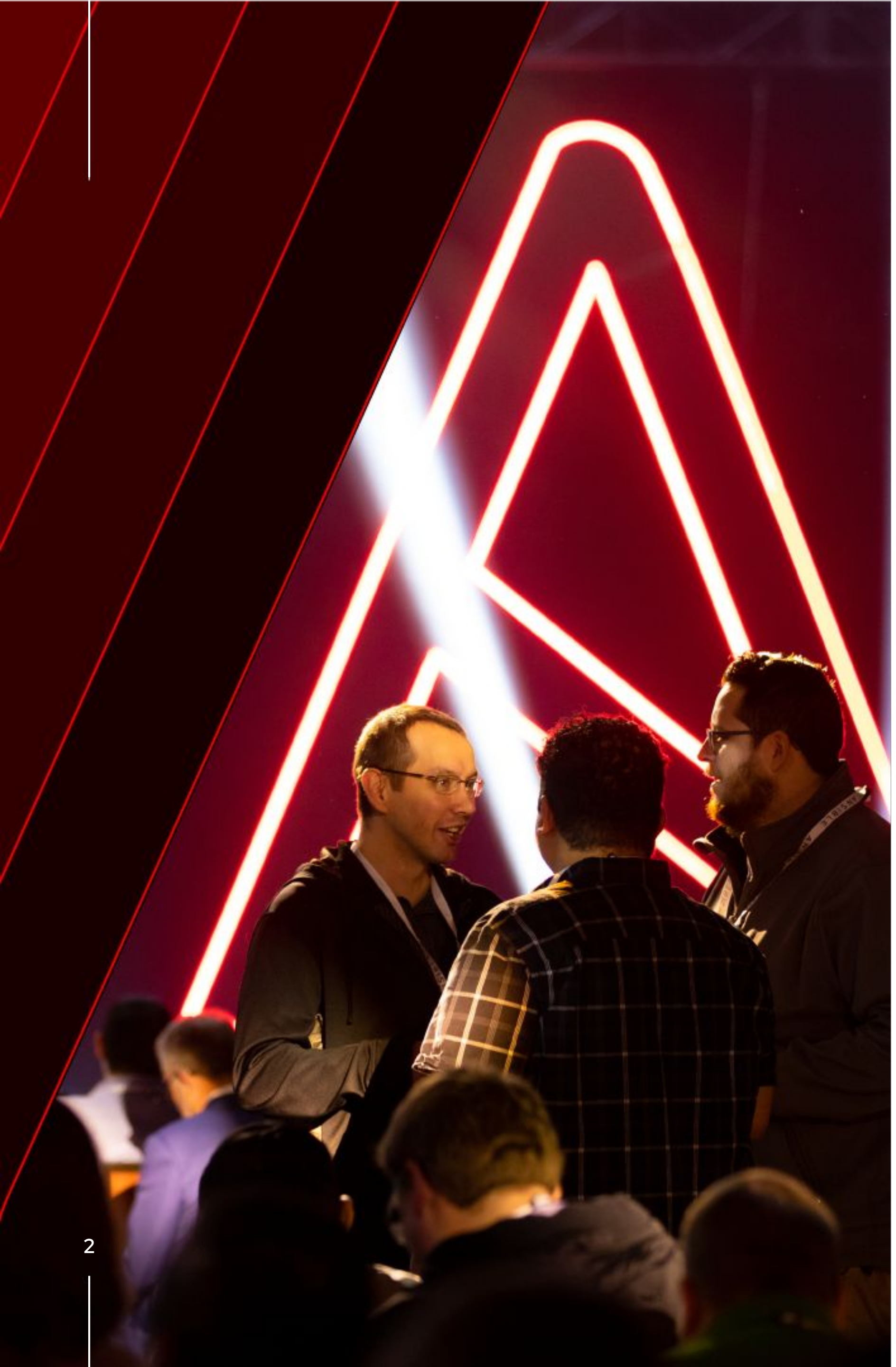
Red Hat
Ansible Automation
Platform

Streamlining Security

Unleashing Ansible Automation

Chris Jenkins
Principal Chief Architect,
Global Engineering

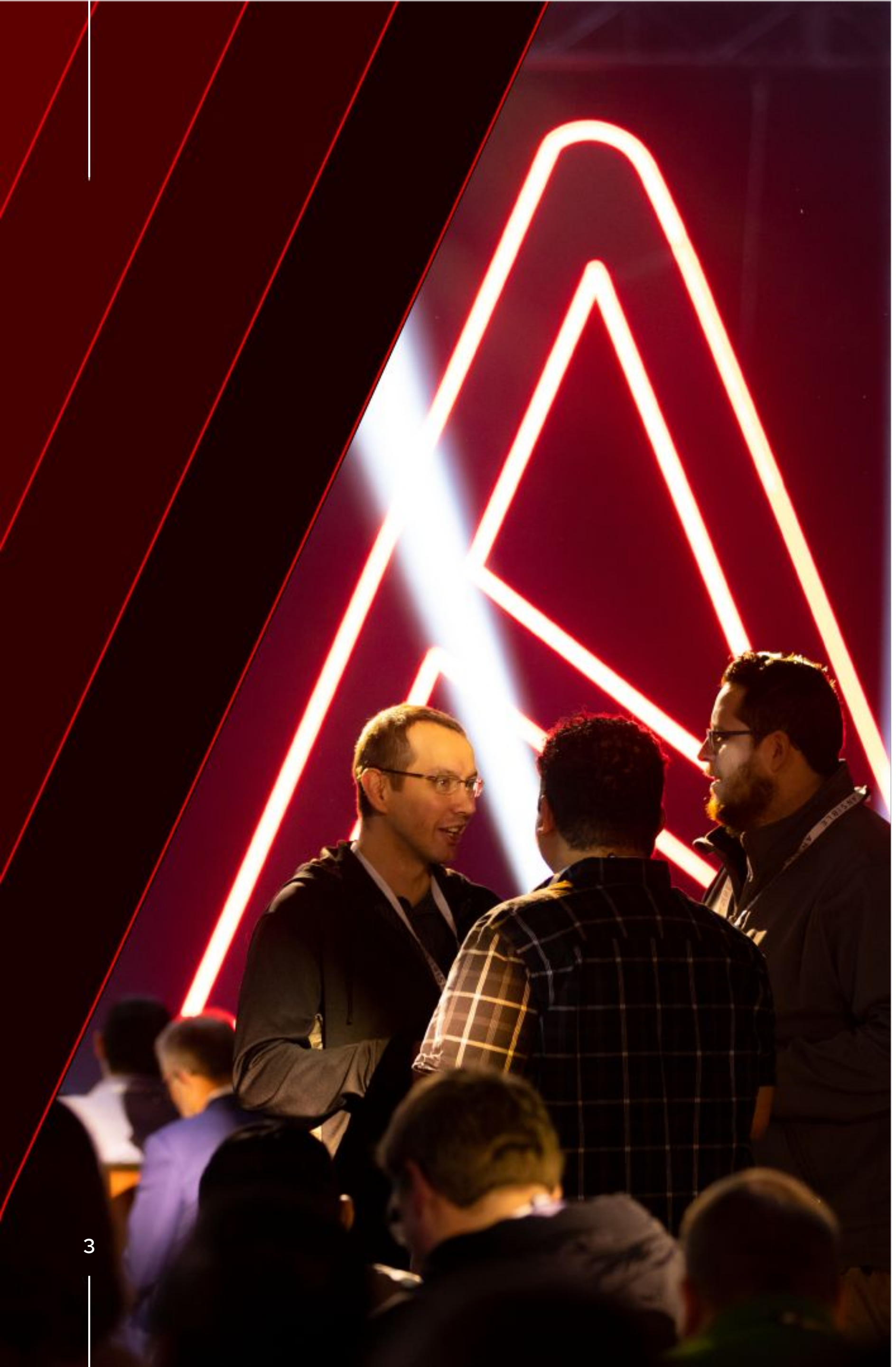
Matt York
Senior Specialist Solution Architect, Ansible



From today's Keynote Speech

"The top 2 skills in demand at the moment are cybersecurity and automation"

You're in the right session for both!



