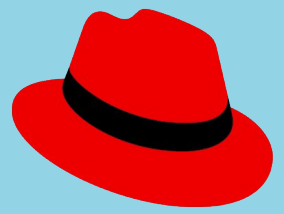


Red Hat

Chris Jenkins

Unleashing Ansible Security Automation

Principal Chief Architect
Cybersecurity Strategy & Adoption
Red Hat

Red Hat

I ask CISOs what keeps them awake at night, here's my favourite answer:

"People who work in my organisation and people who don't"

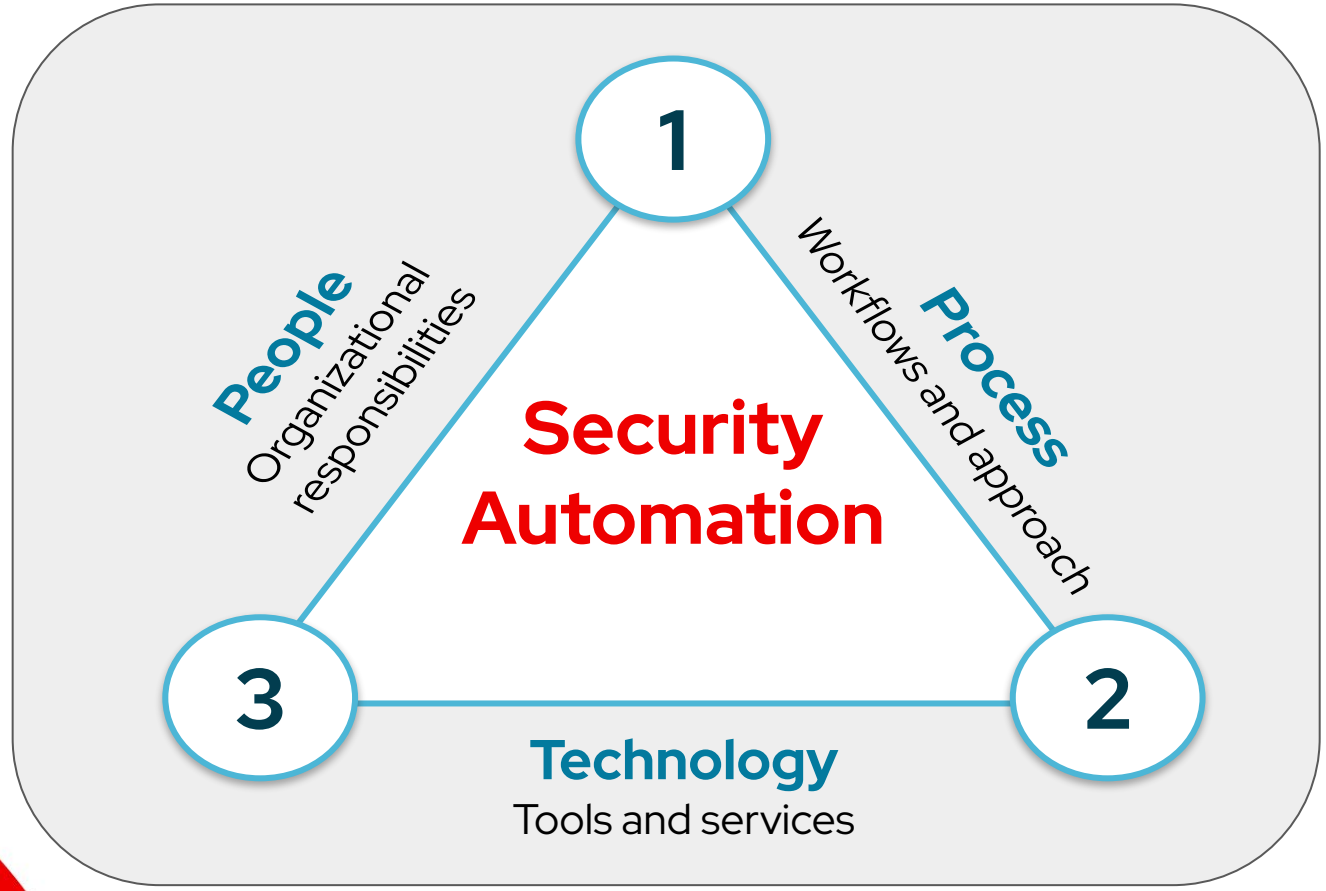
Photo by Sander Sammy on Unsplash

Red Hat

It’s more than just tech ….

