

Ansible security automation

Automating security response and remediation

Craig Brandt

Principal Technical Marketing Manager

<https://www.linkedin.com/in/automaticcraig/>

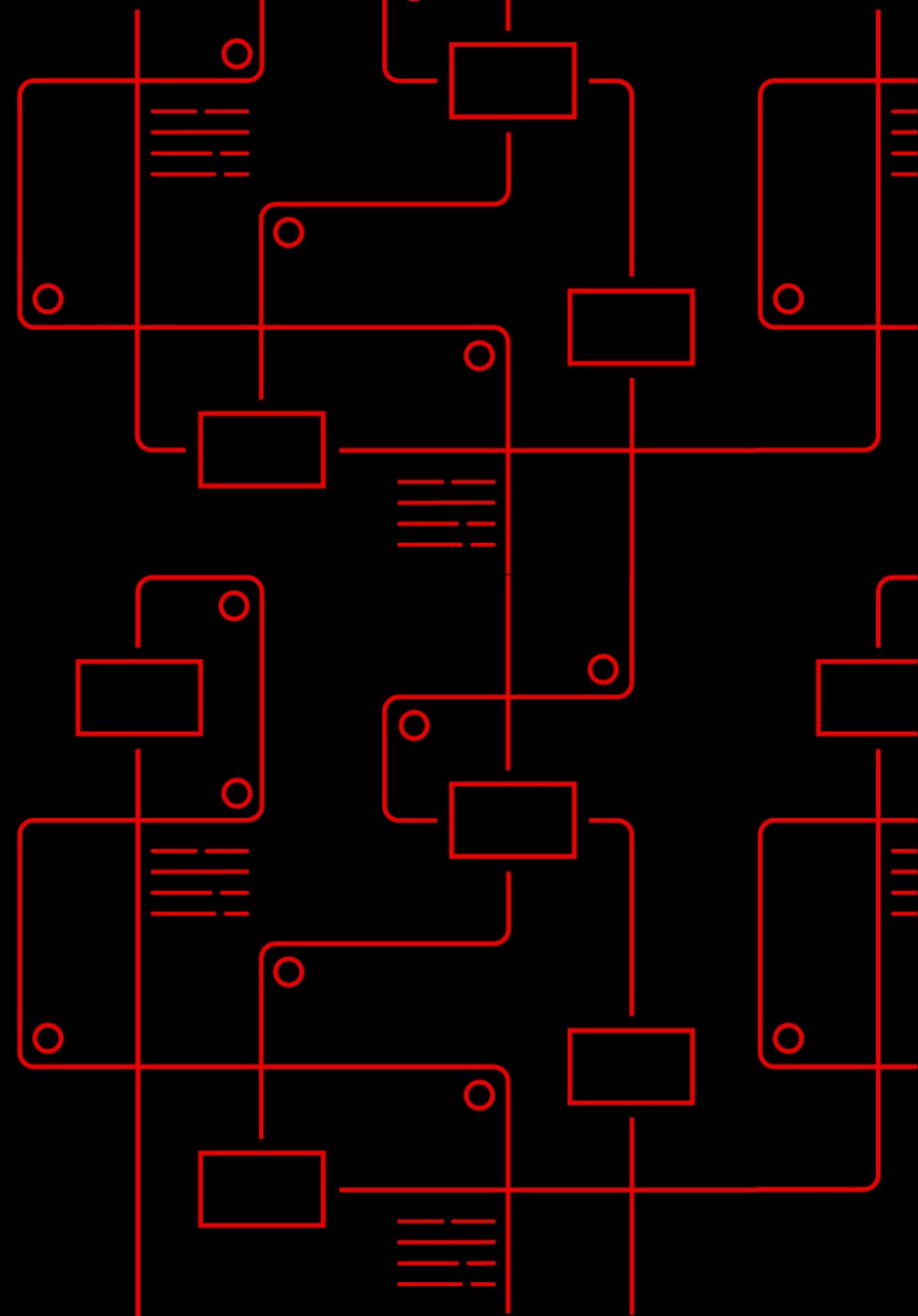


What we'll cover today

- ▶ Industry security challenges
- ▶ What is Ansible security automation?
- ▶ Ansible security automation and Zero Trust Architecture
- ▶ Demo!
- ▶ Where to go next

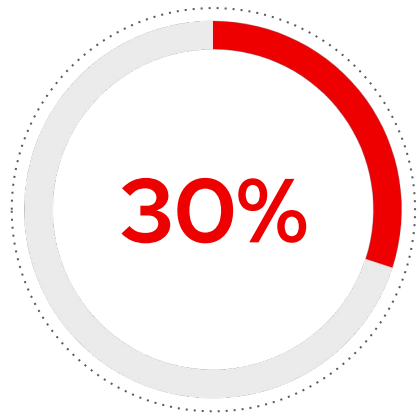


Security challenges



Security team challenges.

