

# ANSIBLE SECURITY AUTOMATION

February 2021

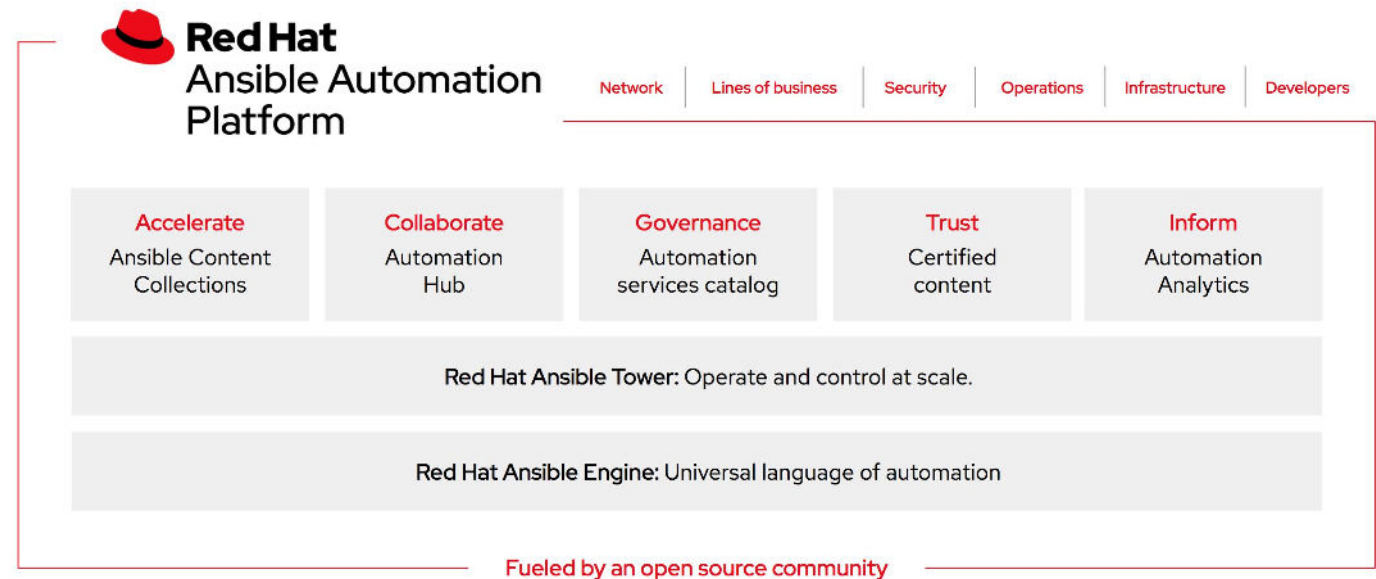
Speaker Name  
Job Title

Corporate Mail  
Twitter Handler

# What Is Ansible Automation Platform?

## Ansible Automation Platform

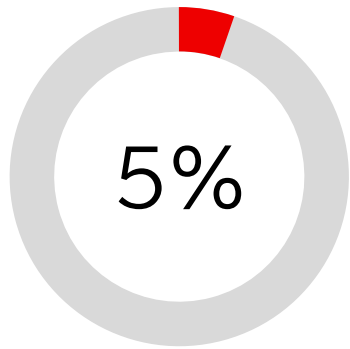
is Red Hat's enterprise automation platform to automate the provisioning and configuration of modern enterprise IT environments, from compute resources, like VMs and containers, to networks, all the way to the application layer.



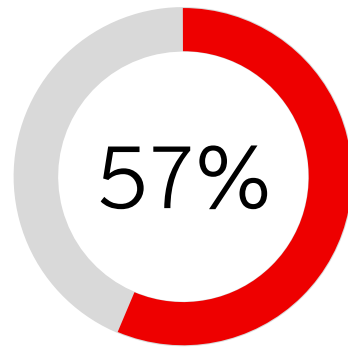
# Introducing Ansible security automation



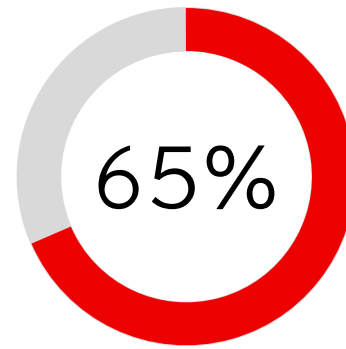
# Why Ansible security automation?



