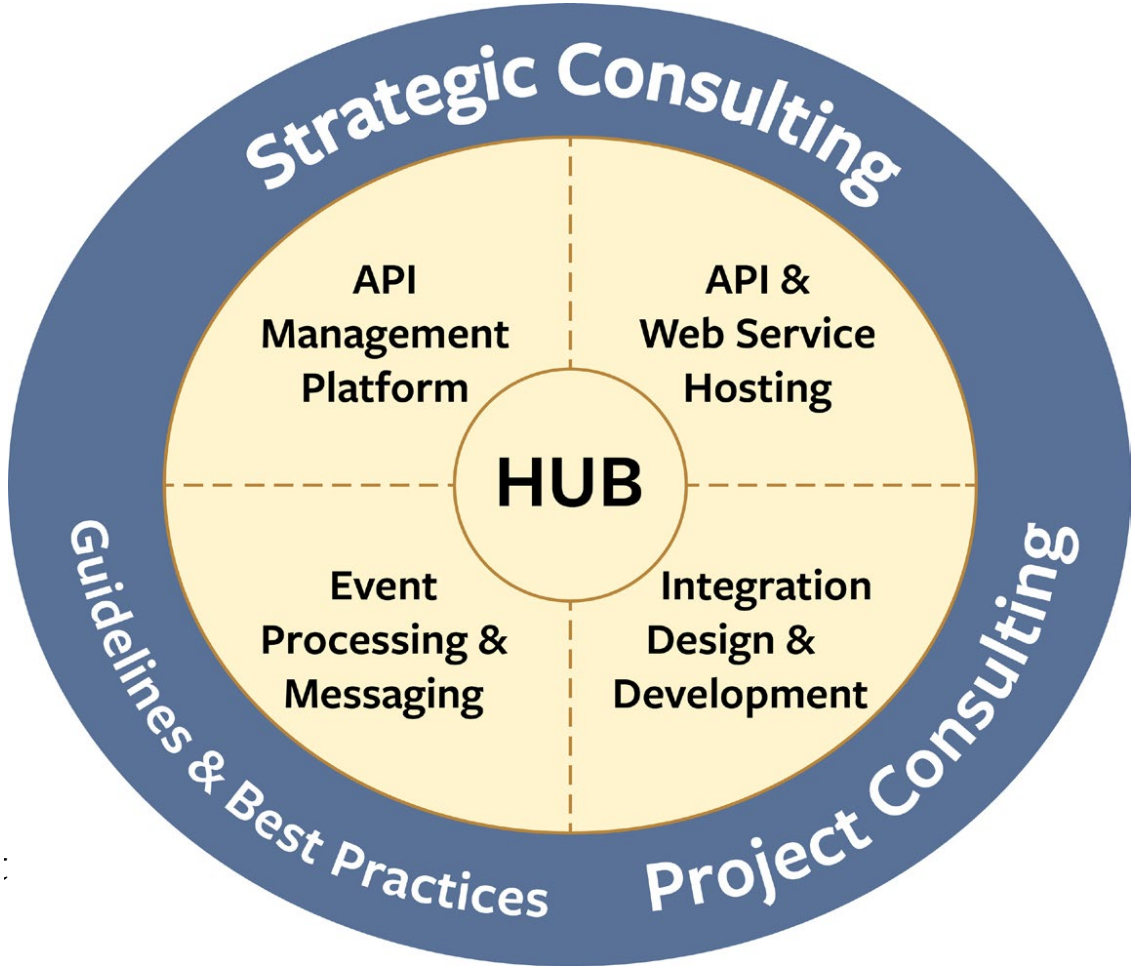
Security in the Cloud @ UC Berkeley

CSG 15.01 Short Discussion 2

William Allison wallison@berkeley.edu

Berkeley
UNIVERSITY OF CALIFORNIA

The Campus API Service …In the Cloud



Berkeley
UNIVERSITY OF CALIFORNIA


Gene Kim
@RealGeneKim
Following
OH: "I love talking security w/cloud people, as opposed to talking cloud w/security people." Haha. @petecheslock @djetue #reinvent
RETWEETS
14
FAVORITES
11
1:51 PM - 12 Nov 2014

http://www.federalnewsradio.com/405/3780452/DoD-rewrites-cloud-security-rules-in-move-toward-risk-acceptance

DISA News

Comment 0 | Share 2 | Tweet 8 | Print | Email | RSS Feeds

DoD rewrites cloud security rules in move toward risk acceptance

Recommend 3 | g+1 1 | LinkedIn

Thursday - 1/15/2015, 11:07am EST

By Jared Serbu

Follow

More Reports

Listen to Jared's story on the Federal Drive

Download mp3

The Defense Department, by the admission of its own top technology officials, has been too slow to take advantage of cloud computing — mostly because it's been hampered by its own stringent security approval processes.

A revamp of those procedures, issued this week by the Defense Information Systems Agency, aims to slightly loosen the reigns and give component-level chief information officers more discretion to decide whether commercial cloud is a good match for the level of risk they're willing to take with their data.

The cloud security requirements guide takes effect immediately, replacing DISA's earlier cloud security model and collapsing six separate data risk levels into four.

The Security Review Process:

https://security.berkeley.edu/data-classification

- Classify Data
- Architect system for actual security
- Review requirements for DPL
- Amend architecture
- Submit MSSEI Self-Assessment
- Iterate over concerns raised by ISP

https://security.berkeley.edu/mssei

Minimum Security Standards for Electronic Information (effective July 2014)

*The following **Minimum Security Standards for Electronic Information (MSSEI)** are issued under the authority vested in the UC Berkeley Chief Information Officer by the UC Business Finance Bulletin IS-3 Electronic Information Security: "All campuses shall establish an Information Security Program (Program) in conformance with the provisions in this bulletin. In order to achieve a secure information technology environment, the campus Program shall comprise a comprehensive set of strategies that include a range of related technical and non-technical measures." (Section III)*

Issue Date: April 23, 2013
Effective Date: July 1, 2014
Supersedes: Minimum Security Standard for Electronic Information (Issued: July 16, 2012/Effective: July 16, 2013)

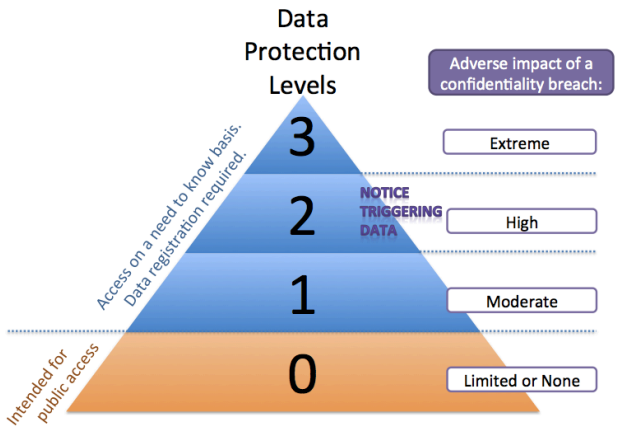
Responsible Executive: Associate Vice Chancellor for Information Technology and Chief Information Officer
Responsible Office: IT Policy Office

Contact: IT Policy Manager, itpolicy@berkeley.edu

[Protection Profile Matrix by role pdf diagram - prints on legal-sized paper]

Data Classification Standard

http://security.berkeley.edu/data-classification



Data Protection Level	Adverse impact*	Sample Data Types (not an exhaustive list)
Level 3	Extreme	Data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles.
Level 2	High	Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach: • **Social security number** • **Driver's license number, California identification number** • **Financial account numbers, credit or debit card numbers; financial account security codes, access codes, or passwords** • **Personal medical information** • **Personal health insurance information**
Level 1	Moderate	Information intended for **release only on a need-to-know basis**, incl.: Personal information not otherwise classified as Level 0, 2 or 3, and Data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.,: • FERPA student records (including Student ID) • Staff and academic personnel records (including Employee ID) • Licensed software/software license keys • Library paid subscription electronic resources
Level 0	Limited or None	Information **intended for public access**, e.g.,: Public websites, Course listings and pre-requisites, and Public directory data: **Staff:** Name, Date of hire, Current position title, Current salary, Organizational unit assignment, Date of separation, Office address, Office telephone number, Current job description, Full-time or part-time, and Appointment type **Students (unless the student has requested that information about them not be released as public information):** Name, Address, Telephone, Email, Dates of attendance, Number of course units in which enrolled, Class level, Major field of study, Last school attended, Degrees and honors received, Participation in official student activities, Weight/height (intercollegiate athletic team members only)

Public records requests, litigation or other legal obligations may require disclosure of information in any data class.

Berkeley
UNIVERSITY OF CALIFORNIA

Self Assessment – Step 1

WHAT IS IT? http://api-central.berkeley.edu

WHAT DOES IT DO? Together the Nginx Reverse Proxy Service and the 3Scale vendor product form a platform that enables APIs to be easily discoverable, well-documented, easy to use, secured, monitored, and metered. API consumers can find and explore APIs on the API Central portal, where reverse proxy simplifies and standardizes endpoint URIs. API providers and data stewards can control access to an API using the API Central Portal's credentialing service, and can limit usage and mitigate abuse using its metering service.

Risk Classification

"After consulting with others in Security, we will be classifying the 3Scale system as a PL3. The reason for the elevated classification is because having credentials (even for short time period of time) to multiple PL2 systems will create a "shared fate" and warrants the elevation."

Step 2 – Target Audience

Describe the users who will use and be affected by the application.

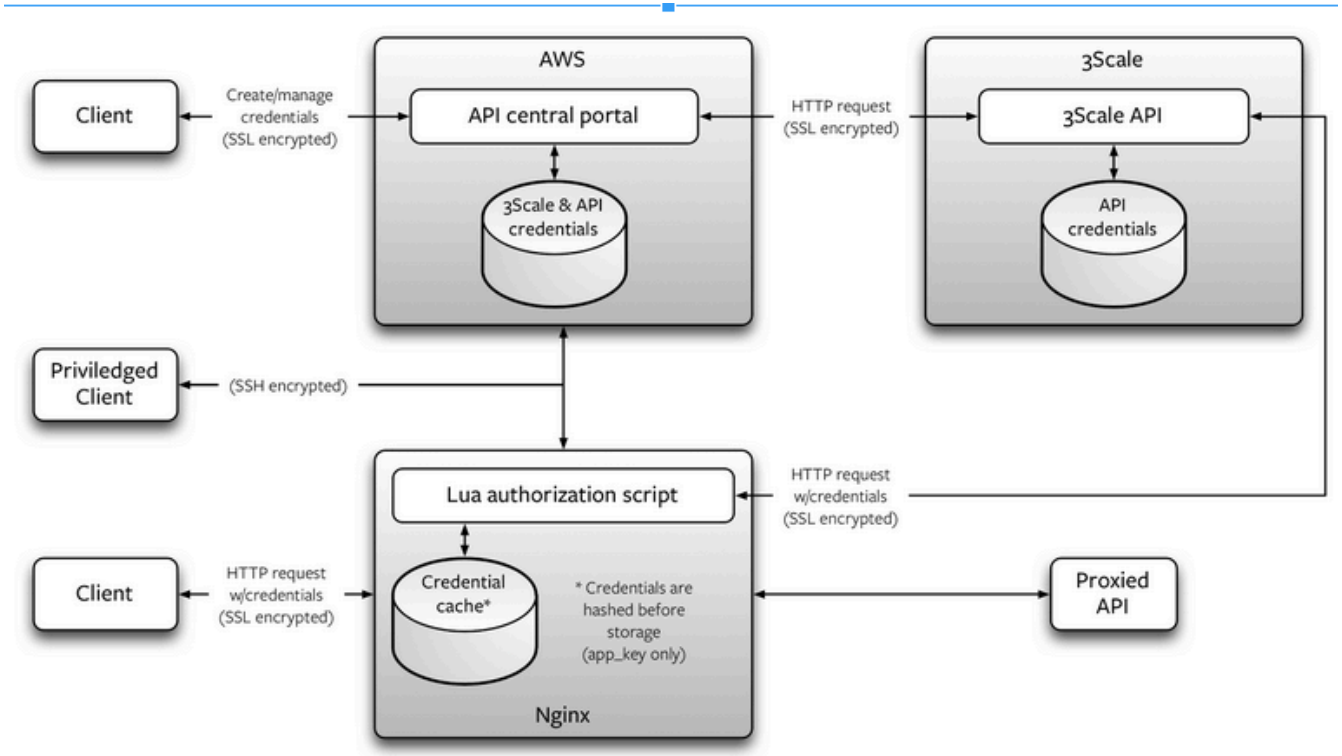
The customers for this API Management and Support Service are system-of-record stewards who provide APIs to access their data and developers who wish to call those APIs. Currently the APIs are REST based, and are almost entirely read-only (using the http GET method). Requests that update data on the backend sources can be identified by use of the http methods POST, DELETE or PUT. They would however go through the same URL endpoints - this core to the semantics of REST APIs.

We are definitely planning to allow APIs that update state on the backend - what exactly gets updated depends on the the particular API involved.

Among the currently deployed APIs, only the Easy Messaging Service allows updating state via the PUT method. Performing a PUT doesn't update any system configuration, but does add an entry into an application message queue.

Step 3 – Architecture Model

Attach a high-level diagram of data flow and data storage, including all the interconnected system names and interfaces.



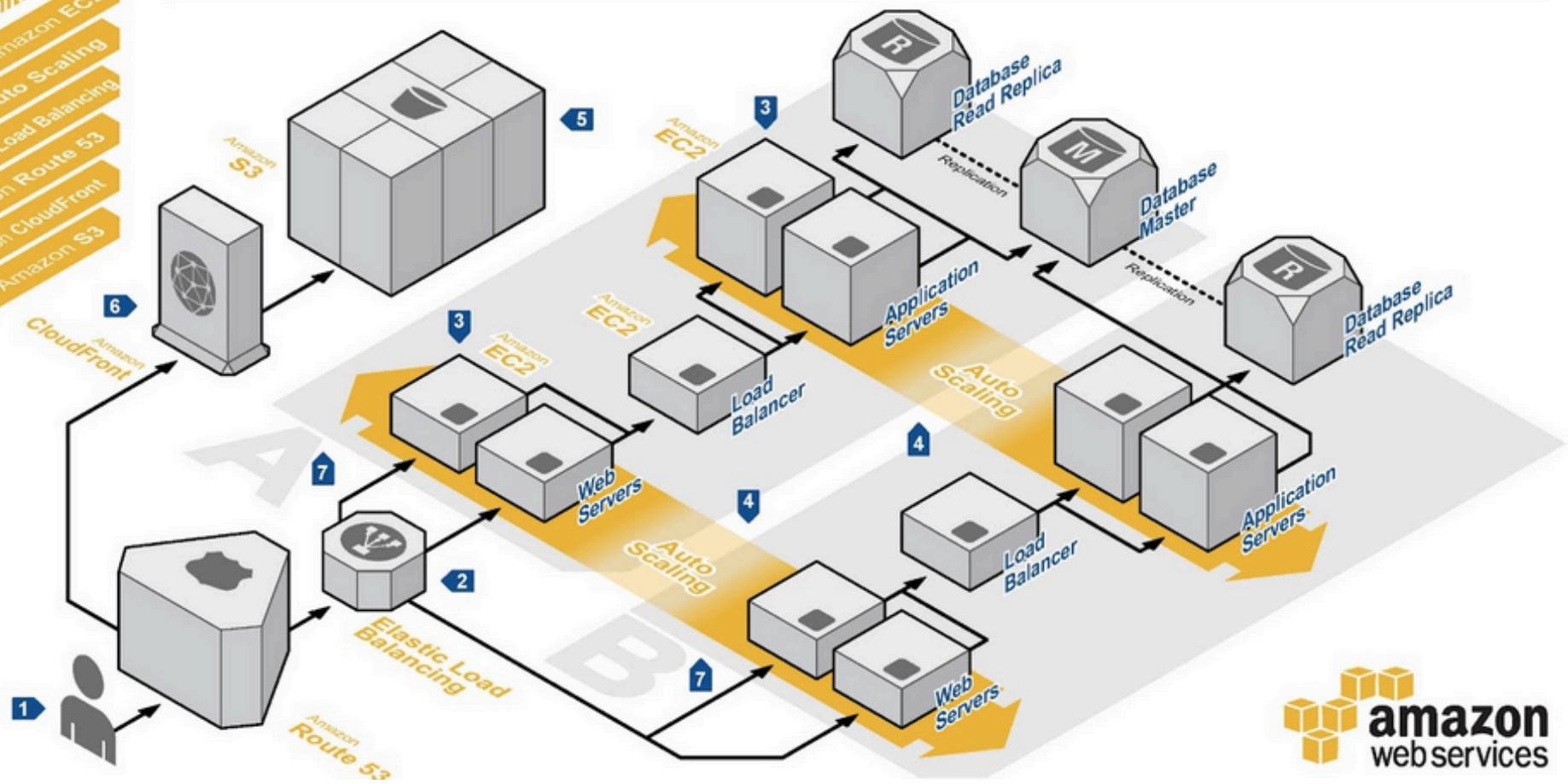
Berkeley
UNIVERSITY OF CALIFORNIA

AWS Reference Architectures

- Amazon EC2
- Auto Scaling
- Elastic Load Balancing
- Amazon Route 53
- Amazon CloudFront
- Amazon S3

WEB APPLICATION HOSTING

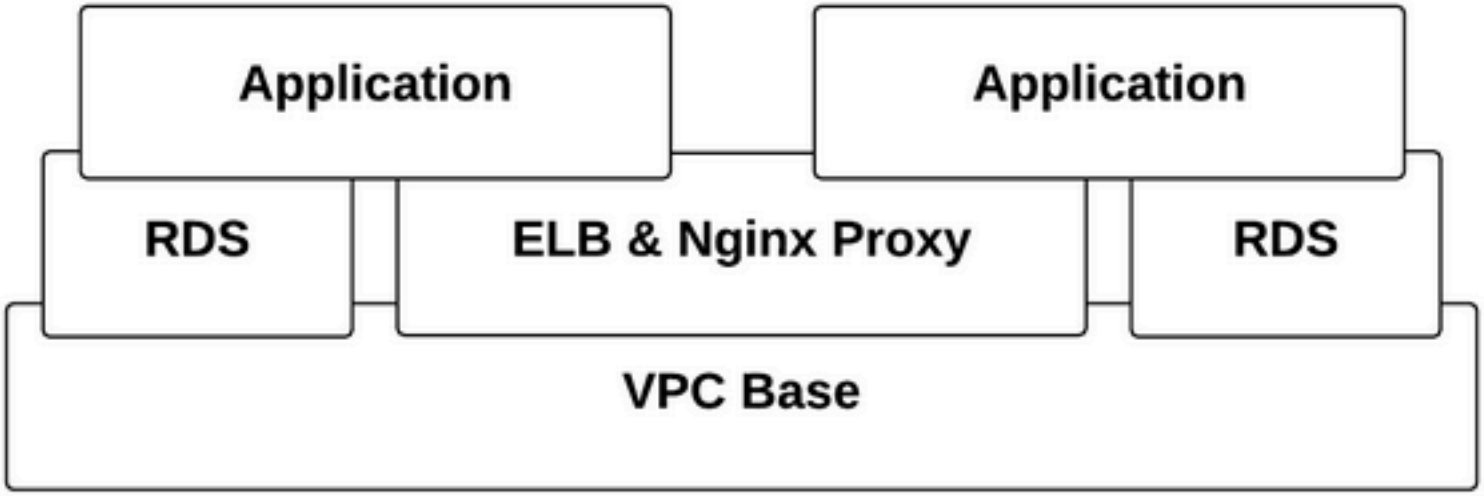
Highly available and scalable web hosting can be complex and expensive. Dense peak periods and wild swings in traffic patterns result in low utilization rates of expensive hardware. Amazon Web Services provides the reliable, scalable, secure, and high-performance infrastructure required for web applications while enabling an elastic, scale out and scale down infrastructure to match IT costs in real time as customer traffic fluctuates.



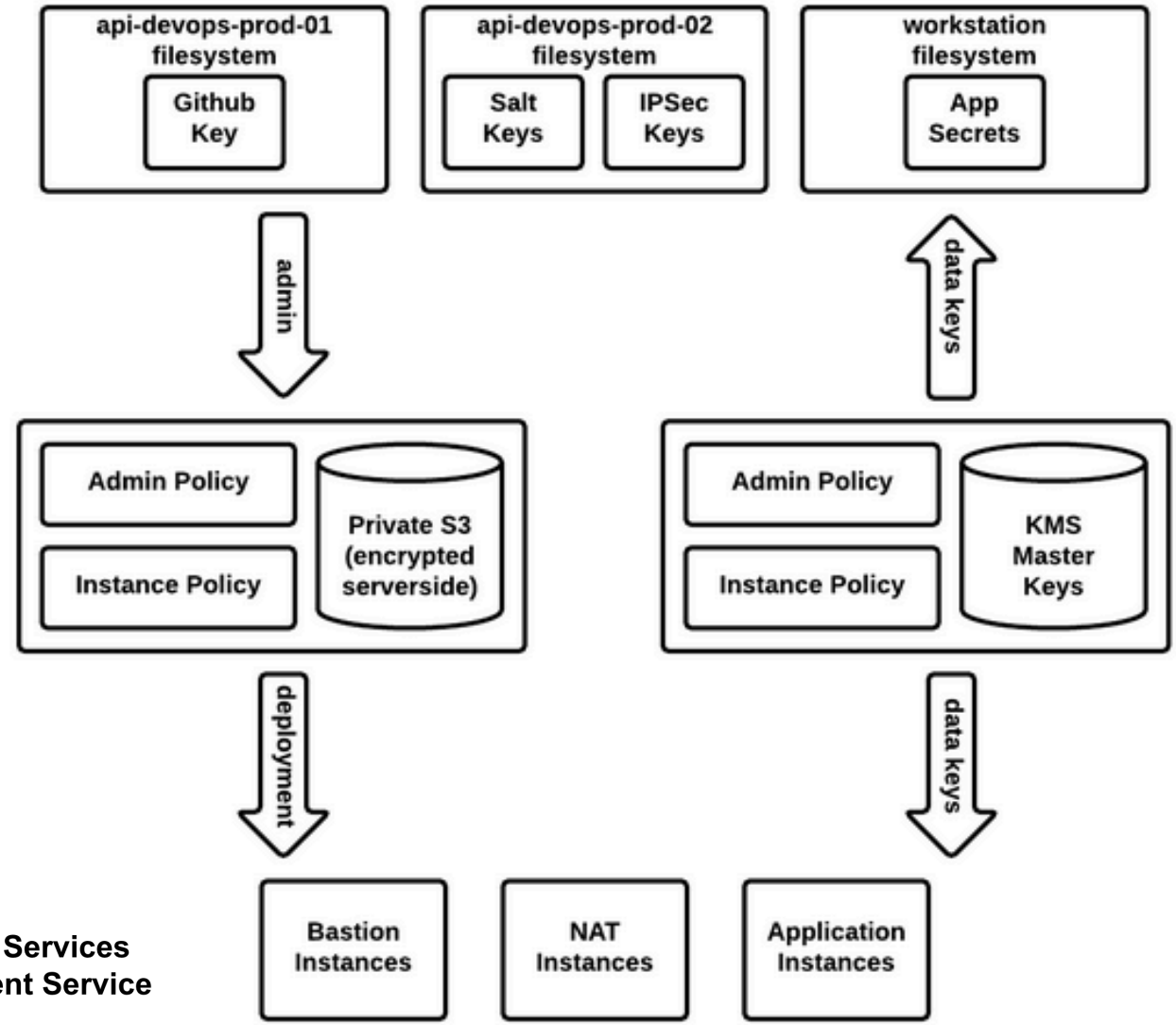
amazon web services

Berkeley
UNIVERSITY OF CALIFORNIA

CloudFormation Stack Layering

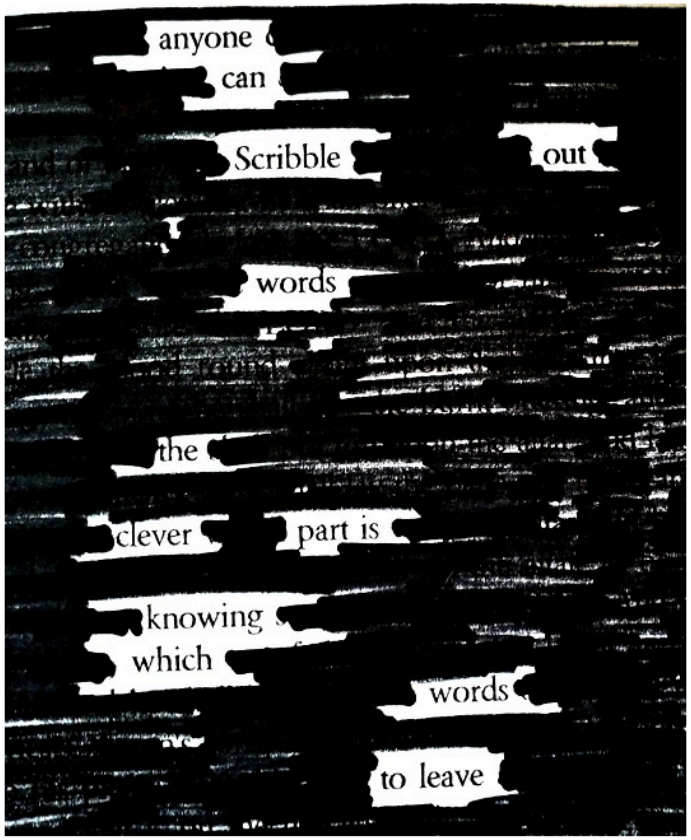


Amazon Web Services
Key Management Service



Step 4 – Data Flow Description

Provide description of data movement and data storage depicted in the architecture model. Please include brief description of how each component in the architecture model is being secured.



Step 5 - Support Model

Please list any support and development staff that have elevated privileges in the application or its underlying systems, including their roles and responsibilities in supporting/developing this application. In the responsibilities column, please make note if a role is temporary. Examples of temporary roles may include short-term contractors or support staff that will lose their elevated access to application in the near future (3 – 6 months). Elevated privileges in this case may mean permissions to change application configuration, bulk access to covered data, etc.

Name	Role	Application Responsibilities	Email Address
J	DevOps lead	permanent	
S	IT Manager	permanent	
K	Lead Developer	permanent	
M	Release Manager	permanent	

Berkeley
UNIVERSITY OF CALIFORNIA

Step 6 -Meeting MSSEI Requirements

Derived from: https://www.sans.org/critical-security-controls/

The Minimum Security Standards for Electronic Information (MSSEI) define the minimum set of confidentiality controls required for Electronic Information as well as the device types for which these controls are applicable.
For each MSSEI standard (1.1 – 17.1), ***describe how compliance with the standard are achieved*** *for the device types listed with existing tools and practices. If a standard is recommended (o) on a device, indicate how the standard will be met or document the considerations for not meeting the control.*
Device type definitions, and detailed descriptions of each control *with links to implementation guidelines are available at: security.berkeley.edu/mssei.* ***Assessment questions are provided here as prompts, with the caveat that they are subject to change. They are not intended to be comprehensive and may not be applicable for all systems.*** *If compliant controls are not yet implemented, describe any future plans or proposal to meet applicable standard, and use "Progress" column to indicate whether implementation status of the security standard is "Not Started", "In Progress", "Fully Implemented".*

MSSEI 1.1 Removal of non-required covered data • *What do you do with systems or storage media that are being replaced or otherwise decommissioned and have handled covered*	**Progress:** Fully Implemented

Berkeley
UNIVERSITY OF CALIFORNIA

MSSEI Self Assessment Plan - High Level Requirements (small subset)

- Authenticated Scans
- Intrusion Detection
- Data flow and review
- Systems Inventory
- Build and Lifecycle
- Account Management
- “Hardware” Firewall
- Network Partitioning
- Audit Logging
- Encryption in Transit
- Secure Deletion

Appendix A – Hardware inventory

Host Name	IP address	Virtual ?	Managed By	OS/Software	Device Type[LW1]	Server Type
eas-api-prod-0	1	y	Unix Team, EIS	RHEL 5.1	Institutional	production API proxy accessible from off campus
eas-api-prod-0		y	Unix Team, EIS	RHEL 5.1	Institutional	production nginx proxy campus only
eas-api-prod-0		y	Unix	RHEL 5.1	Institutional	production

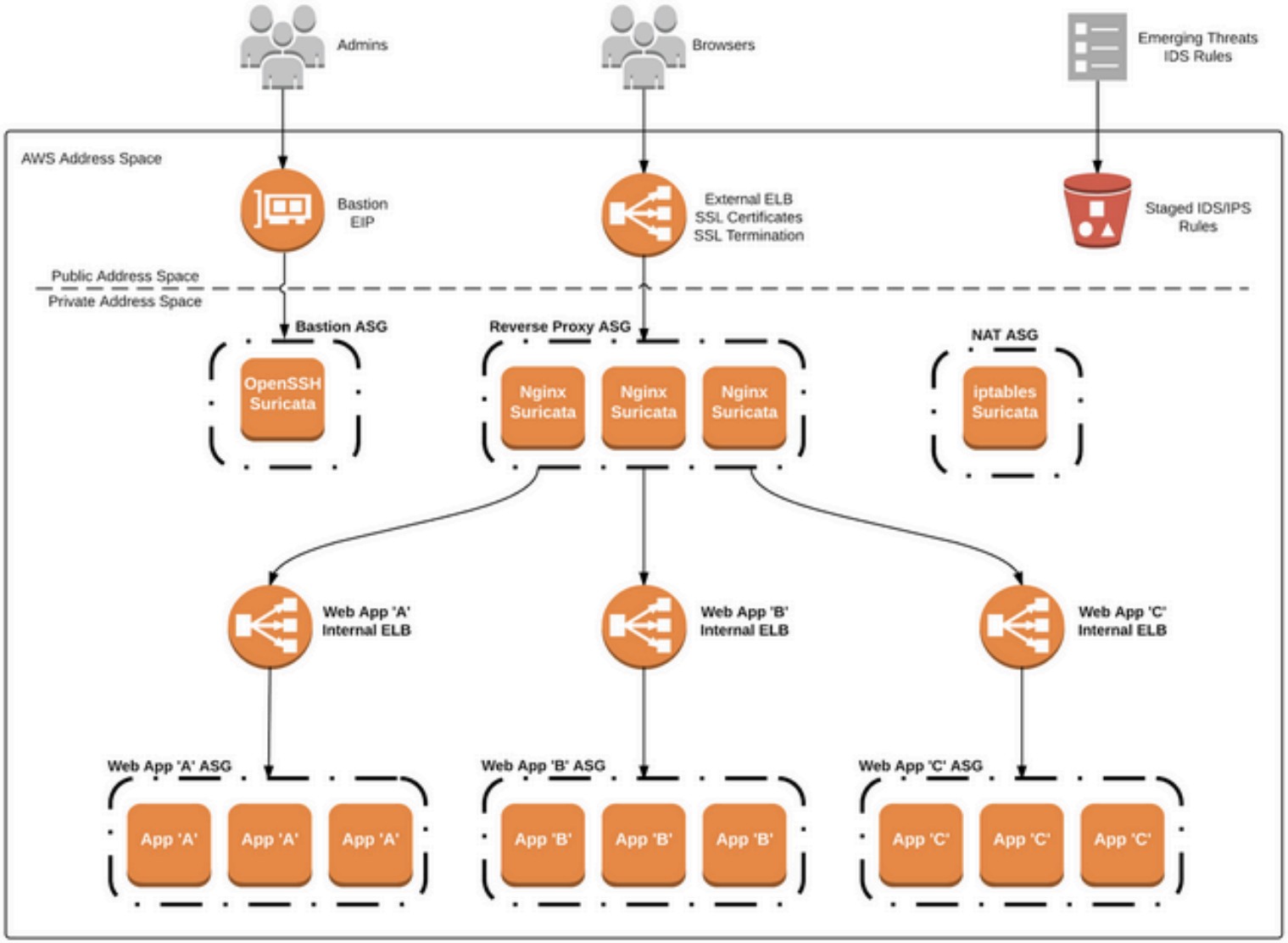
Appendix B – Software Inventory

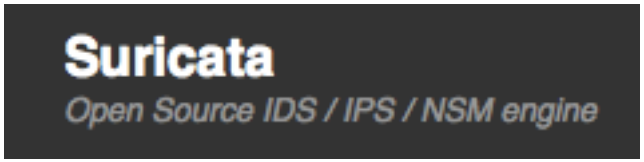
Software	Version	Source	Purpose
e.g., Windows server *Oracle* *Eclipse* *JDK* *Gnu Privacy Guard*	*2008* *11g* *1.6*	*www.eclipse.org* *www.oracle.com* *www.gpg.org*	*Operating System* *Database* *Integrated Development Environment* *Java Libraries* *Encryption Too*
Nginx Openresty	1.4.3.6	http://openresty.org/	Reverse-proxy server
Luarocks	2.1.2	RHEL5 package	Lua package manager

Baseline

http://aws.amazon.com/whitepapers/aws-security-best-practices/

- 2 Factor authentication for AWS Console
- CF defined IAM Roles for all Instances
- Encryption for all comms in and out of VPCs
- Patching of security packages via yum-cron
- Identify credentials and their lifecycle
- Minimal (if any) data on EBS
- Minimal software deployment

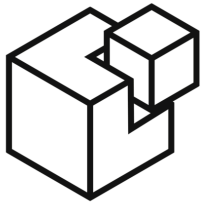

Admins
Browsers
Emerging Threats
IDS Rules
AWS Address Space
Bastion
EIP
External ELB
SSL Certificates
SSL Termination
Staged IDS/IPS
Rules
Public Address Space
Private Address Space
Bastion ASG
OpenSSH
Suricata
Reverse Proxy ASG
Nginx
Suricata
Nginx
Suricata
Nginx
Suricata
NAT ASG
iptables
Suricata
Web App 'A'
Internal ELB
Web App 'B'
Internal ELB
Web App 'C'
Internal ELB
Web App 'A' ASG
App 'A'
App 'A'
App 'A'
Web App 'B' ASG
App 'B'
App 'B'
App 'B'
Web App 'C' ASG
App 'C'
App 'C'
App 'C'

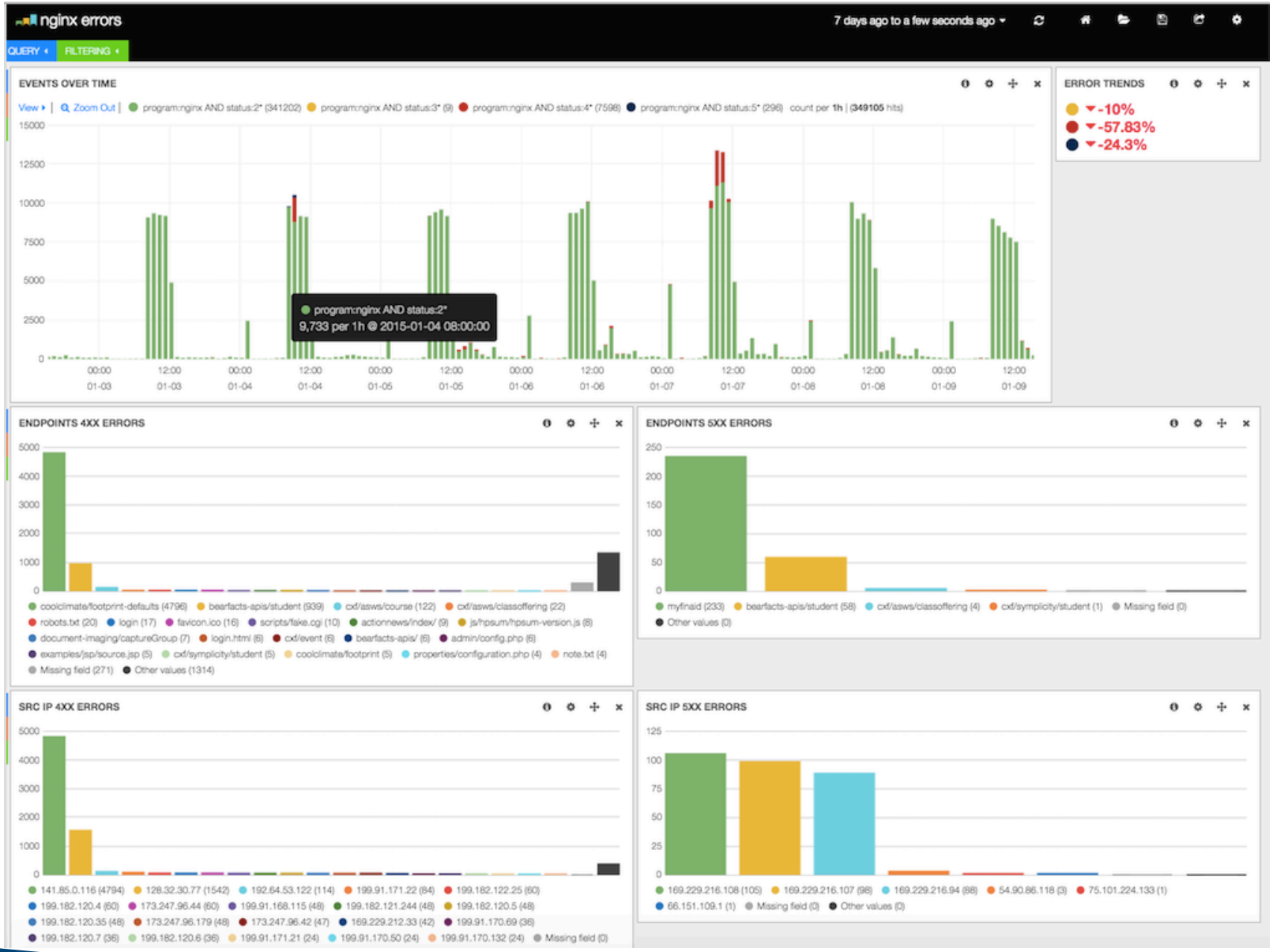


http://suricata-ids.org/

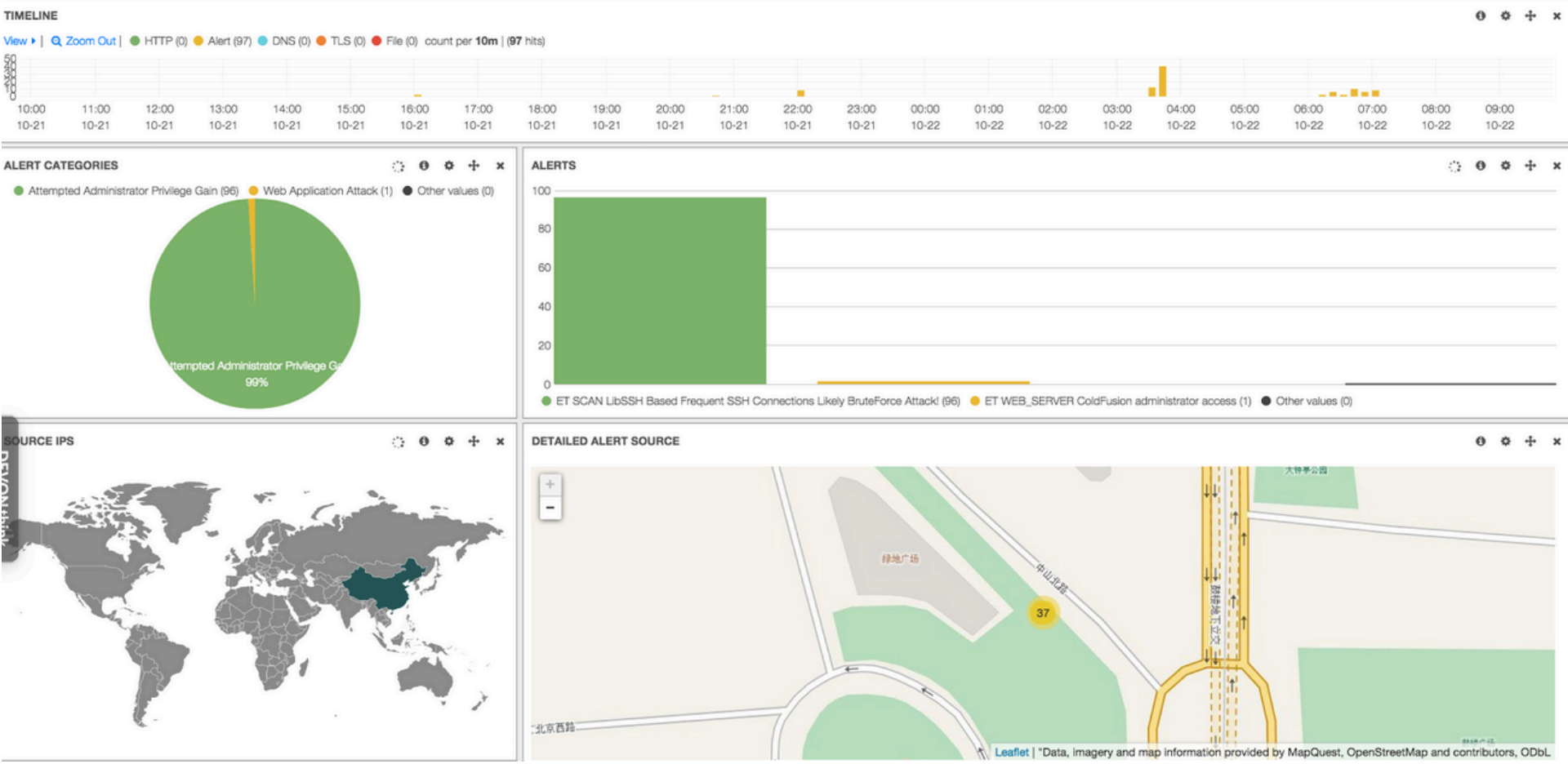
http://emergingthreats.net/products/etpro-ruleset/

http://www.elasticsearch.org/overview/kibana/





Berkeley
UNIVERSITY OF CALIFORNIA



Berkeley
UNIVERSITY OF CALIFORNIA

Discussion!

- What sensitive apps have you put in the cloud?
- How does your setup differ from this?
- Do you see anything missing?
- Are there areas where we the CSG could work together?

Thank you to the UCB IT Security Team and the IST-API Integration Team