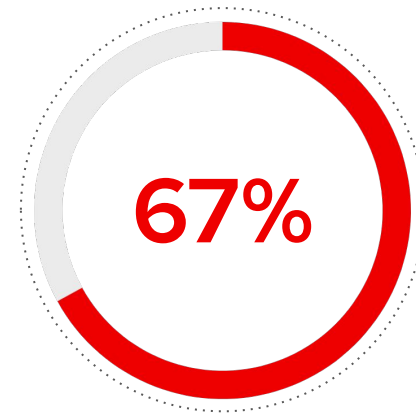
Increased complexity and scope



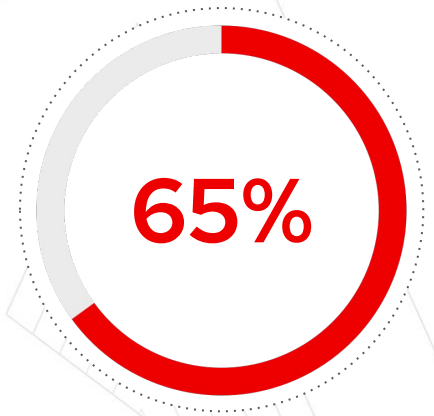
Incoming alerts are ignored or not investigated by the average security team*



Said the time to resolve an incident has grown



Reported increased severity and volume of attacks



Lack of improvement due to fragmented IT and security infrastructure

Security industry challenges.

Lack of automation and orchestration

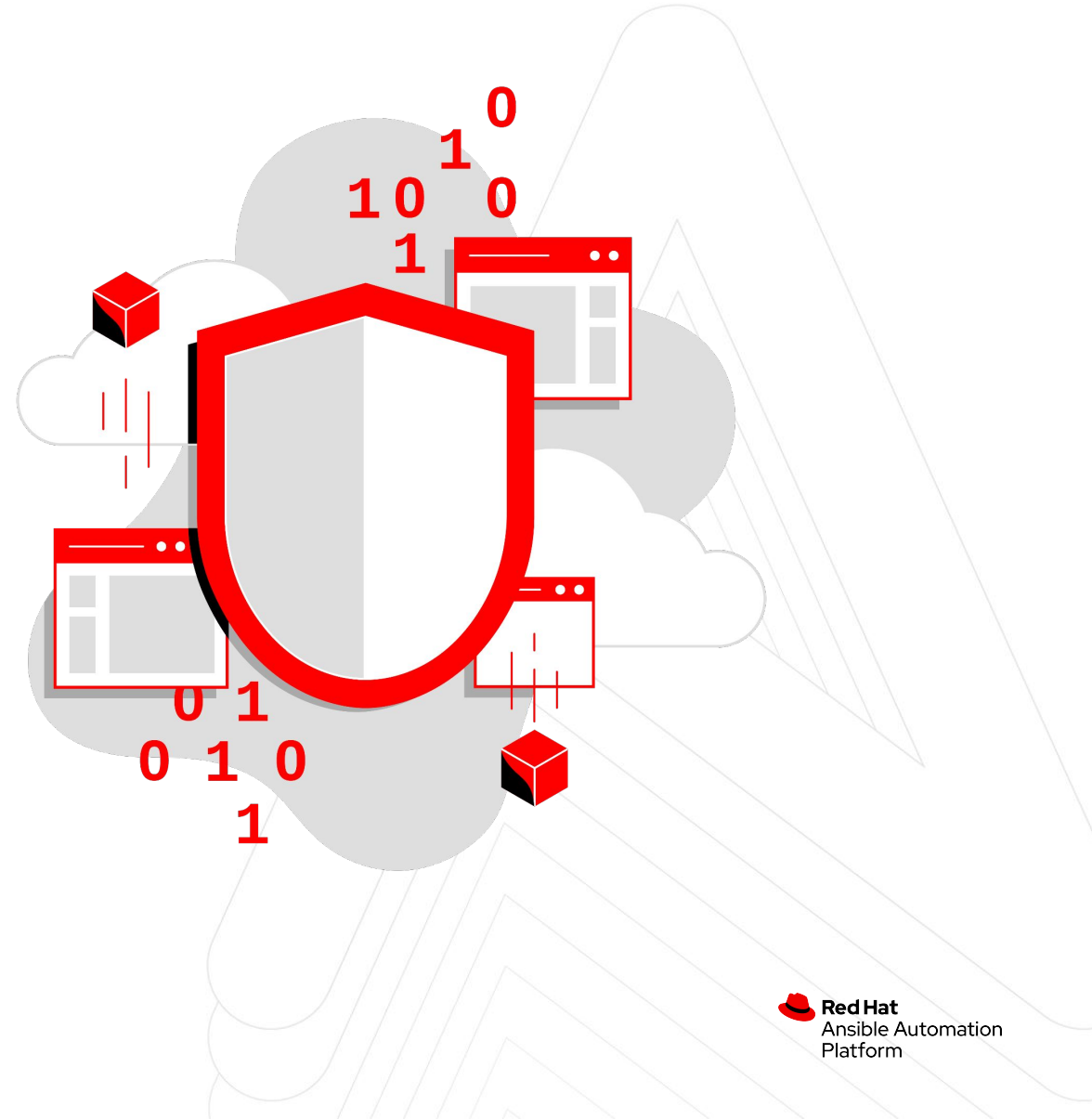
“Lack of automation and orchestration”

ranked third.

