Prove it!

The last mile for DevOps in regulated organizations

Bill Shinn
AWS Principal Security Solutions Architect
#DOES15

Session Goals

Identify Blockers and Friction

Partnership

Control Design

Control Evidence - Proofs!

#DOES14 Research Agenda

Better strategies and tactics for creating automated tests for legacy applications

Addressing culture and leadership aspects during transforming

Top approaches to organizational design, roles and responsibilities

Information security and compliance practices

Identifying metrics to best improve performance with DevOps initiatives.

#DOES14 Research Agenda

Addressing culture and leadership aspects during transforming

Top approaches to organizational design, roles and responsibilities

Information security and compliance practices

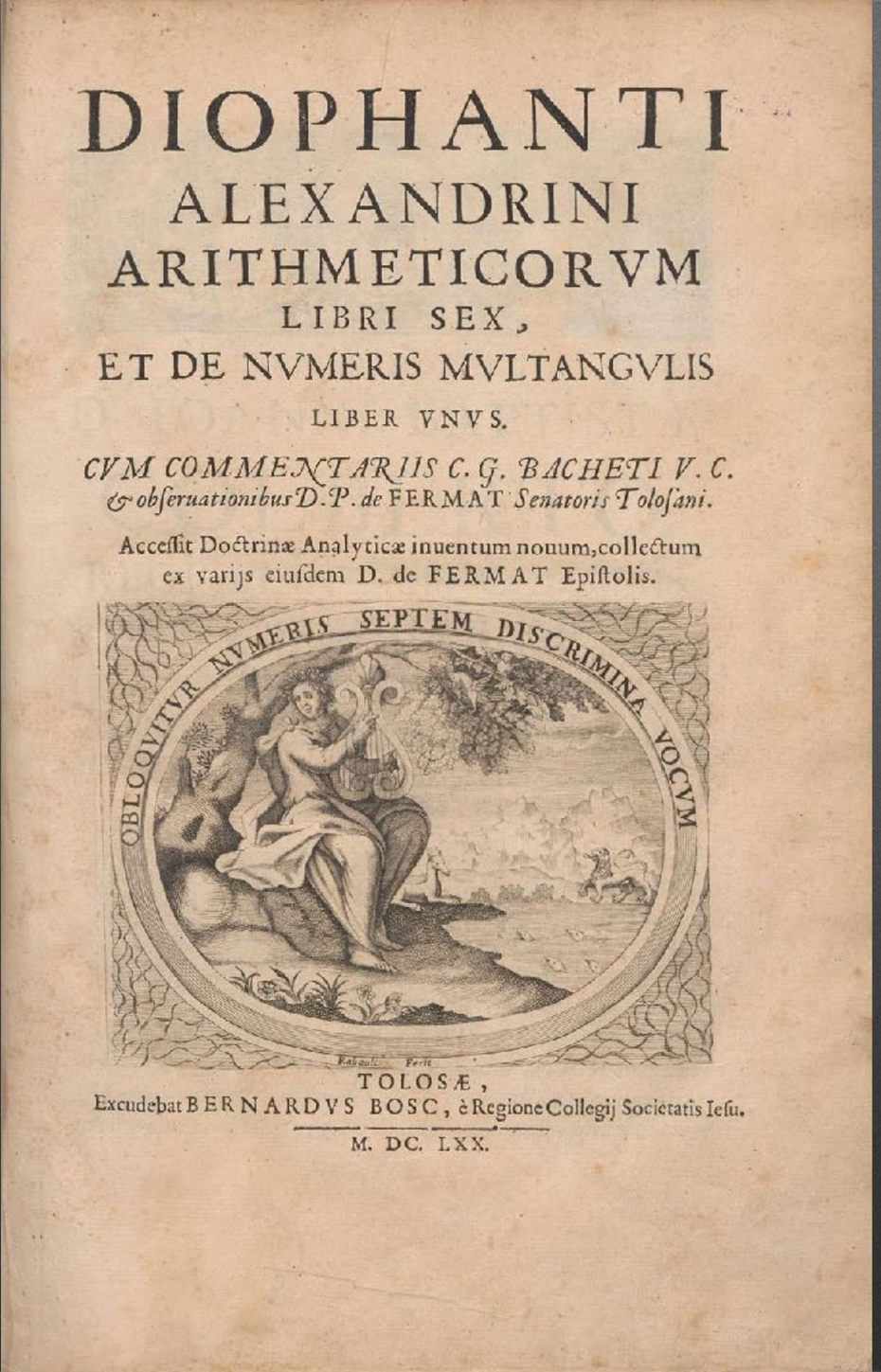
Fermat's Last Theorem

$$x^n + y^n = z^n$$

has no whole number solution for n greater than 2

Pierre de Fermat
(~1601 - 1665)

amazon web services



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT *Senatoris Toloſani.*

Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiuſdem D. de FERMAT Epiſtolis.