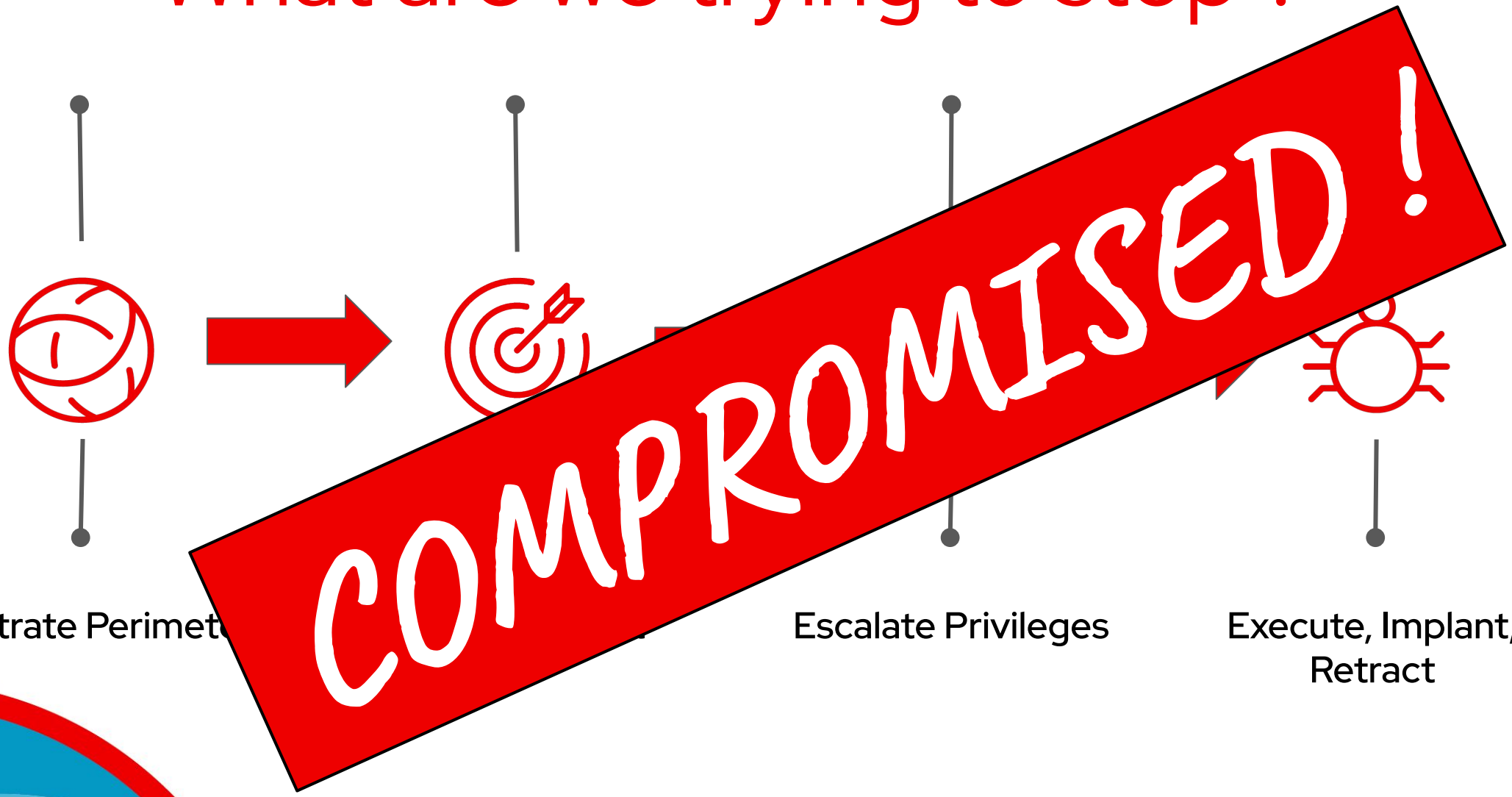
Not all security challenges can be resolved or mitigated through the use of purely technical techniques.

