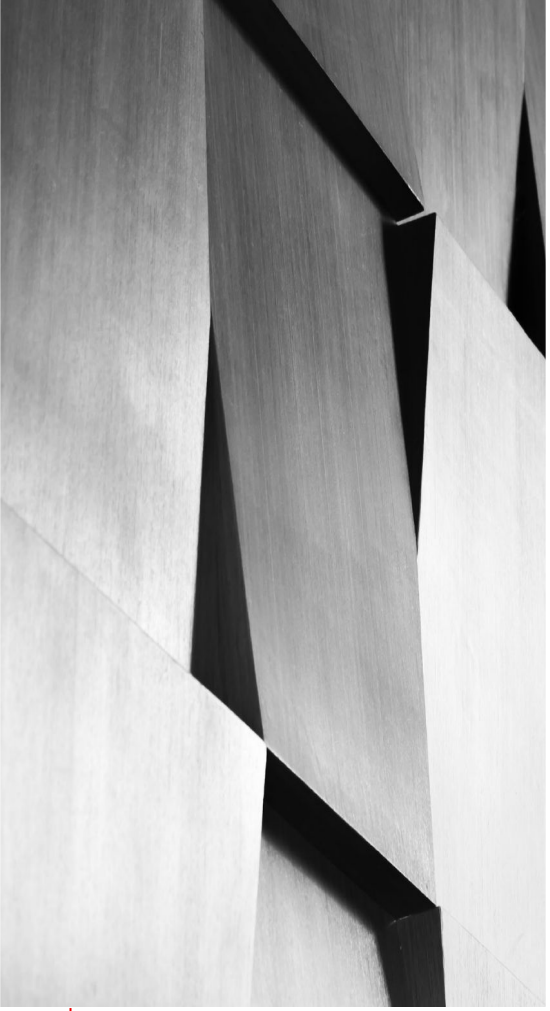
Automate your Security Operations Center (SOC) with Ansible

Ansible Security Automation

Faz Sadeghi
Senior Specialist Solution Architect - Red Hat

Red Hat



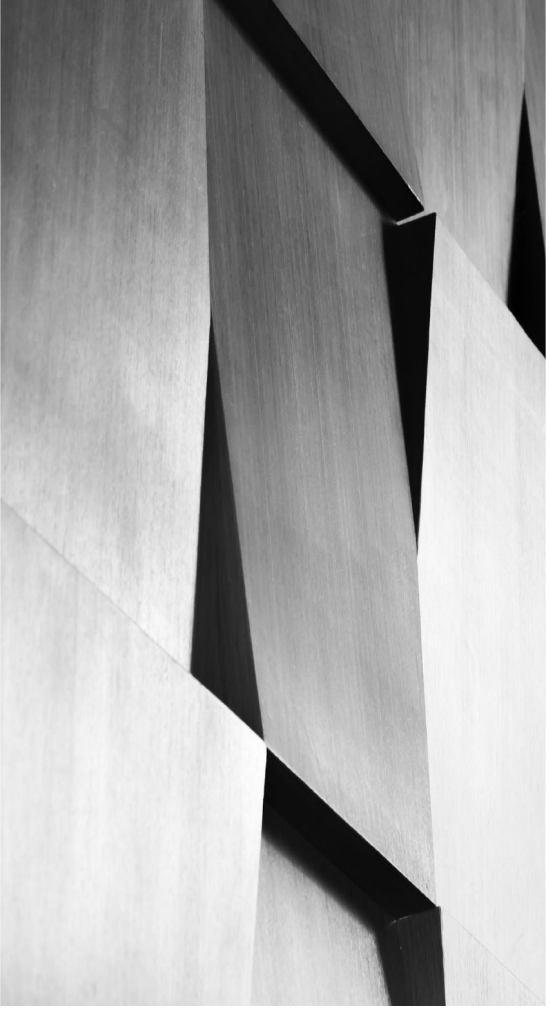
Security Automation

Compliance
Patching
Hardening...

VS

Ansible Security Automation

Red Hat



The State of Enterprise IT Security

$103B

Global spending on security hardware, software and services

40

Average number of security tools used in a SOC

5%

The average security team typically examines less than 5% of the alerts flowing into them every day (and in many cases, much less than that).

57%

(of respondents report)

Time to resolve an incident has increased

65%

(of respondents report)

Severity of attacks has increased

53%

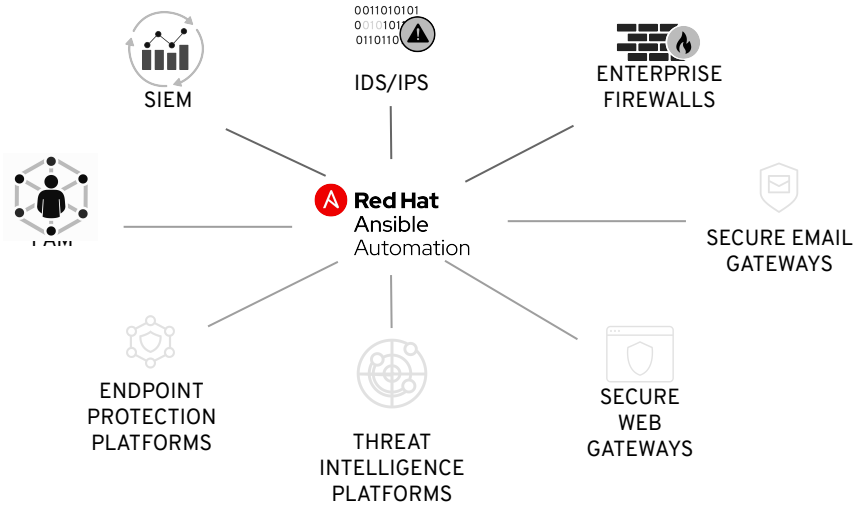
More than half of organizations report a "problematic shortage" of cybersecurity skills, and there is no end in sight.