OBLOQVITVR NVMERIS SEPTEM DISCRIMINA VOCVM

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.

M. DC. LXX.

Fermat's Last Theorem

"I have a truly marvelous demonstration of the proposition which this margin is too narrow to contain."

amazon web services

Andrew Wiles

First encounters Fermat's Last Theorem at age 10

"I loved doing the problems in school. I'd take them home and make up new ones on my own."

amazon web services

Sir Andrew John Wiles
(1953 -)

(Fermat's Enigma - Simon Singh 1997, Walker Publishing, Inc)

Andrew Wiles

Spends 7 years working in isolation

Produces a 200-page proof

Sir Andrew John Wiles
(1953 -)

(Fermat's Enigma - Simon Singh 1997, Walker Publishing, Inc)

Learning from Fermat's Last Theorem: Friction in DevOps & Compliance

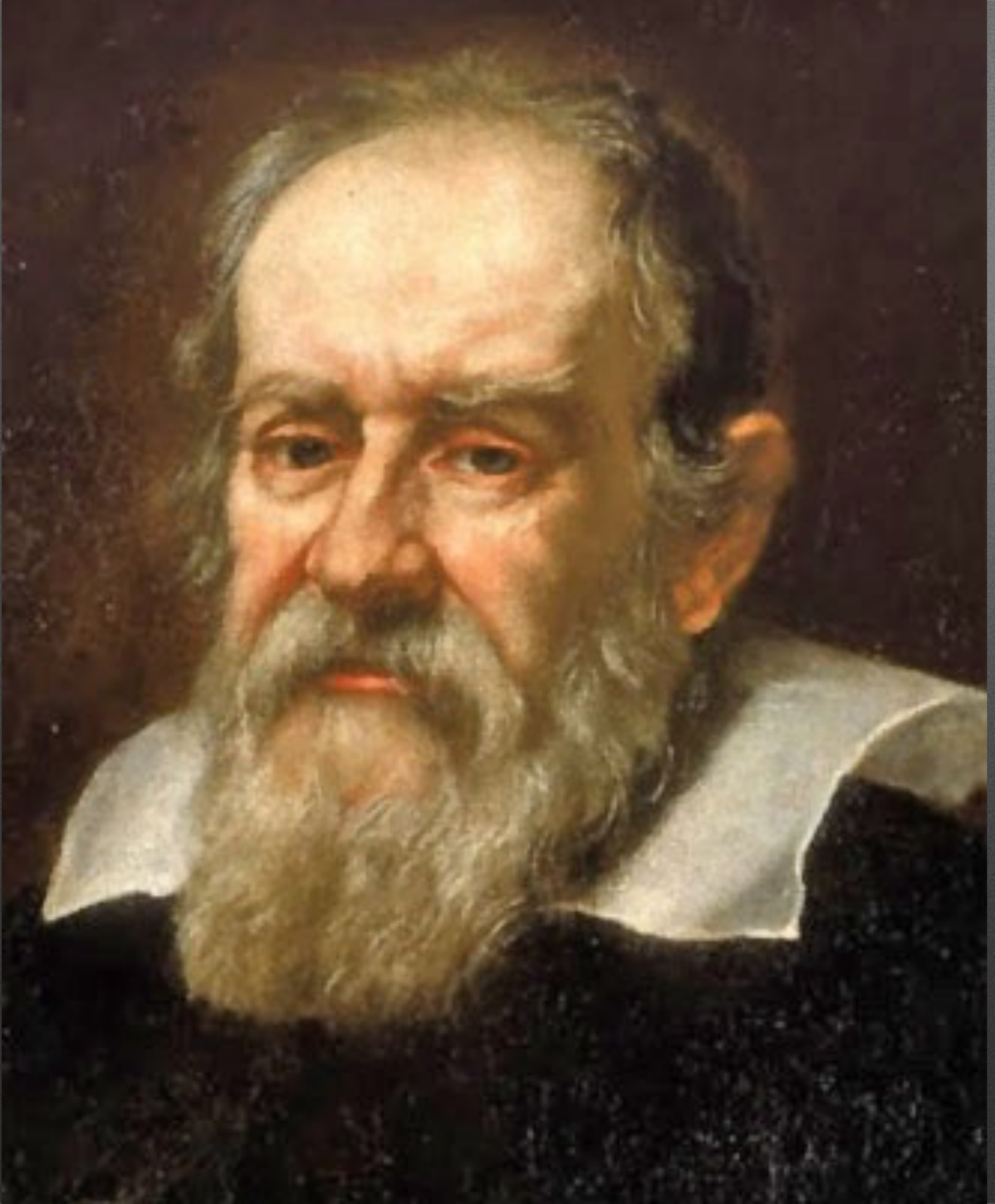
Write down the proof - controls and control evidence is sprints.

