# OpenStack Security Project

Securing the world’s largest, fastest moving open-source project

# Agenda

- Intro to OpenStack
- State of OpenStack Security
- Security Group Projects
- About the Security Group

# Intro to OpenStack

Open source cloud platform

Started in 2010 by NASA and Rackspace

Today: > 2.5 million LoC + 1800 contributors

~77% Python

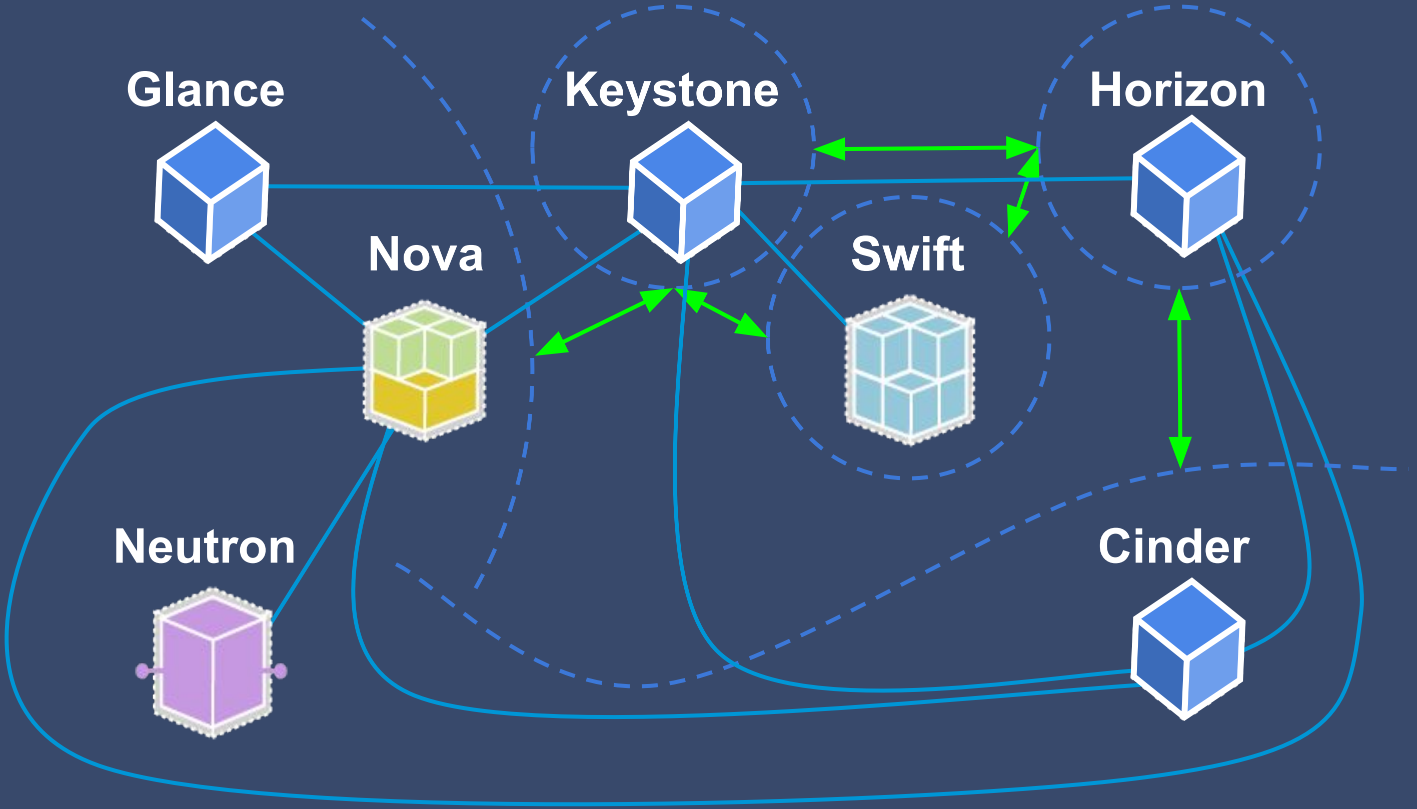
openstack®
CLOUD SOFTWARE

# Cloud?

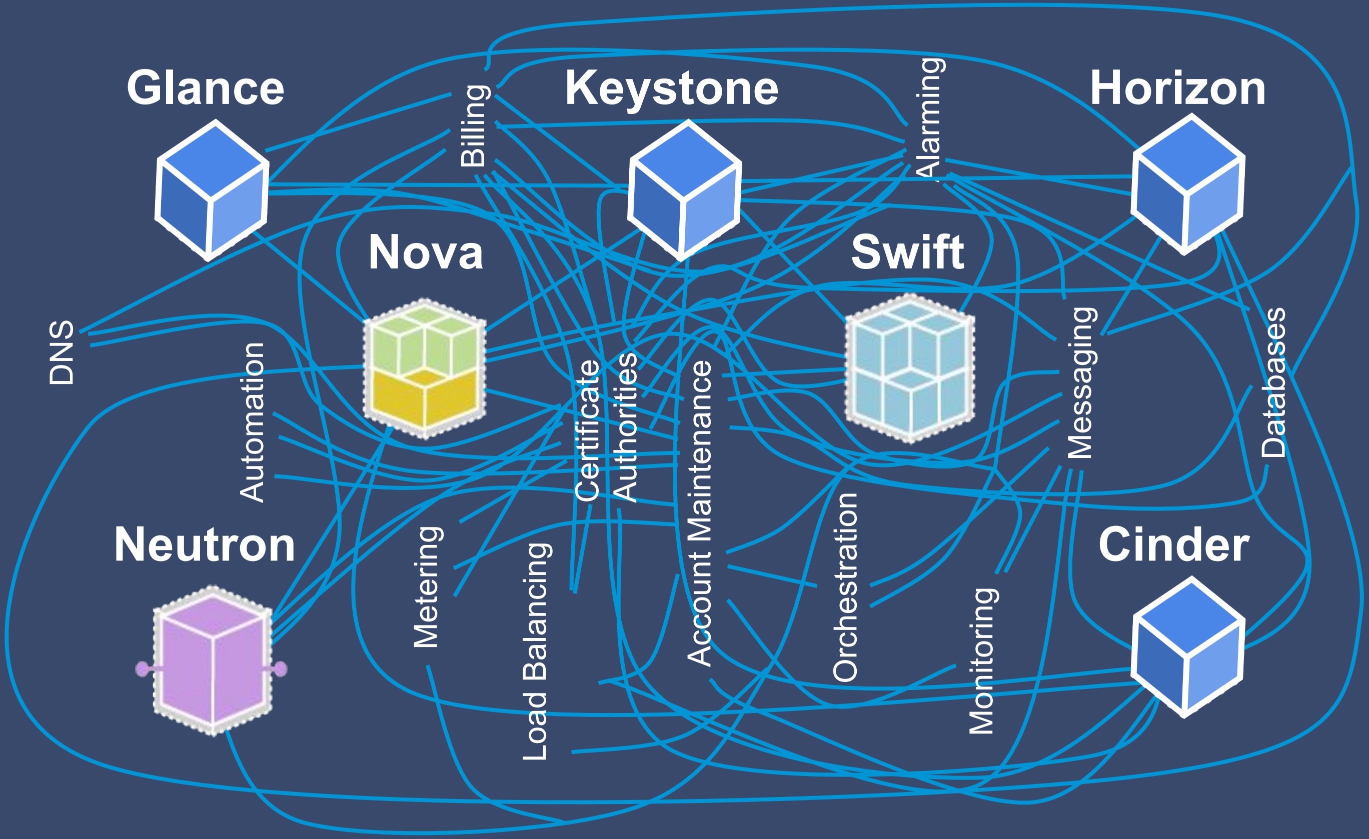
## IaaS Typically Includes:

- Compute
- Storage
- Network
- Identity

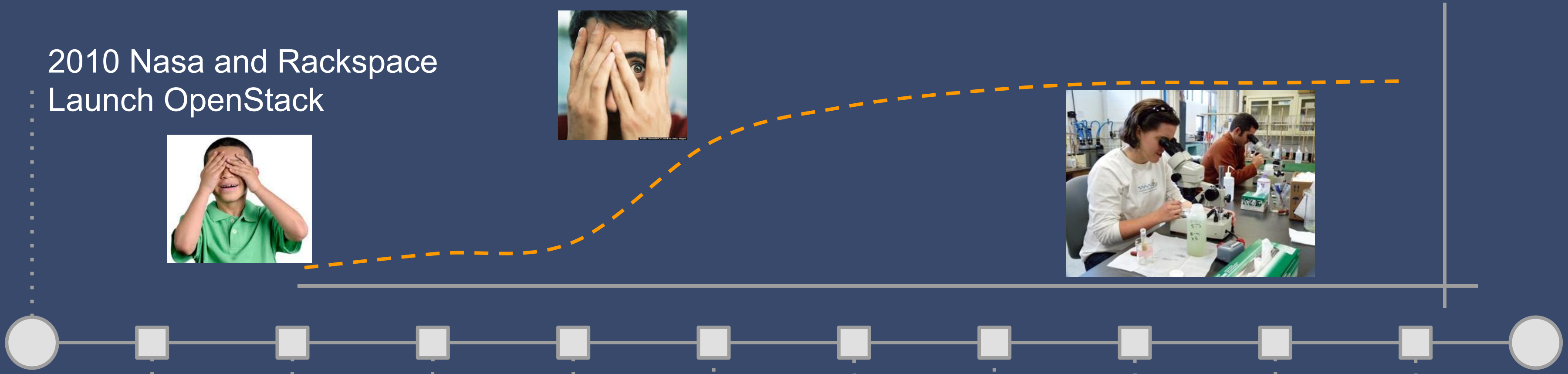
# OpenStack - How Product People See It:



# OpenStack - How Security People See It:



# State of OpenStack Security



2010 Nasa and Rackspace
Launch OpenStack

**Bexar**
02/11

**Cactus**
04/11

**Diablo**
09/11

**Essex**
04/12

**Folsom**
09/12

**Grizzly**
04/13

**Havana**
10/13

**Icehouse**
04/14

**Juno**
10/14

**Kilo**
04/15

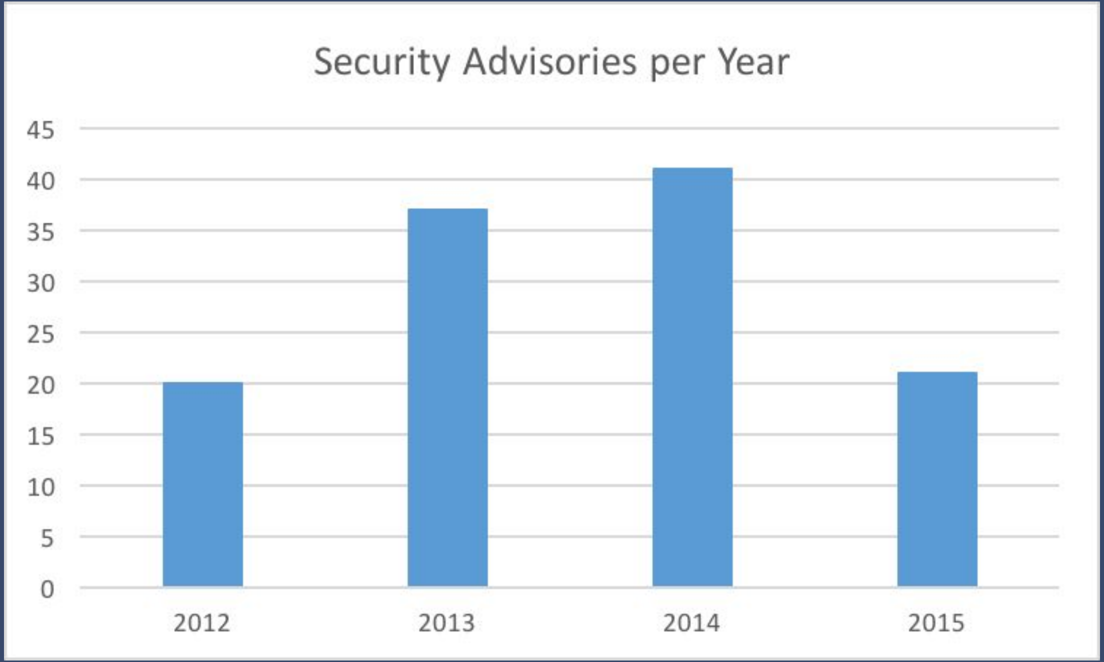
# Examples

- Directory traversal → Arbitrary File Creation (2012)
- Improper sanitization in instance name → XSS (2013)
- Missing SSL certificate check (2014)
- Glance store DoS through disk space exhaustion (2014)
- Unauthorized delete of versioned Swift object (2015)