Source: https://www.idc.com/getdoc.jsp?containerId=prUS44935119
https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/
https://www.esg-global.com/research/esg-research-report-cybersecurity-analytics-and-operations-in-transition

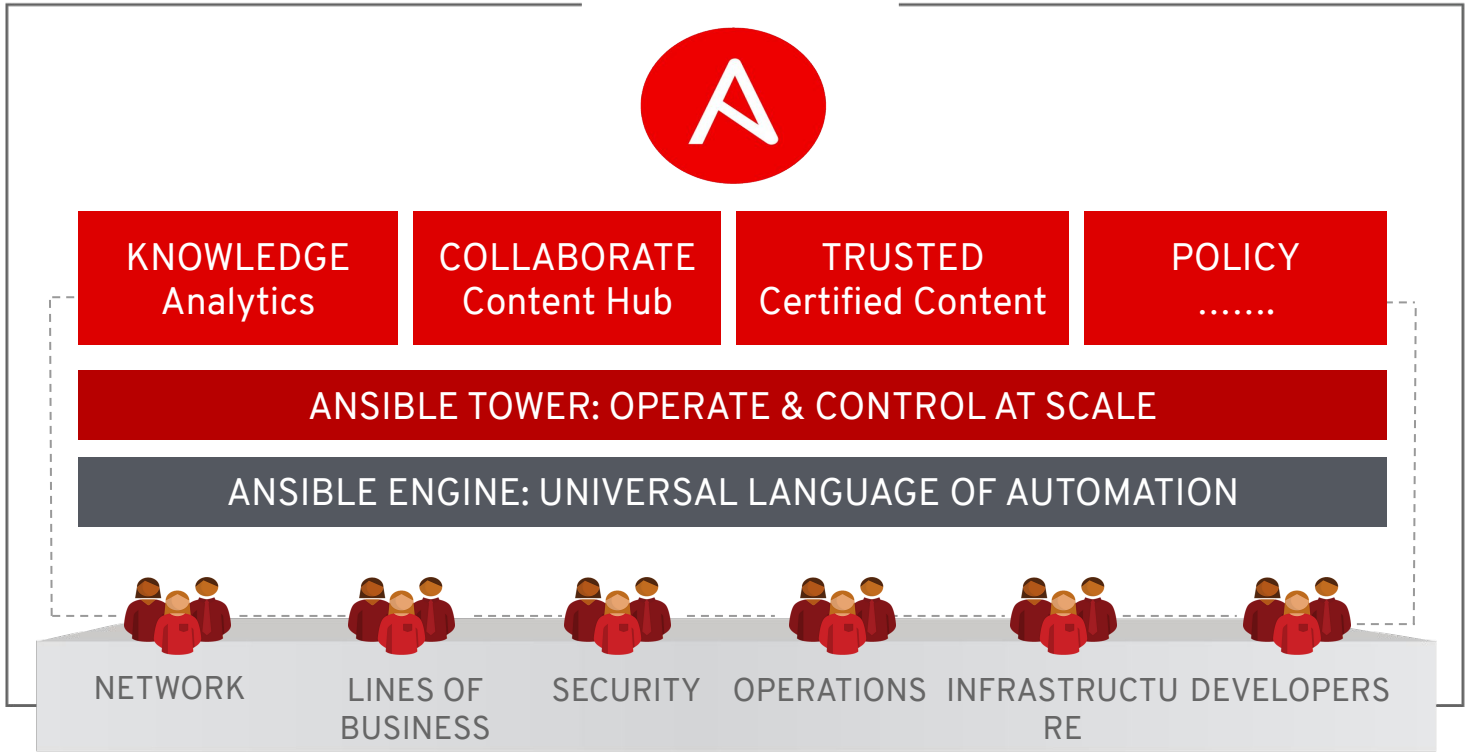
What's Ansible security automation?

DESIGNED TO ORCHESTRATE THREAT RESPONSE ACROSS SECURITY DOMAINS

- Expansion of Ansible as the Enterprise automation platform
- Integrates & orchestrates multiple classes of security solutions
- Provides modules, roles and playbooks to support security use cases across those solutions



Red Hat



CONTINUE TO BE FUELED BY AN INNOVATIVE **OPEN SOURCE** COMMUNITY

Red Hat

Why Ansible?