We also need to focus on the People, Process, Technology and cultural issues when addressing customers security concerns.



Red Hat

What are we trying to stop ?



Red Hat

Security Challenges

What do we hear from our customers?

Challenge #1 - Cyber Threats

Threat actors are constantly developing new tactics and techniques to breach security defenses and customers need to constantly re-asses their security processes.

Challenge #2 - Lack of awareness and education

Some employees are not aware of the risks associated with cybersecurity or how to protect themselves and their organizations from cyber attacks.

Challenge #3 - Complexity of IT

The growing complexity of IT infrastructure, with a combination of on-premises, cloud, and hybrid systems, can make it difficult to provide holistic observability and implement consistent security policies across all systems.

Red Hat

Security Challenges

What do we hear from our customers?

Challenge #4 - Software Supply Chain Management

Software supply chain security combines best practices from risk management and cybersecurity to mitigate against risks that may inadvertently be incorporated during the in-house development of software.

Challenge #5 - Third-party risks

Organizations often rely on third-party vendors for various services and products but these third parties may not have adequate security measures in place which can create vulnerabilities in the organization's overall security posture.

Challenge #6 - Regulatory compliance

Many organizations must comply with various regulations related to data privacy and security, which can be challenging to implement and maintain, especially as regulations continue to evolve.