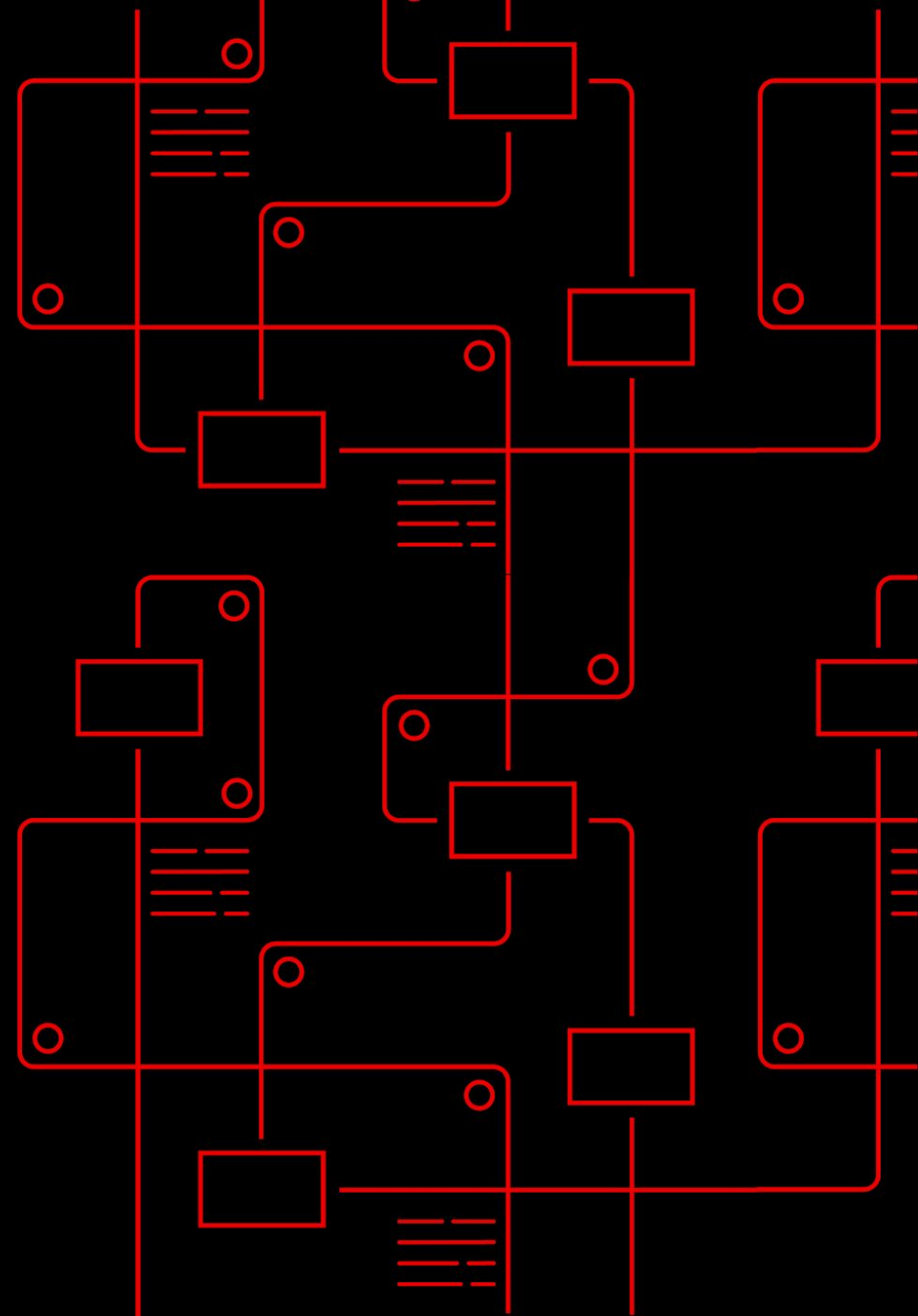
SANS 2022 SOC Survey

“Among respondents, 45% used more than 20 tools when specifically investigating and responding to a cybersecurity incident.”

