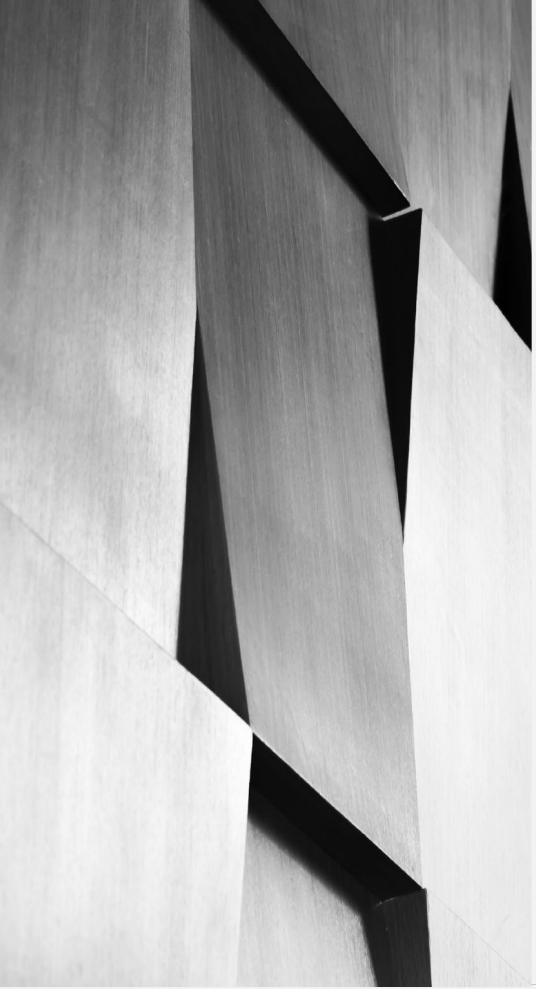
#ANSIBLEFEST2019

Automate your SOC with Ansible

Faz Sadeghi
Specialist Solution Architect - Red Hat

Red Hat | ANSIBLE



$103 bil.

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). "

65%

Severity of attacks has increased

57%

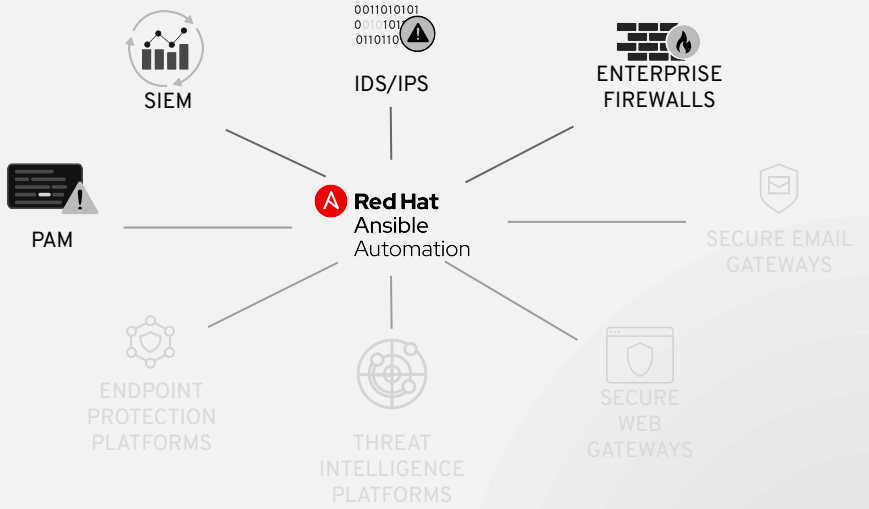
Time to resolve an incident has increased

Source:
https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/
https://venturebeat.com/2017/12/16/the-lesson-behind-2017s-biggest-enterprise-security-story/
https://published-prd.lanyonevents.com/published/rsaap15.6381_ap18/sessionsFiles/4483/TTA-F03%20Security%20Operations%202018%20What%20Is%20Working%20What%20Is%20Not_FINAL.pdf

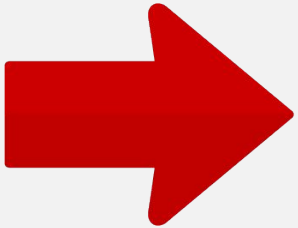
What's Ansible security automation?

