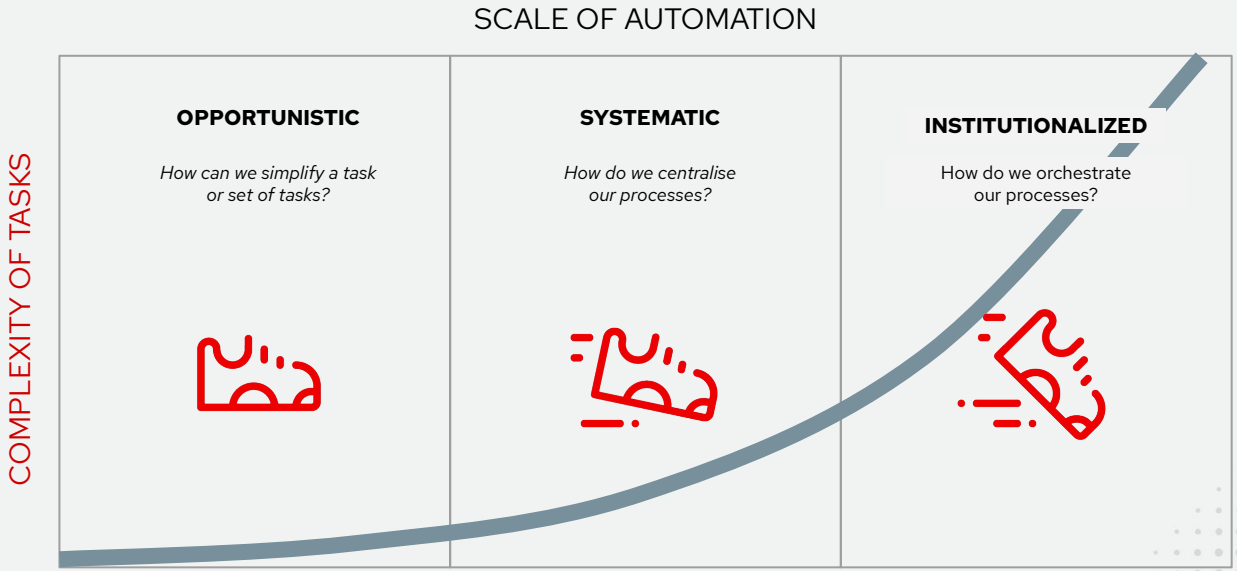
Automation is a Journey

Start simple and small. Improve iteratively



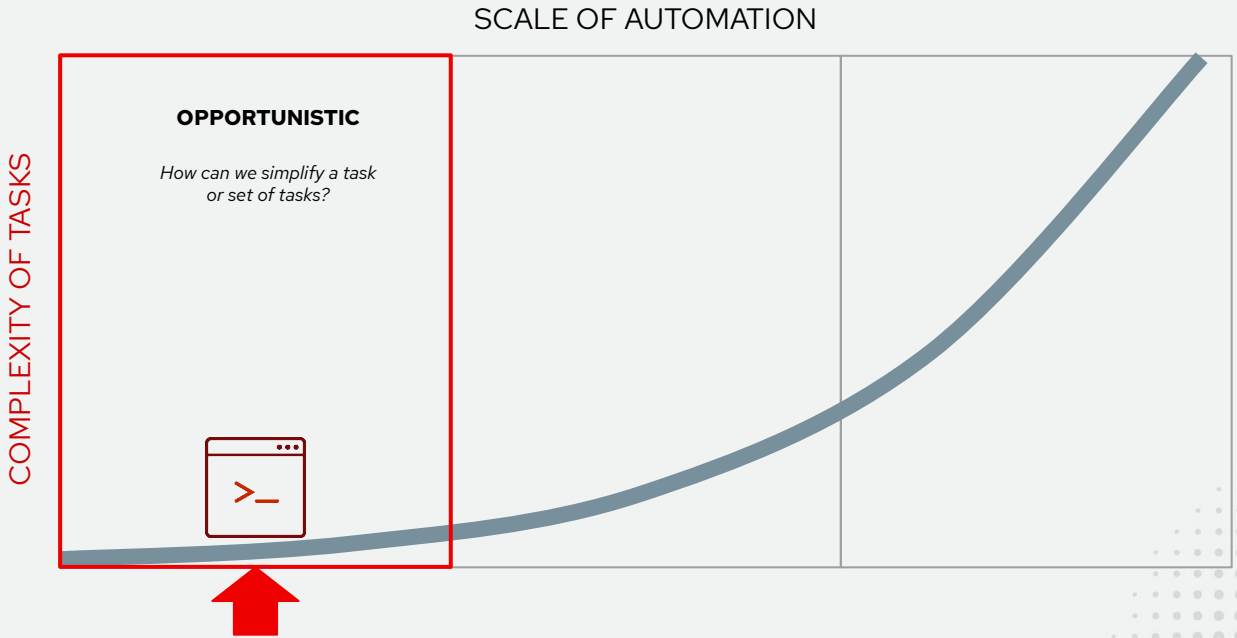
The Security Automation Journey

Start simple and small. Improve iteratively



The Security Automation Journey

Start simple and small. Improve iteratively



The values automation brings to Security

Security Automation 101

INCREASE 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

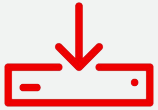
ENFORCE CONSISTENCY

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

Security Automation 101

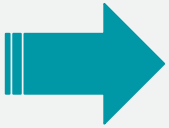
The values automation brings to Security

IT Operations



OS CONFIGURATION MANAGEMENT