Cyber Resilient Organization Study 2021

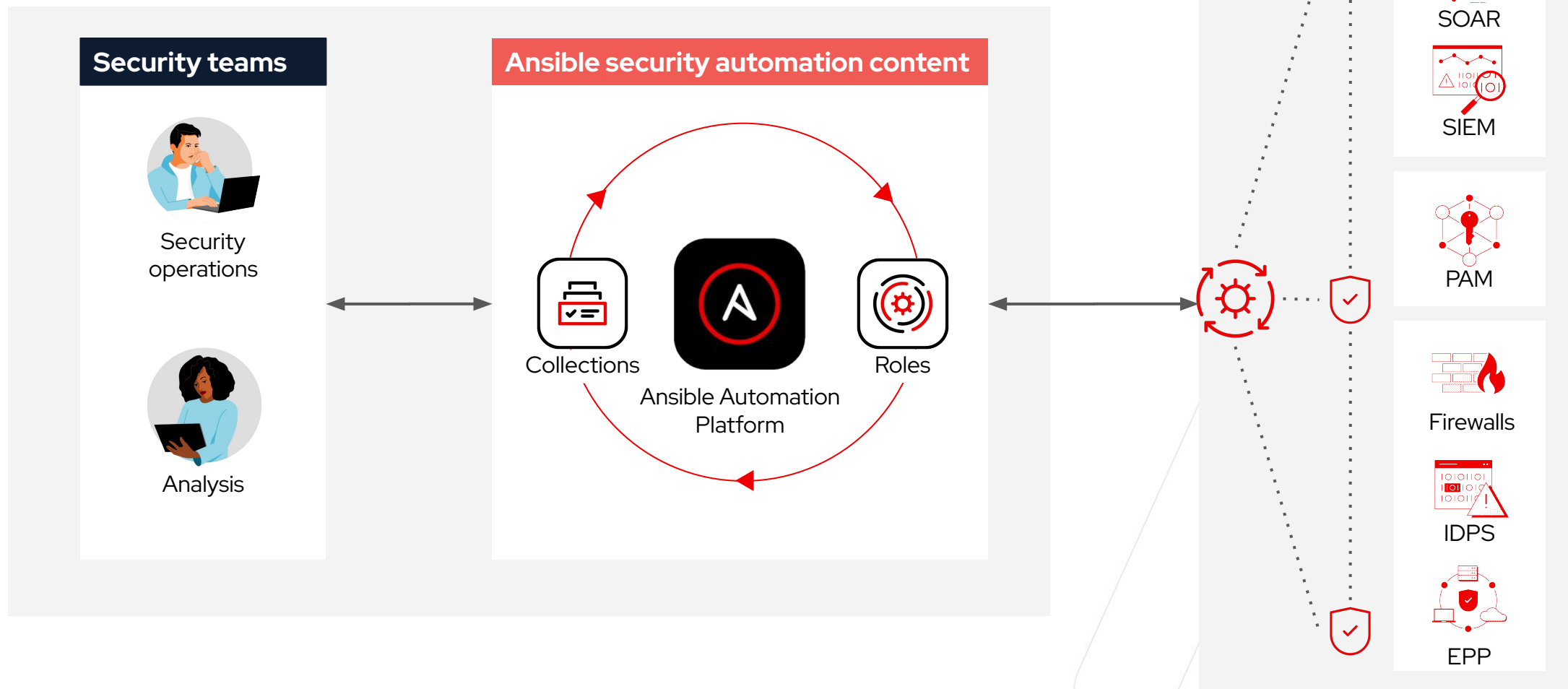


What is Ansible security automation?



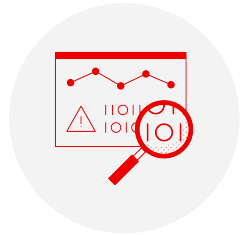
Ansible security automation

Integrate and orchestrate security solutions



Ansible security automation content

Certified Content Collections and the Community



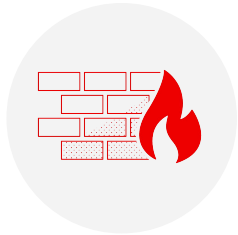
Security Information & Events Management



Enterprise Security



QRadar



Enterprise Firewalls



Check Point
SOFTWARE TECHNOLOGIES LTD

Next Generation Firewall
GAIA OS



Adaptive Security Appliance (ASA)



Advanced Firewall Manager



Fortigate: NGFW



SRX (JunOS)



Intrusion Detection & Prevention Systems



Check Point
SOFTWARE TECHNOLOGIES LTD

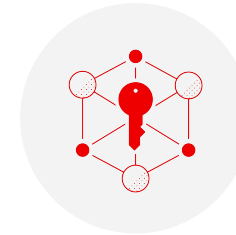
IPS Blade



Fortigate: IPS



Intrusion Detection System



Privileged Access Management



CYBERARK

PAM



Apache Syncope



ISAM



Endpoint Protection



CROWDSTRIKE

Falcon



Deep Security

Ansible security automation

Response and remediation use cases



Investigation enrichment

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



Threat hunting

Automating alerts, correlation searches and signature manipulation.



Incident response

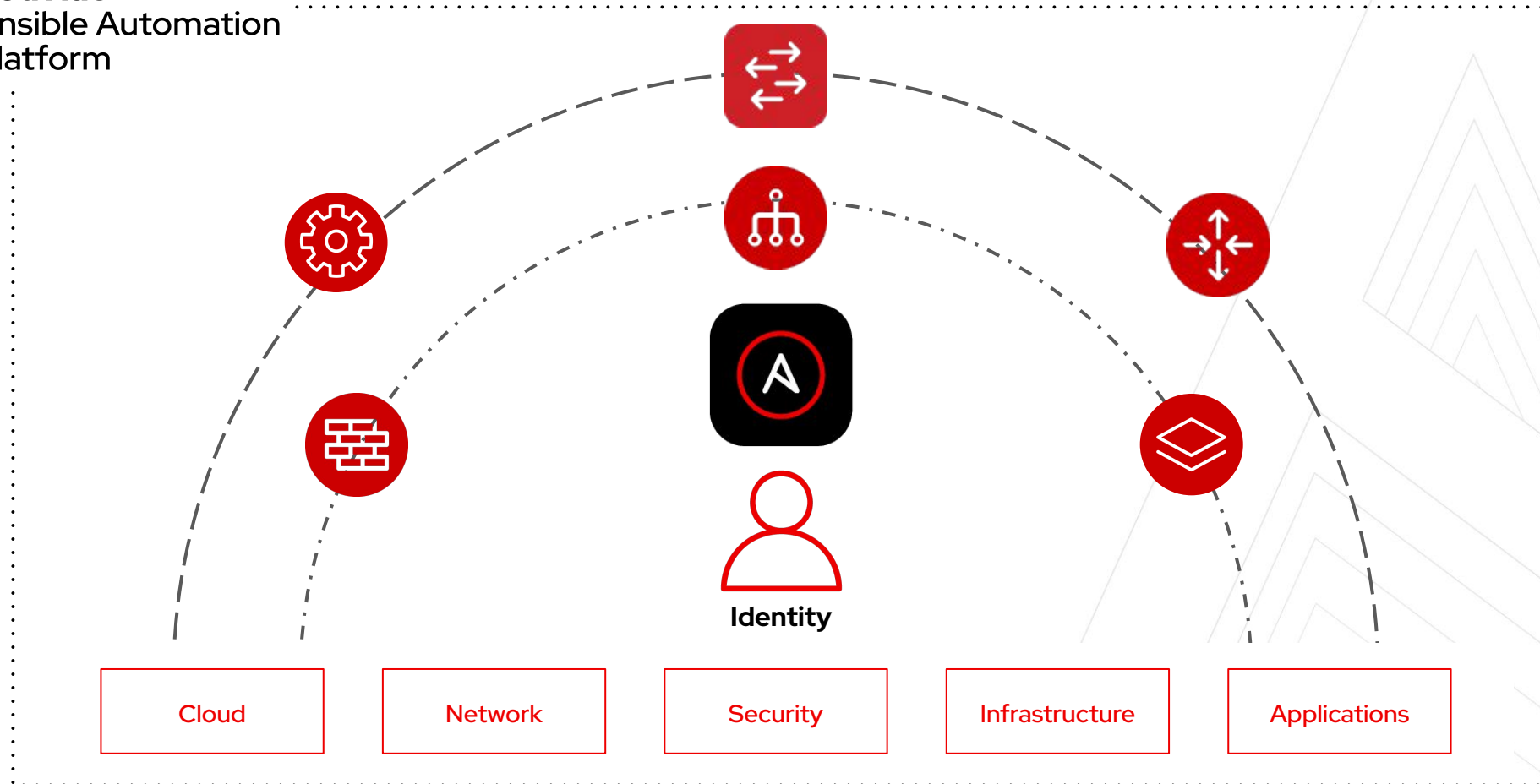
Creating new security policies to allow, deny or quarantine a machine.