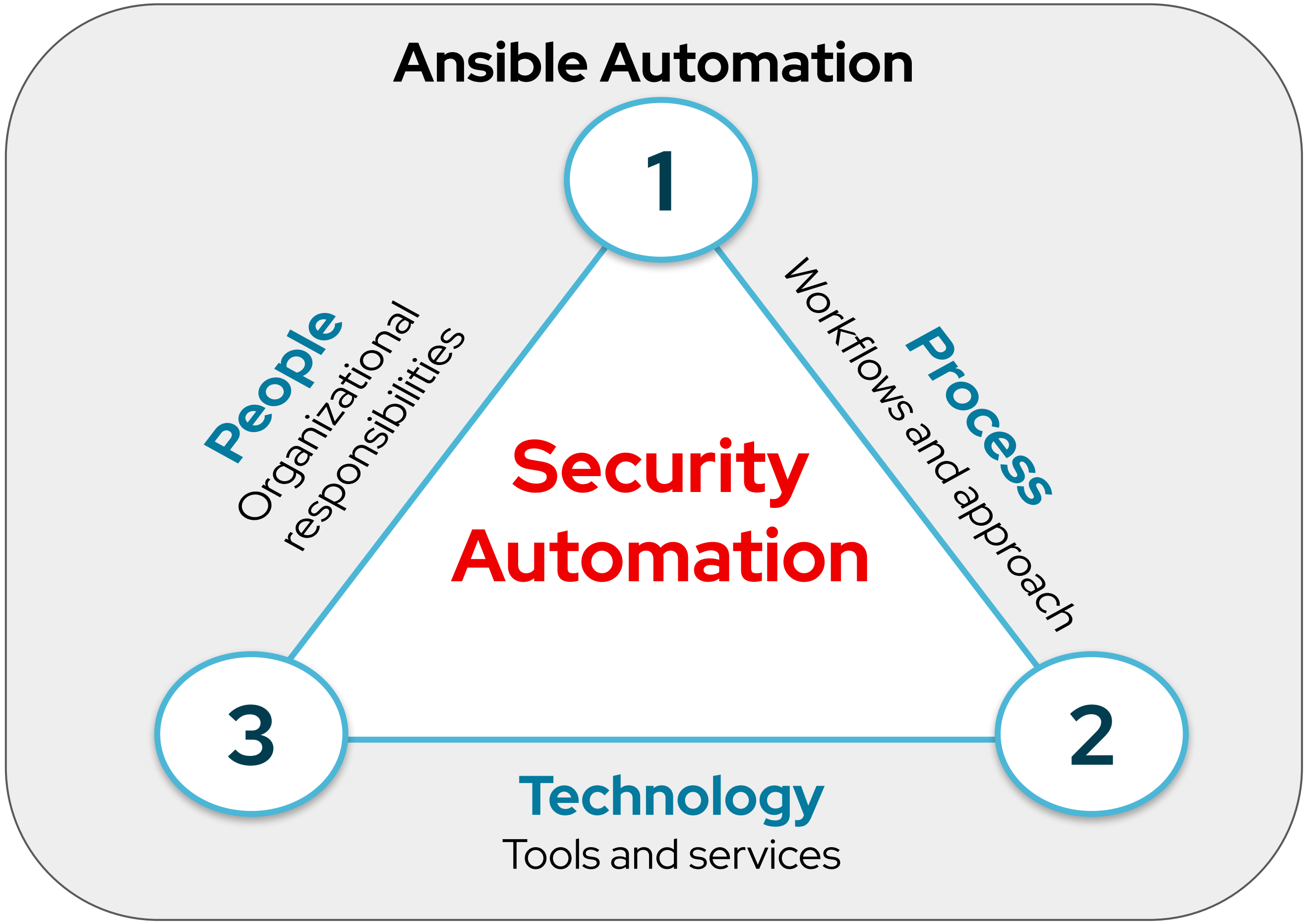
I ask CISOs what keeps them awake at night, here's my favourite answer:

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

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.



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.

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.