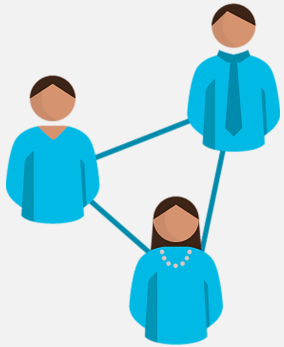
DESIGNED TO ORCHESTRATE THREAT RESPONSE ACROSS SECURITY DOMAINS

- 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



Why should YOU care about security?





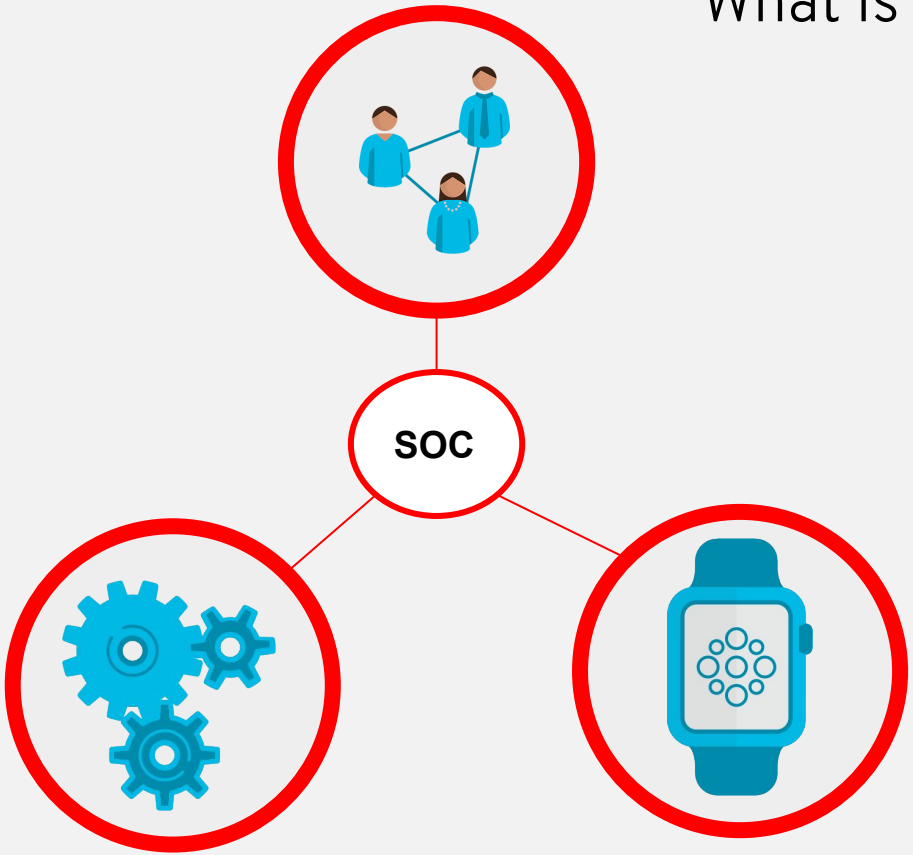
IT Process

Core practitioners.
Experts with deep IT technical knowledge.

Organization-wide Process

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

What is a SOC?

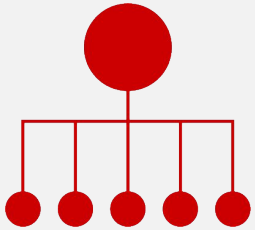


- Prevent
- Detect
- Assess
- Respond

Why do we need a SOC?