Red Hat

Security must be continuous

Identify security requirements & governance models

FedRAMP

NIST National Institute of Standards and Technology U.S. Department of Commerce

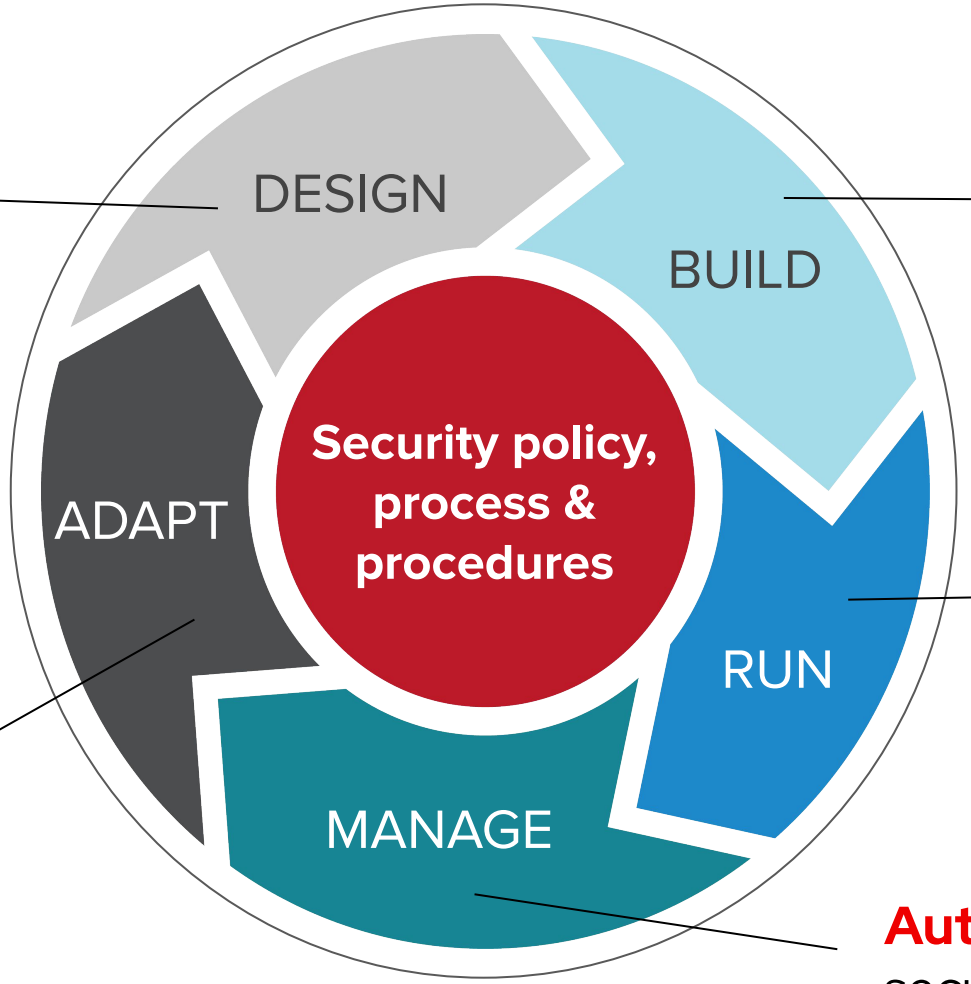
CIS Center for Internet Security

National Cyber Security Centre

PCI Security Standards Council

HIPAA Health Insurance Portability & Accountability Act

Revise, update, remediate as the landscape changes



Built-in from the start; not bolted-on

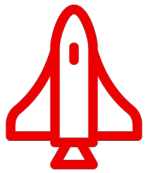
Deploy to trusted platforms with enhanced security capabilities

Automate system config, security & compliance

Red Hat

Security Automation Benefits

Security Automation 101



INCREASE SPEED

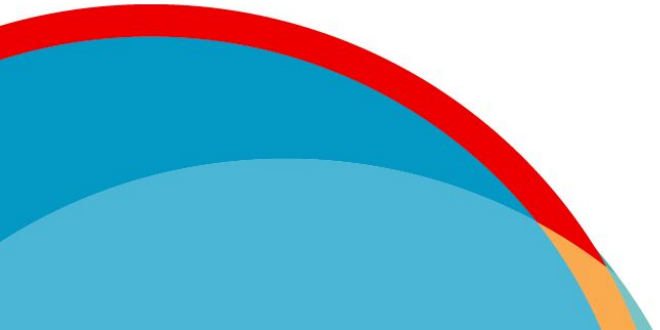
Reduce the number of manual steps and GUI-clicking, enable the orchestration of security tools and accelerate their interaction with each other

REDUCE HUMAN ERRORS

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

ENFORCE CONSISTENCY

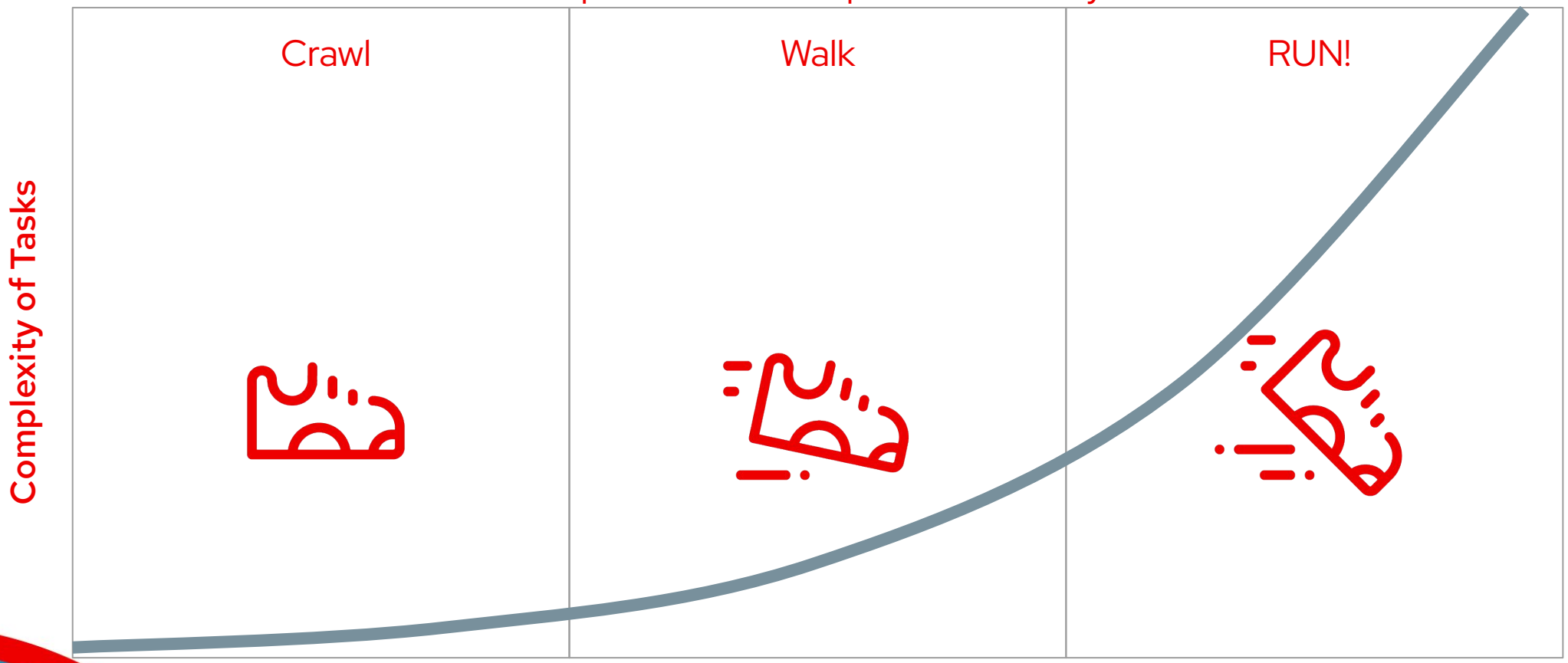
Enable auditable and verifiable security processes by using a single tool and common language covering multiple security tools



Red Hat

Security automation is a journey

Start simple and small. Improve iteratively



Red Hat

Is automation a security solution?

No!

