How to leverage Ansible Security Automation if you are a Dev or a SecOp

Adam Miller
Senior Principal Software Engineer
Technical Architect & Lead Developer, Ansible Security
ANSIBLE SECURITY AUTOMATION
Ansible Security Automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events.
WHY ANSIBLE SECURITY AUTOMATION?

“For one, security teams are overwhelmed. 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).”

Venturebeat

57% of respondents said the time to resolve an incident has increased

65% reported the severity of attacks has increased

63% of respondents say their leaders understand that automation, machine learning, artificial intelligence and orchestration strengthens cyber resilience.

Ponemon Institute

Source:
The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)
WHAT TYPES OF DEVICES?
WHO ARE OUR PARTNERS?

Security Information & Events Management
Enterprise Firewalls
Intrusion Detection & Prevention Systems
Privileged Access Management
ANSIBLE INTEGRATION WITH SOAR

* Orchestrating Response to Cyber Attacks with Ansible and IBM Resilient at 2PM in Rooms 311-312 *
WHICH **SOC** ACTIVITIES CAN BENEFIT THE MOST FROM AUTOMATION?

**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
WHAT **DEVOPS** ACTIVITIES CAN BENEFIT THE MOST FROM AUTOMATION?

**Deployment**

Ensure Code Deployment Commit Has Firewall Rules, IDS Signatures, Passes Validation

**Baselining**

Update relevant security tools to understand the application behaviour

**Integration**

Interact with the broader corporate infrastructure
FIREWALLS
MANAGEMENT
INCIDENT RESPONSE

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

- hosts: checkpoint
  connection: httpapi
  tasks:
  - name: Create blacklist IP
    include_role:
      name: acl_manager
      tasks_from: blacklist_ip
    vars:
      source_ip: "{{ attacker_ip }}"
      destination_ip: "{{ target_ip }}"
  ansible_network_os: checkpoint

ref: https://github.com/ansible-security/acl_manager
INCIDENT RESPONSE

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

```
- hosts: ftd
  connection: httpapi
  tasks:
    - name: Create blacklist URL
      include_role:
        name: acl_manager
        tasks_from: blacklist_url
      vars:
        blacklist_url_type: url
        blacklist_name: "attacker_url"
        blacklist_url_description: "Attacker url description"
        blacklist_url: www.attacker.com
        ansible_network_os: cisco_ftd
```

ref: https://github.com/ansible-security/acl_manager
BRING IT INTO DEV WORKFLOWS WITH CI

DEPLOYMENT

Ensure CI Security Environment Setup on Fresh Deployment Code Commit Has Firewall Rules, IDS Signatures, Passes Validation

```yaml
- hosts: checkpoint
  connection: httpapi
  tasks:
    - name: Grant Access to App Floating IP
      include_role:
        name: acl_manager
      tasks_from: whitelist_ip
      vars:
        source_ip: *
        destination_ip: "{{ app_float_ip }}"
        ansible_network_os: checkpoint

ref: https://github.com/ansible-security/acl_manager
```
DEVSECOPS REAL WORLD SCENARIO - CI PIPELINES (JENKINS)
INTRUSION DETECTION/PREVENTION SYSTEMS MANAGEMENT
IMPLEMENTING A NEW SIGNATURE ON SNORT IDS

vars:
  ids_provider: snort
  protocol: tcp
  source_port: any
  source_ip: any
  dest_port: any
  dest_ip: any

tasks:
  - name: Add snort password attack rule
    include_role:
      name: "ids_rule"
      vars:
        ids_rule: 'alert {{protocol}} {{source_ip}} {{source_port}}
          -> {{dest_ip}} {{dest_port}}  (msg:"Attempted DDoS Attack";
          uricontent:"/ddos_simulation"; classtype:successful-dos;
          sid:99000010; priority:1; rev:1;)'
        ids_rules_file: '/etc/snort/rules/local.rules'
        ids_rule_state: present

THREAT HUNTING

Automating alerts, correlation searches and signature manipulation
IMPLEMENTING A NEW IPS SENSOR ON FORTINET FORTIOS

hosts: fortios
vars:
  vdom: "root"
tasks:
- name: Configure IPS Sensor
  fortios_ips_custom:
    vdom: "{{ vdom }}"
    https: "False"
    ssl_verify: "False"
    state: "present"
    ips_sensor:
      name: default2
      comment: Prevent critical attacks.
      block_malicious_url: disable
      extended_log: disable
      entries:
        - id: 1
          rule: []
          location: all
          severity: medium high critical
          protocol: all
          os: all
          application: all
          status: default
          log: enable
          log_packet: disable
          log_attack_context: disable
          action: default
          rate_count: 0
          rate_duration: 60
          rate_mode: continuous
          rate_track: none
          exempt_ip: []
          quarantine: none
          quarantine_expiry: 5m
          quarantine_log: enable
          filter: []
          override: []