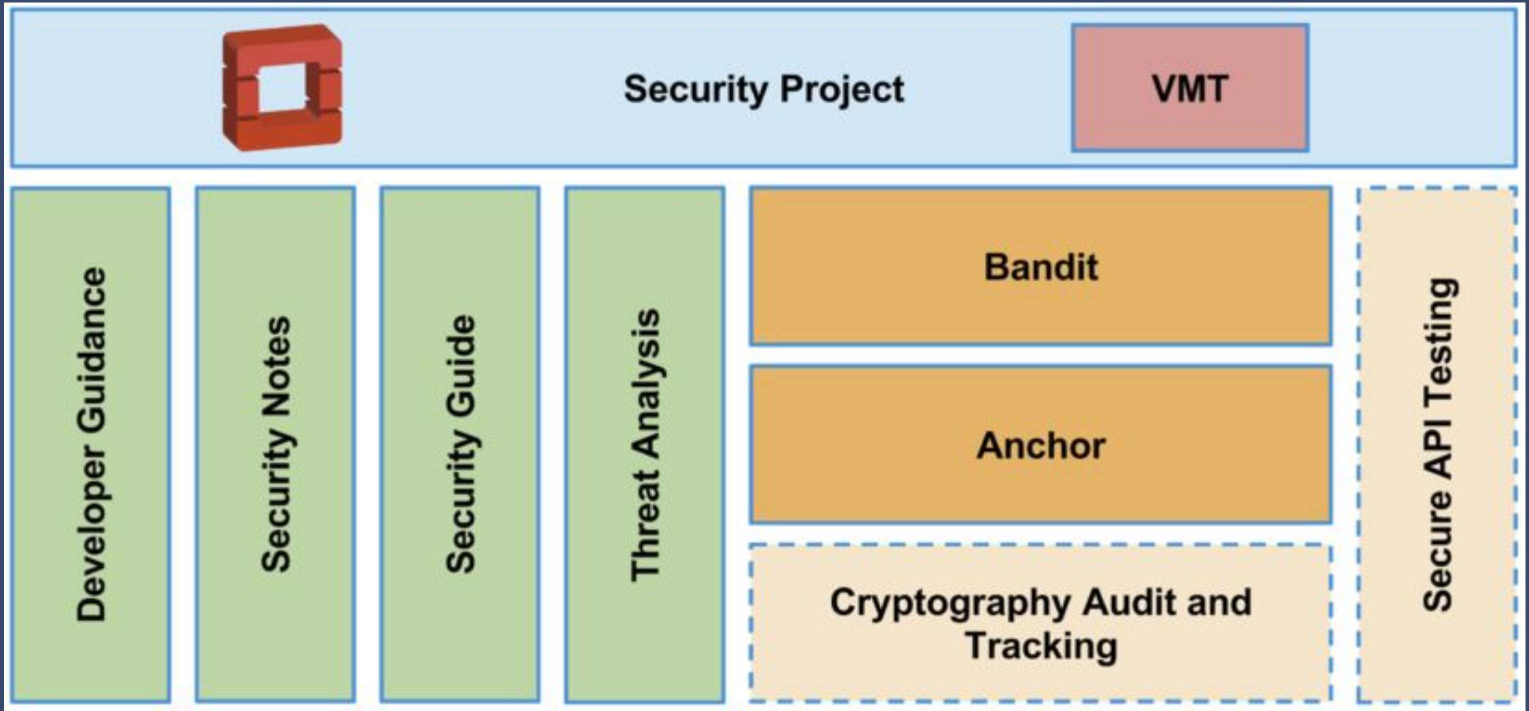
https://security.openstack.org/ossalist.html

# Security Issues

- XSS (web interface)
- Directory traversal
- Missing auth check
- Information leakage
- DoS
- ...



# Security Project Initiatives



Security Project

VMT

Developer Guidance

Security Notes

Security Guide

Threat Analysis

Bandit

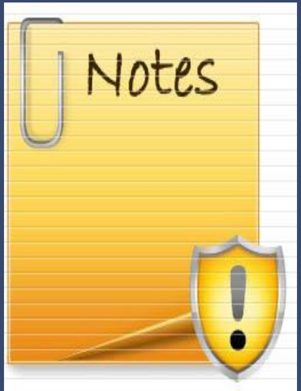
Anchor

Cryptography Audit and Tracking

Secure API Testing

# Security Notes

- Written and managed by OpenStack Security Project
- Compliment advisories (OSSA)
- Can be found on the Security Note Wiki
  - https://wiki.openstack.org/wiki/Security_Notes



# Security Notes

- One-stop-shop for cloud deployers
    - Issues without a patch
    - Insecure defaults
    - Common insecure configurations

- Over 60 listed notes as of December 2015

# Security Notes - Examples

- OSSN-0056 - Cached keystone tokens may be accepted after revocation

- OSSN-0049 - Nova Ironic driver logs sensitive information in DEBUG mode
    - and python-swiftclient
    - Pecan (for some services)

# Security Notes - Process

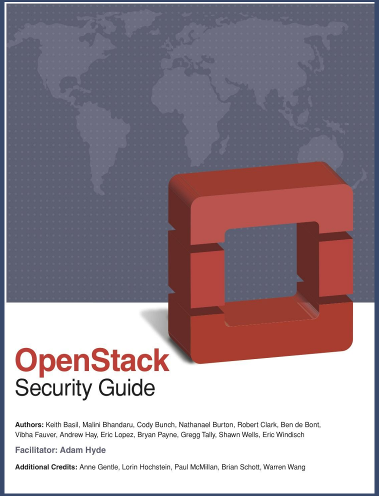
- Writing
  - Number Assignment
  - Template Use
- Testing
  - Researching - Reproducing Issue
- Review Process
  - Peer Review Process Using Gerrit/Git Review
- Get Published
  - Core Reviewers & Service Core/Expert Review
- Full Process:
  - https://wiki.openstack.org/wiki/Security/Security_Note_Process

# Security Guide

Created in June 2013 + living document

Provides best practices and conceptual information about securing an OpenStack cloud

- Reflects the current state of security within the OpenStack community
- Maintained by OpenStack Security project



OpenStack
Security Guide

**Authors:** Keith Basil, Malini Bhandaru, Cody Bunch, Nathanael Burton, Robert Clark, Ben de Bont, Vibha Fauver, Andrew Hay, Eric Lopez, Bryan Payne, Gregg Tally, Shawn Wells, Eric Windisch

