Automate your Security Operations Center (SOC) with Ansible

Ajay Chenampara
Sr. Solution Architect
termlen0@redhat.com
@termlen0
The State of Enterprise IT Security

$103B
Global spending on security hardware, software and services

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

40
Average number of security tools used in a SOC

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
What’s Ansible security automation?

DESIGNED TO ORCHESTRATE THREAT RESPONSE ACROSS SECURITY DOMAINS

- Ansible Security Automation is Ansible’s expansion deeper into the security use case.
- Integrates & orchestrates multiple classes of security solutions
- Provides modules, roles and playbooks to support security use cases across those solutions
Who Are Our Partners?

Security Information & Events Management

Enterprise Firewalls

Intrusion Detection & Prevention Systems

Privileged Access Management

splunk
IBM
Check Point
CISCO
Snort
Check Point
f5
FORTINET
FORTINET
SYNGE
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
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.
Something similar happened in the past, I wrote it down and I can now look at what I've done then.

I learned from what happened in the past and I wrote a process that I can re-use.

Something is happening and I have to find a solution.

Source: The journey to security automation
The Italian Army

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

190,000 Users
National territory and International missions

470+ Barracks
Maintain an Extensive Private Network

15 Datacentres
“"You can’t predict future, but you can plan for it."”

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

Saji Ijiyemi

Michael S. Rogers
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

SOC

NOC

IOC

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
Security Analysts
- Investigate
- Prevent
- Respond

Network Ops
- Administer network endpoints
  - Firewalls
  - VPNs

IT Ops
- Administer server infrastructure, DNS, LDAP/AD, SSO
The Tool Set
Investigation Enrichment
USE CASE 1 - Investigation Enrichment On Firewalls

Investigation Enrichment

1. **IBM QRadar**
   - Generates an offense from an anomaly on mission site.

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

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

4. **IBM QRadar**
   - The additional information allows to dismiss the offense as a false positive.

5. **FORTINET**
   - Local firewalls are rolled back to their previous configurations to avoid overload/fatigue.

6. **REDMINE**
   - The ticket is populated with data from the actions taken and then closed.
USE CASE 1 - Investigation Enrichment On Firewalls

- 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

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

The application server is searched for the malware files.

A ticket is opened and populated with all relevant data.

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

No malware has been found so the offense can be dismissed as a false positive.
USE CASE 2 - Investigation Enrichment On Servers

- 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
USE CASE 3 - MBL* Automation Inwards

Threat Hunting

A new security bulletin is received.

A ticket is opened with the update request.

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

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

*Master Block List
A new signature is created on the IPS to accommodate the new signatures. A ticket is opened with the update request. A new security bulletin is received. The ticket is populated with data from the actions taken and then closed.

Threat Hunting
USE CASE 4 - Implementing A New Custom Signature On IPS

- 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"
Incident Response
The IP address is added to the blacklist object group on the edge firewalls. The offense criteria are no longer met and it can be closed.

A ticket is opened and populated with all relevant data.

The ticket is populated with data from the actions taken and then closed.
USE CASE 5 - Public IP Blacklisting

- hosts: ciscoasa
gather_facts: no
collection: 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
The offense criteria are no longer met and the investigation can proceed.

Credentials are blocked for further investigation.

A ticket is opened and populated with all relevant data.

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

A password reset is forced on the credentials.

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

The ticket is closed. The offense on QRadar is closed.
- 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

Ansible security automation

Source: The journey to security automation