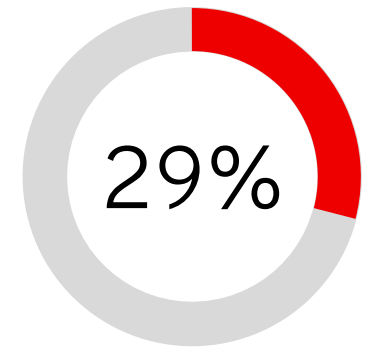
Portion of alerts coming in that the average security team examines every day



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

“““

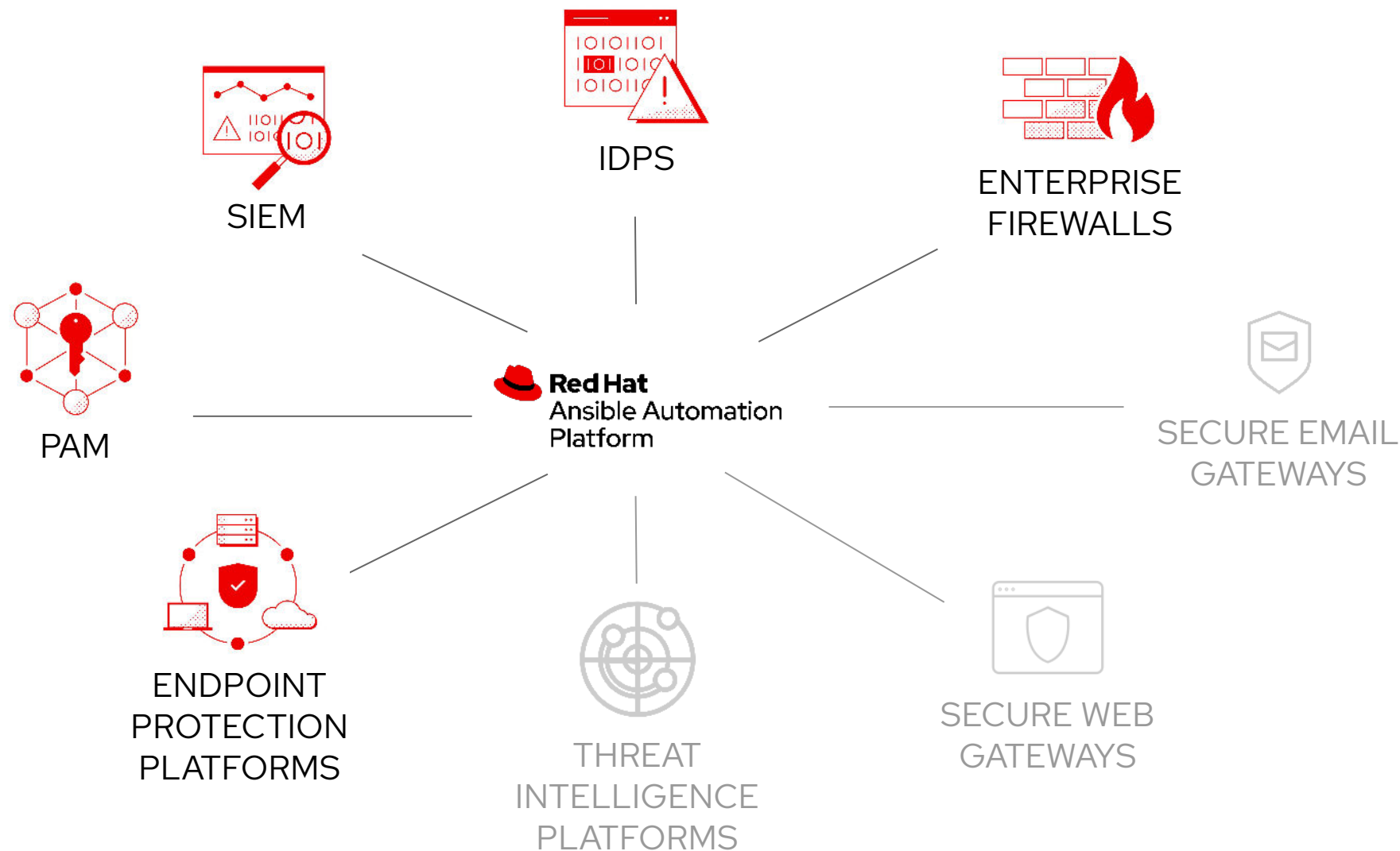


**‘Lack of automation and orchestration’**  
ranked second and  
**‘Too many tools that are not integrated’**  
ranked third on the list of SOC challenges.

---

SANS Institute

# What Is Ansible security automation?



# 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.

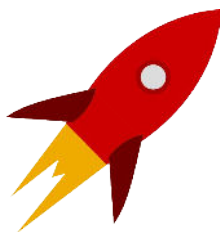
By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.