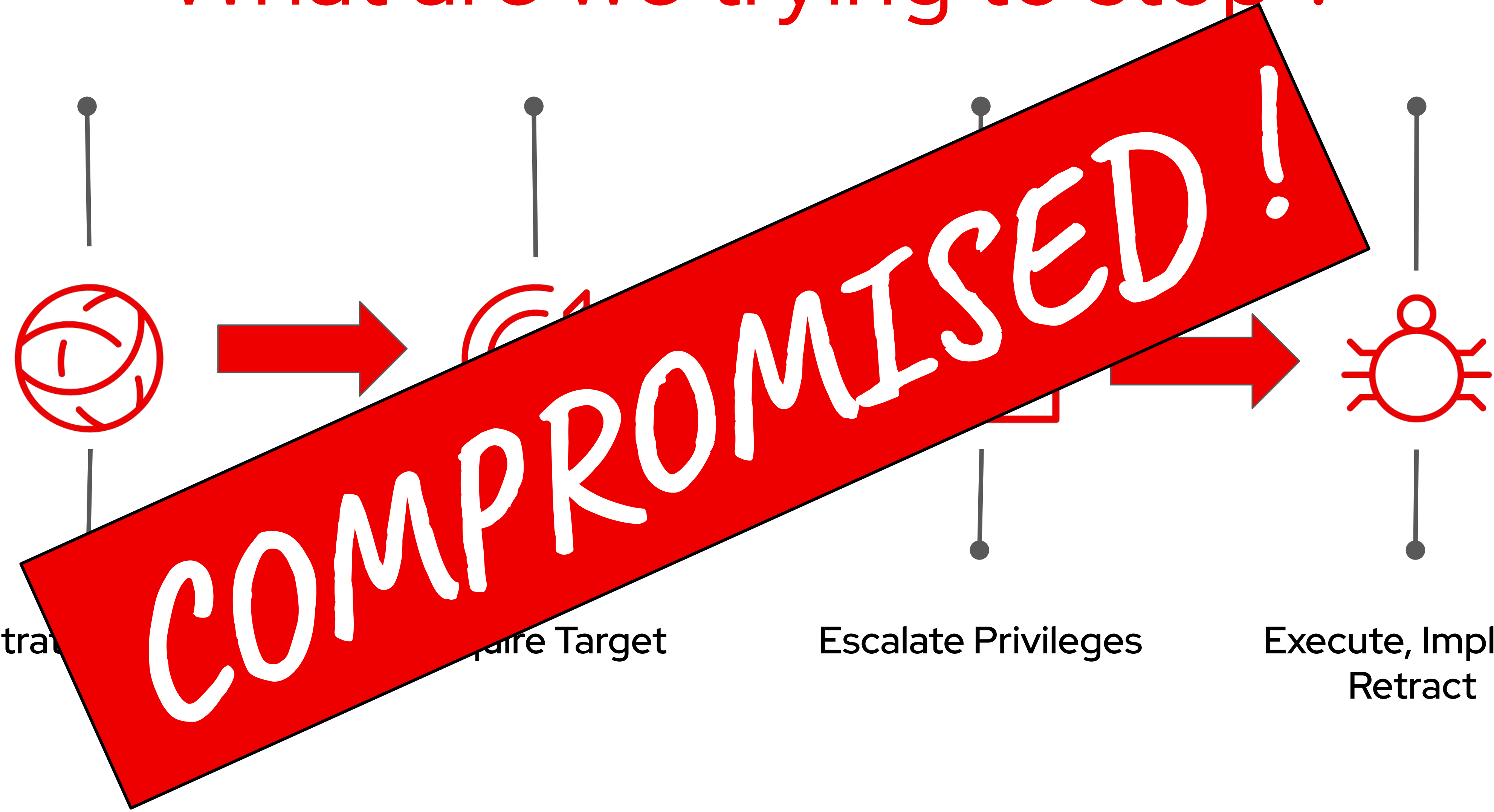
Challenge #5 – Third-party risks

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.

What are we trying to stop ?



COMPROMISED !