Predictable and repeatable process, mitigating risks of service downtime.



Security Operations

FIREWALL POLICIES MANAGEMENT

Automate rule modification and decommissioning to improve performance and ultimately strengthen security reducing the potential attack surface.

Security Automation 101

The values automation brings to Security

INCIDENT RESPONSE

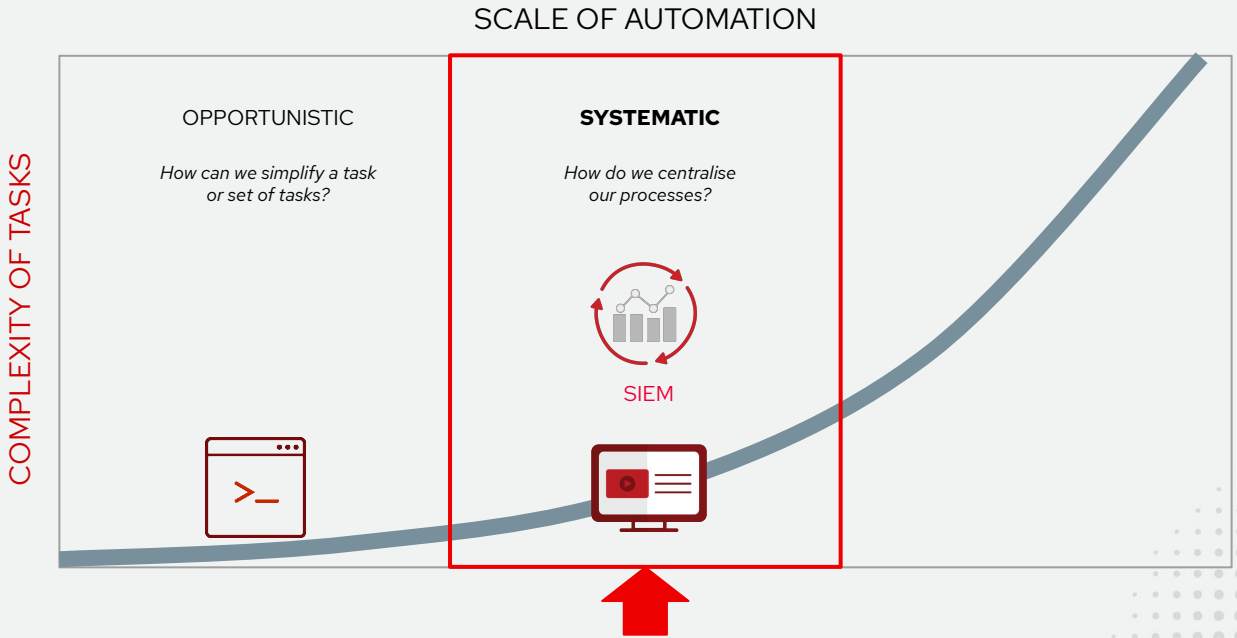
Creating new security policies to grant access, block or quarantine a machine.

```
- hosts: checkpoint
  connection: httpapi
  tasks:
  - name: Create blacklist IP
    include_role:
      name: acl_manager
      tasks_from: blacklist_ip
    vars:
        source_ip: “{{ attacker_ip }}”
        destination_ip: “{{ target_ip }}”
        ansible_network_os: checkpoint
```