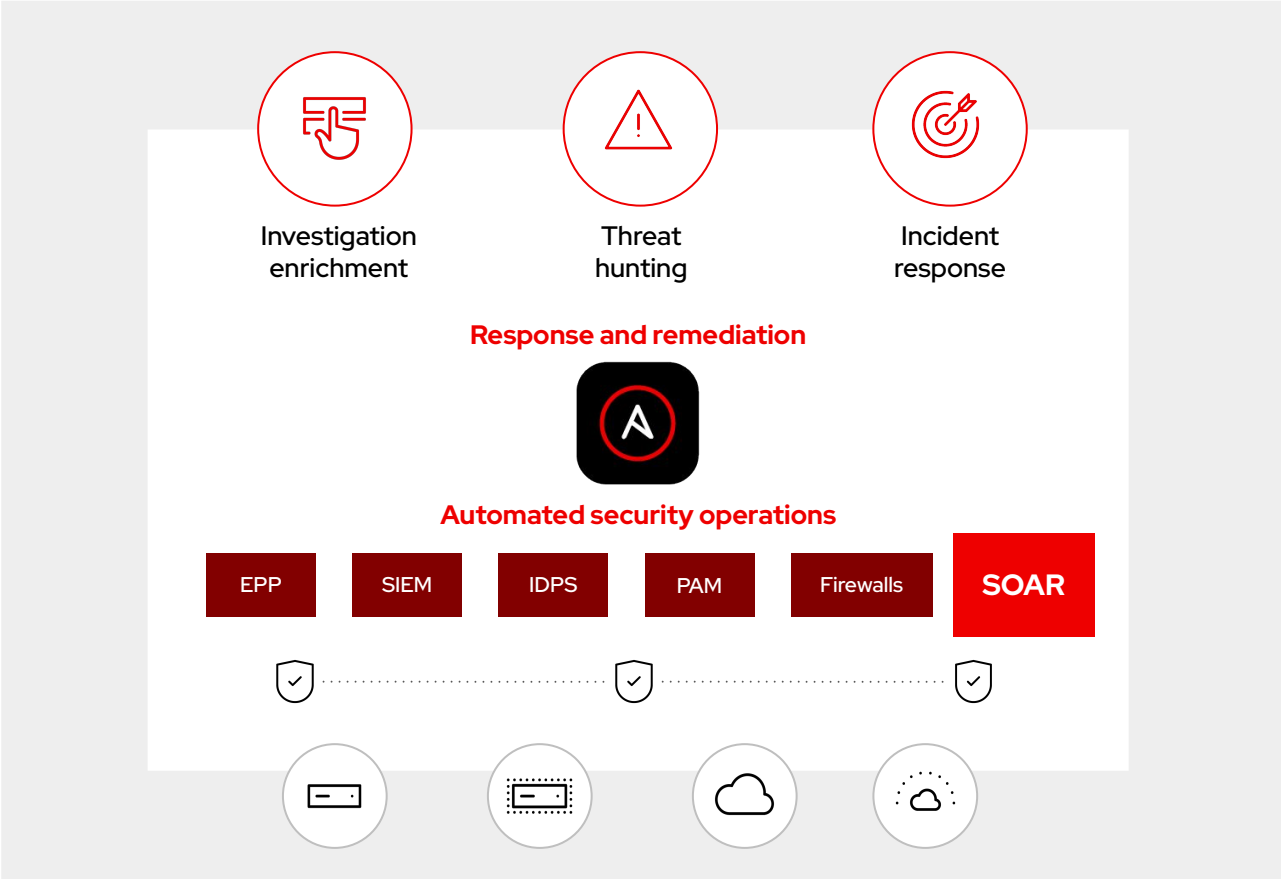
Ansible can help Security teams “stitch together” the numerous security solutions and tools already in their IT environment for a more effective cyber defense.

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.

Ansible security automation is a security enabler

Red Hat

Security Automation



Investigation enrichment

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

Threat hunting

Automating alerts, correlation searches, and signature manipulation

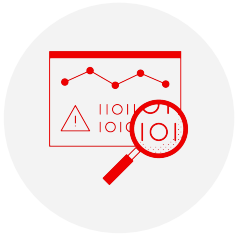
Incident response

Creating new security policies to whitelist, blacklist, or quarantine a machine

Red Hat

Ansible Security Ecosystem

Certified Content Collections



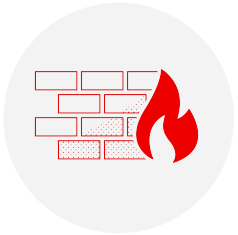
Security Information & Events Management

splunk>

Enterprise Security

IBM

QRadar



Enterprise Firewalls

Check Point
SOFTWARE TECHNOLOGIES LTD

Next Generation Firewall
GAIA OS

paloalto NETWORKS

Palo Alto Networks

CISCO

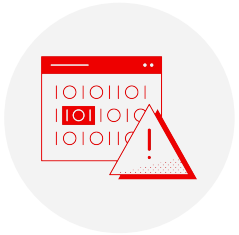
Adaptive Security Appliance

f5

Advanced Firewall Manager

FORTINET

JUNIPER NETWORKS



Intrusion Detection & Prevention Systems

Check Point
SOFTWARE TECHNOLOGIES LTD

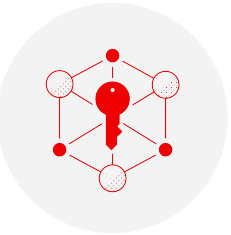
IPS Blade

FORTINET

Fortigate: IPS

SNORT

Intrusion Detection System



Privileged Access Management

CYBERARK

PAM

syncope

Apache Syncope

IBM

ISAM

Endpoint Protection

CROWDSTRIKE

Falcon

TREND MICRO

Deep Security

Red Hat

Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat

Red Hat