BASELINING

Update relevant security tools to understand the application behaviour
DEVSECOPS REAL WORLD SCENARIO - ZUUL CI
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) MANAGEMENT
ADD LOG SOURCE AND ENABLE SIEM RULE TO GENERATE OFFENSES

- name: Create a QRadar Log Source and Enable Offense Rule
  hosts: qradar
  collections:
    - ibm.qradar
  tasks:
    - name: Create QRadar Log Source - CheckPoint
      qradar_log_source_management:
        name: "CheckPoint LogSource: {{ chkpnt_ip_addr }}"
        type_name: "Check Point FireWall-1"
        state: present
        description: "Automated Creation of CheckPoint LS"
        identifier: "{{chkpnt_ip_addr}}"

- name: Enable Remote Excessive Firewall Denies Rule
  qradar_rule:
    name: "Excessive Firewall Denies from Remote Host"
    state: enabled

TRIAGE OF SUSPICIOUS ACTIVITIES

Enabling programmatic access to log configurations such as destination, verbosity, etc.
ADD LOG SOURCE AND ENABLE SIEM RULE TO GENERATE OFFENSES

TRIAGE OF SUSPICIOUS ACTIVITIES

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

- name: Get info about Qradar Offense - Excessive Offense
  qradar_offense_info:
  name: "Excessive Offense"
  register: offense_info

- name: Assign Actions to Offense
  qradar_offense_action:
  id: offense_info["offenses"][0]["id"]
  status: "hidden"
  assigned_to: "admin"
  protected: false

- name: Add Note to Offense
  qradar_offense_note:
  id: offense_info["offenses"][0]["id"]
  note_text: "Run investigate_offense.yml playbook"
ADD LOG SOURCE AND ENABLE SIEM RULE TO GENERATE OFFENSES

- name: Create a Splunk Enterprise Security Input
  hosts: splunk
  collections:
    - splunk.enterprise_security
  tasks:
    - name: Create Splunk Log Source - Web AppX
      splunk_data_input_network:
        name: "Web AppX Log Source {{ appx_id }}"
        port: "8099"
        state: present

INTEGRATION

Interact with the broader corporate infrastructure
SECOPS REAL WORLD SCENARIO

Generates an offense from an anomaly on the intranet perimeter or outbound traffic from an internal machine.

An investigation is opened and populated with all relevant data.

The IP address is added to the blacklist on Firepower through FTD.

The offense criteria are no longer met.

The investigation is populated with data from the actions taken.

The IP address is added to the blacklist on the other firewalls in the perimeter.

The investigation is populated with data from the actions taken and then closed. The offense on QRadar is closed.
SECOPS REAL WORLD SCENARIO - TOWER WORKFLOW
DEV REAL WORLD SCENARIO - DEPLOY WITH TOWER
DEVSECOPS
RELEVANT RESOURCES

Ansible.com: https://www.ansible.com/use-cases/security-automation

Mojo: https://mojo.redhat.com/groups/ansible/projects/ansible-security-automation

Galaxy:
- https://galaxy.ansible.com/ansible_security
- https://galaxy.ansible.com/ibm/qradar
- https://galaxy.ansible.com/splunk/enterprise_security

GitHub: https://github.com/ansible-security

IRC: #ansible-security on irc.freenode.net
QUESTIONS?
#ANSIBLEFEST2019

THANK YOU

youtube.com/AnsibleAutomation  facebook.com/ansibleautomation
linkedin.com/company/Red-Hat  twitter.com/ansible
NARRATIVE

● Ansible security automation intro
  ○ Ansible security automation history
  ○ Ansible security automation available platforms/content

● How SecOps will consume ASA vs how Developers will consume the same content
  ○ SecOps using Ansible for Response and Remediation > Our use cases
  ○ Developers using Ansible for Deployment > Web App CI/CD

● Example 1: Firewall management
  ○ SecOps use these modules to blacklist/whitelist an IP/URL as a result of an investigation
  ○ Devs use these modules to open all the relevant ports on the corporate firewalls when deploying a new application

● Example 2: IDS management
  ○ SecOps use these modules for threat hunting proactively updating the signatures
  ○ Devs use these modules to update snort signatures and identify what is and is not valid traffic

● Example 3: SIEM management
  ○ SecOps use these modules to enable relevant search queries and update investigations
  ○ Devs use these module to send the relevant logs of the new workloads to the SIEM

● All of that comes together
  ○ For SecOps to fully automate end to end investigation and remediation processes
  ○ For Devs to integrate security tools in their CI/CD pipeline

● The future
  ○ DevSecOps > Ansible security automation will support code/dev oriented security tools and Ansible language can be used as the defacto standard for interactions between SecOps and Dev