Penetrat

uire Target

Escalate Privileges

Execute, Implant, Retract

Security must be continuous

Identify security requirements & governance models

FedRAMP

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

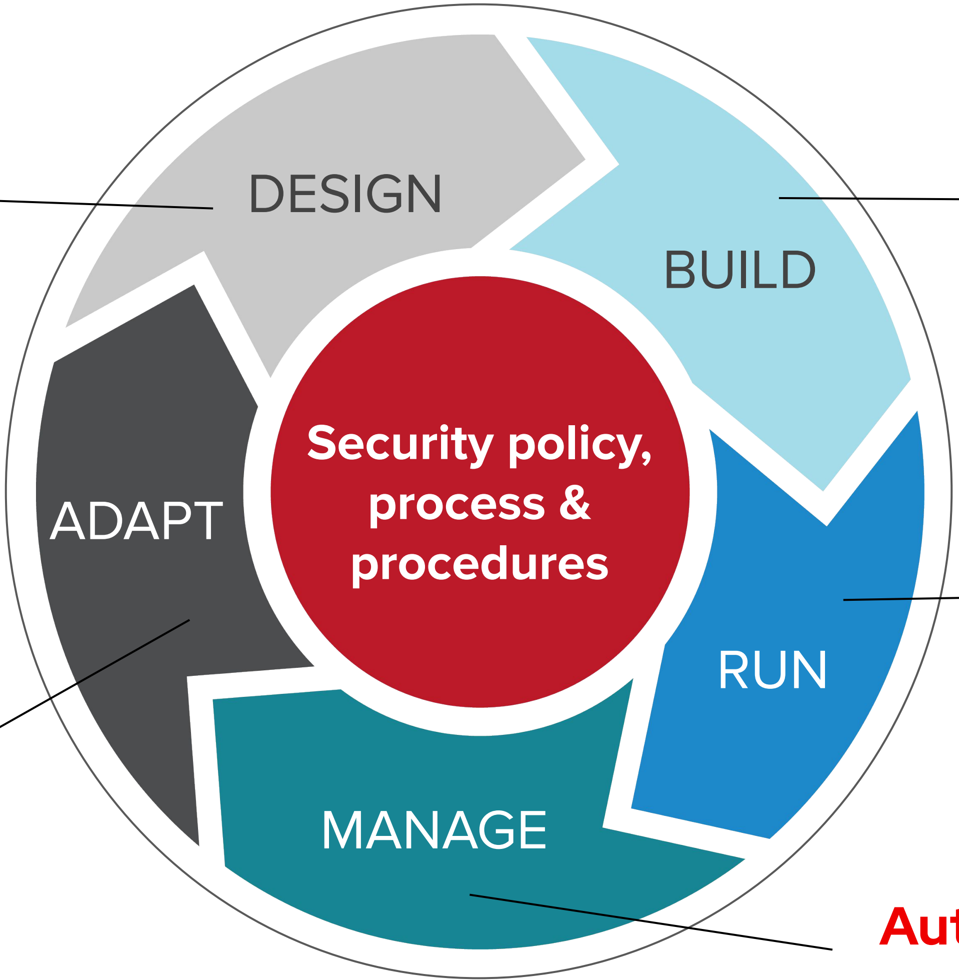
CIS Center for Internet Security

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

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

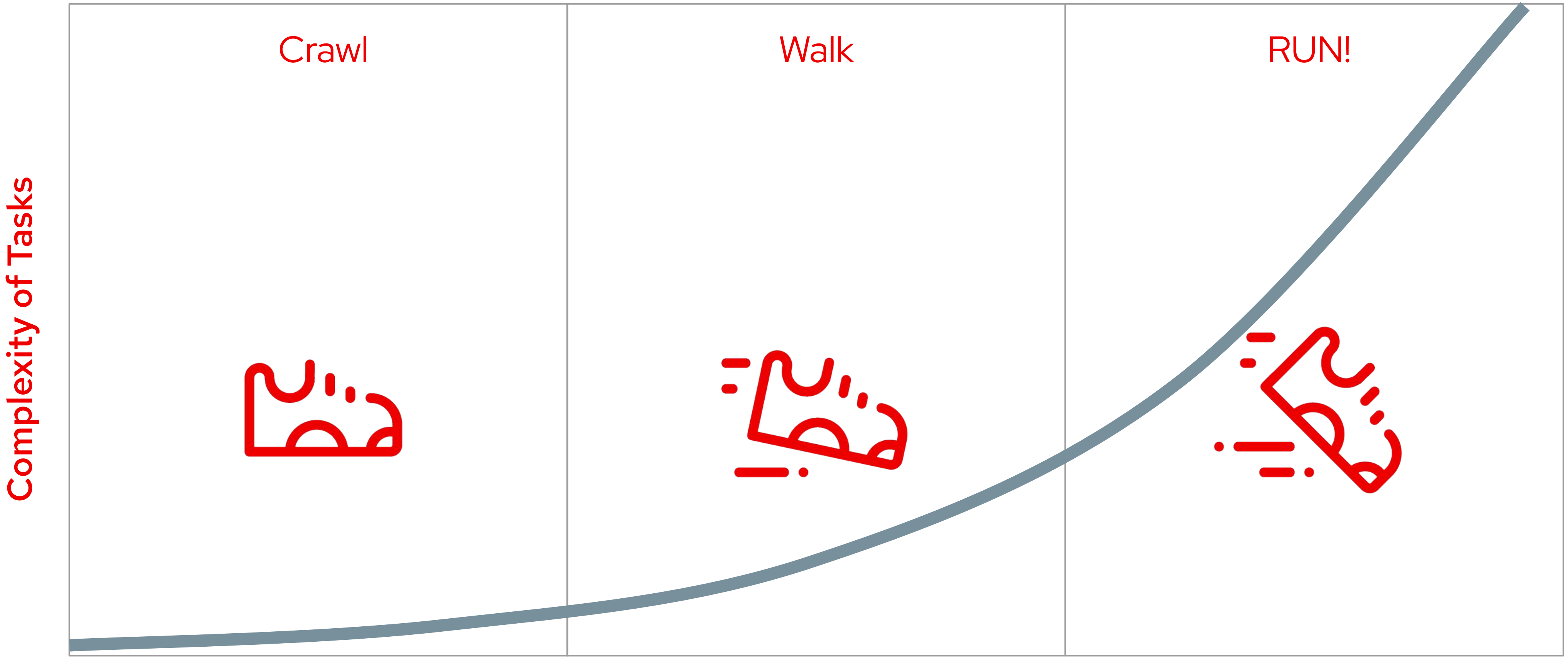
Minimize risks with automated workflows, avoid human operator errors in time-sensitive, stressful situations