Simple

Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

Get productive quickly

Powerful

App deployment

Configuration management

Workflow orchestration

Network automation

Orchestrate the app lifecycle

Agentless

Agentless architecture

Uses OpenSSH & WinRM

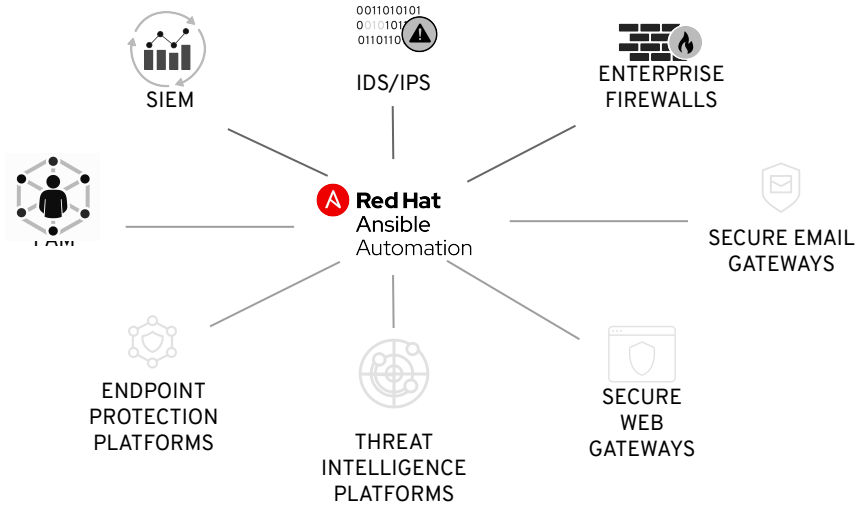
No agents to exploit or update

Get started immediately

More efficient & more secure

Red Hat

Ansible security automation



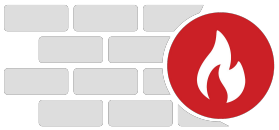
Red Hat

Who Are Our Partners?

Security Information & Events Management

splunk>

IBM



Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

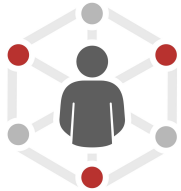
FORTINET

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET



Privileged Access Management

CYBERARK

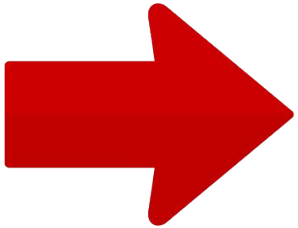
Syncope

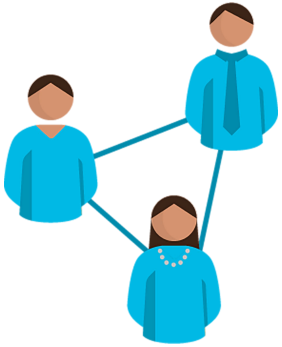
Red Hat

Why should YOU care about security?

IT Process

Core practitioners.
Experts with deep IT technical knowledge.



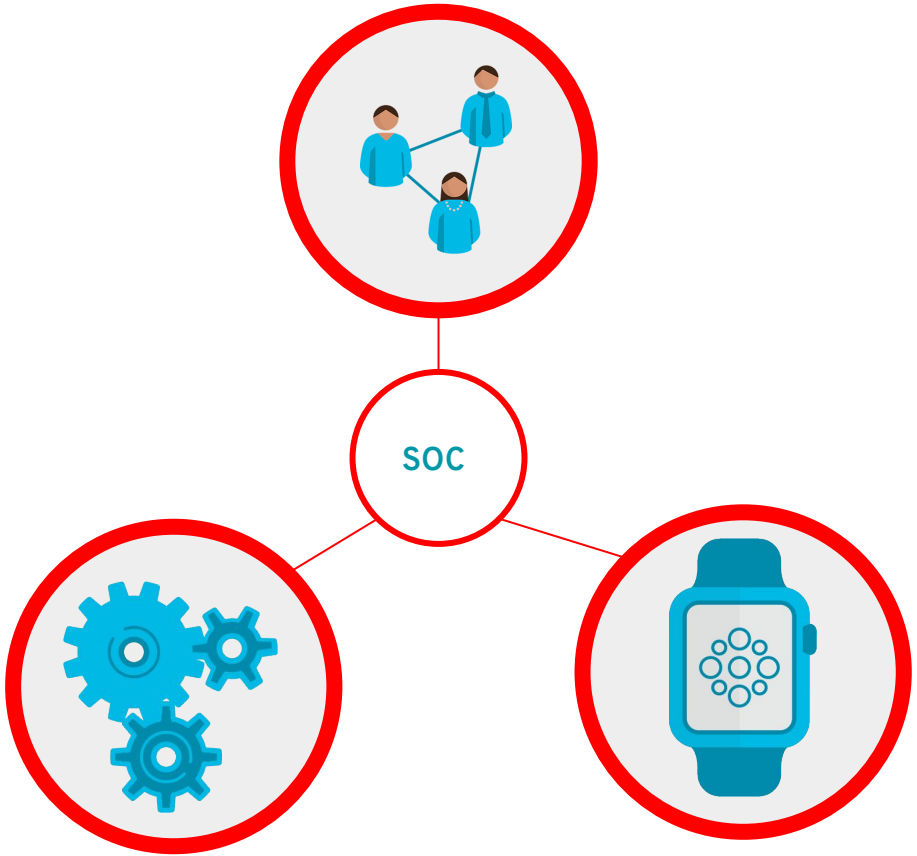


Organization-wide Process

Business process owners, Product Managers, Legal, PR, Customer Relations

Red Hat

What is a SOC?



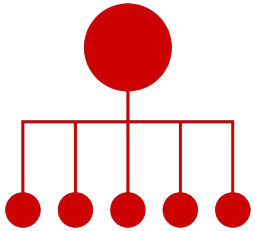
- Prevent
- Detect
- Assess
- Respond

Red Hat

Why do we need a SOC?

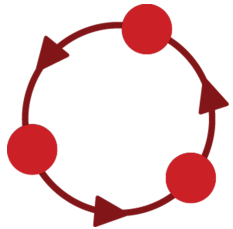
> Organizations are building internal security operations capabilities (even if in a limited sense) because they desire more control over their security monitoring and response process. They also want to have more informed conversations with regulators.
>
> Gartner

What kind of SOCs are out there?



