HUBBLE

SECURITY FOR DEVOPS

INTRODUCTION

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

Built on SaltStack.

COMPONENTS

Nova is Hubble's profile-based auditing engine.

Pulsar is Hubble's real-time event system.

Nebula is Hubble's security snapshot utility.

Quasar is Hubble's flexible reporting suite.

OVERVIEW

Availability

Documentation

Quick Start (Nova)

Audit Modules (Nova)

Audit Profiles (Nova)

File-Integrity & Security Events (Pulsar)

Snapshots (Nebula)

Reporting (Quasar)

Roadmap

AVAILABILITY

- Hubble v2016.7.1 now available!
  - SPM (Salt Package Manager) – https://spm.hubblestack.io/2016.7.1/
  - Manual (git clone) - https://github.com/hubblestack/

DOCUMENTATION

https://docs.hubblestack.io

HUBBLESTACK NOVA

QUICK START

NOVA

Nova is Hubble's auditing engine designed to audit the compliance and security level of a system.

http://docs.hubblestack.io/en/latest/nova/README.html

NOVA QUICK START

1. wget https://spm.hubblestack.io/2016.7.1/hubblestack_nova-2016.7.1-1.spm
2. spm local install hubblestack_nova-2016.7.1-1.spm
3. salt * saltutil.sync_modules
4. salt * hubble.audit

http://docs.hubblestack.io/en/latest/nova/README.html#installation-packages

NOVA + SPLUNK

1. wget https://spm.hubblestack.io/2016.7.1/hubblestack_quasar-2016.7.1-1.spm
2. spm local install hubblestack_quasar-2016.7.1-1.spm
3. [edit /srv/spm/pillar/hubblestack_quasar.sls.orig & add to pillar/top.sls]
4. salt * saltutil.sync_returners
5. salt * hubble.audit --return splunk_nova_return

http://docs.hubblestack.io/en/latest/components/quasar/modules/splunk_nova.html

NOVA OUTPUT

```
minion1:
  ----------
  Compliance:
    37%
  Failure:
    |_
      ----------
      openssl-1.0.1e-51.el7_2.5:
        Important openssl Security Update
    |_
      ----------
      pcre-8.32-15.el7_2.1:
        Important pcre Security Update
... [continued] ...
    |_
      ----------
      CIS-1.1.14:
        Ensure nodev option set on /home partition
    |_
      ----------
      CIS-3.2.4:
        Ensure suspicious packets are logged
    |_
      ----------
      CIS-5.3.2:
        Ensure lockout for failed password attempts is
configured
... [truncated] ...
```

AUDIT MODULES

HUBBLESTACK NOVA

AUDIT MODULES

- grep (configuration values)
- iptables (firewall rules)
- netstat (listening ports)
- openscap (CVE scan)
- openssl (cert validation & expiration)
- pkg (installed packages)
- service (running services)
- stat (ownerships & permissions)
- sysctl (kernel parameters)
- vulners.com (CVE scan)

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

HUBBLESTACK PULSAR

FILE-INTEGRITY & SECURITY EVENTS

PULSAR

Is your infrastructure immutable? Are you sure?

Pulsar is designed to monitor for file system events, acting as a real-time File Integrity Monitoring (FIM) agent.

http://docs.hubblestack.io/en/latest/pulsar/README.html

PULSAR FAQ

Monitored directories are configurable via Salt pillar or minion config

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)

http://docs.hubblestack.io/en/latest/pulsar/README.html#configuration

HUBBLESTACK NEBULA

SNAPSHOTS

NEBULA

Nebula is Hubble's Insight system which allows you to query your infrastructure as if it were a database. This system can be used to take scheduled snapshots of your systems.

http://docs.hubblestack.io/en/latest/nebula/README.html

NEBULA QUERIES

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

HUBBLESTACK QUASAR

REPORTING

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.

http://docs.hubblestack.io/en/latest/quasar/README.html

QUASAR MODULES (CURRENT)

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

ROADMAP

2016-2017

ROADMAP 2016-2017

- 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!
- masterless deployment

HUBBLE

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

Built on SaltStack.

For more information please visit:

https://hubblestack.io

https://docs.hubblestack.io

https://saltstack.com