Ansible Automation Platform and Zero Trust Architecture

Explicit Trust is the Goal

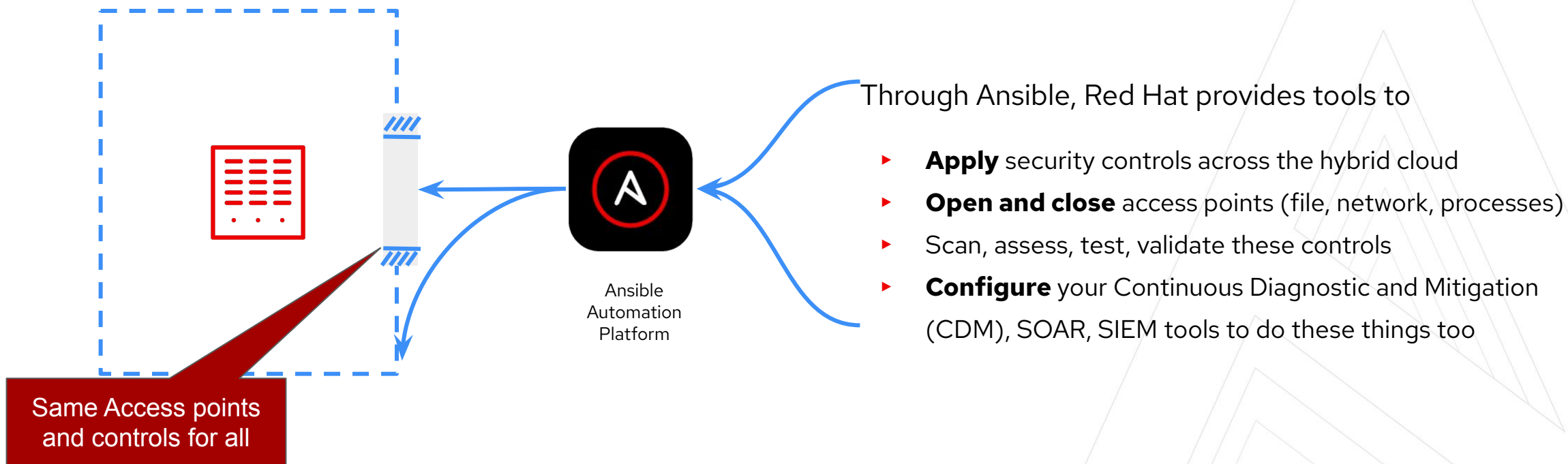


Red Hat
Ansible Automation
Platform

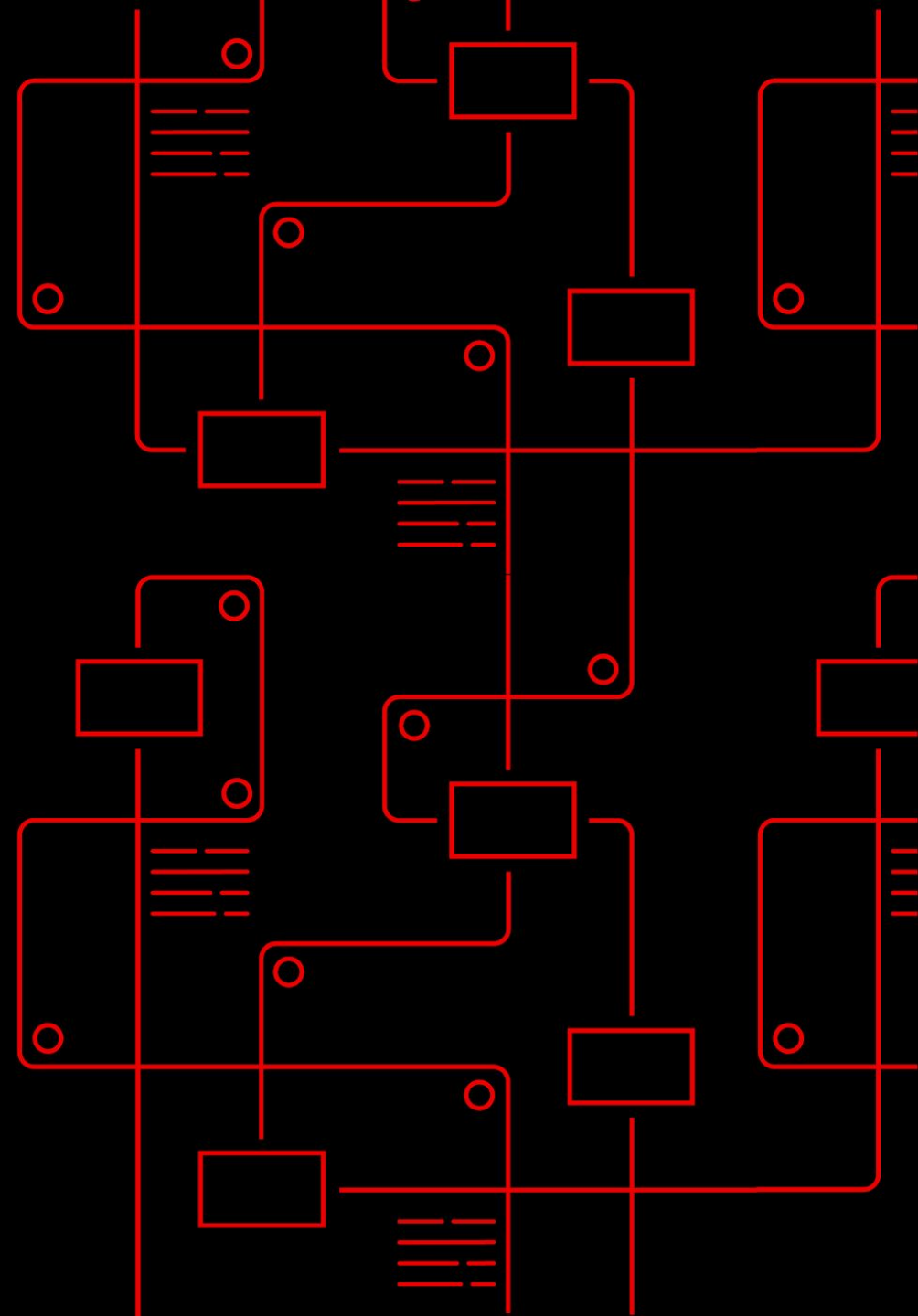


Ansible security automation and Zero Trust Architecture

Dynamic security boundaries