Don't work in isolation. Share.

People will criticize.

Everyone reads each others proofs. (NIST 800-53 vs. Data Flows & Code)

Perseverance pays off.



Heliocentrism

Disproved that servers are not the center of the universe

Spent remaining years of his life under house arrest trying to Prove It.

amazon web services

Learning from Galileo: Friction in DevOps & Compliance

The world does not revolve around servers.

Policies might not accommodate changes to Ops.

Tides: it's ok to iterate….

Longitude

Goes head-to-head with
Astronomer Royal

Humble clock maker, hacker

Relatively short sprints.

John Harrison
(1693 - 1776)

amazon
web services

Learning from Longitude: Friction in DevOps & Compliance

Makers win.

Defer to expertise, not auhority.

Optimism pays off.

Don’t get lost at sea. Automate your navigation.

Deriving Engineering from Regulations

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

Title 45 of the Code of Federal Regulations – Public Welfare

Subtitle A - Health and Human Services

Subchapter C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS

Part 160 - General Administrative Requirements

Part 164 - Security and Privacy

Subpart C - Security Standards for the Protection of Electronic Protected Health Information

Section 164.308 - Administrative Safeguards
Section 164.310 - Physical Safeguards
Section 164.312 - Technical Safeguards
    164.312(b)(2) – Standard: Audit Controls
Section 164.314 - Organizational Safeguards

Deriving Engineering from Regulations

164.312 (b)(2) Standard: Audit Controls

Implement hardware, software, and/or procedural mechanisms that *record and examine activity* in information systems that contain or use electronic protected health information.

Deriving Engineering from Regulations

§164.312(b):

Key Activity
Determine the Activities that Will be Tracked or Audited

Audit Procedures
Inquire of management as to whether audit controls have been implemented over information systems that contain or use ePHI. Obtain and review documentation relative to the specified criteria to determine whether audit controls have been implemented over information systems that contain or use ePHI.

Key Activity
Select the Tools that Will be Deployed for Auditing and System Activity Reviews

Audit Procedures
Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.
Section 164.314 - Organizational Safeguards

Audit Controls 164.308(b)(2) – OCR Audit Protocol

§164.312(b):

Something you have to do.

Key Activity
Determine the Activities that Will be Tracked or Audited

Audit Procedures
Inquire of management as to whether audit controls have been implemented over information systems that contain or use ePHI. Obtain and review documentation relative to the specified criteria to determine whether audit controls have been implemented over information systems that contain or use ePHI.

Key Activity
Select the Tools that Will be Deployed for Auditing and System Activity Reviews

Audit Procedures
Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.

amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Determine the Activities

EC2 CloudTrail Events

AttachVolume
AuthorizeSecurityGroupIngress
CopySnapshot
CreateNetworkAclEntry
CreateSnapshot
DeleteSnapshot
DeleteTags
DeleteVolume
TerminateInstance

RDS CloudTrail Events

AuthorizeDBSecurityGroupIngress
CopyDBSnapshot
CreateDBSnapshot
DeleteDBInstance
DeleteDBSnapshot
ModifyDBInstance

Amazon Glacier CloudTrail Events

DeleteArchive
DeleteVault

DynamoDB CloudTrail Events

DeleteTable
UpdateTable

Amazon Redshift CloudTrail Events

AuthorizeClusterSecurityGroupIngress
CopyClusterSnapshot
CreateClusterSnapshot
DeleteCluster
DeleteClusterSnapshot
DisableLogging