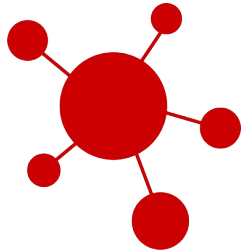
Command

Coordinates other SOCs.
Provides threat intelligence, situational awareness and additional expertise.
Rarely directly involved in day-to-day operations.



Multifunction

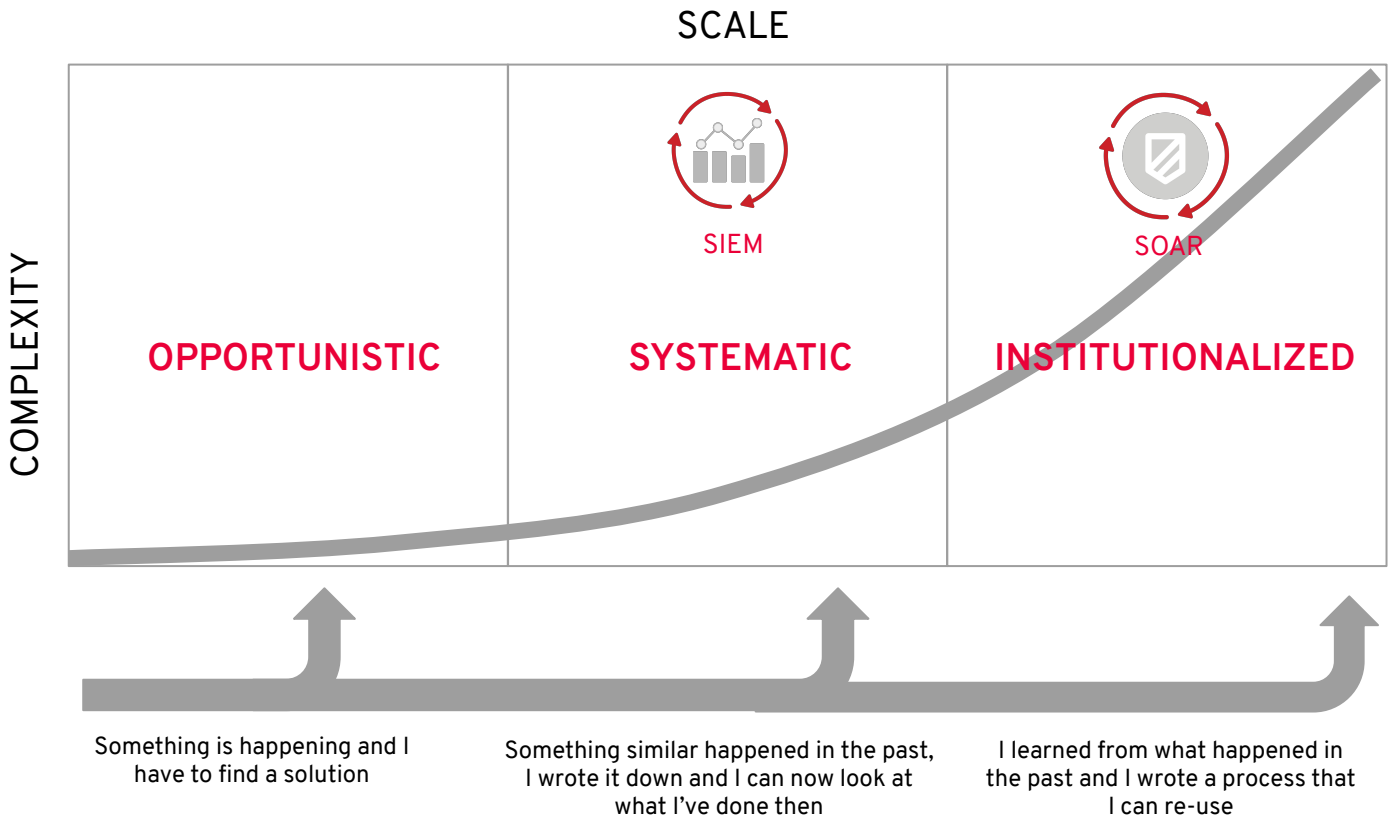
Dedicated facility with a dedicated team performing not just security, but other critical 24/7 IT operations from the same facility to reduce costs.



Fusion

Traditional SOC functions and new ones, such as threat intelligence, computer incident response team (CIRT) and operational technology (OT) functions, are integrated into one SOC facility.

Security Processes Maturity Model



Source: The journey to security automation

Red Hat

The Italian Army

ESERCITO

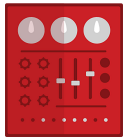
The **C4 Command, Development, management and security** of of enterprise applications, systems and networks

190,000 Users

National territory and International missions

470+ Barracks

Maintain an Extensive Private Network



15 Datacentres

“”

In the interconnected digital world, every individual becomes an operator and we’re often only as strong as our weakest link.

Michael S. Rogers

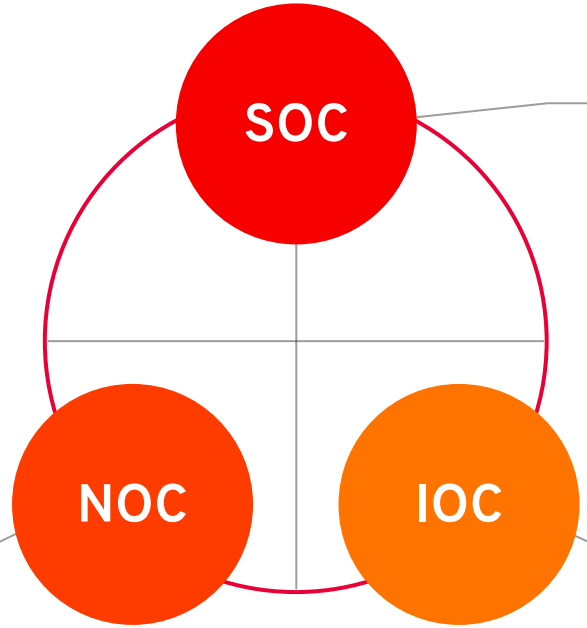
You can’t predict future, but you can plan for it.