Check Point
SOFTWARE TECHNOLOGIES LTD

The Security Automation Journey

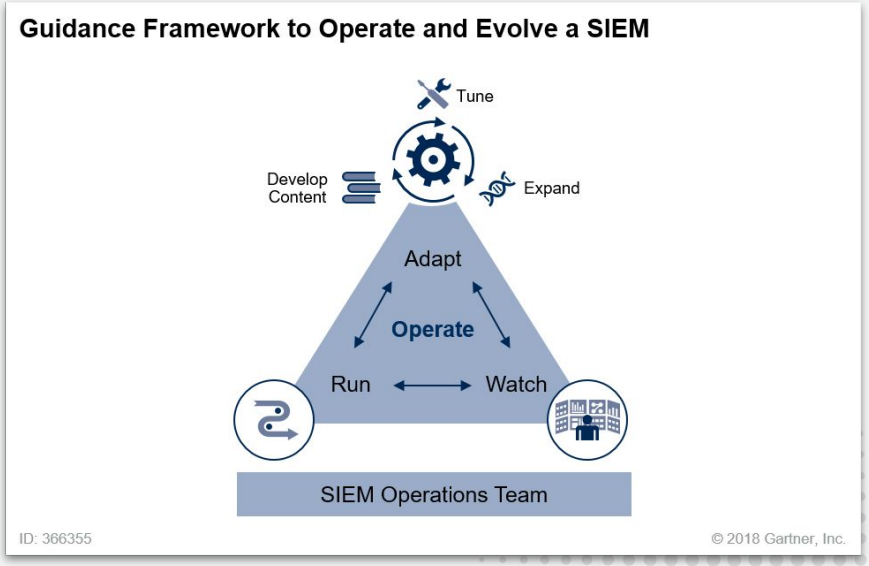
Start simple and small. Improve iteratively



What is a SIEM?

Security Automation 201

> Gartner defines the security and information event management (SIEM) market by the customer's need to analyze event data in real time for **early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response**, forensics and regulatory compliance. SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications.



Security Automation 201

The values automation brings to SIEM

SIMPLICITY

Automate deployment, configuration and mundane tasks

CONSISTENCY

Interoperate multiple platforms from multiple vendors

MODERNIZATION

Integrate SIEM in DevSecOps workflows

EXTENSIBILITY

Automate investigation & remediation tasks from the SIEM

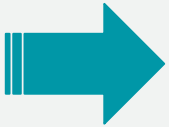
Security Automation 201

The values automation brings to SIEM

Lines of Business

AUTOMATION SERVICE CATALOG

Enabling self-service access to IT Operations assets.