**Facilitator: Adam Hyde**

**Additional Credits:** Anne Gentle, Lorin Hochstein, Paul McMillan, Brian Schott, Warren Wang

# Security Guide - Process

- Bugs in Launchpad
  - Tracks bugs against the guide, and their severity
  - Can assign yourself a sec-guide bug just like code
- Get the doc source
  - Clone the security guide git repo
- Update
  - In RST format it’s security-guide/source/<chaptername>/
- Review
  - Core Reviewers & Service Core/Expert Review
- Publish
  - Changes are merged to the HTML source as quickly as the gate allows

# Security Guide

Example topics:

- Hypervisor selection
- Instance security management
- Tenant data privacy

Available in HTML (current) and print (v1.0) form

http://docs.openstack.org/security-guide

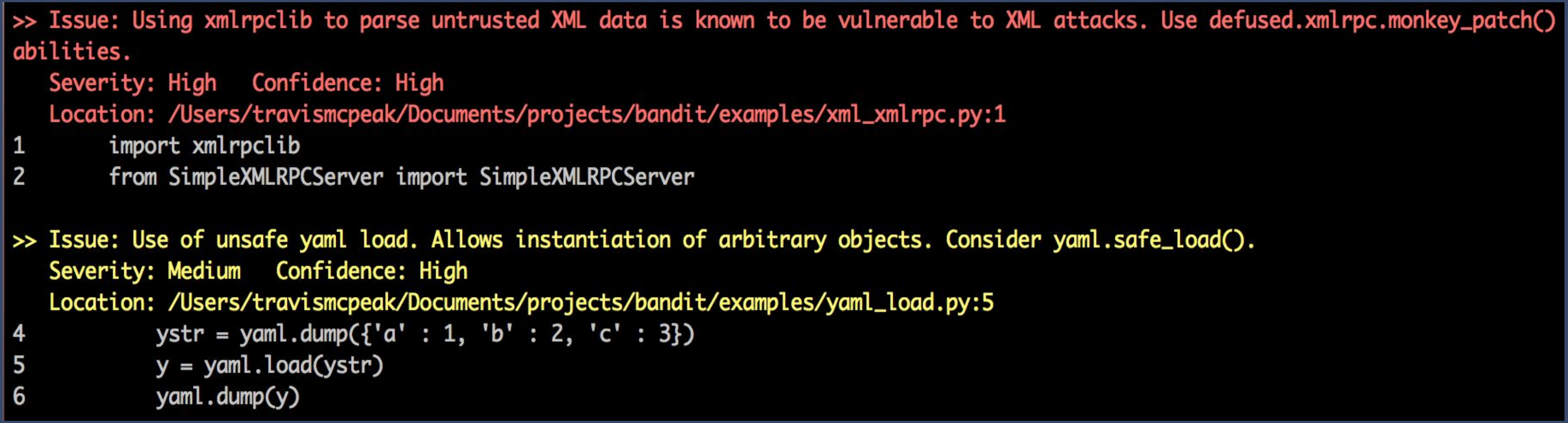
http://docs.openstack.org/sec/

# Bandit - a Python security linter

Finds common security issues in Python code:

- Command injection
- Insecure temp file usage
- Promiscuous file permissions
- Usage of unsafe functions/libraries
- Binding to all interfaces
- Weak cryptography
- …

# Bandit Example



```
>> Issue: Using xmlrpclib to parse untrusted XML data is known to be vulnerable to XML attacks. Use defused.xmlrpc.monkey_patch()
abilities.
   Severity: High   Confidence: High
   Location: /Users/travismcpeak/Documents/projects/bandit/examples/xml_xmlrpc.py:1
1       import xmlrpclib
2       from SimpleXMLRPCServer import SimpleXMLRPCServer

>> Issue: Use of unsafe yaml load. Allows instantiation of arbitrary objects. Consider yaml.safe_load().
   Severity: Medium   Confidence: High
   Location: /Users/travismcpeak/Documents/projects/bandit/examples/yaml_load.py:5
4           ystr = yaml.dump({'a' : 1, 'b' : 2, 'c' : 3})
5           y = yaml.load(ystr)
6           yaml.dump(y)
```

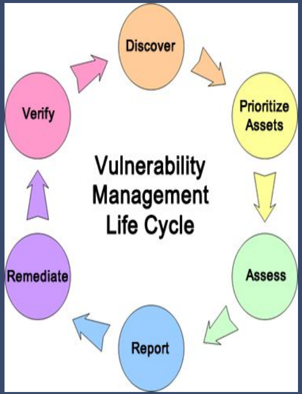
# Bandit

- Open source
- Easy to write new plugins
- Low resource requirements
- Runs quickly

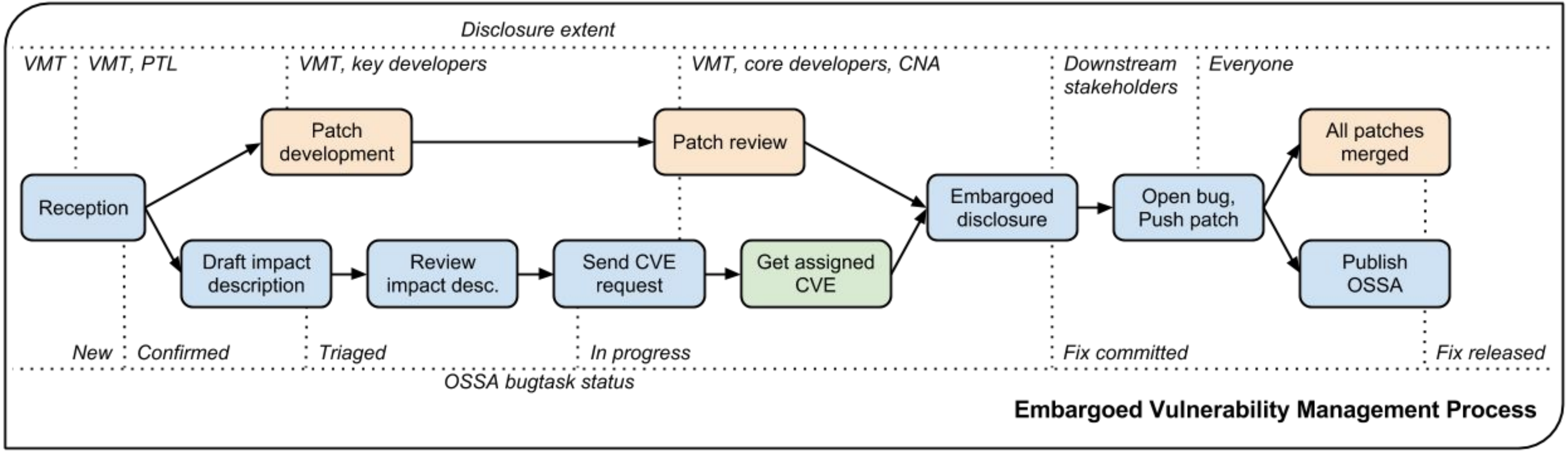
https://git.openstack.org/cgit/openstack/bandit/

# Vulnerability Management

- Ensure that vulnerabilities are dealt with quickly and responsibly.
- When situation requires it, produce OpenStack Security Advisories (OSSAs) - similar to CVEs.



# Vulnerability Management Process



# Example: OSSA-2013-036

11-03-2013: XSS in instance name reported by Cisco employee

11-14-2013: Fix publicly disclosed, bug marked public

11-28-2013: Backports completed

12-04-2013: CVE-2013-6858 Assigned

12-11-2013: Advisory published

# Secure Coding Guidelines

- Examples of common tasks that are often done insecurely
- Written for developers in conversational tone
- With examples on how to perform the tasks securely
- Designed to eventually be linked to by Bandit findings
- https://security.openstack.org/#secure-development-guidelines

# Anchor - Ephemeral PKI System

Existing PKI is broken outside of the browser

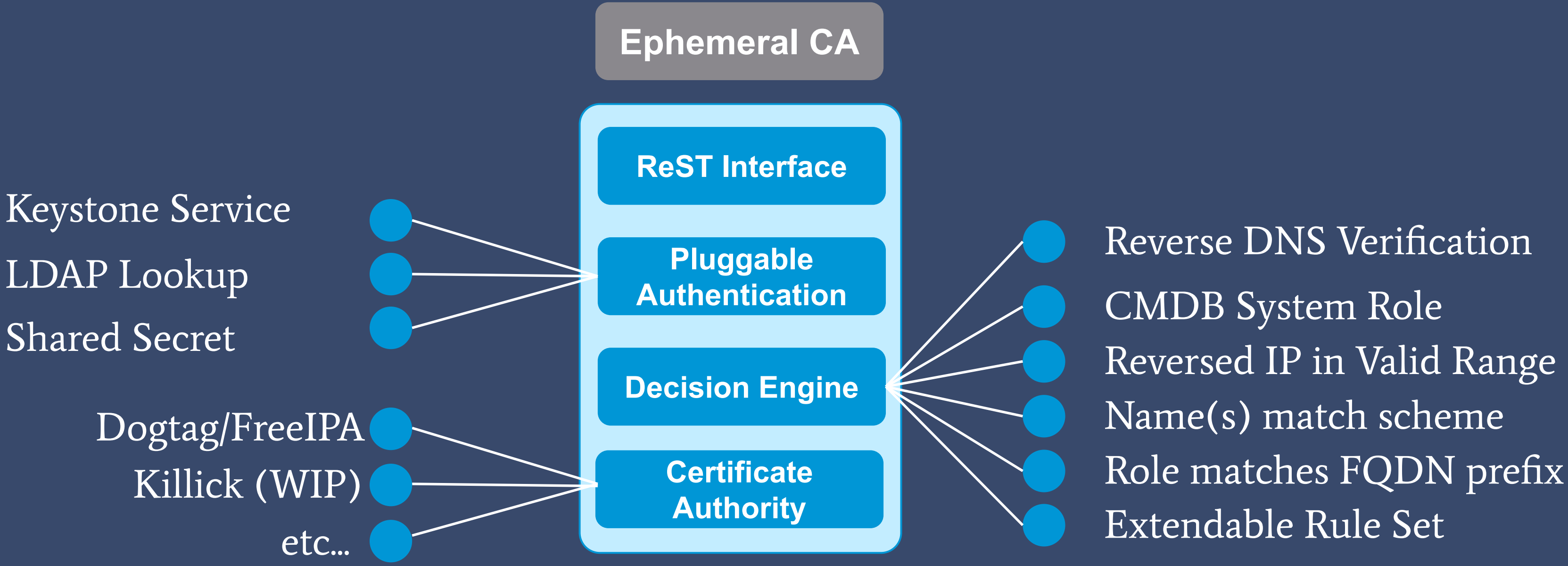
- Revocation does not work in most crypto libraries
  - CRLs are hard to distribute deterministically
  - OCSP doesn’t work in many client TLS libraries
- Provisioning certificates at scale is non-trivial

# Anchor - Ephemeral PKI System

Automatically Verifies and Issues Short-Life Certificates

- Authenticates the requestor (TLS)
- Validates the Certificate Signing Request
- Issues a Certificate
- Then uses Passive Revocation
    - Revoke by denying future requests
    - Certificate life shorter than typical OCSP caches, so there is a shorter exposure time than with OCSP

# Anchor - Ephemeral PKI System

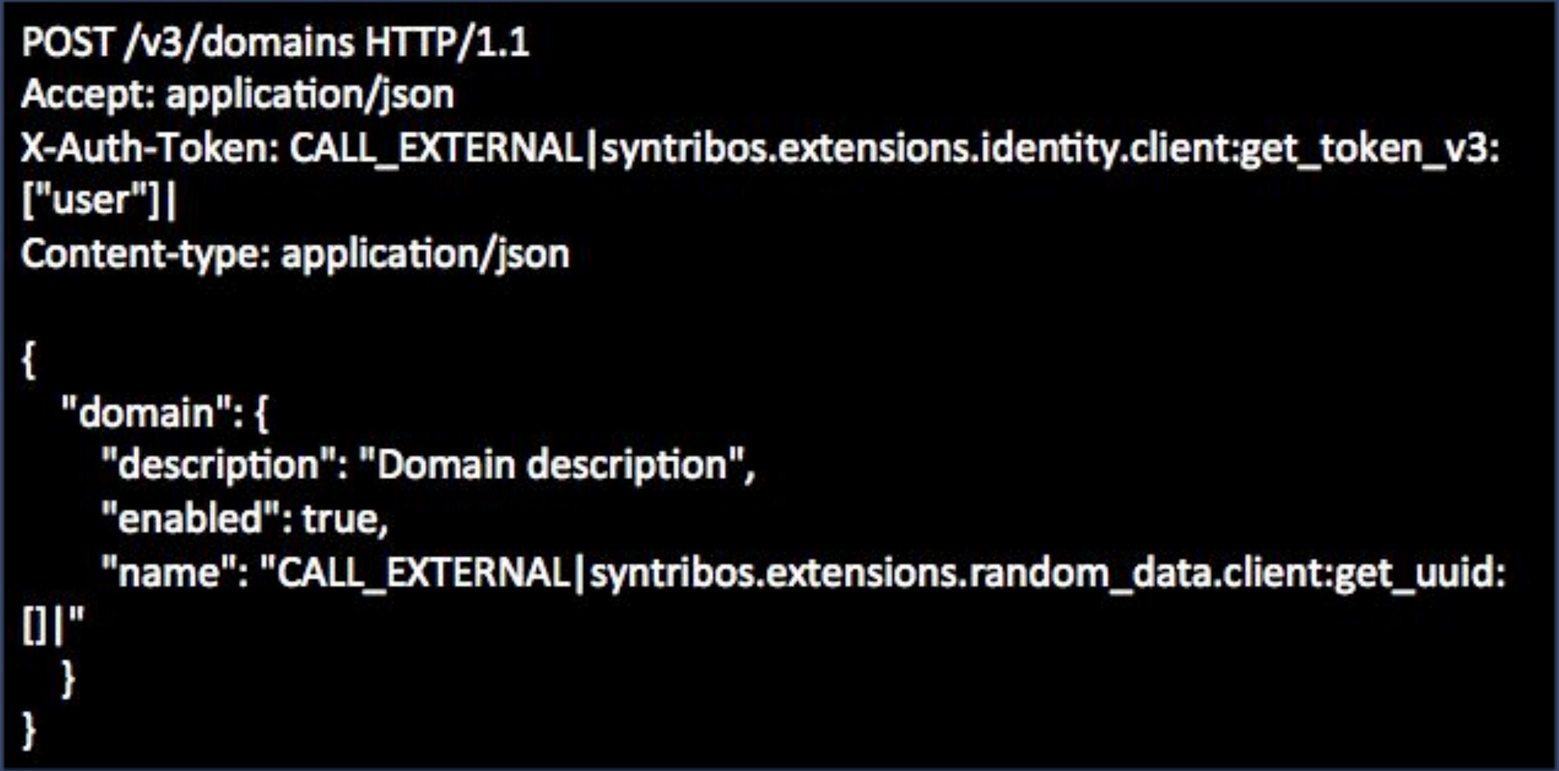


# Syntribos -  API Security Testing Tool

Finds security issues  in restful API

- Fuzz payload, HTTP headers, URL, query string
- Log all requests and responses
- Support keystone authentication
- Detect common security defects
- Help identify unknown security defects

# Syntribos ‘Payload’ Example



```
POST /v3/domains HTTP/1.1
Accept: application/json
X-Auth-Token: CALL_EXTERNAL|syntribos.extensions.identity.client:get_token_v3:
["user"]|
Content-type: application/json

{
   "domain": {
      "description": "Domain description",
      "enabled": true,
      "name": "CALL_EXTERNAL|syntribos.extensions.random_data.client:get_uuid:
[]|"
   }
}
```

# Syntribos Summary Output

```
2015-08-18 14:44:12,466: INFO: root: ========================================================
2015-08-18 14:44:12,466: INFO: root: Test Case......: test_case
2015-08-18 14:44:12,466: INFO: root: Result.........: Passed
2015-08-18 14:44:12,466: INFO: root: Start Time.....: 2015-08-18 14:44:12.464843
2015-08-18 14:44:12,466: INFO: root: Elapsed Time...: 0:00:00.001203
2015-08-18 14:44:12,466: INFO: root: ========================================================
2015-08-18 14:44:12,467: INFO: root: ========================================================
2015-08-18 14:44:12,467: INFO: root: Fixture........: syntribos.tests.fuzz.all_attacks.(agent_patch.txt)_(ALL_ATTACKS_BODY)_(all-attacks.txt)_str1_model1
2015-08-18 14:44:12,467: INFO: root: Result.........: Passed
2015-08-18 14:44:12,467: INFO: root: Start Time.....: 2015-08-18 14:44:11.139070