Saji Ijiyemi

Source: https://ndupress.ndu.edu, https://sajigroup.com

Red Hat

Decision Making Room



Security

Divided in 3 teams:

- CIRT (Response & Audit)
- Monitoring & Analysis
  - + 9 sub groups
- Security Systems

Network

- Private network (EINet) transport and services
- Network Appliances
- Active Directory Domain
- Email services

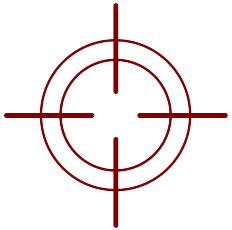
Infrastructure

- Datacenter Management
  - 3 sites in 2 locations
- Mini-datacenter Management
  - 12 sites in 7 locations
- Internet Access Management

Use Cases

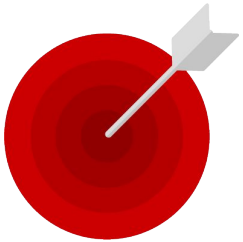
Investigation Enrichment

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



Threat Hunting

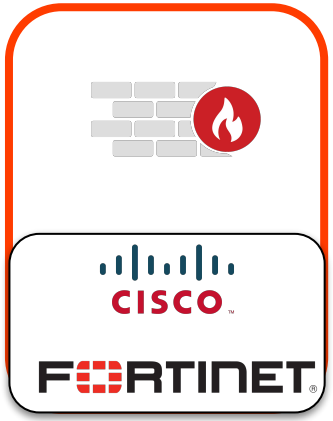
Automating alerts, correlation searches and signature manipulation

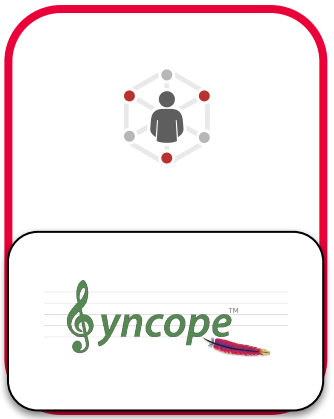


Incident Response

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

The Tool Set

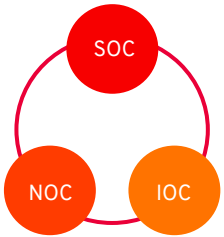




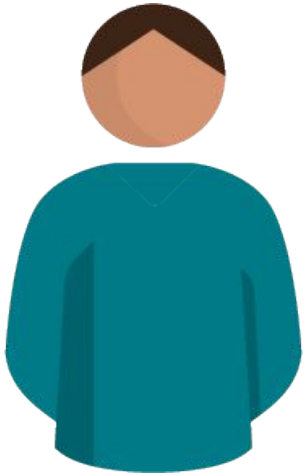
Red Hat

DISCLAIMER

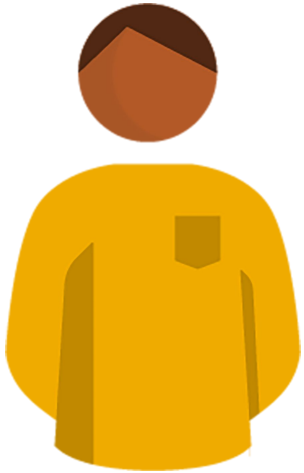
"All characters appearing in this work are fictitious. Any resemblance to real persons, living or dead, is purely coincidental."



SOC
Captain Chiara
SIEM



NOC
Major Marko
Firewalls
IDS/IPS



IOC
Lieutenant Luca
PAM

Investigation Enrichment

Red Hat

USE CASE - Investigation Enrichment On Firewalls

Investigation Enrichment

Generates an *offense* from an anomaly on mission site.

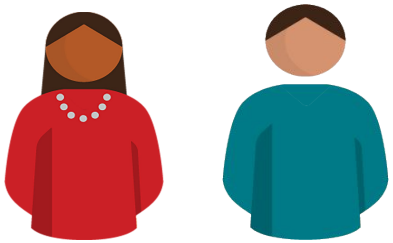
A **ticket is opened** and populated with all relevant data.

Local firewalls are configured to **send their logs to QRadar**. The **log verbosity is set to high**.

The additional information allows to dismiss the offense as a false positive.

Local firewalls are rolled back to their previous configurations to avoid overload/fatigue.

The ticket is **populated** with data from the actions taken and then **closed**.