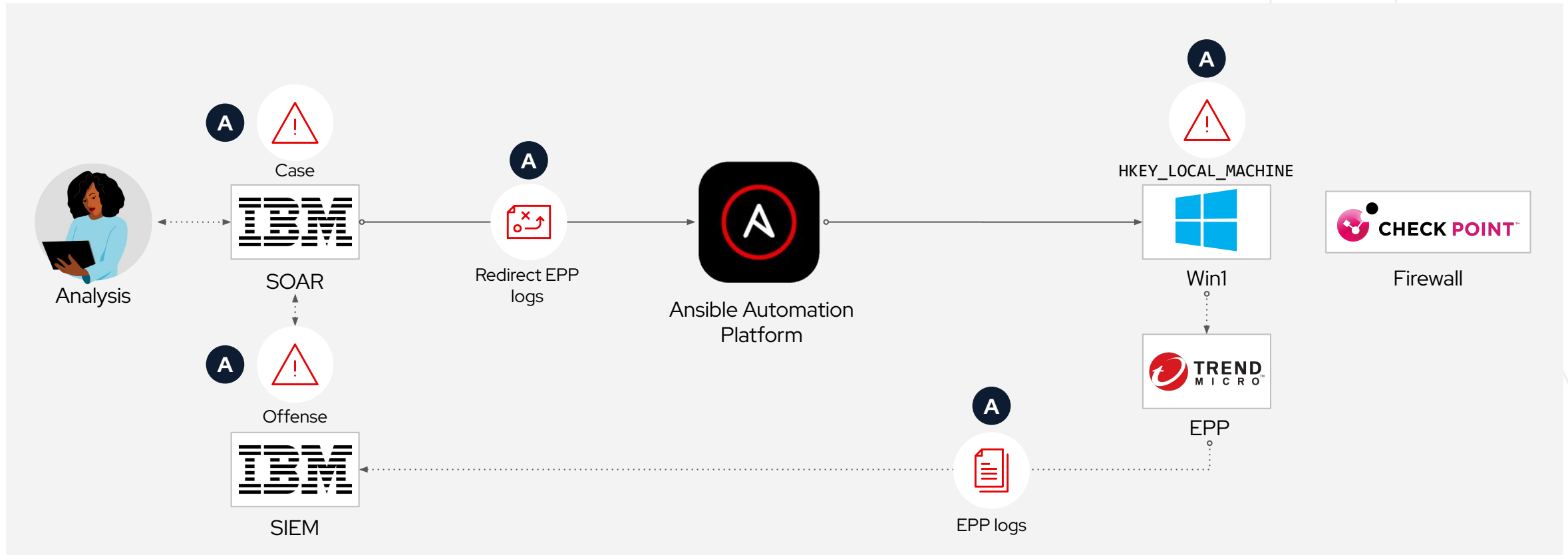


Demo overview



Investigation enrichment zero trust workflow

Collate data and build context

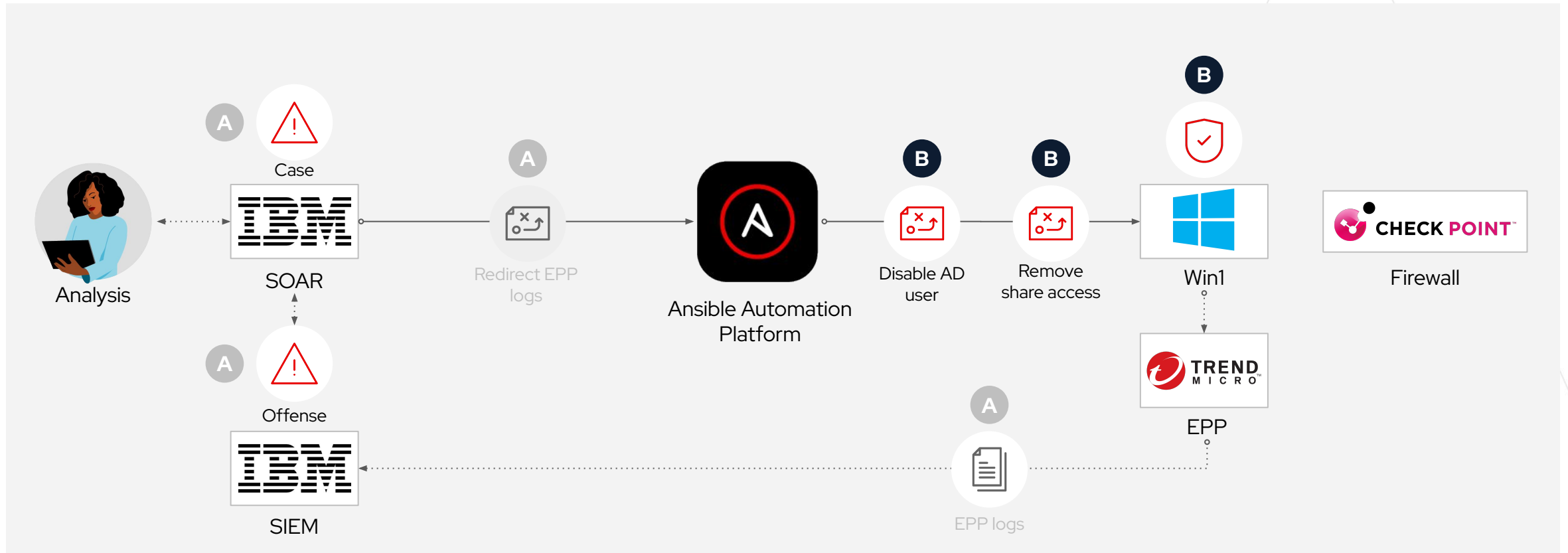


A. Suspicious registry key

- Suspicious registry key detected
- Trend Micro Deep Security log redirection into IBM QRadar
- New Offense created and imported into IBM SOAR

Automated containment zero trust workflow

Automated containment based on context

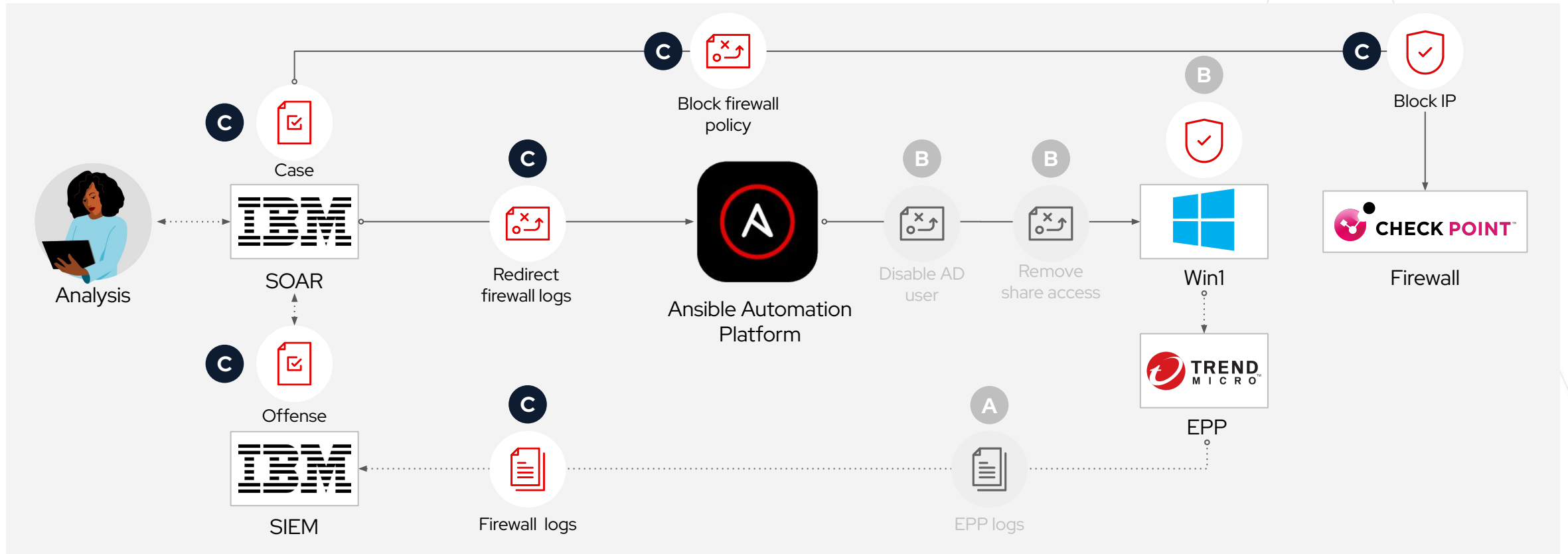


B. Threat mitigation workflow

- Gather information on compromised AD account
- Disable access to corporate data
- Disable AD user account