2015-08-18 14:44:12,467: INFO: root: Elapsed Time...: 0:00:01.328030
2015-08-18 14:44:12,468: INFO: root: Total Tests....: 1
2015-08-18 14:44:12,468: INFO: root: Total Passed...: 1
2015-08-18 14:44:12,468: INFO: root: Total Failed...: 0
2015-08-18 14:44:12,468: INFO: root: Total Errored..: 0
2015-08-18 14:44:12,468: INFO: root: ========================================================
```

# Syntribos

- Open source
- Easy to extend
- Support in-depth fuzzing
- Automatic logging

http://git.openstack.org/cgit/openstack/syntribos

(alternatively, https://github.com/redhat-cip/restfuzz)

# Security Project Blog Posts

http://openstack-security.github.io/

- We’re always looking for people to contribute new content or do editing!

# OpenStack Security Project

# OpenStack Security Project

250 listed members ~ 20 active at any time + **<u>you</u>**?

Lots of ways to participate:

- Write notes/documentation (gets you a technical contributor credit)
- Hack on existing tools: Bandit, Anchor, Syntribos
- Write your own tool (Ansible-security / Tempest checks)
- Pentesting / code review / deployment bugs
- Threat Analysis
- Crypto tracking

# Join Us

#openstack-security on Freenode

#openstack-meeting-alt  @ 1700 UTC Thur

openstack-dev ML with [Security] tag

# Or Jump Right In...

Security Project Page: https://security.openstack.org/

Security Advisories: https://security.openstack.org/ossalist.html

Security Notes: https://wiki.openstack.org/wiki/Security_Notes

Bandit: https://wiki.openstack.org/wiki/Security/Projects/Bandit

Developer Guidelines: https://security.openstack.org/#secure-development-guidelines

Anchor: https://wiki.openstack.org/wiki/Security/Projects/Anchor

Syntribos: http://git.openstack.org/cgit/openstack/syntribos

Security Guide: http://docs.openstack.org/sec/

OpenStack Ansible Security: https://github.com/openstack/openstack-ansible-security

# Thank you!

Eric Brown - VMware - browne on Freenode

Travis McPeak - HPE - tmcpeak on Freenode