SOC NOC

Red Hat

USE CASE - Investigation Enrichment On Firewalls

Investigation Enrichment

```
- name: Forward Cisco ASA Logs
  hosts: ciscoasa
  tasks:
    include_role:
      name: log_manager
      tasks_from: forward_logs_to_syslog
    vars:
      syslog_server: 192.168.0.1
      ciscoasa_server_name: test
      firewall_provider: ciscoasa
```

USE CASE - Investigation Enrichment On Firewalls

Investigation Enrichment

```
- hosts: fortios
  vars:
   vdom: "root"
  tasks:
  - name: Global settings for remote syslog server.
    fortios_log_syslogd_setting:
       vdom:  "{{ vdom }}"
       https: "False"
       log_syslogd_setting:
         custom_field_name:
         - custom: “cef”
           id:  "6"
           name: "default_name_7"
         enc_algorithm: "high-medium"
         facility: "kernel"
         mode: "udp"
         port: "12"
         server: "192.168.0.1"
         source_ip: "84.230.14.43"
         ssl_min_proto_version: "default"
         status: "enable"
```

FORTINET

USE CASE - Investigation Enrichment On Firewalls

Investigation Enrichment

```yaml
- name: Create a QRadar Log Source and Enable Offense Rule
  hosts: qradar
  collections:
    - ibm.qradar
  tasks:
    - name: Create QRadar Log Source - FortiGate
      qradar_log_source_management:
        name: "FortiGate LogSource: {{ fgate_ip_addr }}"
        type_name: "Fortinet FortiGate Security Gateway"
        state: present
        description: "Automated Creation of QRadar LS"
        identifier: "{{ fgate_ip_addr }}"
```

IBM QRadar

Threat Hunting

Red Hat

USE CASE - MBL* Automation Inwards

Threat Hunting

A new security bulletin is received.

REDMINE

A **ticket is opened** with the update request.

IBM Radar

An existing *offense rule* is updated to **accommodate the new offenses**.

REDMINE

The ticket is **populated** with data from the actions taken and then **closed**.

SOC

*Master Block List

Red Hat

USE CASE - MBL* Automation Outwards

Threat Hunting

A new security bulletin is received.

REDMINE

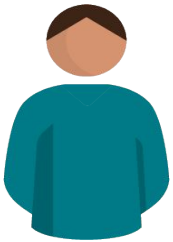
A **ticket is opened** with the update request.

FORTINET

A new signature is created on the IPS to **accommodate the new signatures**.

REDMINE

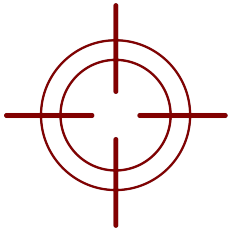
The ticket is **populated** with data from the actions taken and then **closed**.



NOC

Red Hat

USE CASE - Implementing A New Custom Signature On IPS

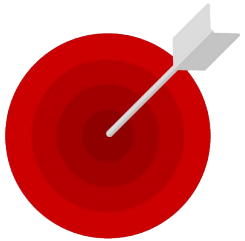


Threat Hunting

```
- hosts: fortios
  vars:
    vdom: "root"
  tasks:
    - name: Configure IPS custom signature
      fortios_ips_custom:
        vdom: "{{ vdom }}"
        https: “False"
        ssl_verify: “False"
        state: “present"
        ips_custom:
          action: “pass"
          application: “Other"
          comment: "TEST IPS Comment"
            location: "client"
            log: "disable"
            log_packet: "disable"
            os: "Linux"
            protocol: "TCP"
            severity: "info"
            signature: "F-SBID( --name 'Block.example.com'; --pattern 'example.com';
--service HTTP; --no_case; --flow from_client; --context host; )"
           status: "disable"
            tag: "ipsSignature"
```

FORTINET

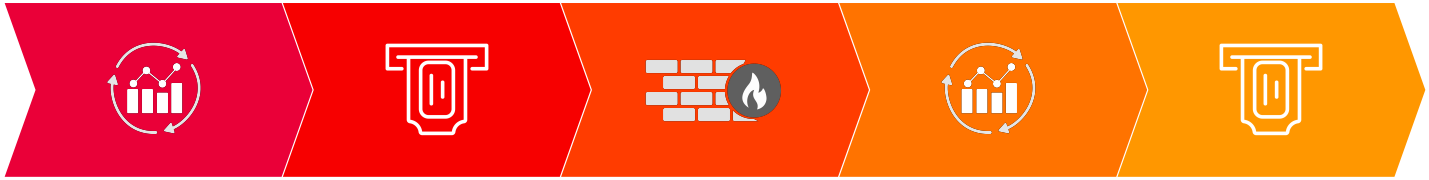
Incident Response



Red Hat

USE CASE - Public IP Blacklisting

Incident Response



IBM QRadar

Generates an *offense* from an anomaly on the external network perimeter or access from an IP flagged on a security bulletin.

REDMINE

A **ticket is opened** and populated with all relevant data.

CISCO

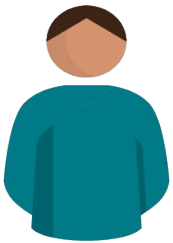
The IP address is **added to the *blacklist*** *object group* on the edge firewalls.

IBM QRadar

The *offense* criteria are no longer met and it **can be closed**.

REDMINE

The ticket is **populated** with data from the actions taken and then **closed**.

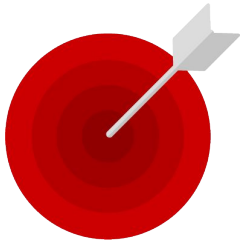


NOC

SOC

Red Hat

USE CASE - Public IP Blacklisting



Incident Response

```
- hosts:  ciscoasa
  gather_facts: no
  connection:   network_cli
  vars:
    acl_name:

  tasks:
    - asa_acl:
        lines:
            - access-list ACL-ANSIBLE extended deny ip host {{
ip_address }} any log

        match:   strict
        replace: block
```

CISCO

USE CASE - SSO Credentials Quarantine

+ Force Password Reset

Incident Response

IBM QRadar

Generates an *offense* from an authentication anomaly.

