CorwdSec

Status	Production
Supported distro	CentOS 7/8

This role deploys the crowdsec agent.

CrowdSec agent

Here's a sample config for the agent. Running with local and central API enabled, using a MySQL bakend

```
cs_db_engine: mysql
cs_capi_enabled: True
cs_lapi_enabled: True
cs_lapi_src_ip:
  - 10.29.1.14 # Only the rev proxy can reach the API
cs_use_x_forwarded_for: True
cs_acquis:
  - filenames:
      - /run/g2cs/logs/syslog.log
    labels:
      type: syslog
  - filenames:
      - /run/g2cs/logs/nginx/access.log
      - /run/g2cs/logs/nginx/error.log
    labels:
      type: nginx
  - filenames:
      - /run/g2cs/logs/httpd/access.log
      - /run/g2cs/logs/httpd/error.log
    labels:
      type: apache2
  - filenames:
      - /run/g2cs/logs/zimbra/mailbox.log
```

```
    labels:
      type: zimbra

cs_parsers:
  - crowdsecurity/syslog-logs
  - crowdsecurity/geoip-enrich
  - crowdsecurity/dateparse-enrich
  - crowdsecurity/whitelists
  - crowdsecurity/sshd-logs
  - crowdsecurity/iptables-logs
  - crowdsecurity/nginx-logs
  - crowdsecurity/apache2-logs
  - crowdsecurity/http-logs
  - crowdsecurity/postfix-logs
  - crowdsecurity/postscreen-logs
  - firewallservices/zimbra-logs
  - firewallservices/lemonldap-ng
cs_scenarios:
  - crowdsecurity/ban-defcon-drop_range
  - crowdsecurity/ssh-bf
  - crowdsecurity/http-bf-wordpress_bf
  - crowdsecurity/http-generic-bf
  - crowdsecurity/http-sensitive-files
  - crowdsecurity/http-sqli-probing
  - crowdsecurity/http-xss-probing
  - crowdsecurity/http-backdoors-attempts
  - crowdsecurity/http-path-traversal-probing
  - crowdsecurity/iptables-scan-multi_ports
  - crowdsecurity/postfix-spam
  - firewallservices/zimbra-bf
  - firewallservices/lemonldap-ng-bf
```

g2cs

You can use the g2cs companion role. This small daemon can receive a syslog stream from graylog (in CEF format) and write files for crowdsec to consume

```
cs_user: g2cs
```

```
g2cs_port: 514
g2cs_src_ip:
  - 10.29.1.20 # Graylog FWS
```

CrowdSec Firewall Bouncer

You can deploy firewall bouncers with the crowdsec_firewall_bouncer role

```
# Use crowdsec local API
cs_lapi_url: https://cs.example.org/
cs_lapi_server: crowdsec.example.org
```

Reverse proxy

You can use a reverse proxy to expose your local API to your other machines. Here's a sample on a machine using the nginx role to provide the reverse proxy functionnality

```
nginx_vhosts:
  # Crowdsec Local API
  - name: cs.example.org
    proxy:
      backend: http://crowdsec.example.org:8080
    auth: False
    src_ip:
      - "{{ trusted_ip }}"
      - 10.29.0.0/16
      - 10.30.0.0/16
      - 10.99.0.0/16
      - 192.168.7.0/24
```

Révision #4
Créé 17 mars 2021 21:52:57 par Daniel Berteaud
Mis à jour 18 mars 2021 09:23:04 par Daniel Berteaud