ENFORCE CONSISTENCY

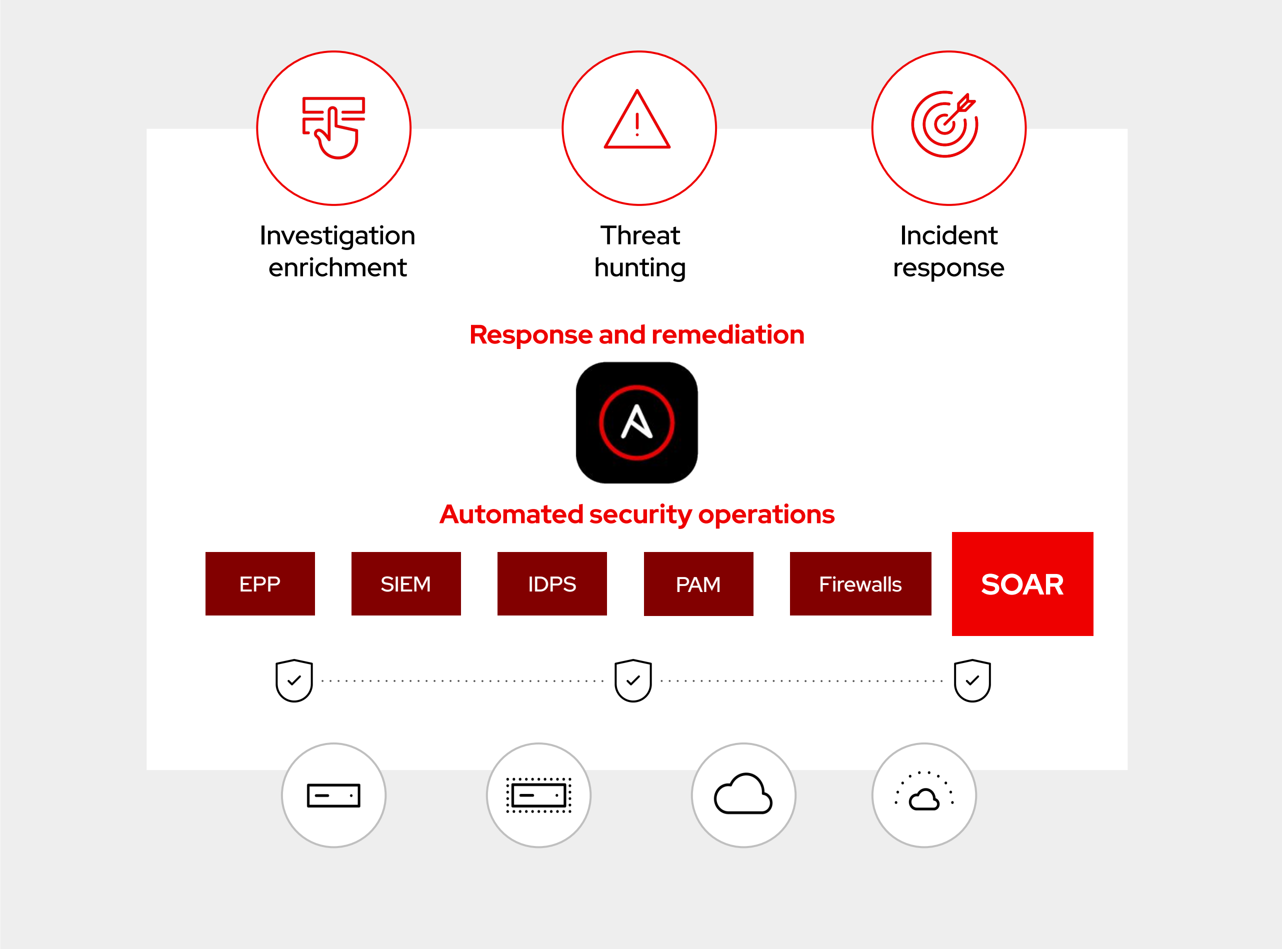
Enable auditable and verifiable security processes by using a single tool and common language covering multiple security tools

Security automation is a journey

Start simple and small. Improve iteratively



Security Automation



Investigation enrichment

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

Threat hunting

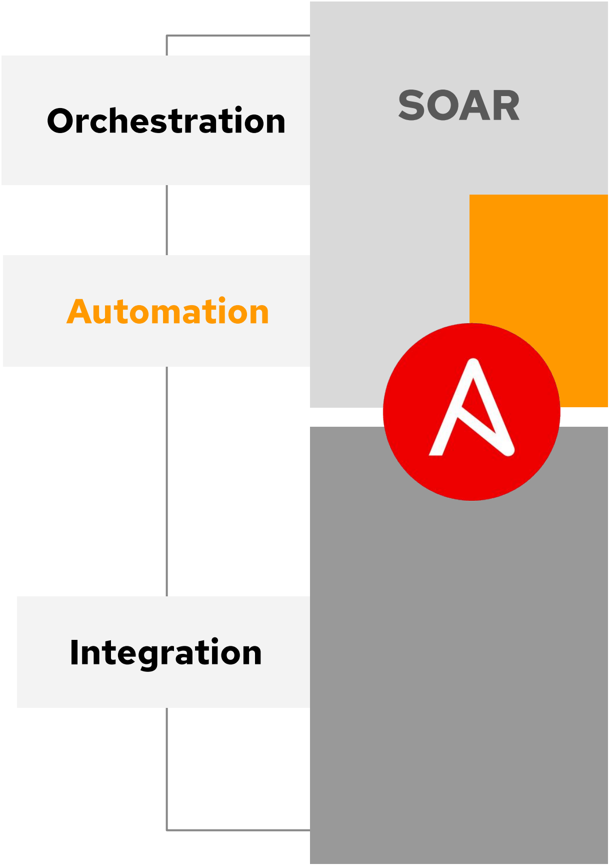
Automating alerts, correlation searches, and signature manipulation

Incident response

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

SOAR Automation

Security Orchestration, Automation, and Response



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**.

What else can you automate?

You name it, we can automate it!

