HUBBLE

SECURITY FOR DEVOPS

INTRODUCTION

Hubble is a modular, open-source security & compliance auditing framework.

Built on SaltStack.

OVERVIEW

Quick Start

Audit Modules (Nova)

Audit Profiles (Nova)

File-Integrity Events (Pulsar)

Snapshots (Nebula)

Reporting (Quasar)

Roadmap

QUICK START - SALTSTACK

INSTALLATION

Installation (GitFS)

This installation method subscribes directly to our GitHub repository, pinning to a tag or branch. This method requires no package installation or manual checkouts.

Requirements: GitFS support on your Salt Master. (Usually just requires installation of `gitpython` or `pygit2`. `pygit2` is the recommended gitfs provider.)

/etc/salt/master.d/hubblestack-nova.conf

```
fileserver_backend:
  - roots
  - git
gitfs_remotes:
  - https://github.com/hubblestack/hubble-salt.git:
    - base: v2017.1.0
    - root: ''
```

> Remember to restart the Salt Master after applying this change.

You can then run `salt '*' saltutil.sync_all` to sync the modules to your minions.

See `pillar.example` for sample pillar data for configuring the pulsar beacon and the splunk/slack returners.

QUICK START - STANDALONE

RPM / DEB

NOW WITH 50% LESS SALT!

Hubble supports one-off invocations of specific functions:

```
[root@host1 hubble-v2]# hubble nova.audit cis.centos-7-level-1-scored-v2-1-0 tags=CIS-3.\*
{'Compliance': '45%',
 'Failure': [{'CIS-3.4.2': 'Ensure /etc/hosts.allow is configured'},
             {'CIS-3.4.3': 'Ensure /etc/hosts.deny is configured'},
             {'CIS-3.6.2': 'Ensure default deny firewall policy'},
             {'CIS-3.6.3': 'Ensure loopback traffic is configured'},
             {'CIS-3.6.1_running': 'Ensure iptables is installed'},
             {'CIS-3.2.4': 'Ensure suspicious packets are logged'},
             {'CIS-3.2.2': 'Ensure ICMP redirects are not accepted'},
             {'CIS-3.2.3': 'Ensure secure ICMP redirects are not accepted'},
             {'CIS-3.1.2': 'Ensure packet redirect sending is disabled'},
             {'CIS-3.3.1': 'Ensure IPv6 router advertisements are not accepted'},
             {'CIS-3.3.2': 'Ensure IPv6 redirects are not accepted'}],
 'Success': [{'CIS-3.6.1_installed': 'Ensure iptables is installed'},
             {'CIS-3.4.1': 'Ensure TCP Wrappers is installed'},
             {'CIS-3.4.5': 'Ensure permissions on /etc/hosts.deny are 644'},
             {'CIS-3.4.4': 'Ensure permissions on /etc/hosts.allow are configured'},
             {'CIS-3.2.5': 'Ensure broadcast ICMP requests are ignored'},
             {'CIS-3.2.6': None},
             {'CIS-3.2.1': 'Ensure source routed packets are not accepted'},
             {'CIS-3.1.1': 'Ensure IP forwarding is disabled'},
             {'CIS-3.2.8': 'Ensure TCP SYN Cookies is enabled'}]}
```

STANDALONE SCHEDULER

Scheduler

Hubble supports scheduled jobs. See the docstring for `schedule` for more information, but it follows the basic structure of salt scheduled jobs. The schedule config should be placed in `/etc/hubble/hubble` along with any other hubble config:

```
schedule:
  job1:
    function: hubble.audit
    seconds: 60
    splay: 30
    args:
      - cis.centos-7-level-1-scored-v2-1-0
    kwargs:
      verbose: True
      show_profile: True
    returner: splunk_nova_return
    run_on_start: True
```

Note that you need to have your splunk_nova_return configured in order to use the above block:

```
hubblestack:
  nova:
    returner:
      splunk:
        token: <token>
        indexer: <hec endpoint>
        sourcetype: hubble_audit
        index: <index>
```

AUDIT MODULES

HUBBLESTACK NOVA

AUDIT MODULES

- grep
- iptables
- netstat
- openscap
- openssl
- pkg
- service
- stat
- sysctl
- vulners.com

AUDIT PROFILES

HUBBLESTACK NOVA

PROFILES

- Profiles are written in YAML
- Nova audits are profile driven
- Audit modules read profiles for instructions
- Sample profiles shipped in `hubblestack_nova/samples`
- Profiles are meant to be customized
- Customize to match *your* security policy

FILE-INTEGRITY EVENTS

HUBBLESTACK PULSAR

PULSAR

Pulsar's `inotify` module watches for file system events in real-time. When Pulsar detects a CREATE, MODIFY or DELETE file system event it takes a snapshot of the file attributes. This data can be tracked and analyzed using Splunk (or similar). See Quasar for more details.

PULSAR FAQ

Monitored directories are configurable

Exceptions are supported (ie; monitor /var/ but not /var/log)

Multiple Quasar modules are supported (ie; Splunk + Slack)

Not currently compatible with prelinking

Gathered file attributes are configurable (checksum type, file stats)

SNAPSHOTS

HUBBLESTACK NEBULA

NEBULA

Nebula's `osquery` module allows you to query your systems for information just like a database. Running these queries on a cadence allows for regular, scheduled snapshots of activity on your running systems. This data can then be tracked and analyzed using Splunk (or similar). See Quasar for more details.

NEBULA QUERIES

- running processes
- established outbound connections
- listening processes
- suid binaries
- crontab
- installed packages
- ...anything else you'd like to query

REPORTING

HUBBLESTACK QUASAR

QUASAR

Quasar is a collection of custom modules that collect data from Nova, Nebula and Pulsar and deliver it for processing. Quasar modules can connect to just about anything, including Splunk, Slack, email, SMS, etc.

QUASAR MODULES

- Nova to Splunk
- Nebula to Splunk
- Pulsar to Splunk
- Pulsar to Slack

ROADMAP

2017

ROADMAP 2017

- add trigger functionality to Nova (remediation)
- add alert functionality to Nova (slack, sms, email, jabber)
- extend Pulsar to include login events
- extend Pulsar to include shell events
- template (jinja, includes) support in Nova profiles
- extend Nova profile templates (CIS level 2, STIG, etc)
- extend Windows support
- containers, containers, containers!

HUBBLESTACK

Hubble is a modular, open-source security & compliance auditing framework.

Built on SaltStack.

For more information please visit:

https://hubblestack.io

https://github.com/hubblestack