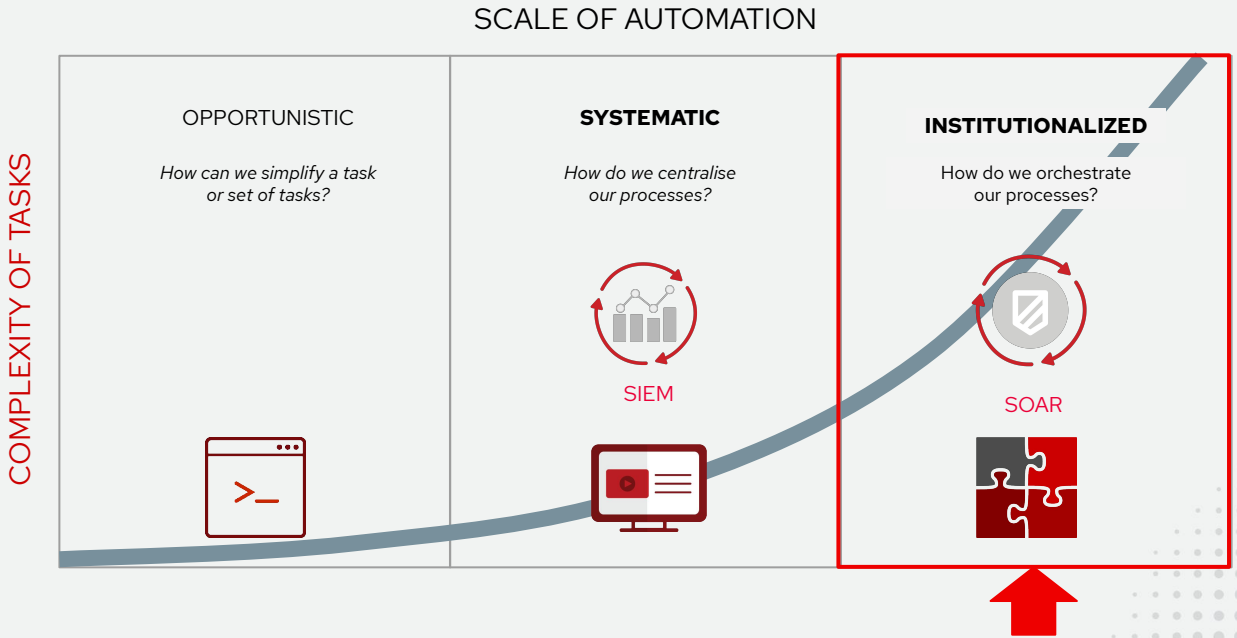
Security Analysts

SIEM INTEGRATION

Reusing the assets created by security operations to automate investigation & remediation tasks directly from the SIEM UI

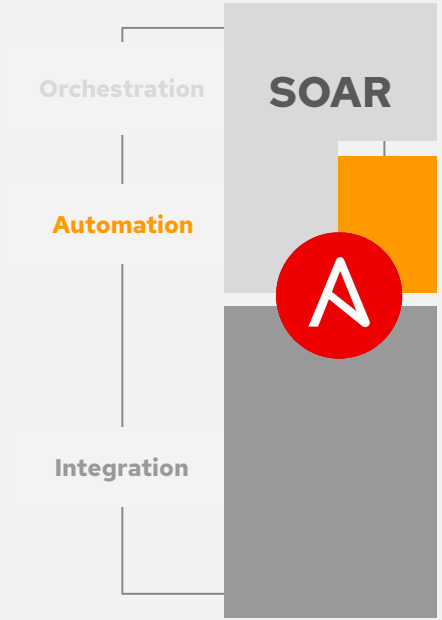
The Security Automation Journey

Start simple and small. Improve iteratively



How Ansible security automation relates to SOAR?

Security Automation 301



SOAR orchestrates the high-level threat response process. Their Security 'Playbooks' focus on Who is doing What, Why and When.

The Ansible Automation Platform automates tasks: the How.

The Ansible Automation Platform content initiatives, like Ansible security automation, provide technology integration: the Where.

Security Automation 301

The values automation brings to SOAR

COLLABORATION

Makes security a team play

ECOSYSTEM

Removes integration challenges

SIMPLICITY

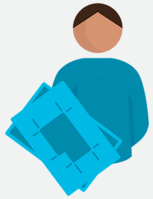
Makes security experts productive faster

ACCESSIBILITY

Enables quick wins from the beginning

Security Automation 301

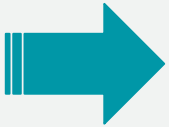
The values automation brings to SIEM



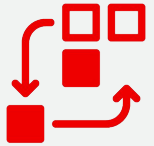
Business Process Owners

ITSM INTEGRATION

Connecting automation jobs to business processes.