Red Hat will not become a security vendor, we want to be a security enabler.

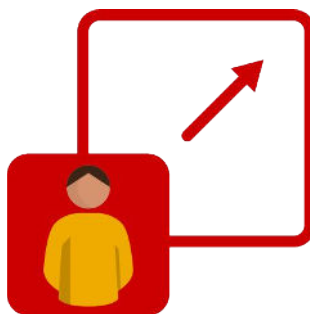


# How Automation solves today's security operations challenges



## 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

# Who Is It For?



## Security Teams In Large Organizations

Security Operations Centres (SOCs)  
dealing with increasingly fast and  
complex attacks



## Managed Security Service Providers

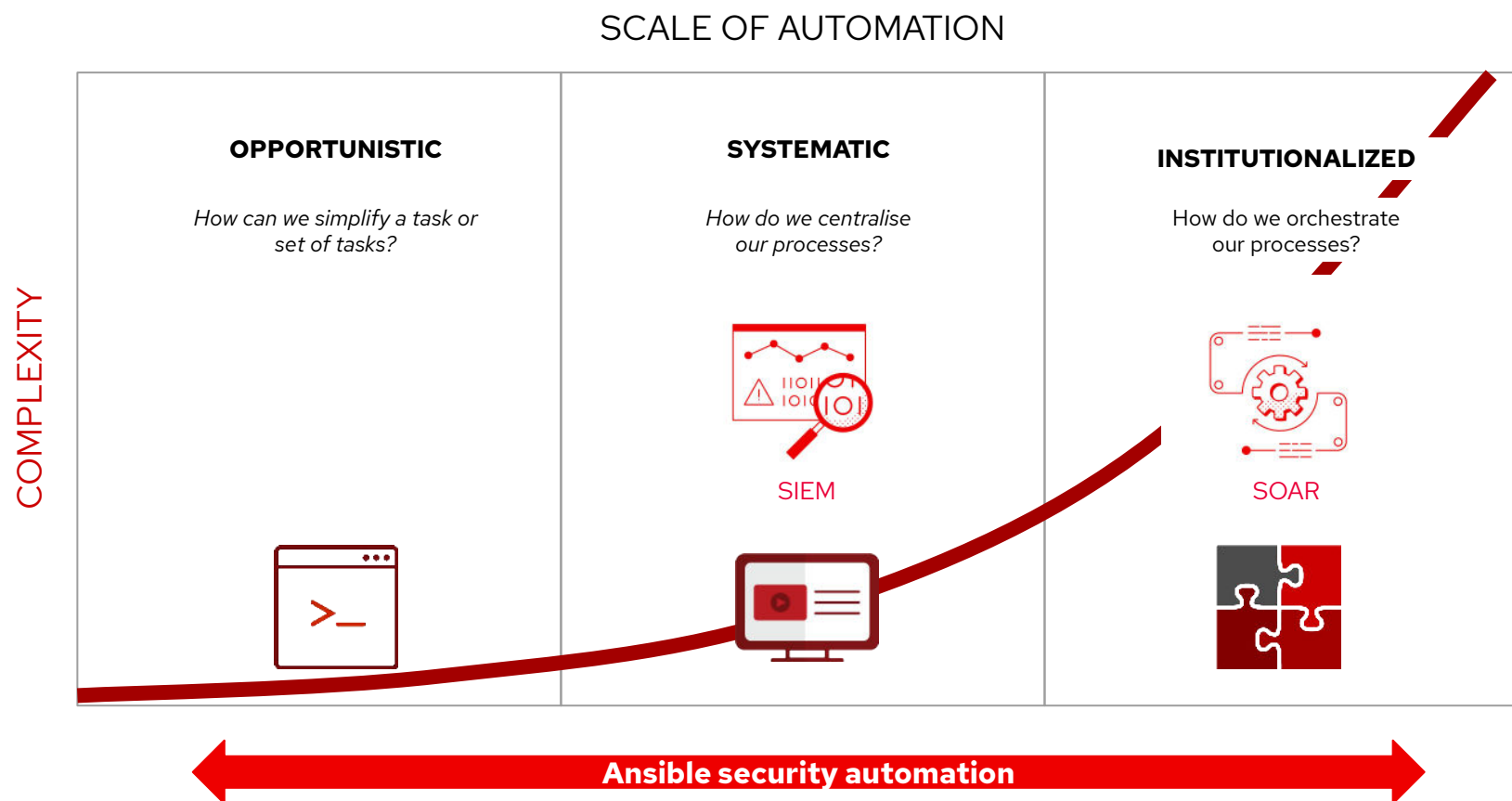
Dealing with thousands of security  
solutions across their whole customer  
base