Remediation zero trust workflow

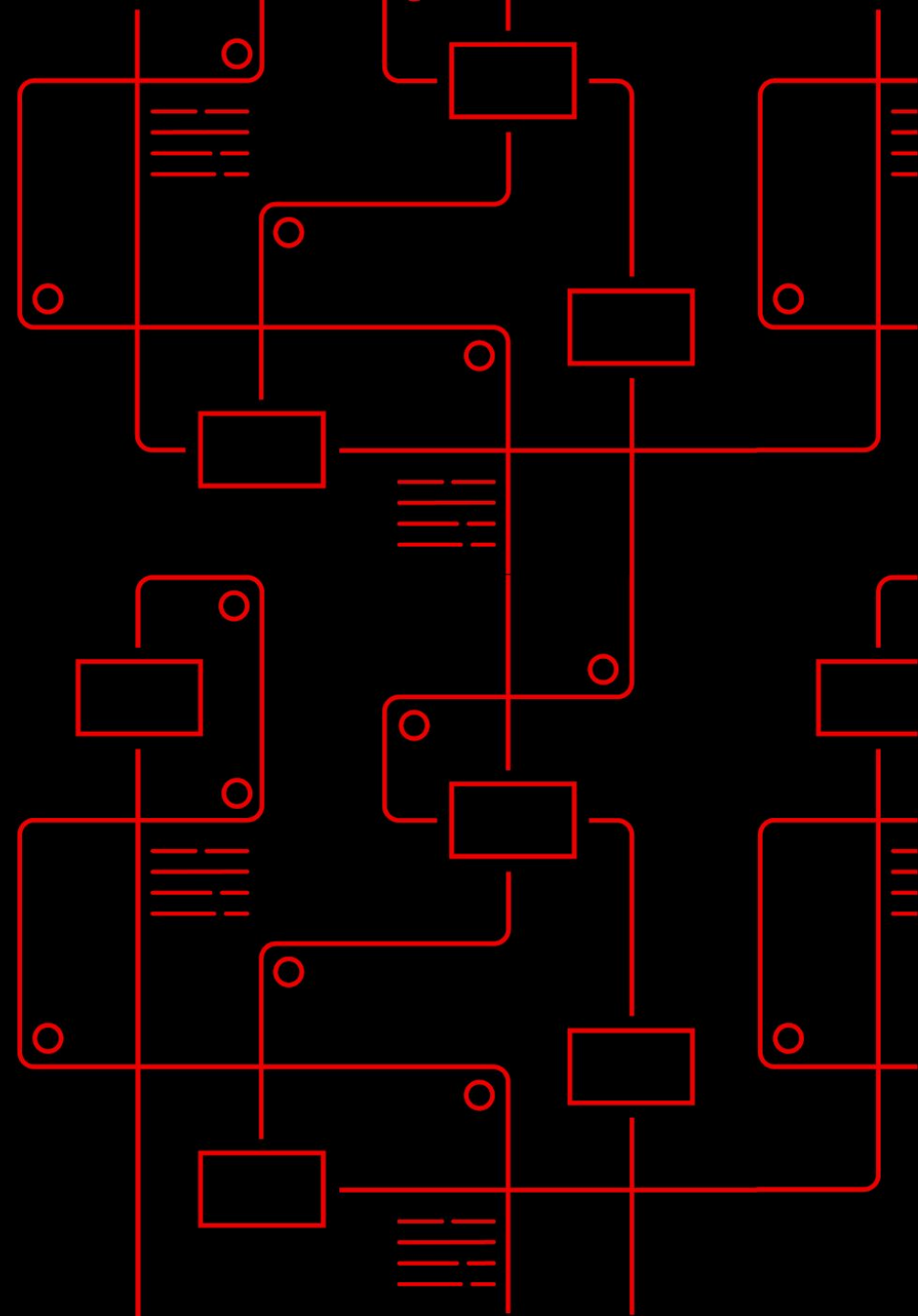
Remediate threat



C. Threat remediation workflow

- Redirect CheckPoint NGFW logs to QRadar SIEM
- Analyse network traffic
- Block malicious IP

Demo time!





Where to go **next**



Learn more

- ▶ Demonstration examples and slides
- ▶ Security automation on ansible.com
- ▶ Simplify your security operations center - eBook
- ▶ Documents
- ▶ Youtube



Get started

- ▶ Self-paced labs
- ▶ Ansible security automation workshop
- ▶ Ansible Automation Platform Trial
- ▶ console.redhat.com



Get serious

- ▶ Red Hat Automation Adoption Journey
- ▶ Red Hat Training
- ▶ Red Hat Consulting

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.



linkedin.com/company/red-hat



youtube.com/c/AnsibleAutomation



facebook.com/redhatinc



twitter.com/ansible