Next-gen network operations

- Configuration accuracy
- Operational state management
- Automated NetOps
- Network compliance

Cloud Orchestration

- Deployment and retirement
- Cloud migration
- Cloud operations
- Automated troubleshooting

Windows Management

- Install and uninstall MSIs, .exes
- Start, stop, and manage Windows services
- Manage and install Windows updates
- Push and execute Powershell scripts

Red Hat OpenShift

- Infrastructure coordination
- Lifecycle management
- Day 2 configuration

Event-Driven Ansible

- Listen for events
- Create event conditions which once met will trigger an action
- Trigger playbooks, modules, notifications based on the conditions

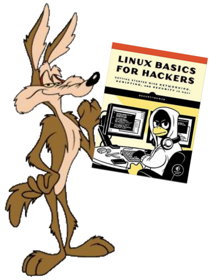
Linux Management

- Provisioning
- Configuration Management
- Application Deployment

IBM Security

QRadar

QRadar - SIEM



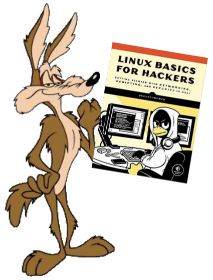
Attacker

Checkpoint Firewall

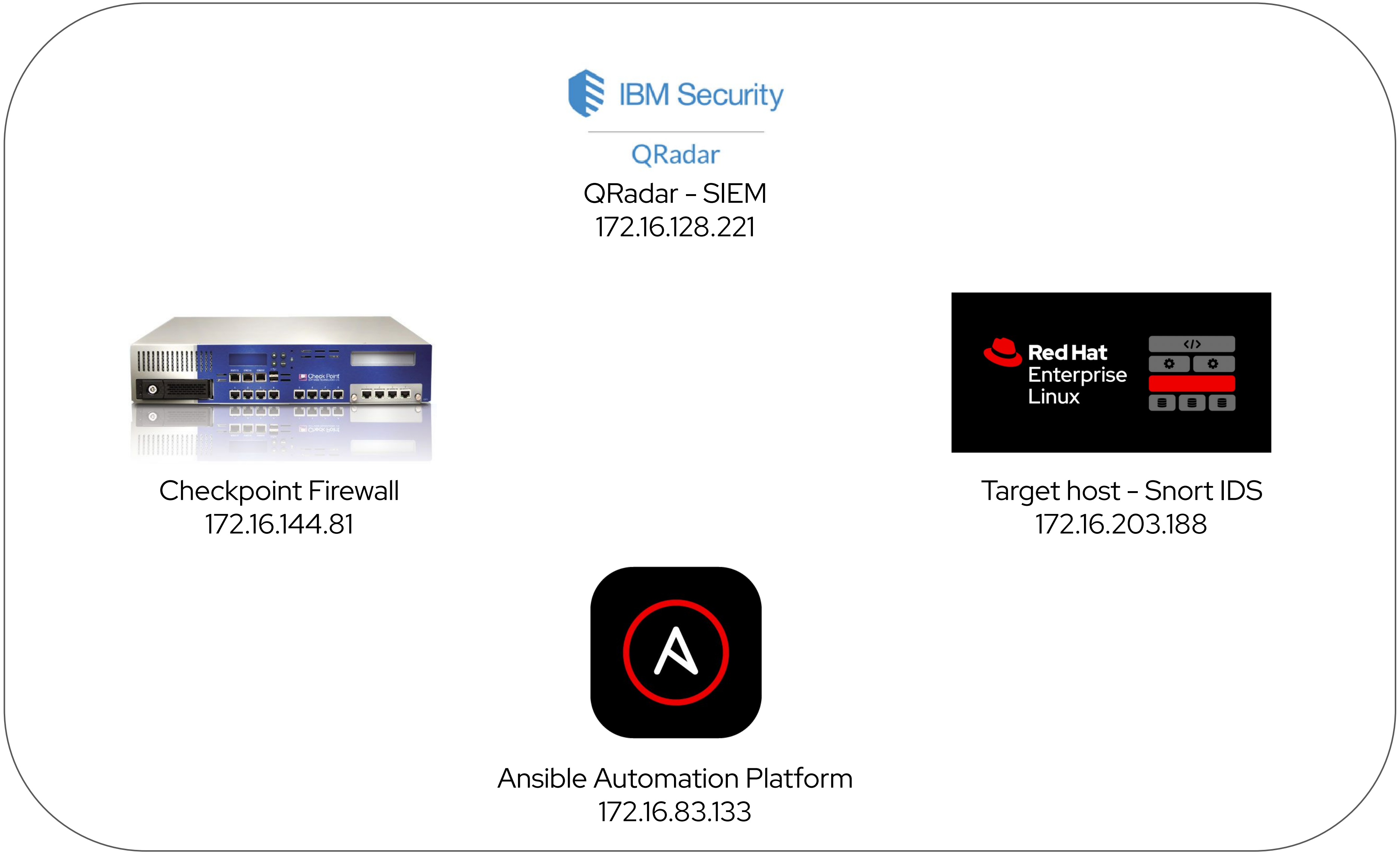
Red Hat Enterprise Linux

Target host - Snort IDS

Ansible Automation Platform



Attacker
172.16.39.218

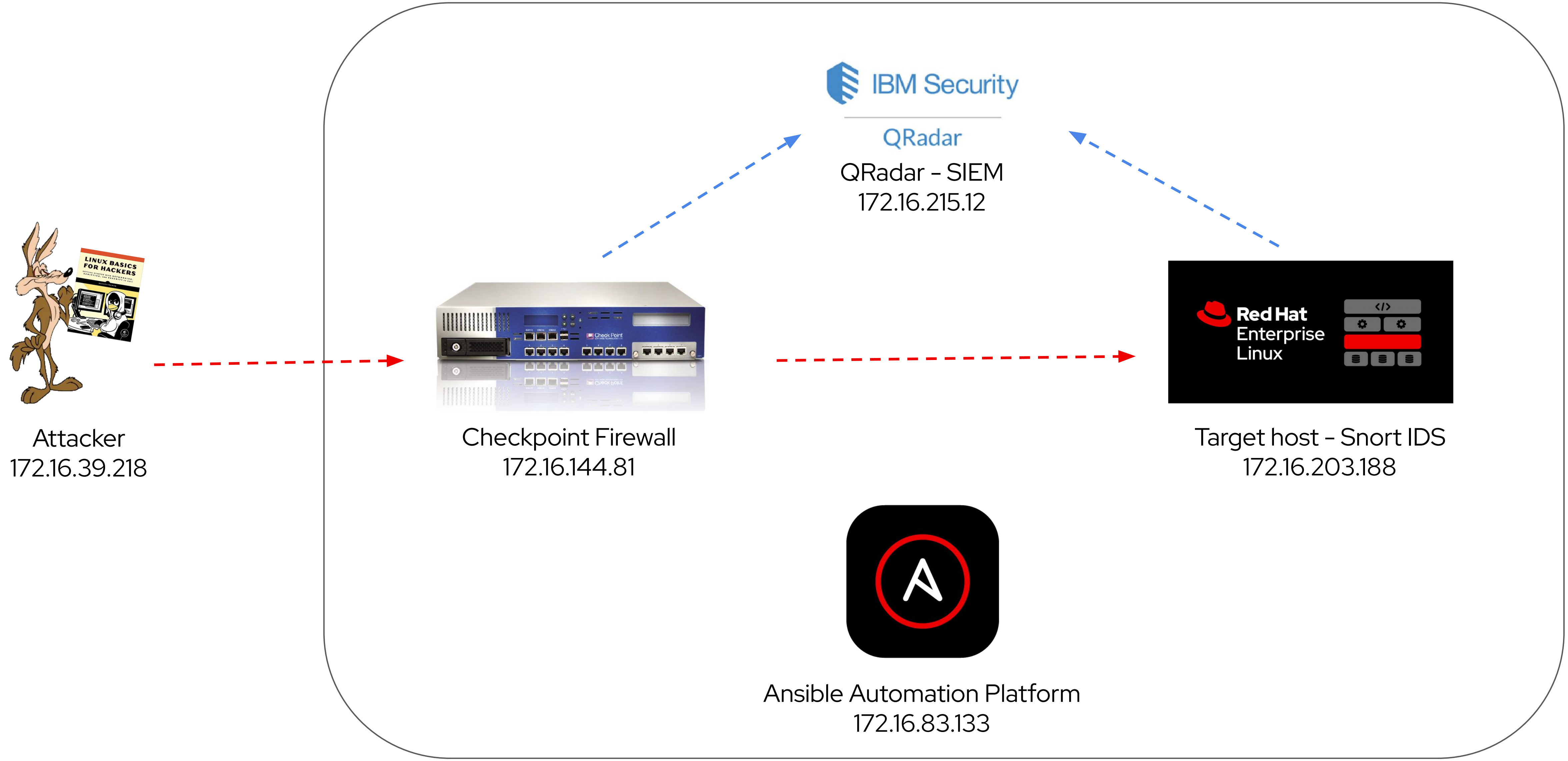


QRadar – SIEM
172.16.128.221

Checkpoint Firewall
172.16.144.81

Target host – Snort IDS
172.16.203.188

Ansible Automation Platform
172.16.83.133



QRadar - SIEM
172.16.215.12

Attacker
172.16.39.218

Checkpoint Firewall
172.16.144.81

Target host - Snort IDS
172.16.203.188

Ansible Automation Platform
172.16.83.133

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.

facebook.com/ansibleautomation

twitter.com/ansible

linkedin.com/company/ansible/

youtube.com/user/RedHatVideos