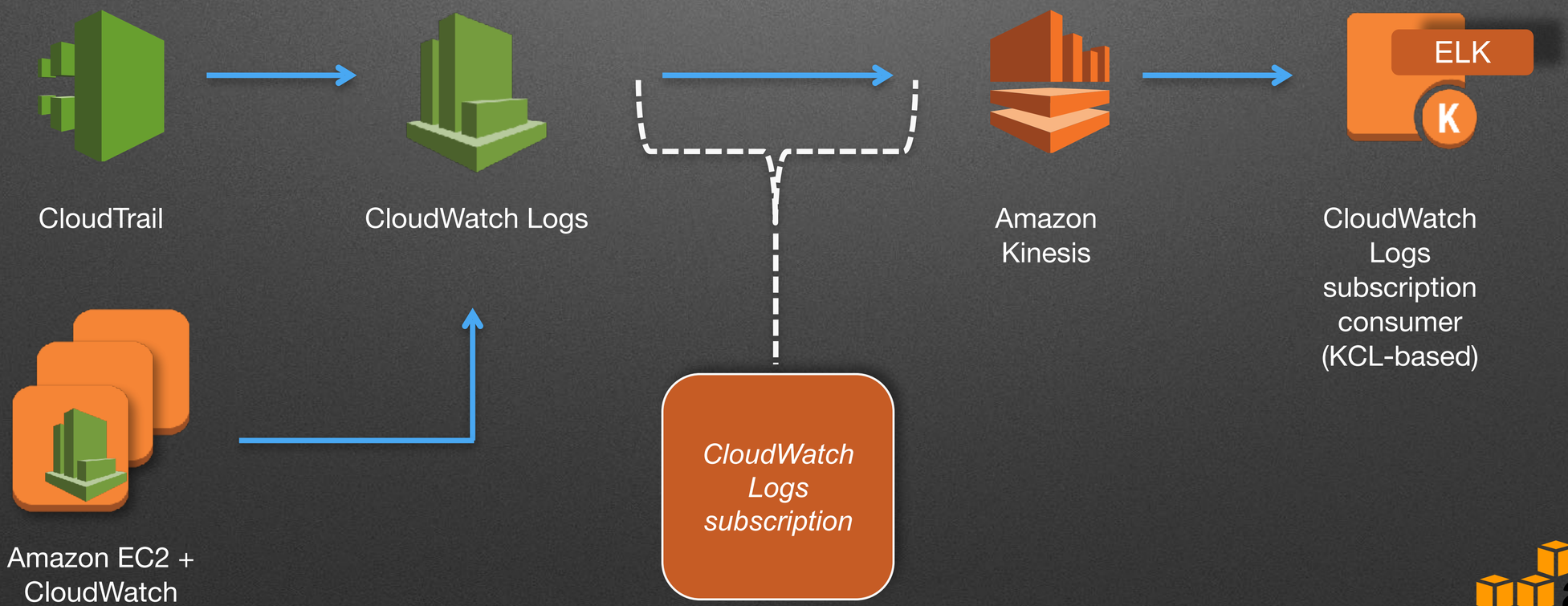
Audit Controls 164.312(b)(2) – OCR Audit Protocol – Document Implementation

Capture CloudTrail Configuration (CLI Example)

```
$ aws cloudtrail describe-trails
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "S3KeyPrefix": ”CloudTrail",
            "S3BucketName": "us-east-1.logging",
            "CloudWatchLogsRoleArn": "arn:aws:iam::663354267581:role/
CloudTrail_CloudWatchLogs_Role",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:663354267581:log-
group:CloudTrail/us-east-1-LogGroup:*"
        }
    ]
}
```

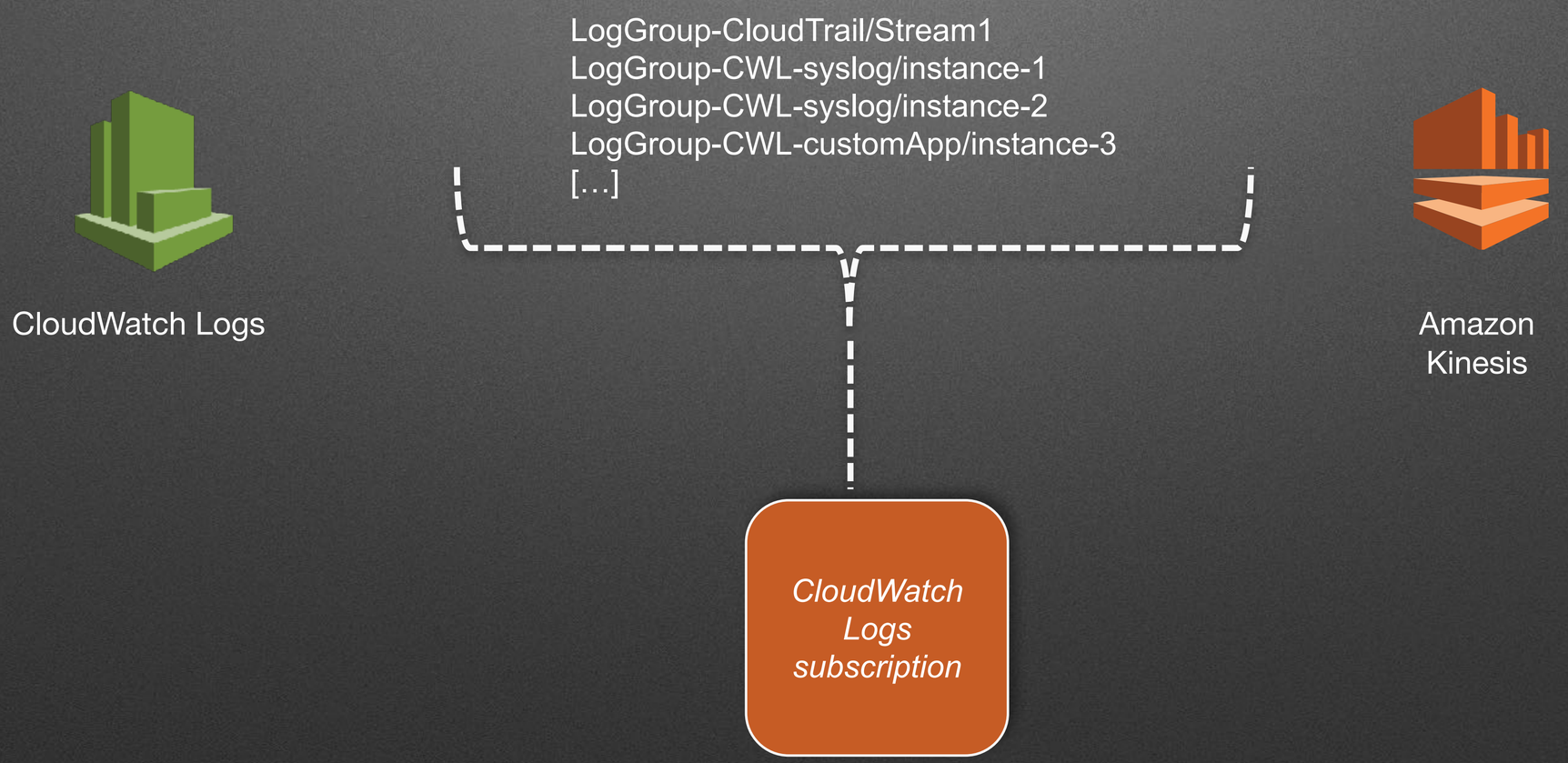
amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Select the Tools

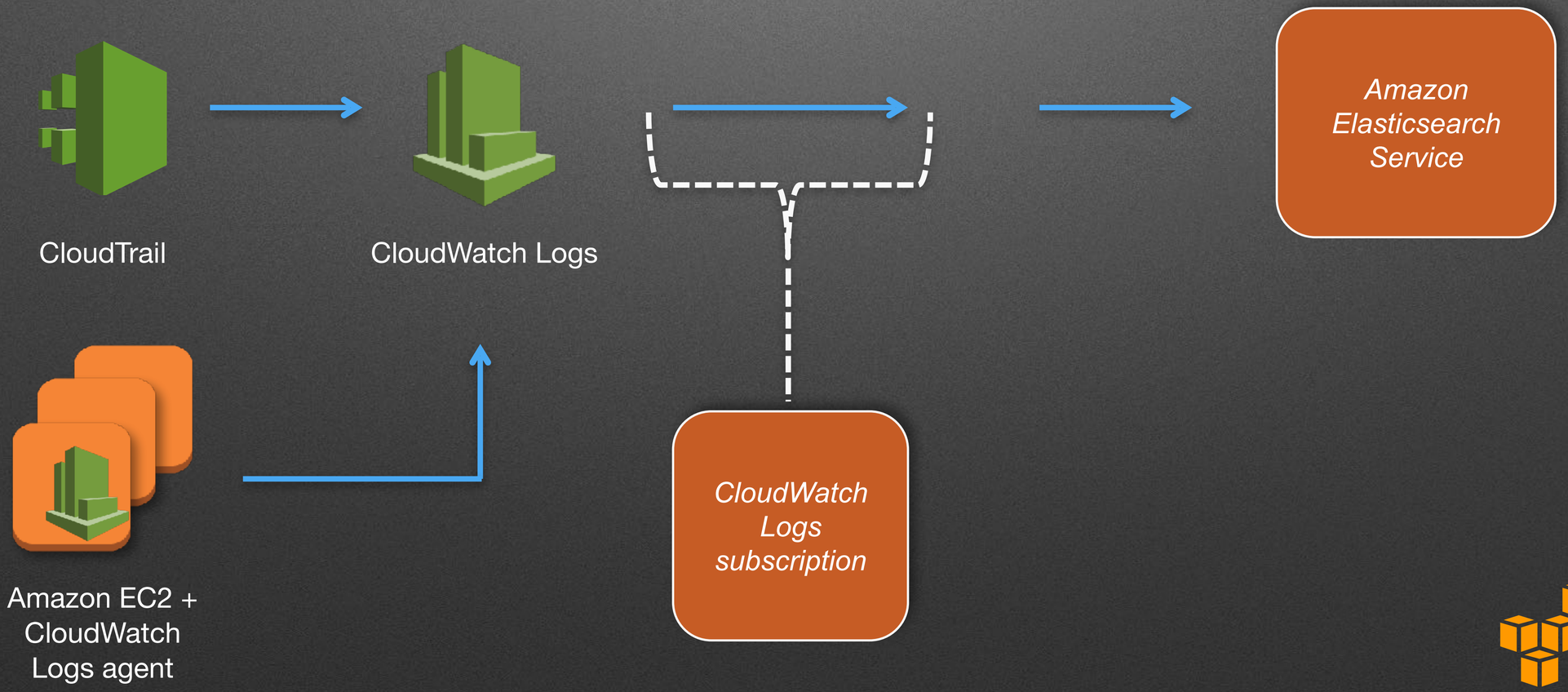


amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Select the Tools



Audit Controls 164.312(b)(2) – OCR Audit Protocol – Select the Tools



amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Document Implementation

§164.312(b):

Key Activity
Select the Tools that Will be Deployed for Auditing and System Activity Reviews

Audit Procedures
[…] Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.

```
$ aws logs describe-log-groups --log-group-name-prefix "CloudTrail"
{
    "logGroups": [
        {
            "arn": "arn:aws:logs:us-east-1:663354267581:log-group:CloudTrail/us-east-1-LogGroup:*",
            "creationTime": 1439155915783,
            "metricFilterCount": 0,
            "logGroupName": "CloudTrail/us-east-1-LogGroup",
            "storedBytes": 411573
```

amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Document Implementation

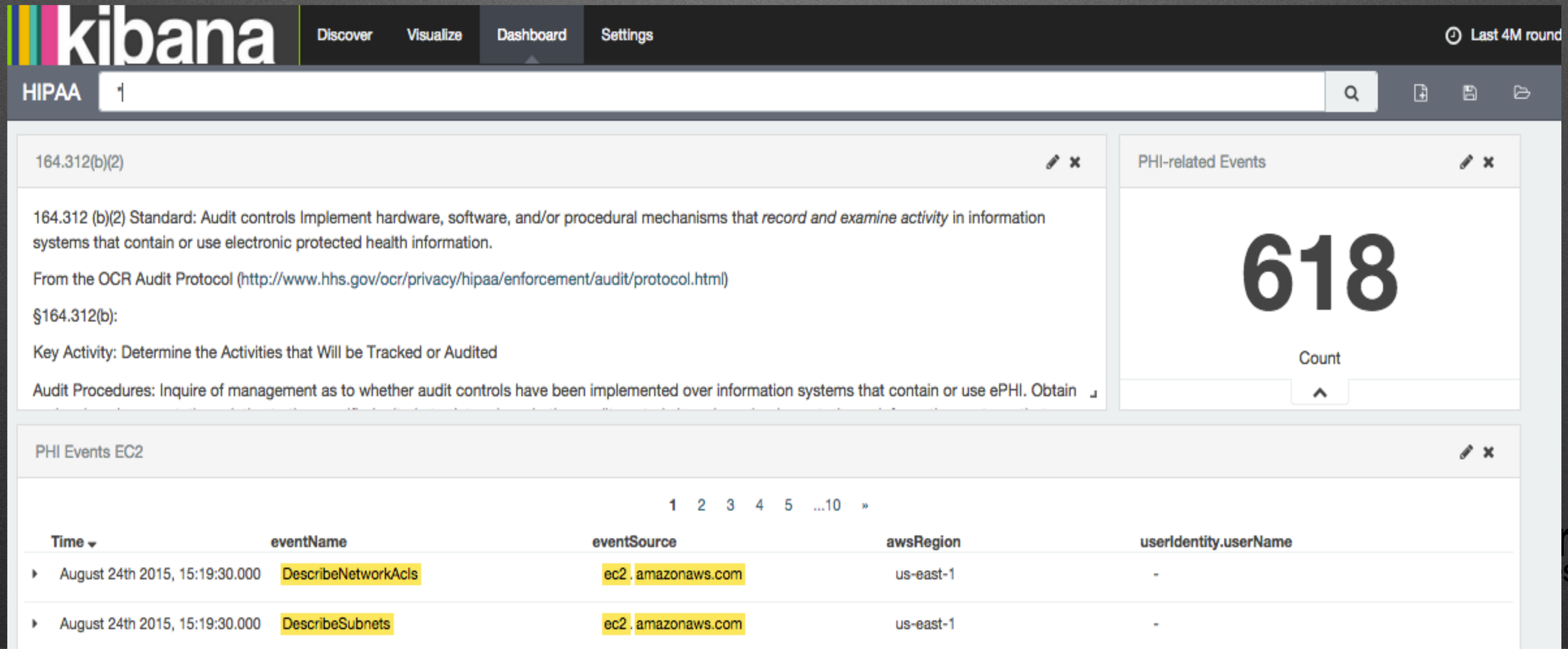
§164.312(b):

Audit Procedures
[…] Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.

```
$ aws logs describe-subscription-filters --log-group-name CloudTrail/us-east-1-LogGroup
{
    "subscriptionFilters": [
        {
            "filterPattern": "",
            "filterName": "cwl-cfn-es-CWL-Elasticsearch-KinesisSubscriptionStream-1KSJUFTUP6K5K",
            "roleArn": "arn:aws:iam::663354267581:role/CWL-Elasticsearch-
CloudWatchLogsKinesisRole-4DVR5UWI4QBR",
            "creationTime": 1439157386140,
            "logGroupName": "CloudTrail/us-east-1-LogGroup",
            "destinationArn": "arn:aws:kinesis:us-east-1:663354267581:stream/CWL-Elasticsearch-
KinesisSubscriptionStream-1KSJUFTUP6K5K"
```

amazon web services

Audit Controls 164.312(b)(2) – OCR Audit Protocol – Activity Reviews



Similar Controls

PCI DSS 3.1 Requirement 10.1 - 10.8 — Track and monitor all access to network resources and cardholder data.

NIST 800-53r4 (AU-1 - AU-16) Audit and Accountability Controls

ISO 27001 A.10.10 - Monitoring - Objective: To detect unauthorized information processing activities.

Additional Resources

The DevOps Audit Defense Tool Kit (http://itrevolution.com/devops-and-auditors-the-devops-audit-defense-toolkit/)

AWS re:Invent SEC310 - Splitting the Check on Compliance and Security: Keeping Developers and Auditors Happy in the Cloud - Jason Chan, Engineering Director @NetFlix, October 2015 (https://youtu.be/I0oo_K4v12Y)

Singh, S. (1997). Fermat's enigma: The epic quest to solve the world's greatest mathematical problem. New York: Walker.

Sobel, D. (1995). Longitude: The true story of a lone genius who solved the greatest scientific problem of his time. New York: Walker.

Sobel, D. (1999). Galileo's daughter: A historical memoir of science, faith, and love. New York: Walker

amazon web services

Thank You!

Bill Shinn - billshin@amazon.com
@packet791