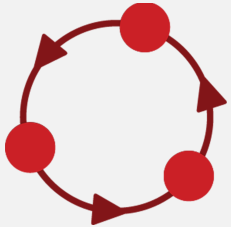
> Organizations are building internal security operations capabilities (even if in a limited sense) because they desire more control over their security monitoring and response process. They also want to have more informed conversations with regulators.
>
> Gartner

What kind of SOCs are out there?



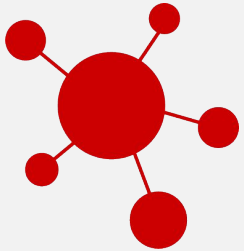
Command

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



Multifunction

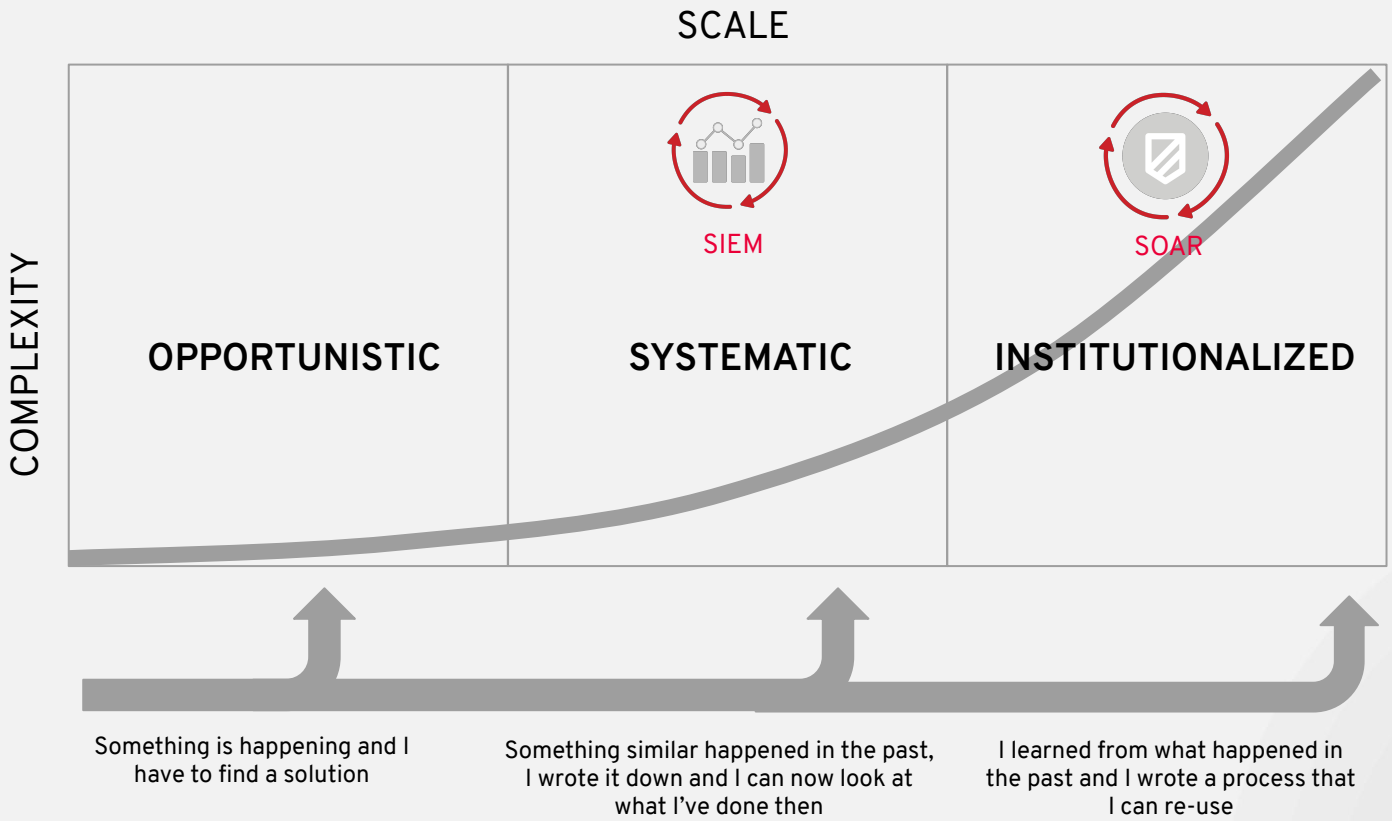
Dedicated facility with a dedicated team performing not just security, but other critical 24/7 IT operations from the same facility to reduce costs.



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



The Italian Army

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

190,000 Users

470+ Barracks

15 Datacentres

National territory and International missions

Maintain an Extensive Private Network

“”

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

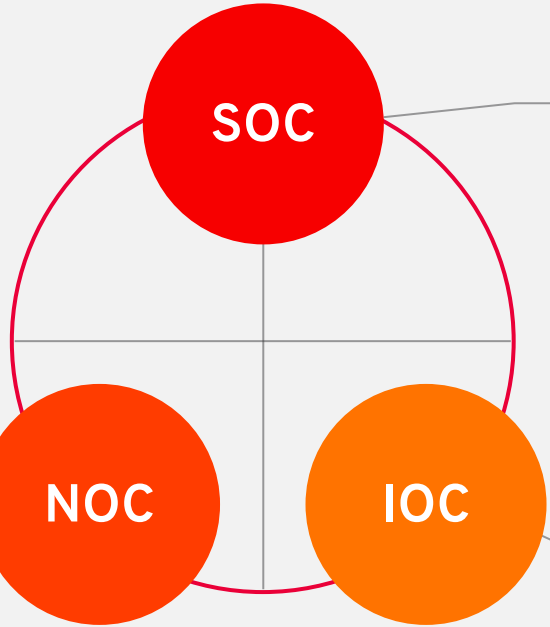
Michael S. Rogers

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

Saji Ijiyemi

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

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

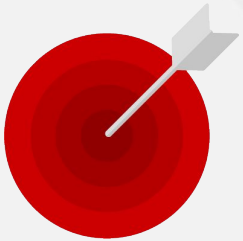
USE CASES

Triage Of Suspicious Activities

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

Threat Hunting

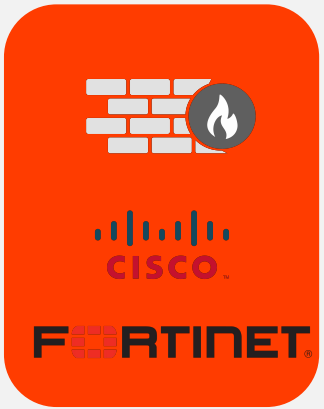
Automating alerts, correlation searches and signature manipulation

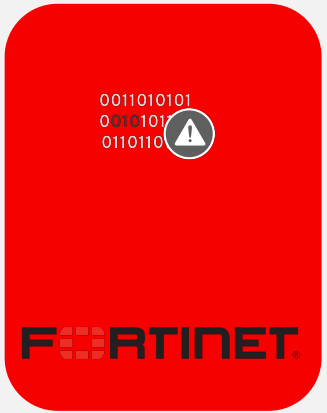


Incident Response

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

The Tool Set



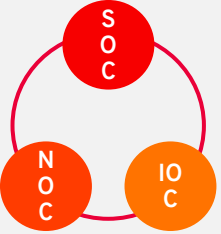


Offense

Signature

DISCLAIMER

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



Lieutenant Luigi
SOC
QRADAR

Captain Chiara
IOC
IDM

Major Mario
NOC
IDS/IPS

Triage Of Suspicious Activities

USE CASE 1 - INVESTIGATION ENRICHMENT ON FIREWALLS

Lieutenant Luigi

Triage OfSuspicious Activities

IBM QRadar

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

REDMINE

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

CISCO FORTINET

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

IBM QRadar

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

CISCO FORTINET

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

REDMINE

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

USE CASE 1 - INVESTIGATION ENRICHMENT ON FIREWALLS

Triage Of Suspicious Activities

```
- 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 1 - INVESTIGATION ENRICHMENT ON FIREWALLS

Triage Of Suspicious Activities

```
- 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 1 - INVESTIGATION ENRICHMENT ON FIREWALLS

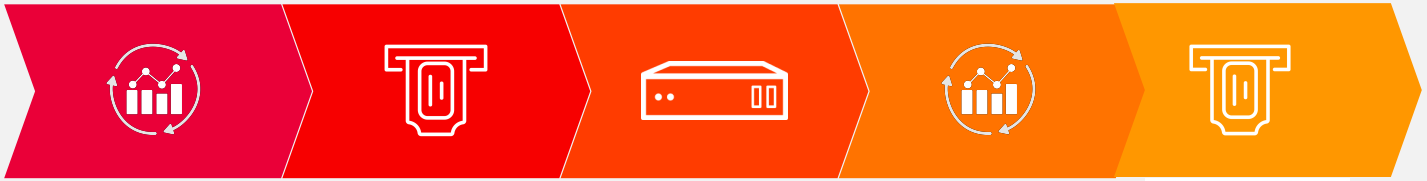
Triage Of Suspicious Activities

```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

Lieutenant Luigi

USE CASE 2 - INVESTIGATION ENRICHMENT ON SERVER



IBM QRadar

Generates an *offense* indicating a malware has been installed on an application server.

REDMINE

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

Linux

The application server is searched for the malware files.

IBM QRadar

No malware has been found so the offense can be dismissed as a false positive.

REDMINE

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

USE CASE 2 - INVESTIGATION ENRICHMENT ON SERVER

Triage Of Suspicious Activities

```yaml
- name: Gather log files from remote systems
  hosts: lab
  become: yes
  tasks:
    - name: Find logs
      find:
        paths: /var/log/
        patterns: '*.log'
        recurse: yes
      register: _logs
    - name: Fetch logs
      fetch:
        src: "{{ item.path }}"
        dest: logs
      with_items: "{{ _logs.files }}"
```

Threat Hunting

Lieutenant Luigi

USE CASE 3 - MBL* Automation Inwards

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.**

Master Block List

Major Mario

USE CASE 4 - MBL* Automation Outwards

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**.

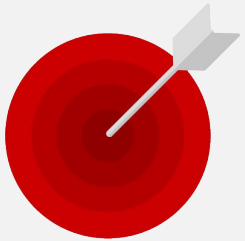
USE CASE 4 - IMPLEMENTING A NEW CUSTOM SIGNATURE ON IPS

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"
```

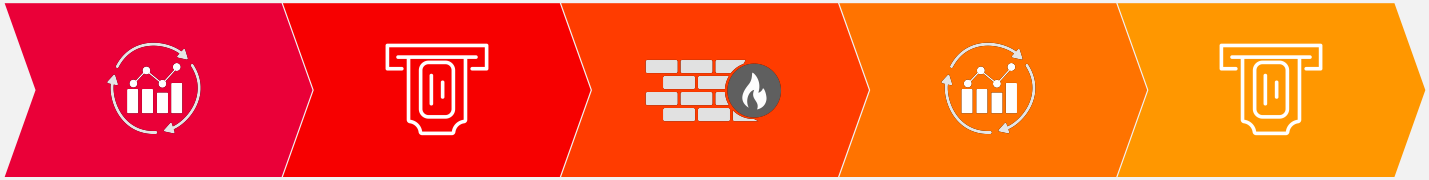
FORTINET

Incident Response



Lieutenant Luigi

USE CASE 5 - PUBLIC IP BLACKLISTING



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.

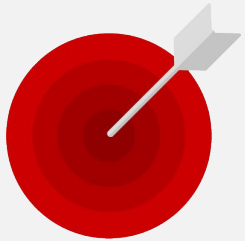
IBM QRadar

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**.

USE CASE 5 - INCIDENT RESPONSE



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
```

Captain Chiara

USE CASE 6 - SSO CREDENTIALS QUARANTINE + FORCE PASSWORD RESET

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.

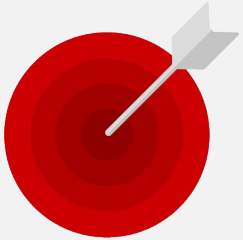
Syncope

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**.

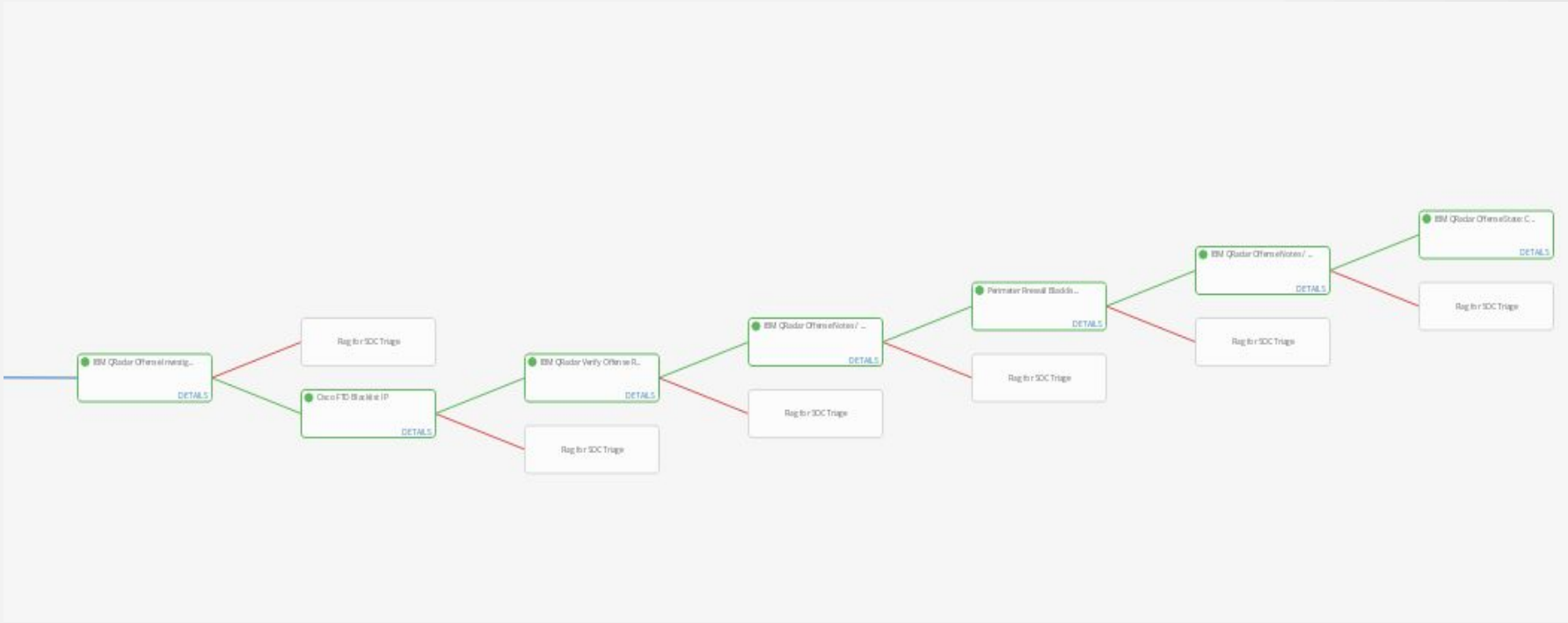
USE CASE 6 - SSO CREDENTIALS QUARANTINE



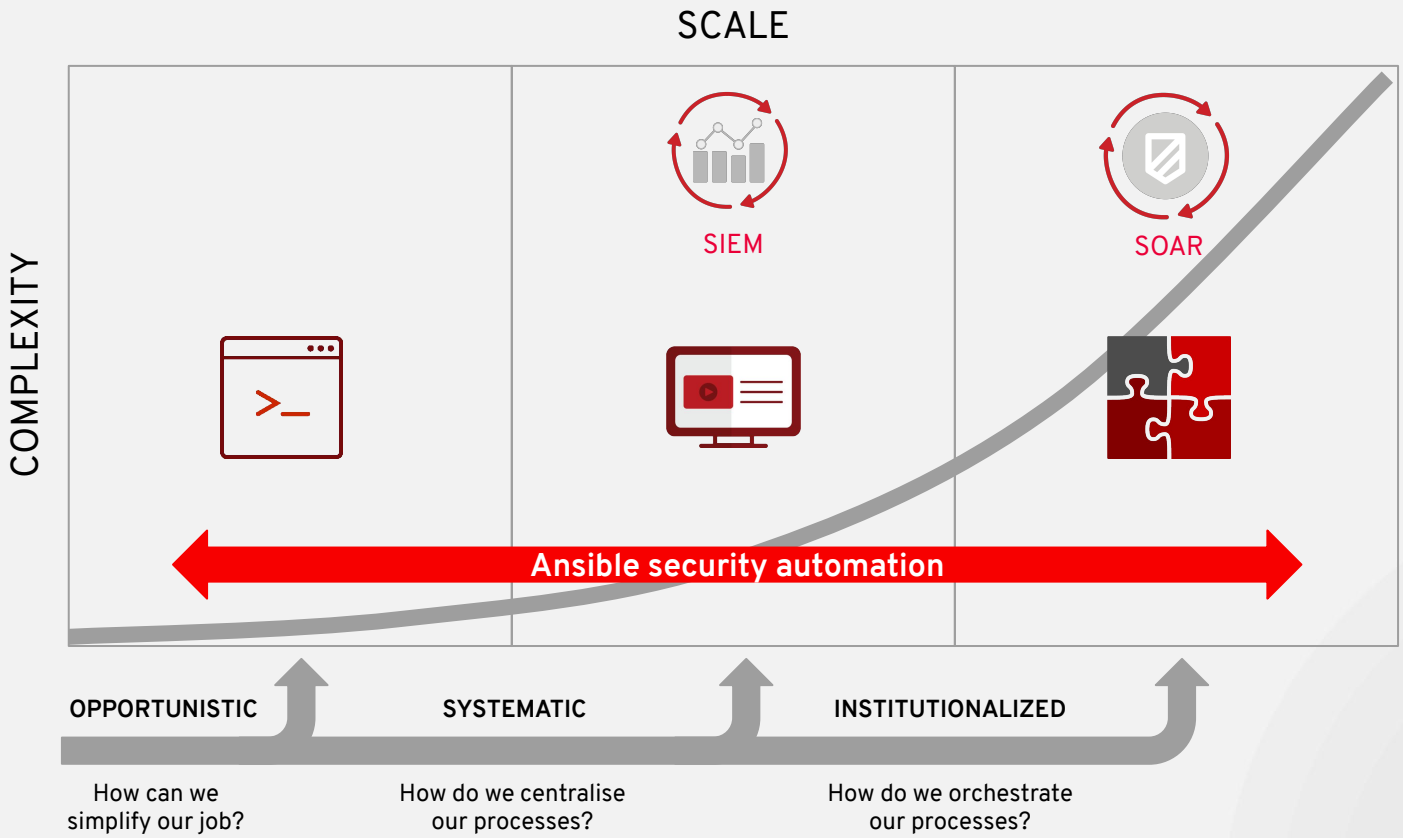
Incident Response

```
- 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



Where are you in the Automation Journey



#ANSIBLEFEST2019

THANK YOU


youtube.com/AnsibleAutomation


facebook.com/ansibleautomation


linkedin.com/company/Red-Hat


twitter.com/ansible