Security Analysts

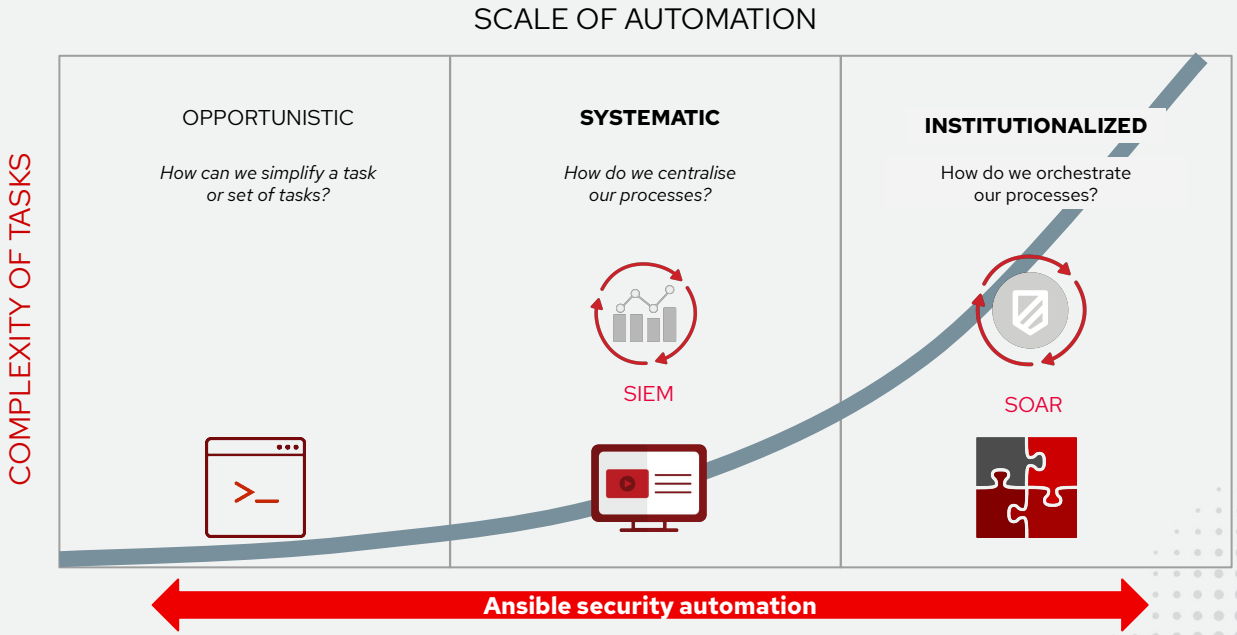


SOAR INTEGRATION

Integrating cross-functional automation assets into investigation & response processes.

The Security Automation Journey

Start simple and small. Improve iteratively



So what's in for you?

Become the automation rockstar!

Contribute to the growth of automation in your organization

Automation expertise is among the most desirable and lucrative skills for I&O technical professionals. Gartner predicts that, through 2023, I&O staff with automation skills will command up to a 40% salary premium versus those without.

Gartner

Source:
Essential Skills for Automation Engineers

Accelerate your career!

Find the pockets of ad hoc automation in your company, and grow them into a formal automation program. Bottom-up automation initiatives that grow organically are more likely to succeed than top-down, mandate-driven projects.

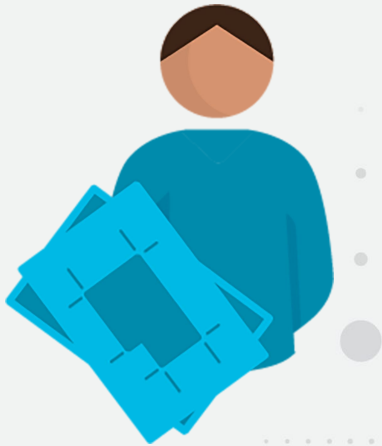
Gartner

Source:
Essential Skills for Automation Engineers

Become an Automation Architect

Find the pockets of ad hoc automation in your company, and grow them into a formal automation program. Bottom-up automation initiatives that grow organically are more likely to succeed than top-down, mandate-driven projects.

Gartner



Source:
Essential Skills for Automation Architects

Where do I start?

Get Started

Security automation on ansible.com

Simplify your security operations center - **eBook**

Join the Community

Security automation community wiki

Blog posts

#ansible-security on irc.freenode.net

Check out the Code

Ansible security on Ansible Galaxy

Check Point collections

Cisco ASA collection

Cyberark collections

F5 Networks collections

Fortinet collections

IBM Qradar collection

Splunk Enterprise Security collection

Tirasa Syncope collection

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.

youtube.com/user/RedHatVideos

linkedin.com/company/Red-Hat

facebook.com/ansibleautomation

twitter.com/ansible