## Security ISVs

Offering solutions for security analytics,  
intelligence, response and orchestration

# How customers adopt security automation?



# What Does It Do?



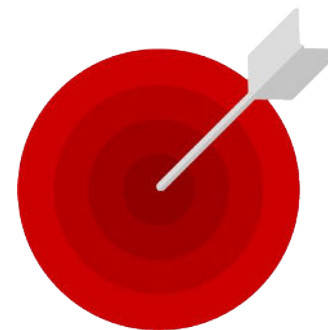
## Investigation Enrichment

Enabling programmatic access to log configurations such as destination, verbosity, etc.



## Threat Hunting

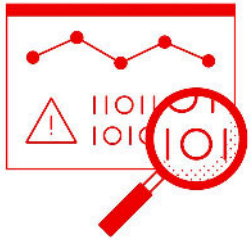
Automate alerts, correlation searches and signature manipulation to preemptively identify threats



## Incident Response

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

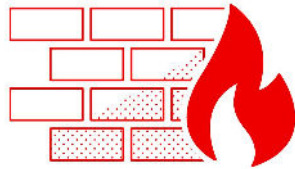
# Ansible Security Ecosystem



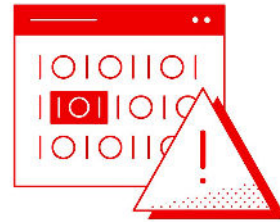
**Security Information &  
Events Management**

splunk>

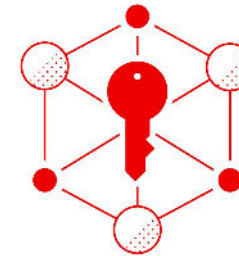
IBM



**Enterprise  
Firewalls**



**Intrusion Detection &  
Prevention Systems**



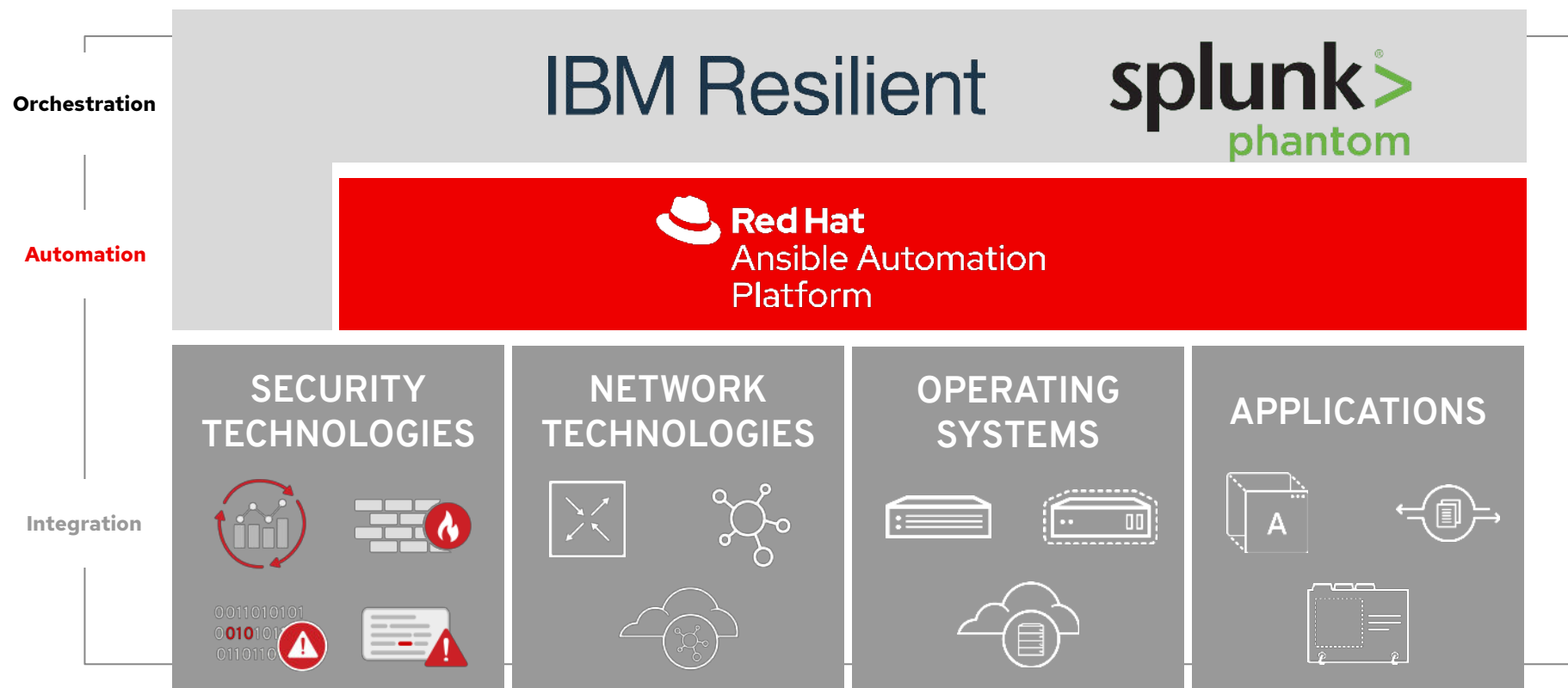
**Privileged Access  
Management**



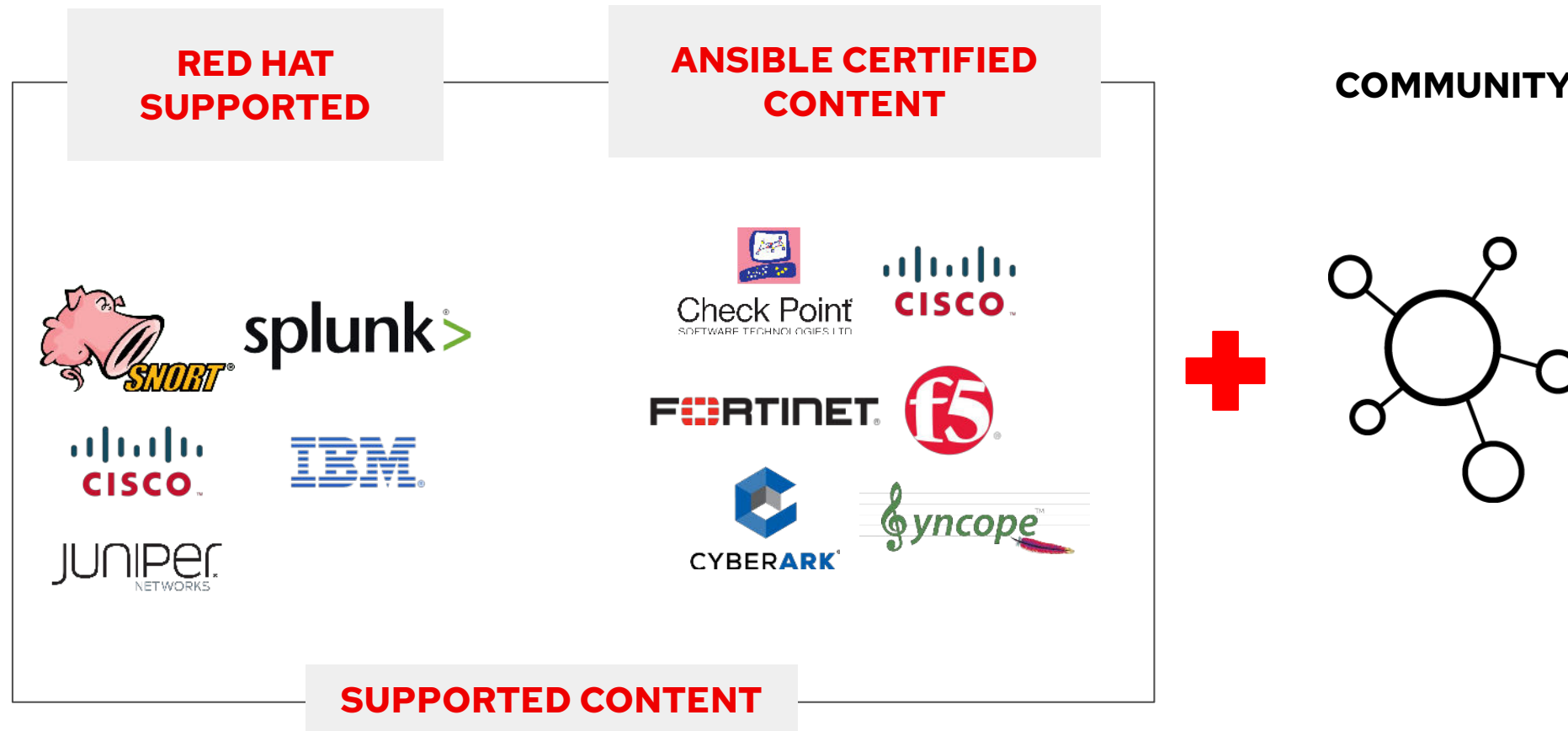
**Endpoint Protection**



# Ansible Automation Platform Integration With SOAR

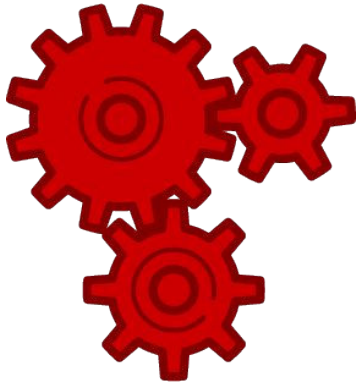


# Ok, But In The End What's In The Solution?



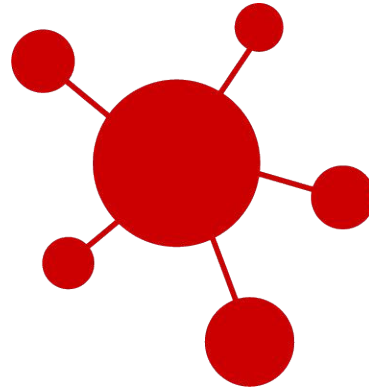
# Value For Non-Security Professionals

Integrating Well With Existing Automation Efforts



## IT Operations

Add new security profiles to existing deployment use cases.  
Extends compliance to contain security technologies.



## Network Operations

Expand firewalls support.  
Extend networking use cases with network security.



## Team Cooperation

Make security consumable to others.  
Integrate security procedures with operation and development workflows.



# Relevant Resources



## Get Started

Security automation on [ansible.com](#)

Simplify your security operations center - **eBook**



## 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




## Join the Community

Security automation community wiki


Blog posts

#ansible-security on [irc.freenode.net](#)

# Thanks

 [linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)

 [facebook.com/redhatinc](https://facebook.com/redhatinc)

 [youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)

 [twitter.com/RedHat](https://twitter.com/RedHat)