REDMINE

A **ticket is opened** and populated with all relevant data.

Syncope

Credentials are **blocked** for further investigation.

IBM QRadar

The *offense* criteria are no longer met and the **investigation can proceed**.

REDMINE

The ticket is **populated** with data from the actions taken. Investigation proceeds and credentials sanitised.

Syncope

A **password reset is forced** on the credentials.

IBM QRadar REDMINE

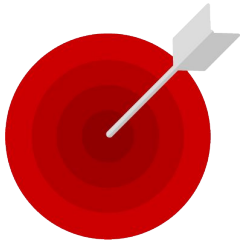
The ticket is **populated** with data from the actions taken and then **closed**. The *offense* on QRadar is **closed**.

SOC

PAM

Red Hat

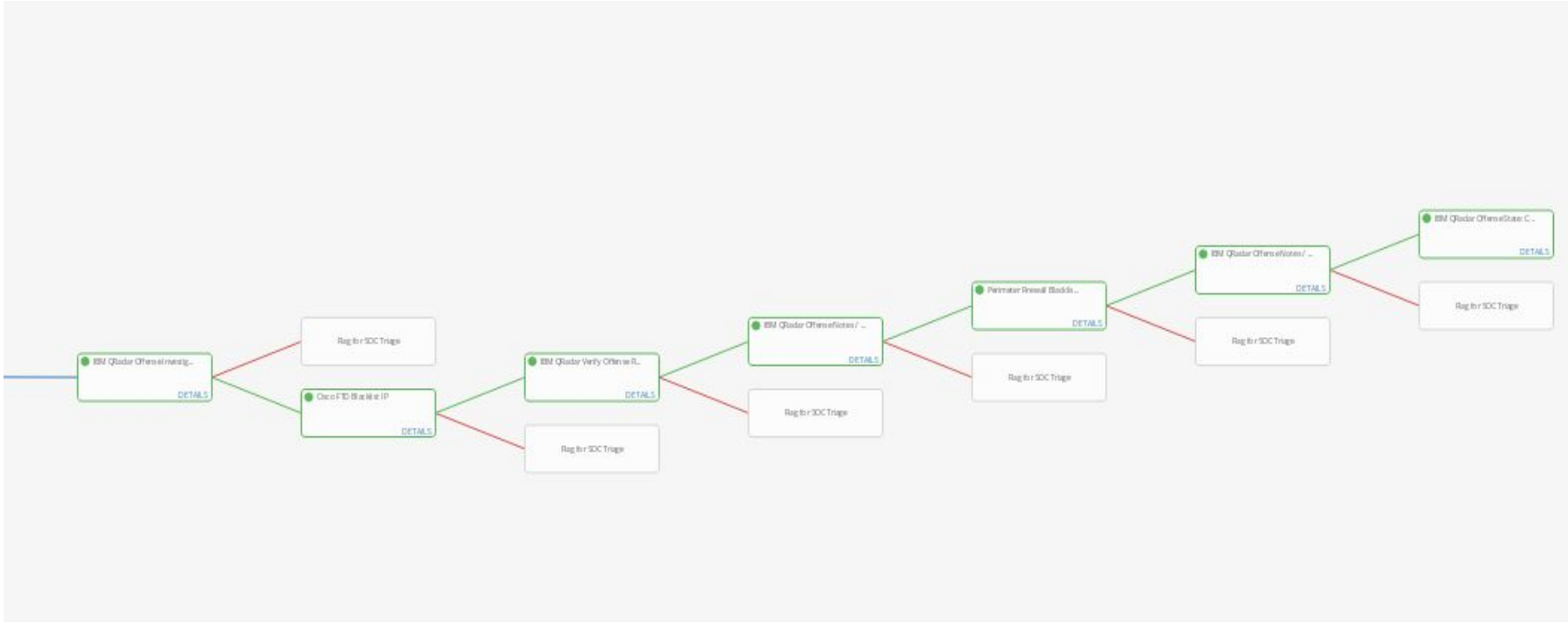
USE CASE - SSO Credentials Quarantine + Force Password Reset



