Cybersecurity Automation and Prevention with Check Point and Ansible

Amiad Stern
Team leader, Check Point
amiads@checkpoint.com

Sumit Jaiswal (justjais)
Senior Software Engineer, Ansible
sjaiswal@redhat.com
AGENDA

● Check Point:
  ○ who we are, the challenges of our customers
● Ansible security automation:
  ○ what it is, which problems is it trying to solve
● Ansible & Check Point: better together
● Demos
The Largest Global Cyber Security Company

- Global Leader – 100,000+ Customers, 88+ Countries, 6,200+ Partners
- Over 25 years of cutting edge technologies, Industry’s most visionary player
- Innovation leadership - more than twice the developers of closest competitor
- Traded on Nasdaq since 1996 - CHKP
- 5,100+ Employees worldwide, top talent

TRUSTED BY FORTUNE 500 COMPANIES
Check Point is the Most Recommended

INNOVATION. VISION. LEADERSHIP.

#ANSIBLEFEST2019
Check Point’s Typical Customer
Check Point’s Typical Customer

+500 Offices
+500,000 Assets
Cloud Setups
+1000 Firewalls

+150,000 Employees
+500 Developers
Typical Customers’ Challenges

Connect

Protect, Remediate

Protect

Automate

CI/CD

Maintain, Prevent
Check Point’s Central Management

The key to managing security complexity is security **consolidation**
Why Ansible?

**Simple**
- Human readable automation
- No special coding skills needed
- Hides away complexity
- Usable by every team
- Makes users productive faster

**Powerful**
- Configuration management
- Deployment & Integration
- Workflow orchestration
- Multi domain automation
- Able to orchestrate complex processes

**Agentless**
- Agentless architecture
- Uses OpenSSH, WinRM, API
- No agents to exploit or update
- More efficient & secure
- Easier to integrate in existing infrastructures
Why Ansible Security Automation?

- Reported increased severity of attacks: 65%
- Said the time to resolve an incident has grown: 57%
- Have their ideal security-skilled staffing level, making it the #2 barrier to Cyber resilience: 29%
- Portion of alerts coming in that the average security team examines every day: 5%

Source:
1 The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)
Why Ansible Security Automation?

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

Ponemon Institute

Source:
1 The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute, 2018 (Sponsored by IBM)
What Is 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

What Is It?
What Does It Do?

- **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.
Check Point Integration With Ansible

The Ansible 2.9 release includes following Checkpoint enablement:

- Modules to manage Checkpoint Firewall
- Facts Modules to query Checkpoint Firewall objects
- All Modules are Certified and Jointly supported by Ansible and Check Point
- Collections soon available at: https://galaxy.ansible.com/check_point
- Module Guide is available at: https://docs.ansible.com/ansible/devel/modules/list_of_network_modules.html#check-point
- All Check Point R80 versions are supported by this integration.

For more details and relevant Hotfixes, see sk114661
Ansible-Check Point Modules

CP_MGMT_THREAT_RULE
Module handles the Check Point API - *add-threat-rule* which manages threat-rule objects on Check Point

CP_MGMT_THREAT_RULE_FACTS
Facts Module handles the Check Point API - *show-threat-rule* which gets threat-rule objects facts on Check Point

Red Hat
Ansible
Automation

How Checkpoint modules are structured in Ansible 2.9 release
ENABLING LOG FORWARDING ON CHECK POINT NGFW

TRIAGE OF SUSPICIOUS ACTIVITIES

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

- name: Forward CheckPoint NGFW Logs
  hosts: checkpoint
  tasks:
    include_role:
      name: log_manager
      tasks_from: forward_logs_to_syslog
  vars:
    syslog_server: 192.168.0.1
    checkpoint_server_name: test
    firewall_provider: checkpoint

ref: https://github.com/ansible-security/log_manager
---
- hosts: checkpoint
  connection: httpapi
  gather_facts: false
  tasks:
  - name: add-threat-rule
    cp_mgmt_threat_rule:
      comments: Set New IPS rule
      install_on: Policy Targets
      layer: 598fd9ab-93e4-465b-9725-d228f3905cae
      name: new_ips_rule
      position: bottom
      protected_scope: All_Internet
      state: present
      track: None
      auto_publish_session: true

Threat Hunting

Automating alerts, correlation searches and signature manipulation
Threat Hunting

Automating alerts, correlation searches and signature manipulation

---
- hosts: checkpoint
  connection: httpapi
  gather_facts: False
  tasks:
    - name: Show Check Point threat rule facts
cp_mgmt_threat_rule_facts:
    name: new_ips_rule
    layer: 598fd9ab-93e4-465b-9725-d228f3905cae
    register: show_threat_rule_response
  - debug:
    var: show_threat_rule_response
BLACKLIST THE ATTACKER IP ON CHECK POINT NGFW

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

```yaml
- hosts: checkpoint
  connection: httpapi
  tasks:
    - name: Create blacklist IP
      include_role:
        name: acl_manager
      tasks_from: blacklist_ip
      vars:
        source_ip: 192.168.0.10
        destination_ip: 192.168.0.11
        ansible_network_os: checkpoint
```

ref: https://github.com/ansible-security/acl_manager
How Ansible and Checkpoint Work together

Security Engineer

ANSIBLE + CHECK POINT Platform

Round the clock Security Automation
Demo
Day-to-Day Configuration
DevOps Approach

#ANSIBLEFEST2019
Basically, the end goal is to have firewall configuration updated be a part of CI/CD pipeline for application deployments.

Security Team

IT team

Configuration files + Version Control

Jenkins

Red Hat Ansible Automation

Check Point Security Management Server & Gateways

Get recorded demo here
Basically, the end goal is to have firewall configuration updated be a part of CI/CD pipeline for application deployments.
Setup
Maintenance
If I had to manually deploy a patch to all firewalls, it would consume a full time resource
Cloud Setup
Provisioning
Call to Action

Push the New Modules to Ansible Github repo & New Roles to Galaxy repo

Develop & Test New Modules and Roles to Support the Integration

Understand & Experience Ansible + Check Point Firewall
Q and A
THANK YOU