Incident Response

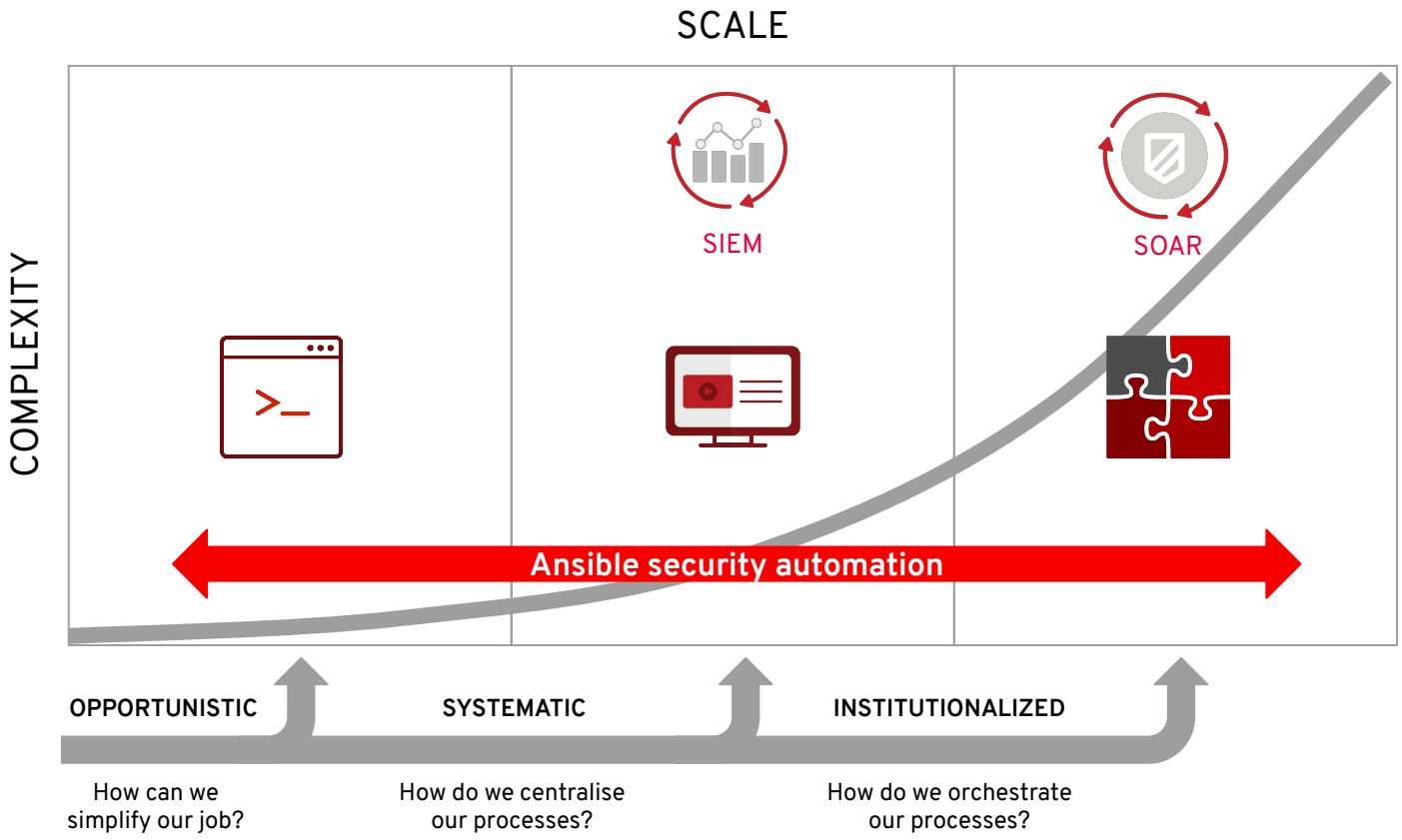
```
- name: syncope change user status
  hosts: syncopeserver
  vars:
     vars_files:
    - group_vars/pam.yml

  tasks:
    - name: change credential status

      Syncope_change_user_status:

         changeStatusOnSyncope: true
         adminUser: "{{ adminUser }}"
         adminPwd: "{{ password }}"
         serverName: "{{ syncope-server }}"
         syncopeUser: "{{ syncope-user }}"
         newStatus: SUSPEND
```

Automate An Entire Process Through Tower



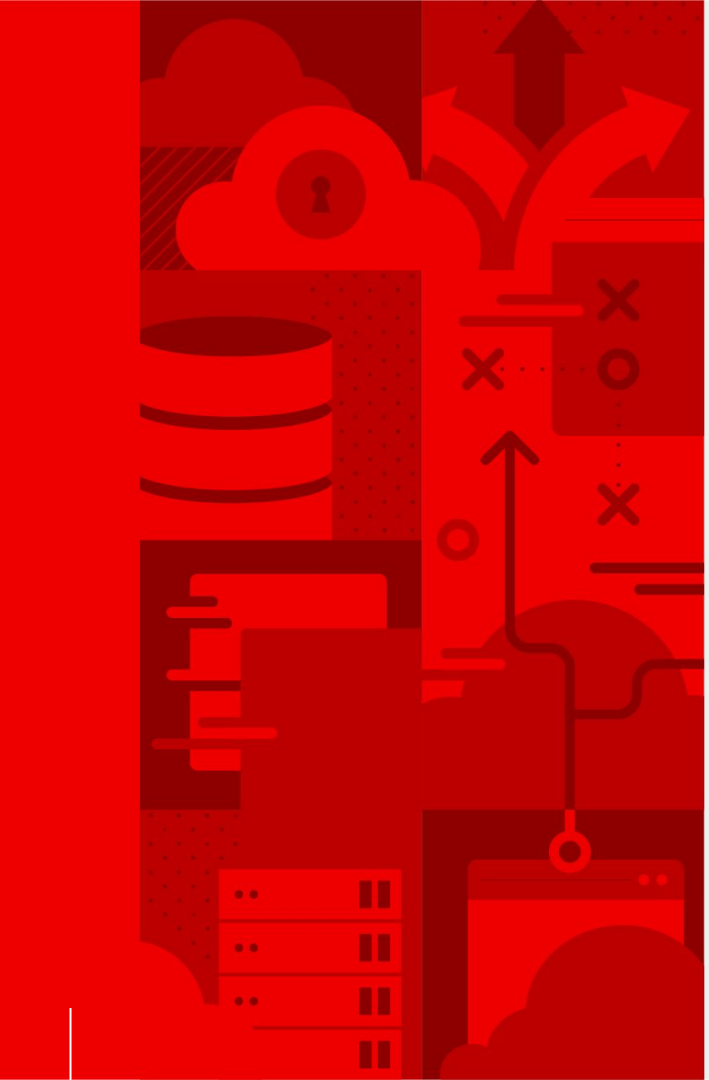
Red Hat

Where are you in the Automation Journey



Source: The journey to security automation

Red Hat



Thanks

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat