

FINRA AWS Role Permissions Compliance System

Shijie Zhang



AGENDA

■ How It Works

■ System Components

- Gold Source
- Amazon Web Services
- Developed Scripts
- Splunk
- AWS Compliance Dashboard

■ Demo

■ Summary

AGENDA

■ How It Works

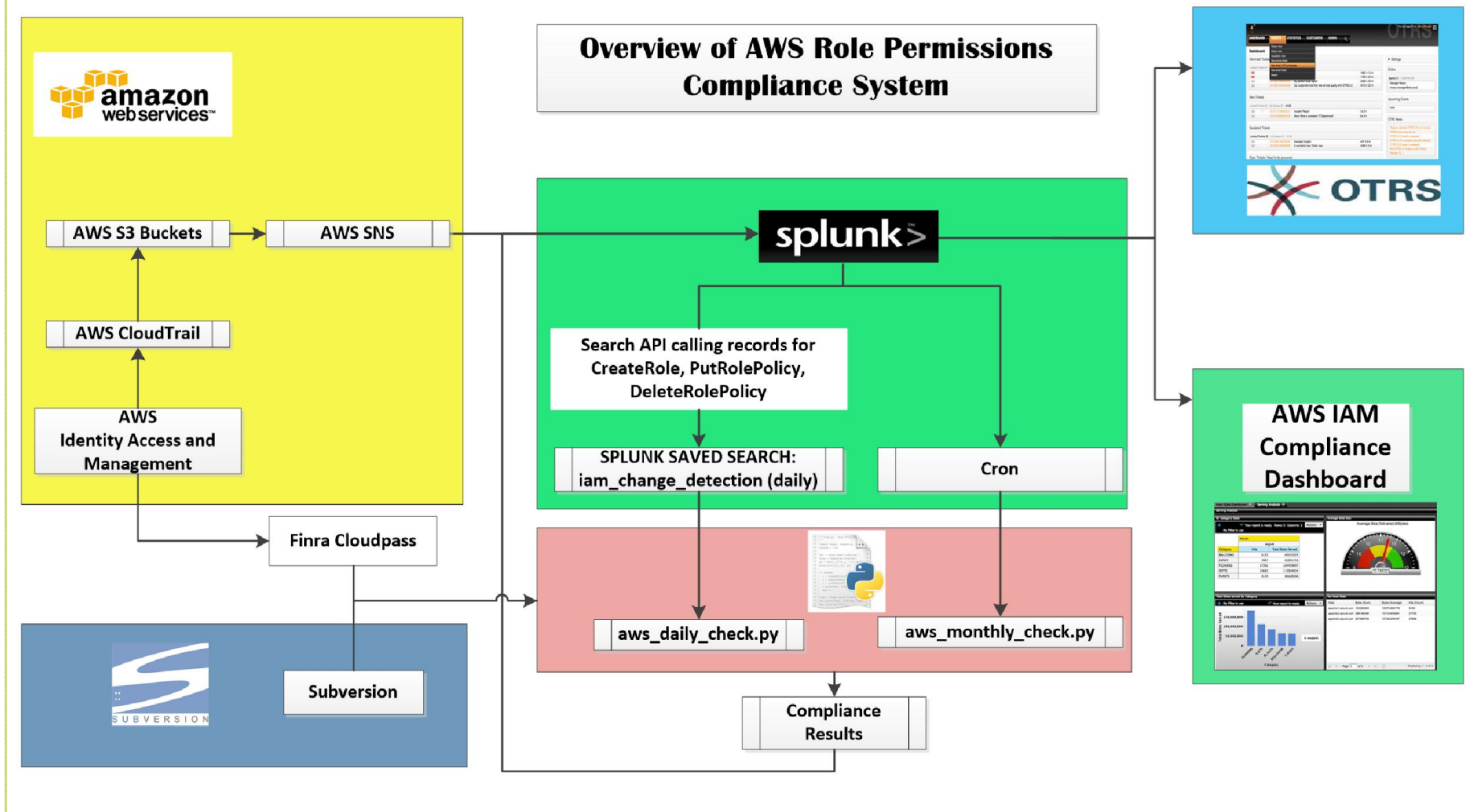
■ System Components

- Gold Source
- Amazon Web Services
- Developed Scripts
- Splunk
- AWS Compliance Dashboard

■ Demo

■ Summary

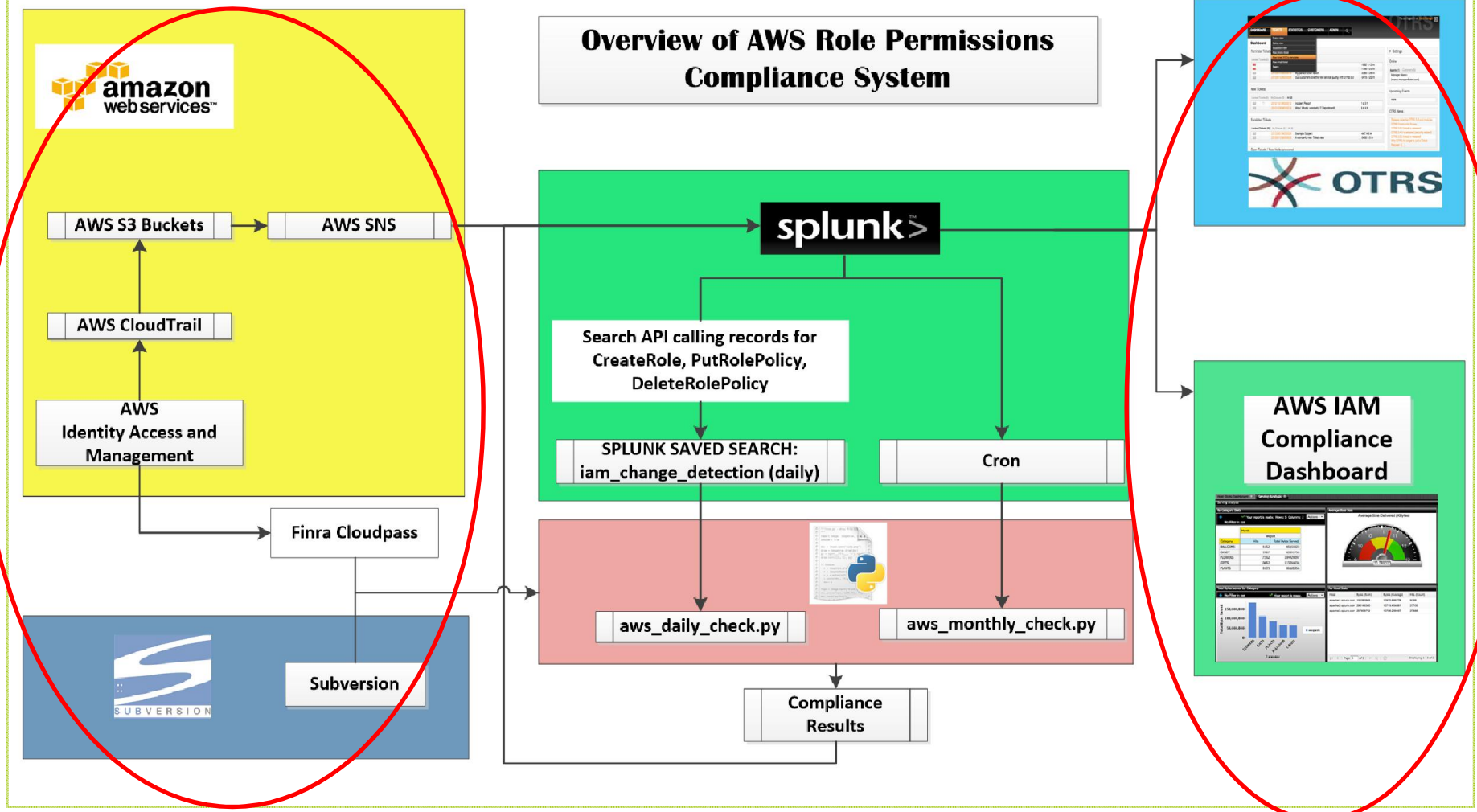
How It Works



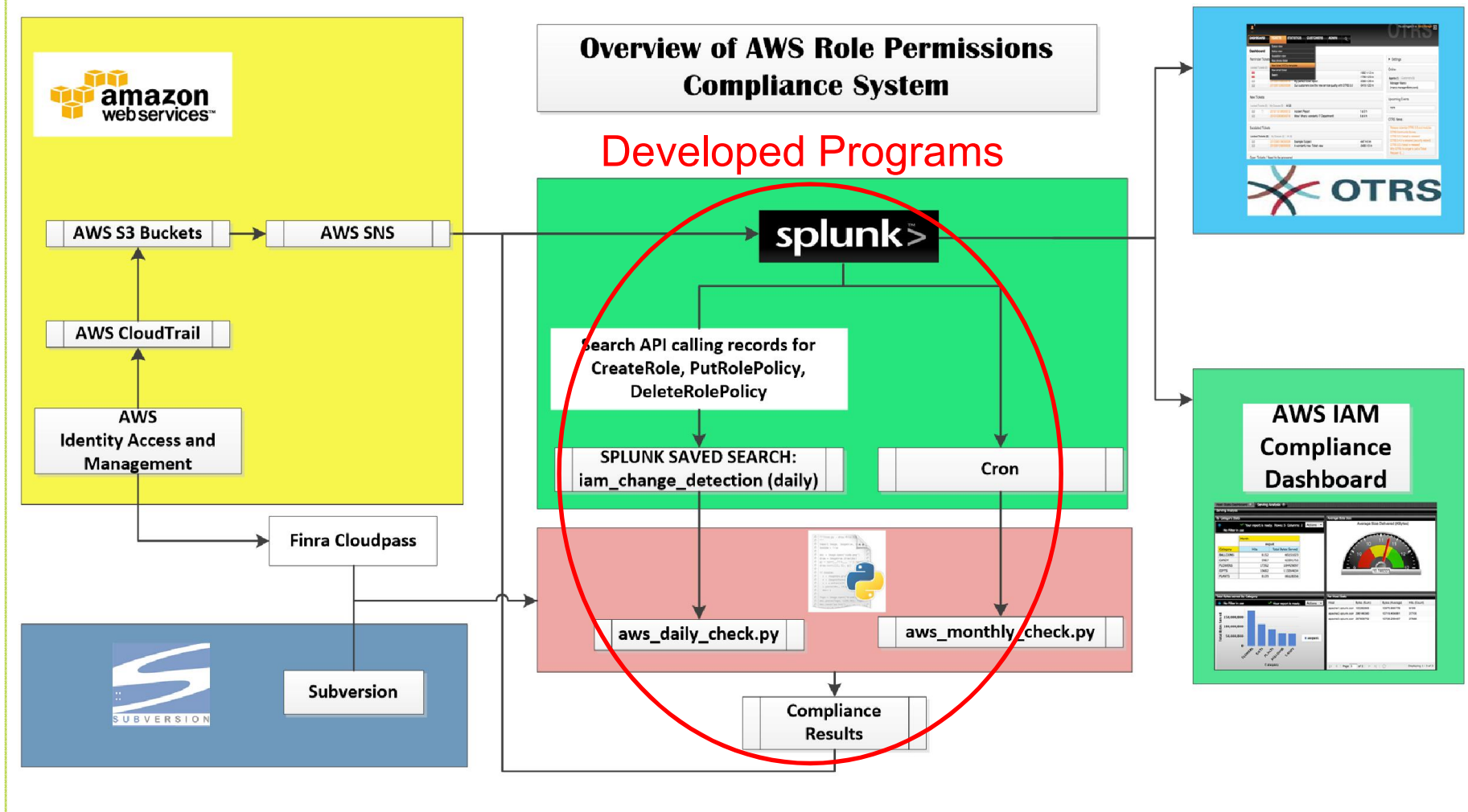
How It Works

Input

output



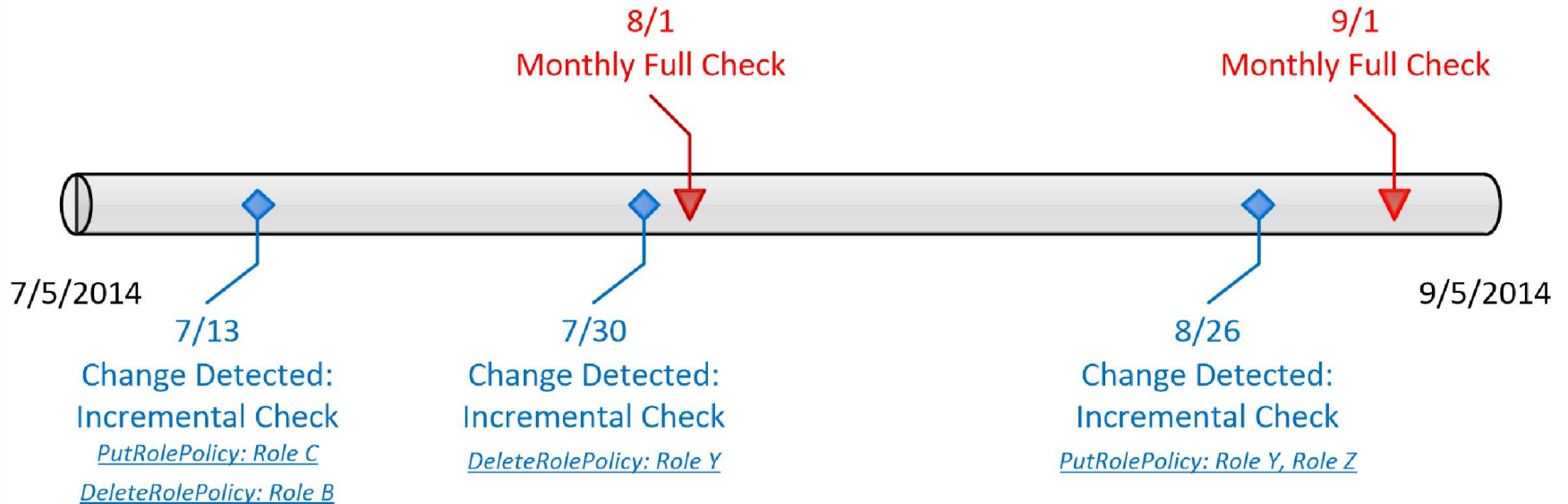
How It Works



How It Works?

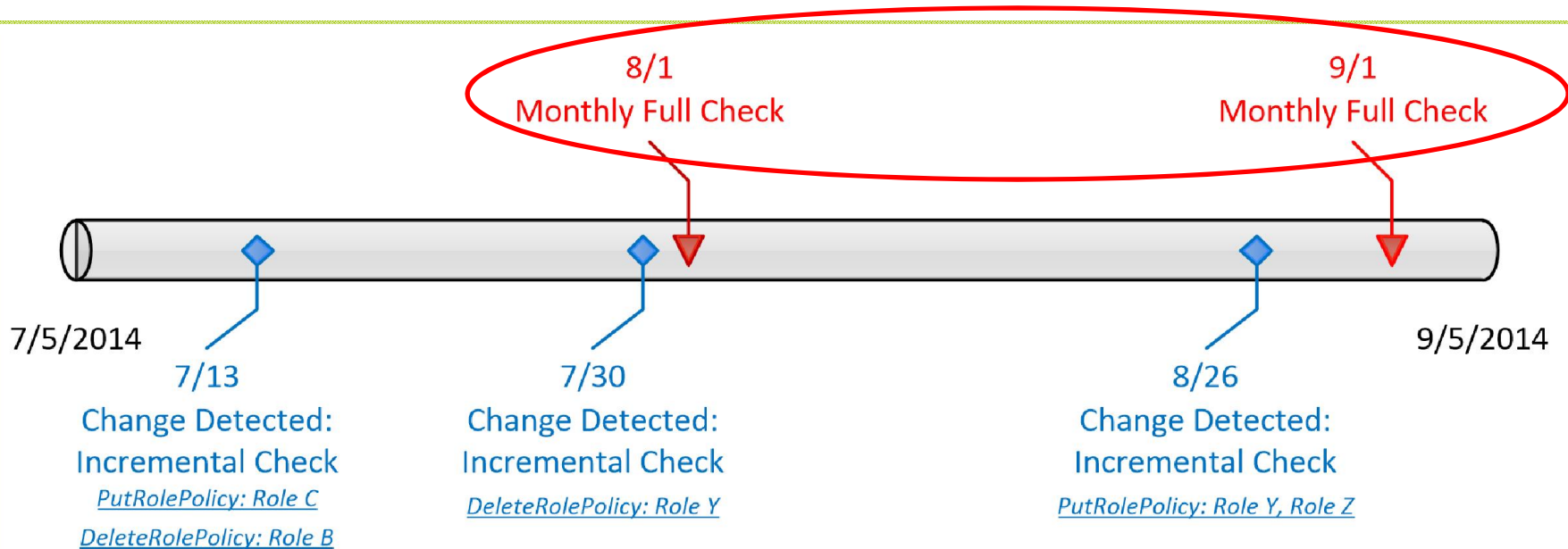
- Two Use Cases of the Developed Programs:
 - **Monthly full check:**
Check compliant status for all the roles in all environments
 - **When changes to role permissions are detected:**
Check compliant status for the changed role

How It Works?



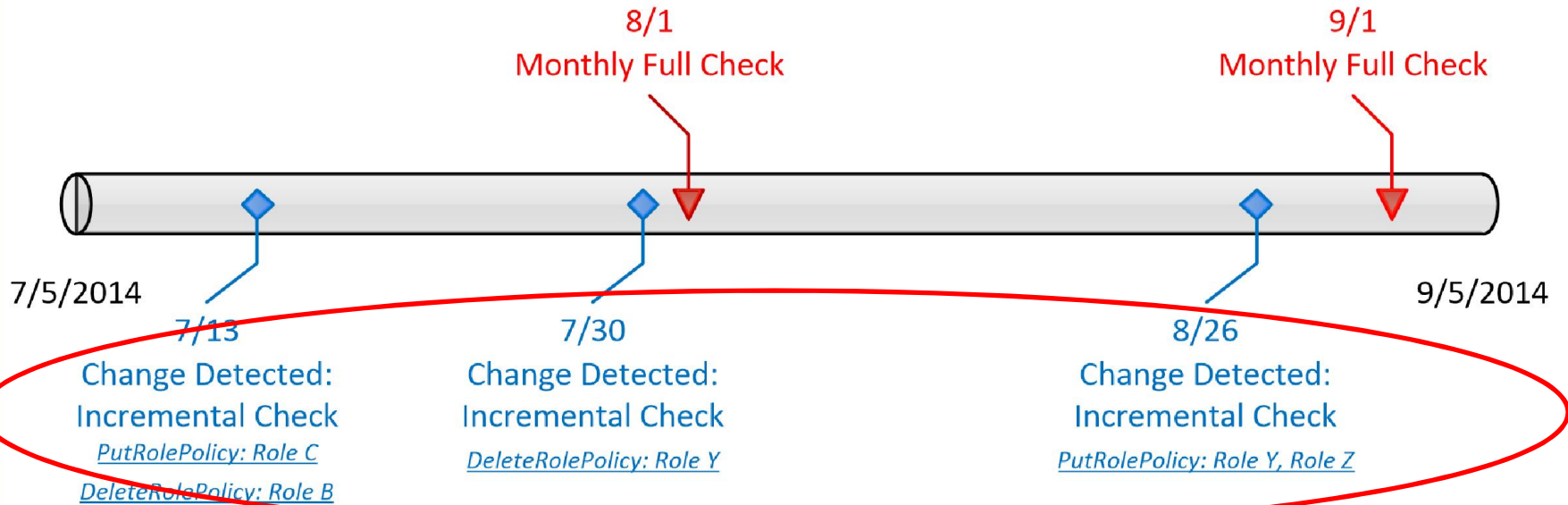
ROLE\DATE	INITIAL STATUS	DAILY CHECK	DAILY CHECK	MONTHLY CHECK	DAILY CHECK	MONTHLY CHECK	FINAL STATUS
	7/5/2014	7/13/2014	7/30/2014	8/1/2014	8/26/2014	9/1/2014	9/5/2014
Role A	A0			A1		A2	A2
Role B	B0	B1		B2		B3	B3
Role C	C0	C1		C2		C3	C3
Role X	X0			X1		X2	X2
Role Y	Y0		Y1	Y2	Y3	Y4	Y4
Role Z	Z0			Z1	Z2	Z3	Z3

How It Works?



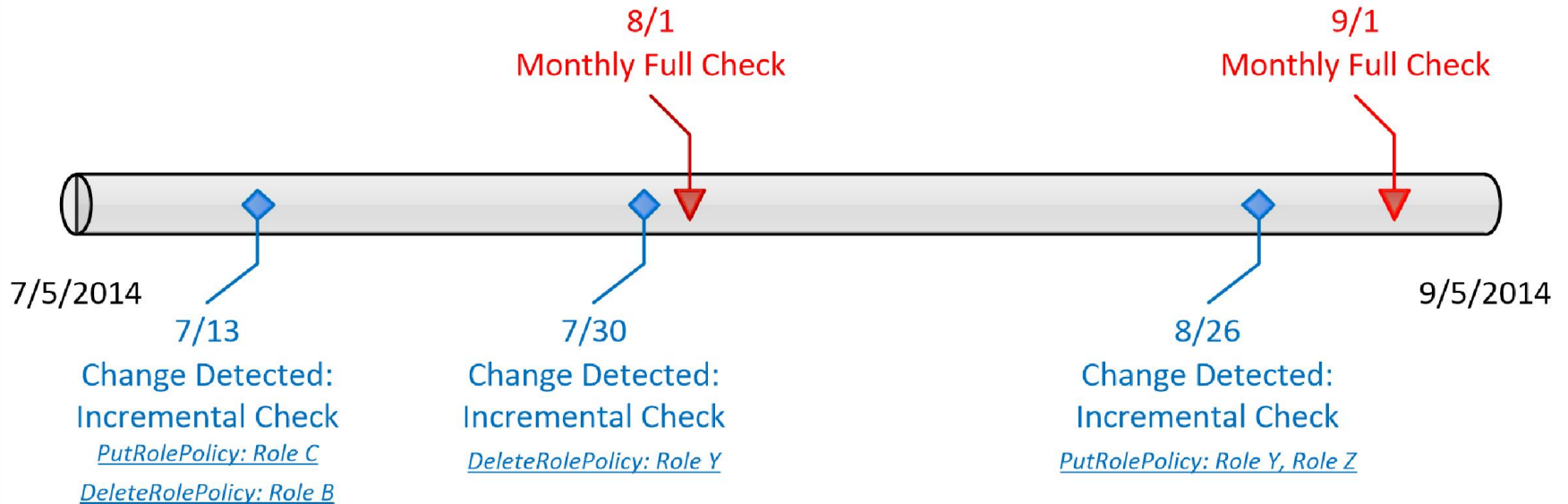
ROLE\DATE	INITIAL STATUS	DAILY CHECK	DAILY CHECK	MONTHLY CHECK	DAILY CHECK	MONTHLY CHECK	FINAL STATUS
	7/5/2014	7/13/2014	7/30/2014	8/1/2014	8/26/2014	9/1/2014	9/5/2014
Role A	A0			A1		A2	A2
Role B	B0	B1		B2		B3	B3
Role C	C0	C1		C2		C3	C3
Role X	X0			X1		X2	X2
Role Y	Y0		Y1	Y2	Y3	Y4	Y4
Role Z	Z0			Z1	Z2	Z3	Z3

How It Works?



ROLE\DATE	INITIAL STATUS	DAILY CHECK	DAILY CHECK	MONTHLY CHECK	DAILY CHECK	MONTHLY CHECK	FINAL STATUS
	7/5/2014	7/13/2014	7/30/2014	8/1/2014	8/26/2014	9/1/2014	9/5/2014
Role A	A0			A1		A2	A2
Role B	B0	B1		B2		B3	B3
Role C	C0	C1		C2		C3	C3
Role X	X0			X1		X2	X2
Role Y	Y0		Y1	Y2	Y3	Y4	Y4
Role Z	Z0			Z1	Z2	Z3	Z3

How It Works?



ROLE\DATE	INITIAL STATUS	DAILY CHECK	DAILY CHECK	MONTHLY CHECK	DAILY CHECK	MONTHLY CHECK	FINAL STATUS
	7/5/2014	7/13/2014	7/30/2014	8/1/2014	8/26/2014	9/1/2014	9/5/2014
Role A	A0			A1		A2	A2
Role B	B0	B1		B2		B3	B3
Role C	C0	C1		C2		C3	C3
Role X	X0			X1		X2	X2
Role Y	Y0		Y1	Y2	Y3	Y4	Y4
Role Z	Z0			Z1	Z2	Z3	Z3

AGENDA

■ How It Works

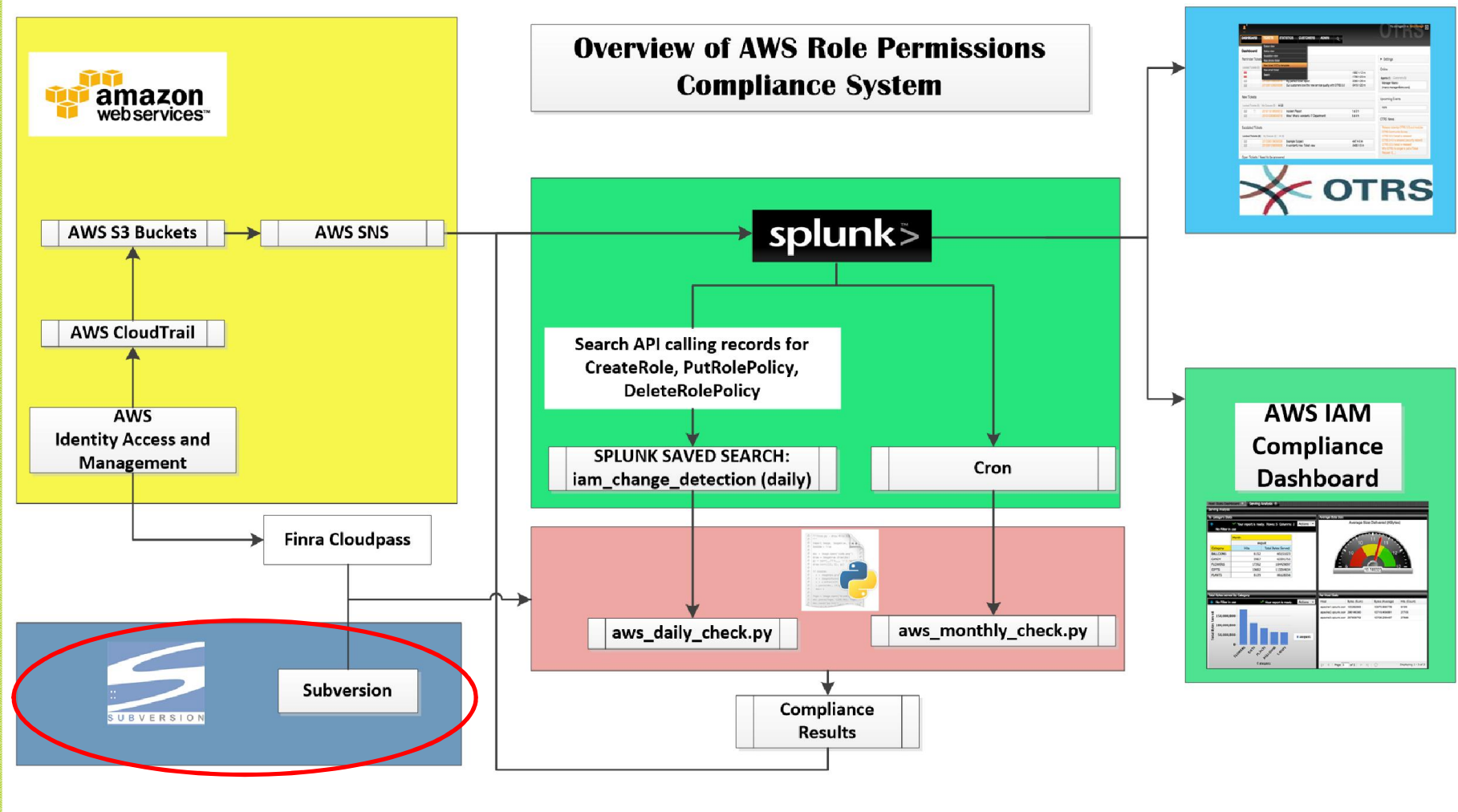
■ System Components

- Gold Source
- Amazon Web Services
- Developed Scripts
- Splunk
- AWS Compliance Dashboard

■ Demo

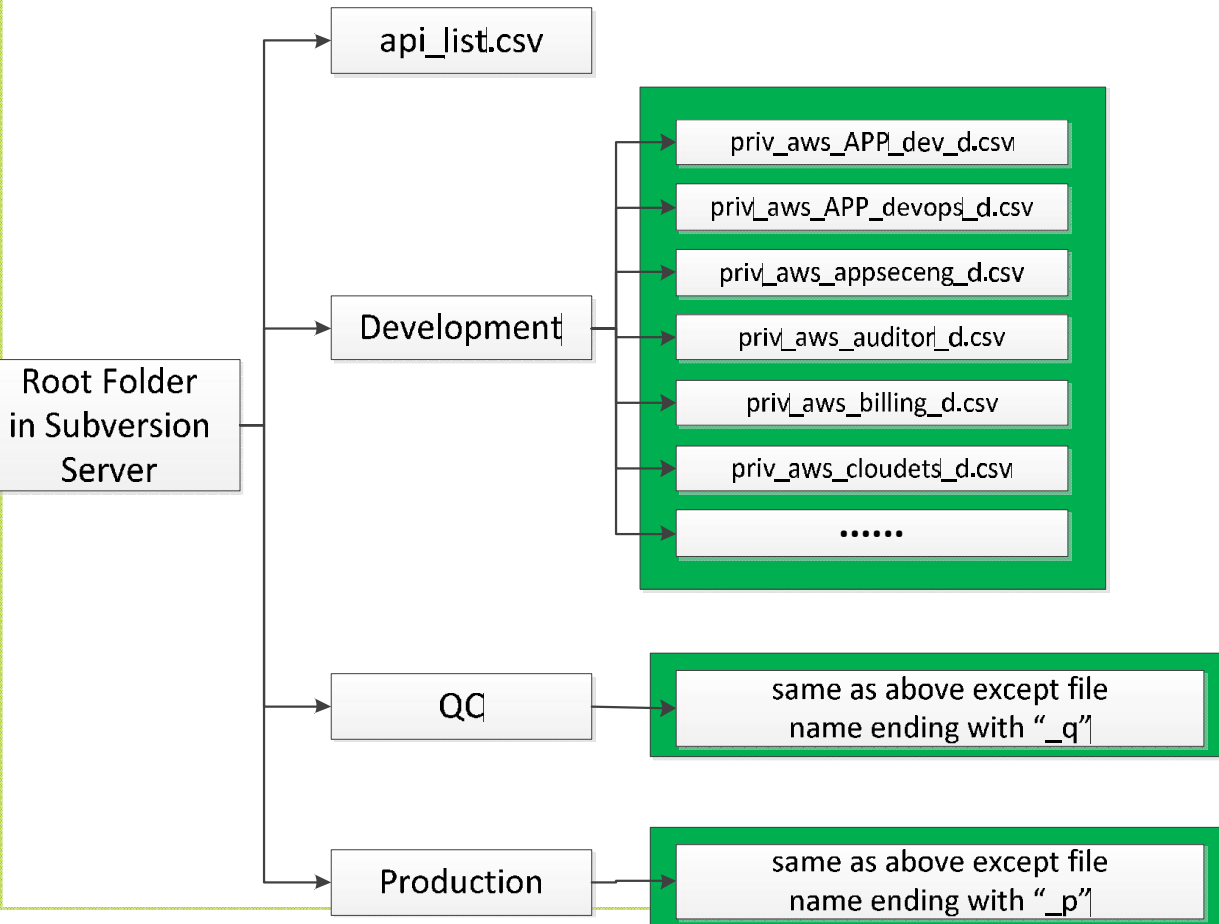
■ Summary

COMPONENTS – Gold Source



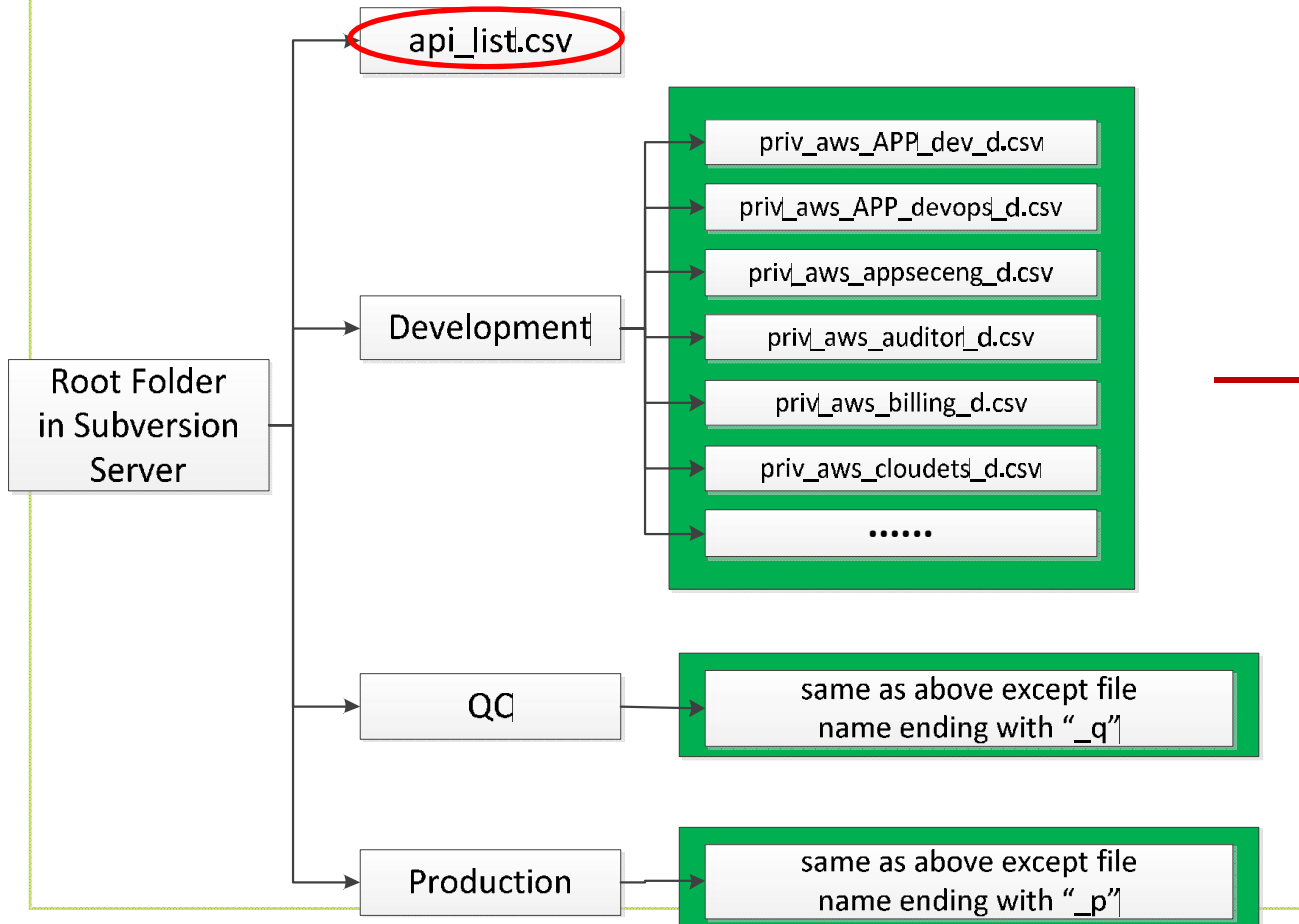
COMPONENTS – Gold Source

GoldSource Structure of AWS Compliance System



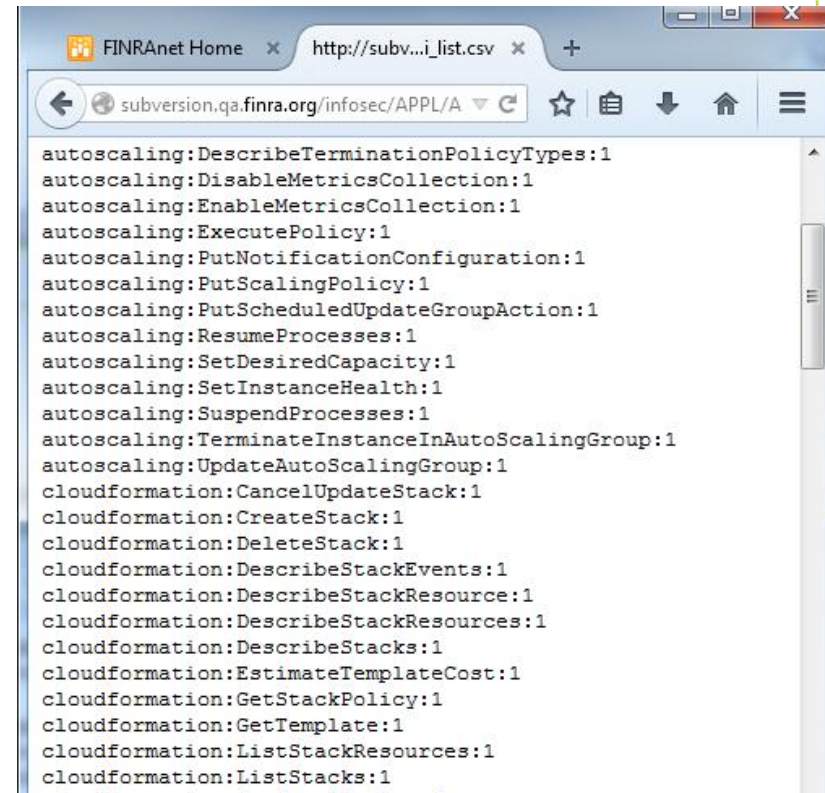
COMPONENTS – Gold Source

GoldSource Structure of AWS Compliance System



COMPONENTS – Gold Source

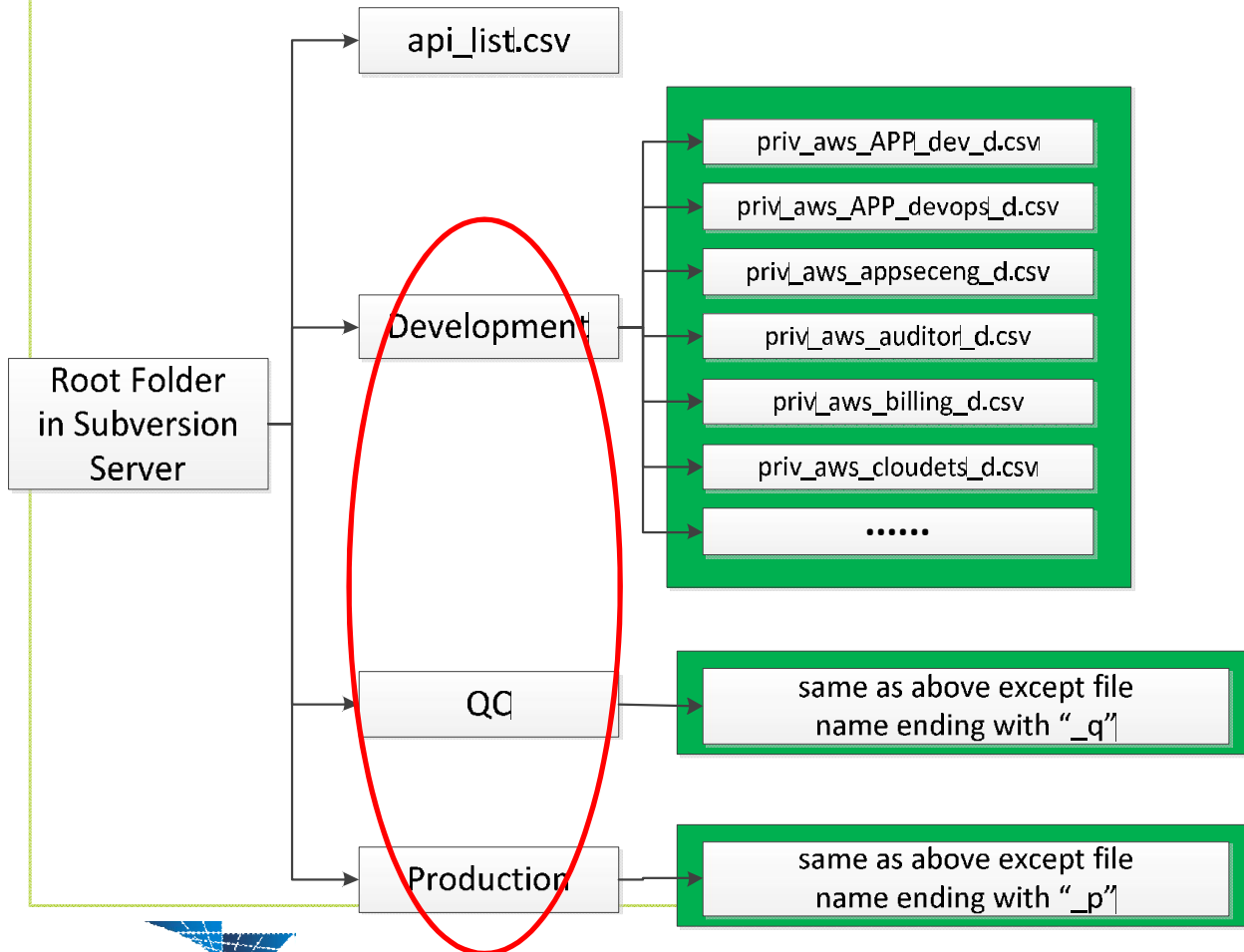
■ api_list.csv



service **api** risk rating

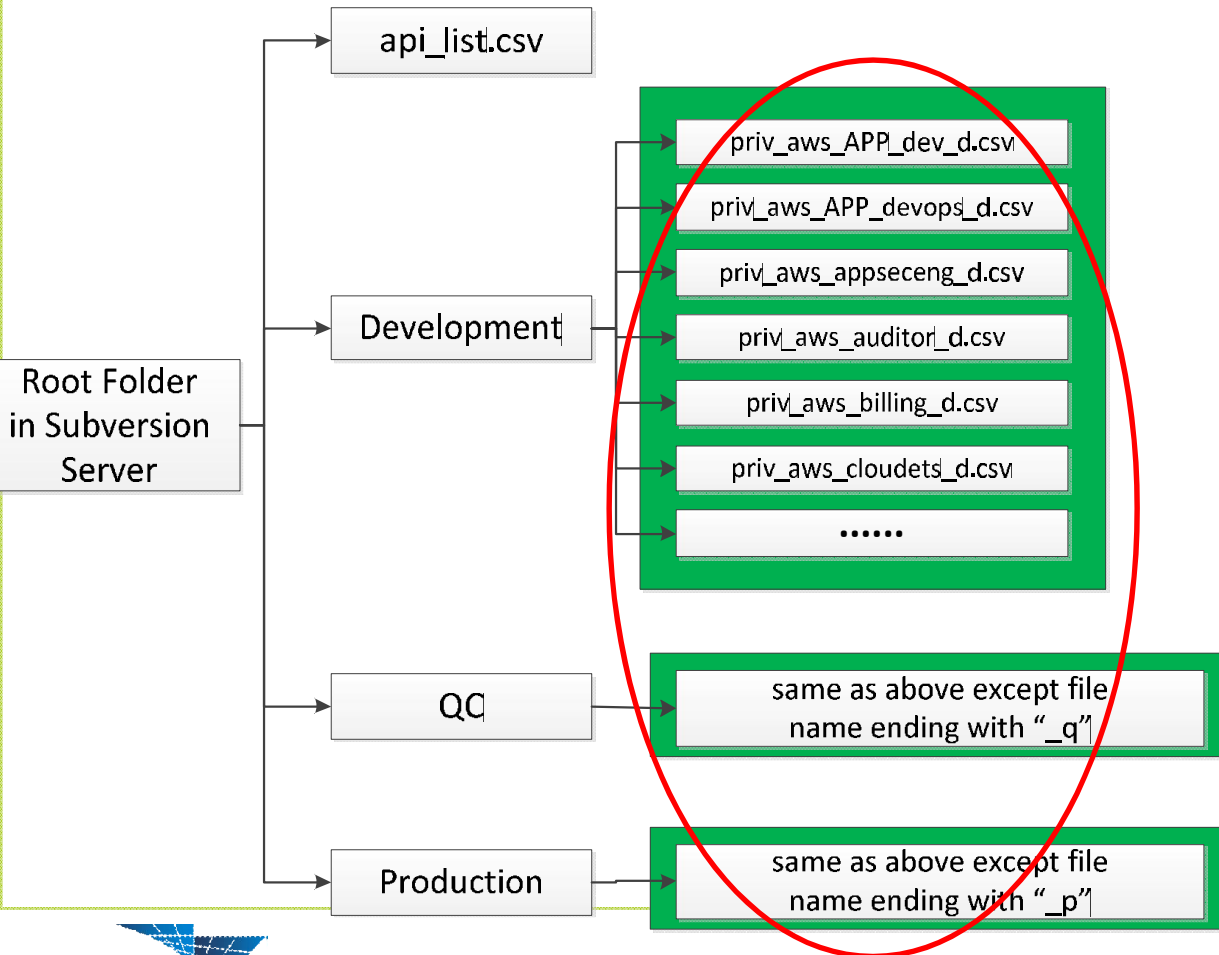
COMPONENTS – Gold Source

GoldSource Structure of AWS Compliance System

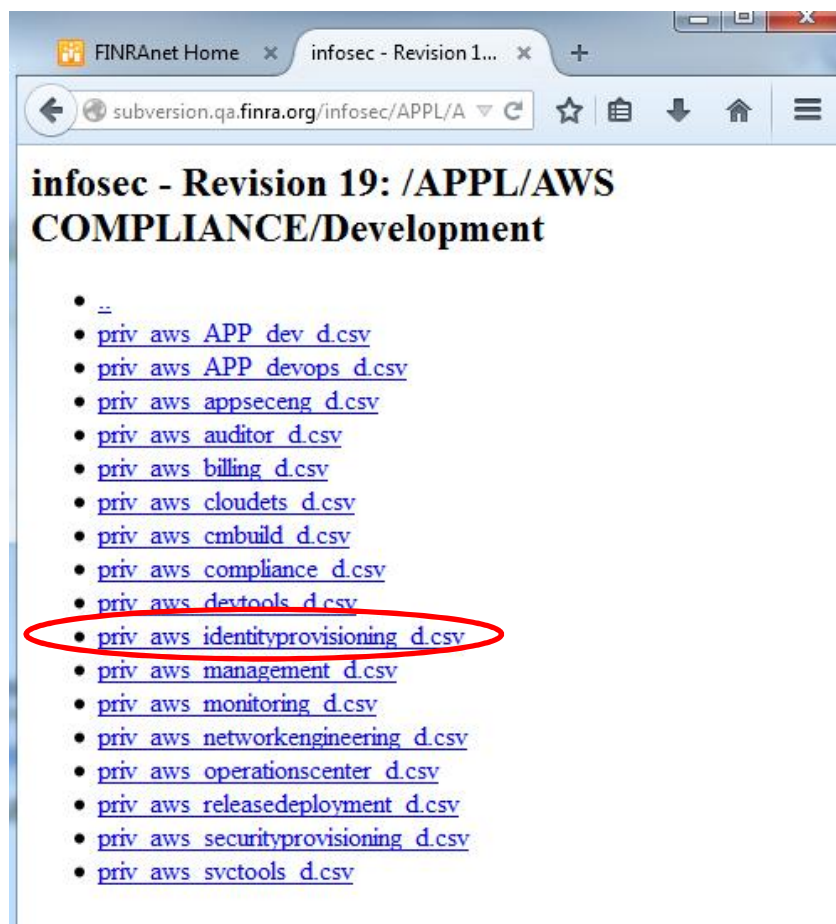


COMPONENTS – Gold Source

GoldSource Structure of AWS Compliance System



COMPONENTS – Gold Source

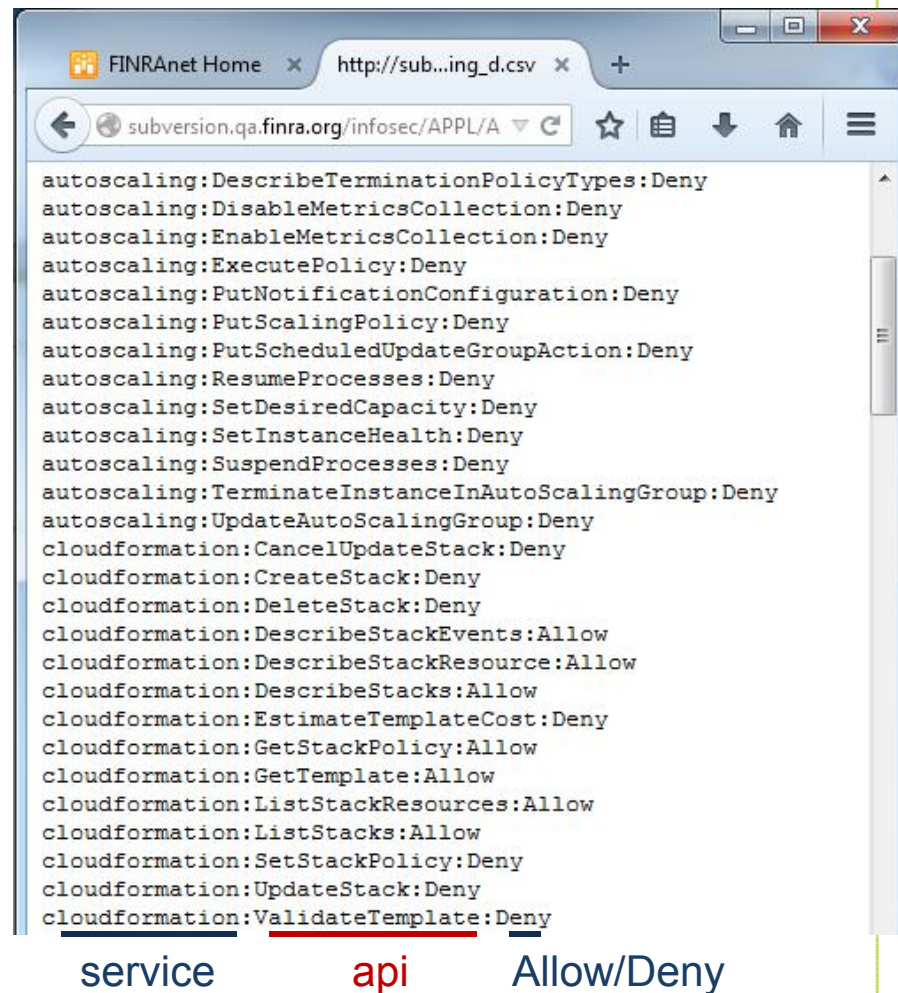


FINRAnet Home x infosec - Revision 1... x +

subversion.qa.finra.org/infosec/APPL/A

infosec - Revision 19: /APPL/AWS COMPLIANCE/Development

- ..
- [priv aws APP dev d.csv](#)
- [priv aws APP devops d.csv](#)
- [priv aws appseceng d.csv](#)
- [priv aws auditor d.csv](#)
- [priv aws billing d.csv](#)
- [priv aws cloudets d.csv](#)
- [priv aws cmbuild d.csv](#)
- [priv aws compliance d.csv](#)
- [priv aws dextools d.csv](#)
- [priv aws identityprovisioning d.csv](#)
- [priv aws management d.csv](#)
- [priv aws monitoring d.csv](#)
- [priv aws networkengineering d.csv](#)
- [priv aws operationscenter d.csv](#)
- [priv aws releasedeployment d.csv](#)
- [priv aws securityprovisioning d.csv](#)
- [priv aws svctools d.csv](#)



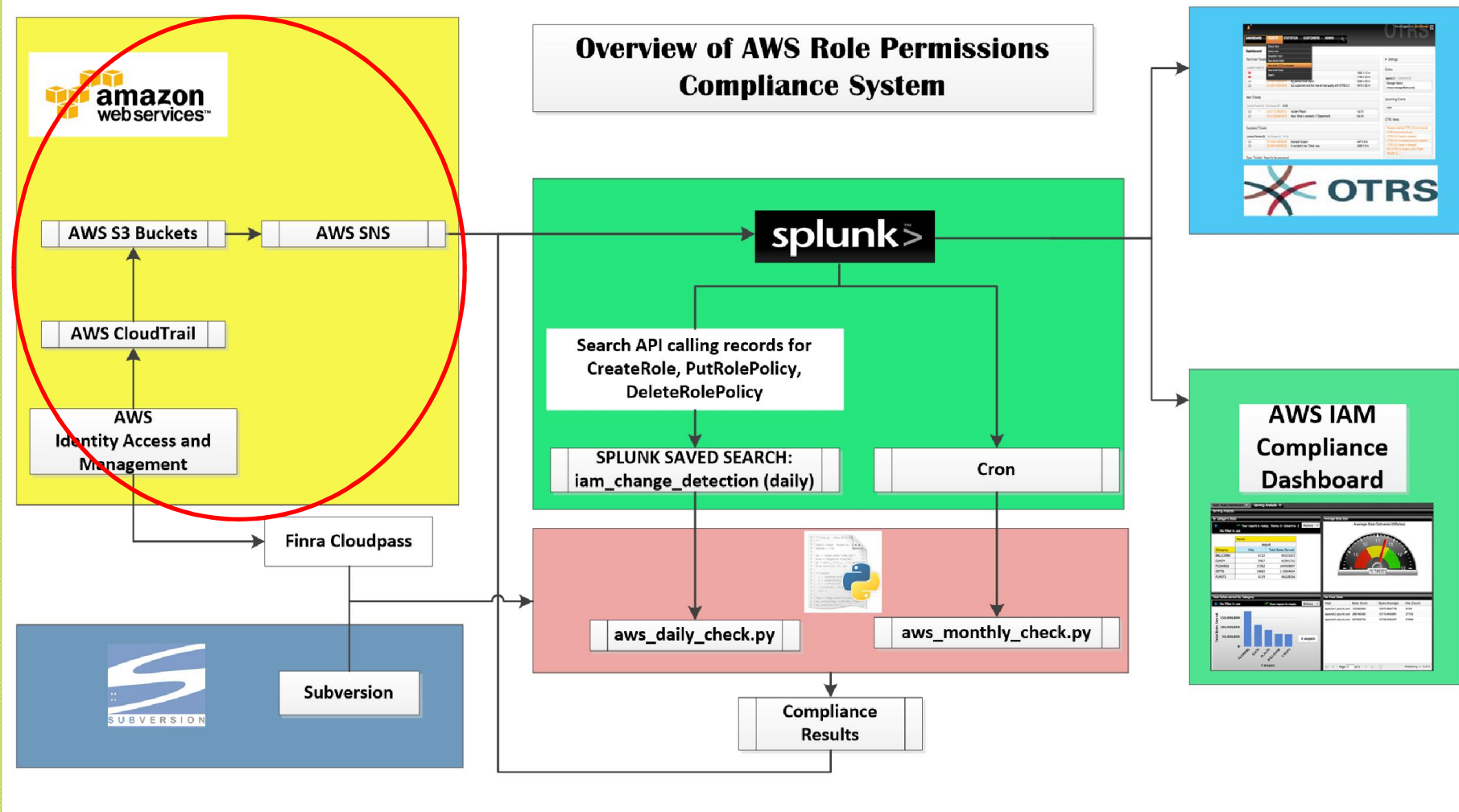
FINRAnet Home x http://sub...ing_d.csv x +

subversion.qa.finra.org/infosec/APPL/A


```
autoscaling:DescribeTerminationPolicyTypes:Deny
autoscaling:DisableMetricsCollection:Deny
autoscaling:EnableMetricsCollection:Deny
autoscaling:ExecutePolicy:Deny
autoscaling:PutNotificationConfiguration:Deny
autoscaling:PutScalingPolicy:Deny
autoscaling:PutScheduledUpdateGroupAction:Deny
autoscaling:ResumeProcesses:Deny
autoscaling:SetDesiredCapacity:Deny
autoscaling:SetInstanceHealth:Deny
autoscaling:SuspendProcesses:Deny
autoscaling:TerminateInstanceInAutoScalingGroup:Deny
autoscaling:UpdateAutoScalingGroup:Deny
cloudformation:CancelUpdateStack:Deny
cloudformation:CreateStack:Deny
cloudformation>DeleteStack:Deny
cloudformation:DescribeStackEvents:Allow
cloudformation:DescribeStackResource:Allow
cloudformation:DescribeStacks:Allow
cloudformation:EstimateTemplateCost:Deny
cloudformation:GetStackPolicy:Allow
cloudformation:GetTemplate:Allow
cloudformation>ListStackResources:Allow
cloudformation>ListStacks:Allow
cloudformation:SetStackPolicy:Deny
cloudformation:UpdateStack:Deny
cloudformation:ValidateTemplate:Deny
```

service api Allow/Deny

COMPONENTS – Amazon Web Services







COMPONENTS – Amazon Web Services





 **Services** ▾ **Edit** ▾ priv_aws_compliance_d/K242... ▾ Oregon ▾ Help ▾

Amazon Web Services





Compute & Networking

-  **Direct Connect**
Dedicated Network Connection to AWS
-  **EC2**
Virtual Servers in the Cloud
-  **Route 53**
Scalable Domain Name System
-  **VPC**
Isolated Cloud Resources








Storage & Content Delivery

-  **CloudFront**
Global Content Delivery Network
-  **Glacier**
Archive Storage in the Cloud
-  **S3**
Scalable Storage in the Cloud
-  **Storage Gateway**
Integrates On-Premises IT Environments with Cloud Storage




Database

-  **DynamoDB**
Predictable and Scalable NoSQL Data Store
-  **ElastiCache**
In-Memory Cache
-  **RDS**
Managed Relational Database Service
-  **Redshift**
Managed Petabyte-Scale Data Warehouse Service




Deployment & Management

-  **CloudFormation**
Templated AWS Resource Creation
-  **CloudTrail**
User Activity and Change Tracking
-  **CloudWatch**
Resource and Application Monitoring
-  **Elastic Beanstalk**
AWS Application Platform
-  **IAM**
Secure AWS Access Control
-  **OpsWorks**
DevOps Application Management Service
-  **Trusted Advisor**
AWS Cloud Optimization Expert







Analytics

-  **Data Pipeline**
Orchestration for Data-Driven Workflows
-  **Elastic MapReduce**
Managed Hadoop Framework
-  **Kinesis**
Real-time Processing of Streaming Big Data



Mobile Services

-  **Cognito**
User Identity and App Data Synchronization
-  **Mobile Analytics**
Understand App Usage Data at Scale
-  **SNS**
Push Notification Service

App Services

-  **AppStream**
Low Latency Application Streaming
-  **CloudSearch**
Managed Search Service
-  **Elastic Transcoder**
Easy-to-use Scalable Media Transcoding
-  **SES**
Email Sending Service
-  **SQS**
Message Queue Service
-  **SWF**
Workflow Service for Coordinating Application Components

Applications

-  **WorkSpaces**
Desktops in the Cloud
-  **Zocalo**
Secure Enterprise Storage and Sharing Service


Additional Resources

[Getting Started](#)
See our documentation to get started and learn more about how to use our services.

[AWS Console Mobile App](#)
View your resources on the go with our AWS Console mobile app, available from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

[AWS Marketplace](#)
Find and buy software, launch with 1-Click and pay by the hour.

Service Health

 All services operating normally.


Updated: Aug 05 2014 11:30:00 GMT-0400

[Service Health Dashboard](#)

Set Start Page





Console Home ▾

COMPONENTS – Amazon Web Services





 **Services** ▾ **Edit** ▾ priv_aws_compliance_d/K242... ▾ Oregon ▾ Help ▾

Amazon Web Services





Compute & Networking

-  **Direct Connect**
Dedicated Network Connection to AWS
-  **EC2**
Virtual Servers in the Cloud
-  **Route 53**
Scalable Domain Name System
-  **VPC**
Isolated Cloud Resources








Storage & Content Delivery

-  **CloudFront**
Global Content Delivery Network
-  **Glacier**
Archive Storage in the Cloud
-  **S3**
Scalable Storage in the Cloud
-  **Storage Gateway**
Integrates On-Premises IT Environments with Cloud Storage




Database

-  **DynamoDB**
Predictable and Scalable NoSQL Data Store
-  **ElastiCache**
In-Memory Cache
-  **RDS**
Managed Relational Database Service
-  **Redshift**
Managed Petabyte-Scale Data Warehouse Service




Deployment & Management

-  **CloudFormation**
Templated AWS Resource Creation
-  **CloudTrail**
User Activity and Change Tracking
-  **CloudWatch**
Resource and Application Monitoring
-  **Elastic Beanstalk**
AWS Application Deployment
-  **IAM**
Secure AWS Access Control
-  **OpsWorks**
DevOps Application Management Service
-  **Trusted Advisor**
AWS Cloud Optimization Expert







Analytics

-  **Data Pipeline**
Orchestration for Data-Driven Workflows
-  **Elastic MapReduce**
Managed Hadoop Framework
-  **Kinesis**
Real-time Processing of Streaming Big Data



Mobile Services

-  **Cognito**
User Identity and App Data Synchronization
-  **Mobile Analytics**
Understand App Usage Data at Scale
-  **SNS**
Push Notification Service

App Services

-  **AppStream**
Low Latency Application Streaming
-  **CloudSearch**
Managed Search Service
-  **Elastic Transcoder**
Easy-to-use Scalable Media Transcoding
-  **SES**
Email Sending Service
-  **SQS**
Message Queue Service
-  **SWF**
Workflow Service for Coordinating Application Components

Applications

-  **WorkSpaces**
Desktops in the Cloud
-  **Zocalo**
Secure Enterprise Storage and Sharing Service

Additional Resources

Getting Started

See our documentation to get started and learn more about how to use our services.


AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

Service Health

 All services operating normally.

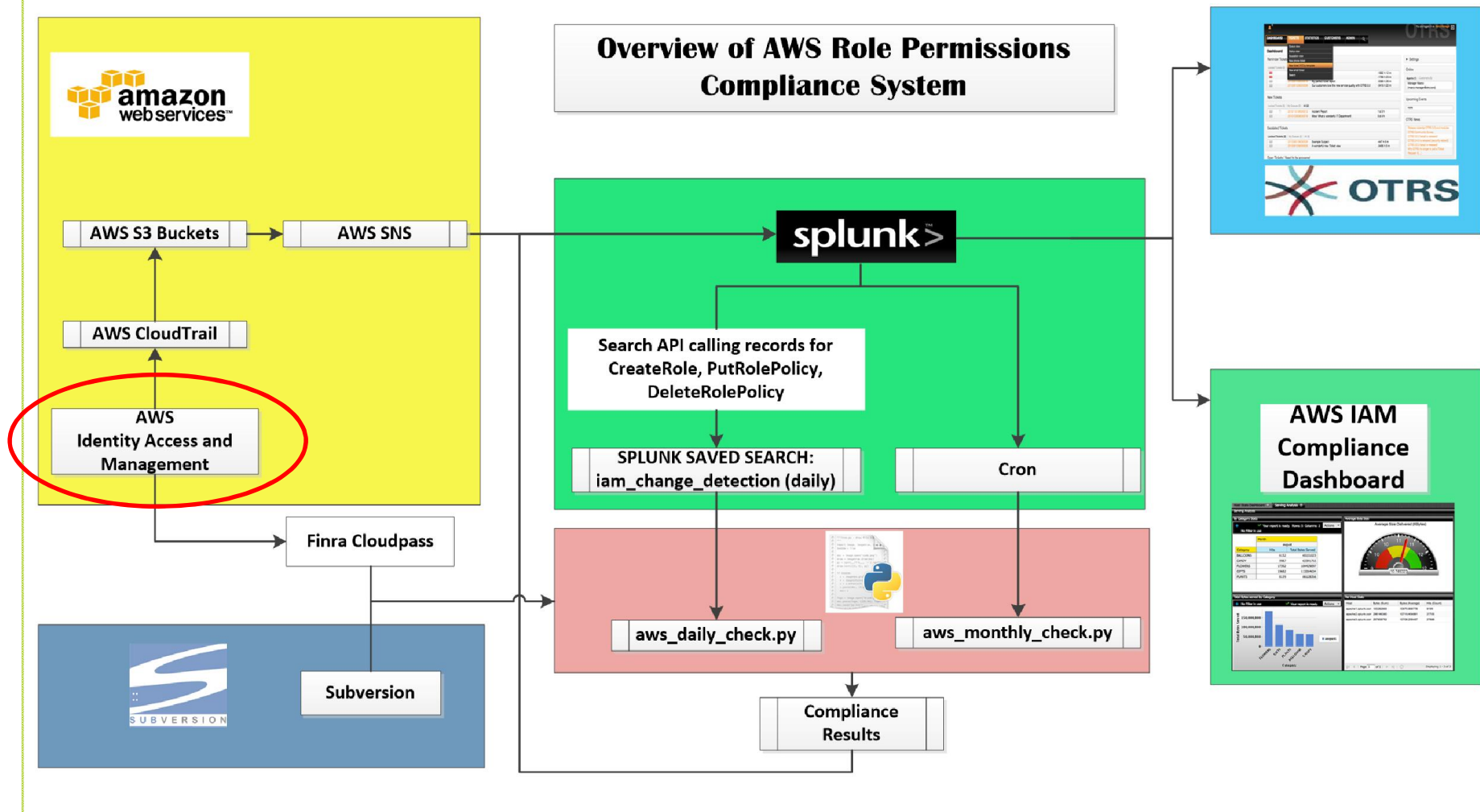
Updated: Aug 05 2014 11:30:00 GMT-0400

[Service Health Dashboard](#)


Set Start Page

Console Home ▾

COMPONENTS – Amazon Web Services







COMPONENTS – Amazon Web Services





**Services** ▾ **Edit** ▾ priv_aws_compliance_d/K242... ▾ Oregon ▾ Help ▾

Amazon Web Services





Compute & Networking

-  **Direct Connect**
Dedicated Network Connection to AWS
-  **EC2**
Virtual Servers in the Cloud
-  **Route 53**
Scalable Domain Name System
-  **VPC**
Isolated Cloud Resources








Storage & Content Delivery

-  **CloudFront**
Global Content Delivery Network
-  **Glacier**
Archive Storage in the Cloud
-  **S3**
Scalable Storage in the Cloud
-  **Storage Gateway**
Integrates On-Premises IT Environments with Cloud Storage




Database

-  **DynamoDB**
Predictable and Scalable NoSQL Data Store
-  **ElastiCache**
In-Memory Cache
-  **RDS**
Managed Relational Database Service
-  **Redshift**
Managed Petabyte-Scale Data Warehouse Service




Deployment & Management

-  **CloudFormation**
Templated AWS Resource Creation
-  **CloudTrail**
User Activity and Change Tracking
-  **CloudWatch**
Resource and Application Monitoring
-  **Elastic Beanstalk**
AWS Application Container
-  **IAM**
Secure AWS Access Control
-  **OpsWorks**
DevOps Application Management Service
-  **Trusted Advisor**
AWS Cloud Optimization Expert







Analytics

-  **Data Pipeline**
Orchestration for Data-Driven Workflows
-  **Elastic MapReduce**
Managed Hadoop Framework
-  **Kinesis**
Real-time Processing of Streaming Big Data



Mobile Services

-  **Cognito**
User Identity and App Data Synchronization
-  **Mobile Analytics**
Understand App Usage Data at Scale
-  **SNS**
Push Notification Service

App Services

-  **AppStream**
Low Latency Application Streaming
-  **CloudSearch**
Managed Search Service
-  **Elastic Transcoder**
Easy-to-use Scalable Media Transcoding
-  **SES**
Email Sending Service
-  **SQS**
Message Queue Service
-  **SWF**
Workflow Service for Coordinating Application Components

Applications

-  **WorkSpaces**
Desktops in the Cloud
-  **Zocalo**
Secure Enterprise Storage and Sharing Service


Additional Resources

[Getting Started](#)
See our documentation to get started and learn more about how to use our services.

[AWS Console Mobile App](#)
View your resources on the go with our AWS Console mobile app, available from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

[AWS Marketplace](#)
Find and buy software, launch with 1-Click and pay by the hour.

Service Health

 All services operating normally.

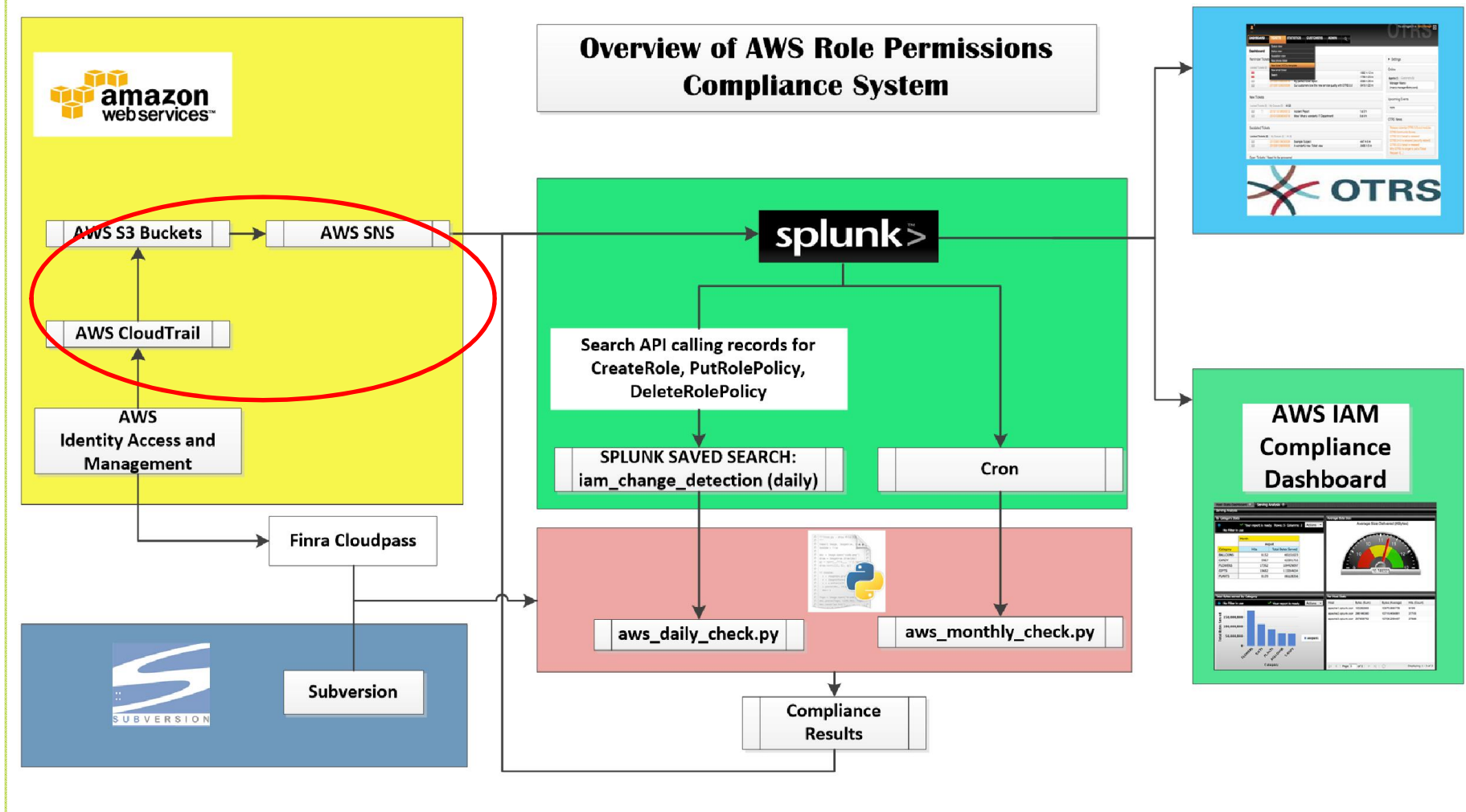
Updated: Aug 05 2014 11:30:00 GMT-0400

[Service Health Dashboard](#)

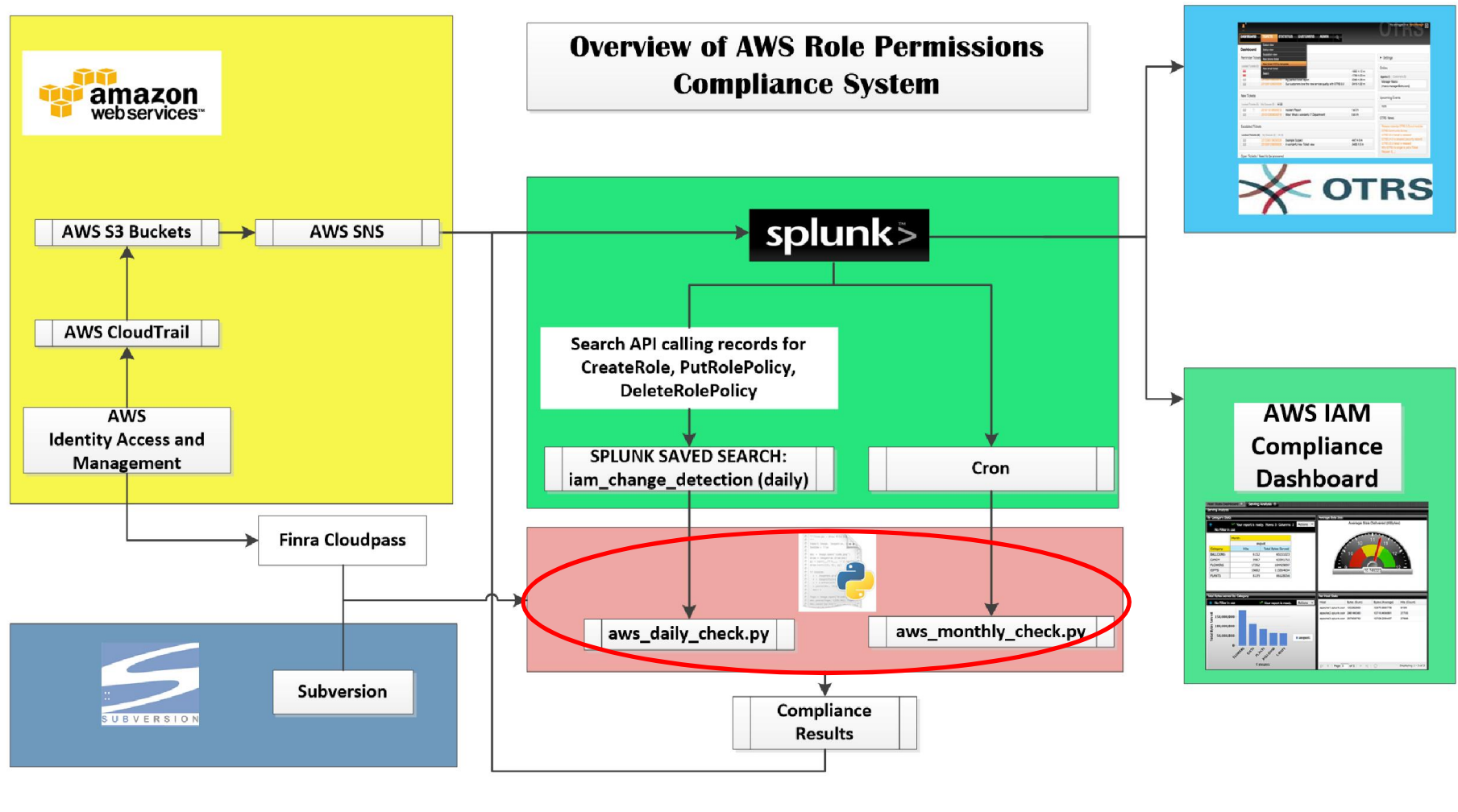
Set Start Page

Console Home ▾

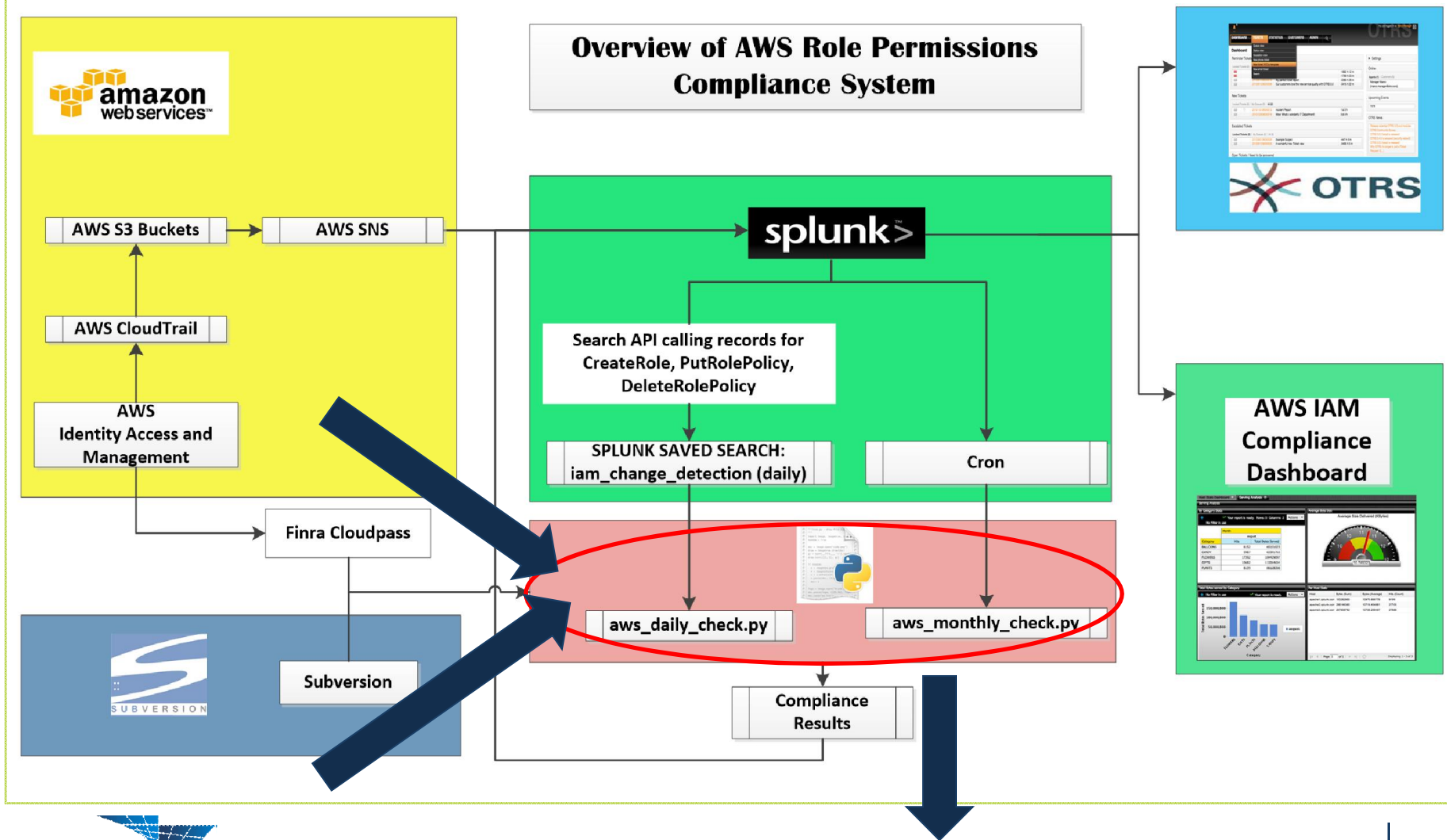
COMPONENTS – Amazon Web Services



COMPONENTS – Python Scripts



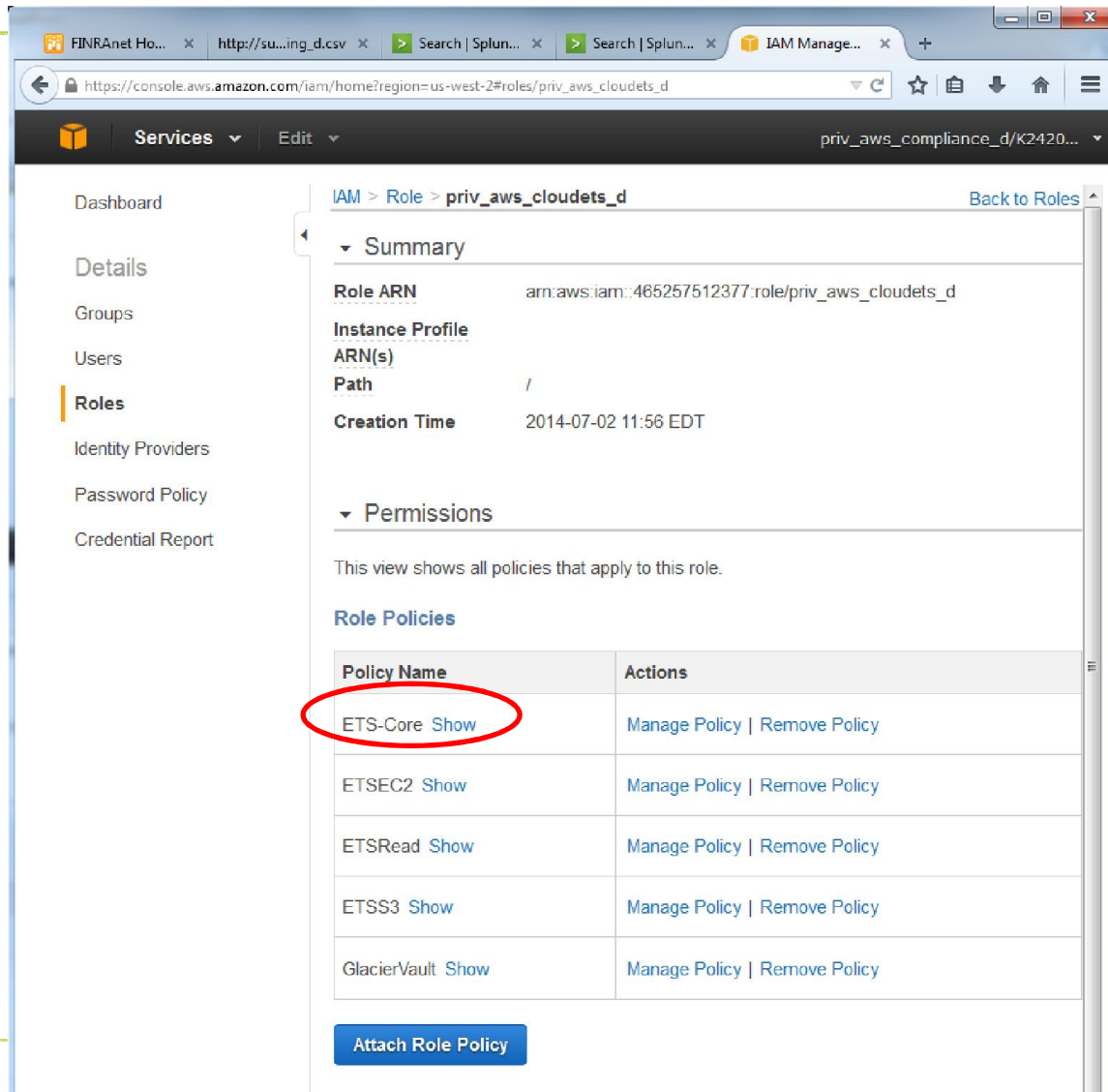
COMPONENTS – Python Scripts



COMPONENTS – Python Scripts

- A simple example:
 - Environment: Development
 - Role name: priv_aws_cloudets_d
 - Service: sqs
 - API: RemovePermission

COMPONENTS – Python Scripts



The screenshot shows the AWS IAM console interface. The breadcrumb navigation indicates the path: IAM > Role > priv_aws_cloudets_d. The left sidebar contains navigation links for Dashboard, Details, Groups, Users, Roles (highlighted), Identity Providers, Password Policy, and Credential Report. The main content area displays the 'Summary' and 'Permissions' for the role. The 'Role Policies' table lists several policies, with 'ETS-Core' circled in red.

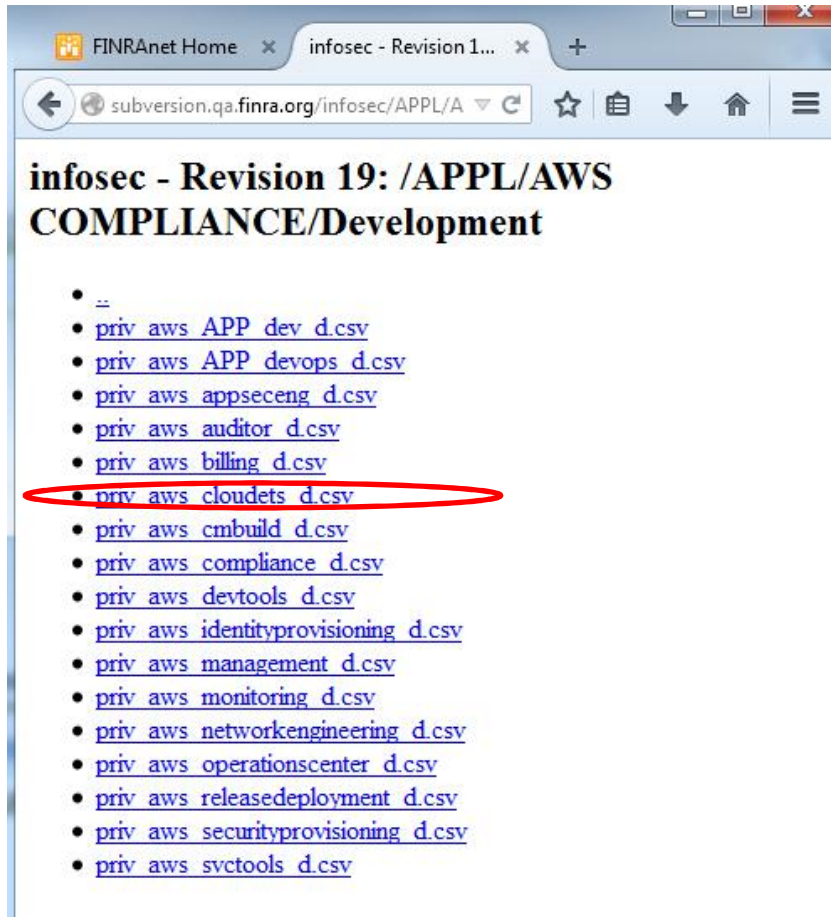
Policy Name	Actions
ETS-Core Show	Manage Policy Remove Policy
ETSEC2 Show	Manage Policy Remove Policy
ETSRead Show	Manage Policy Remove Policy
ETSS3 Show	Manage Policy Remove Policy
GlacierVault Show	Manage Policy Remove Policy

[Attach Role Policy](#)

Part of policies in ETS-Core:

```
    "Statement": [
      {
        "Sid": "StmETS4000",
        "Effect": "Allow",
        "Action": [
          "sns:AddPermission",
          "sns:ConfirmSubscription",
          "sns:GetTopicAttributes",
          "sns:ListSubscriptions",
          "sns:ListSubscriptionsByTopic",
          "sns:ListTopics",
          "sns:Publish",
          "sns:RemovePermission",
          "sns:SetTopicAttributes",
          "sns:Subscribe",
          "sns:Unsubscribe"
        ],
        "Resource": [
          "*"
        ]
      }
    ]
  }
```

COMPONENTS – Python Scripts

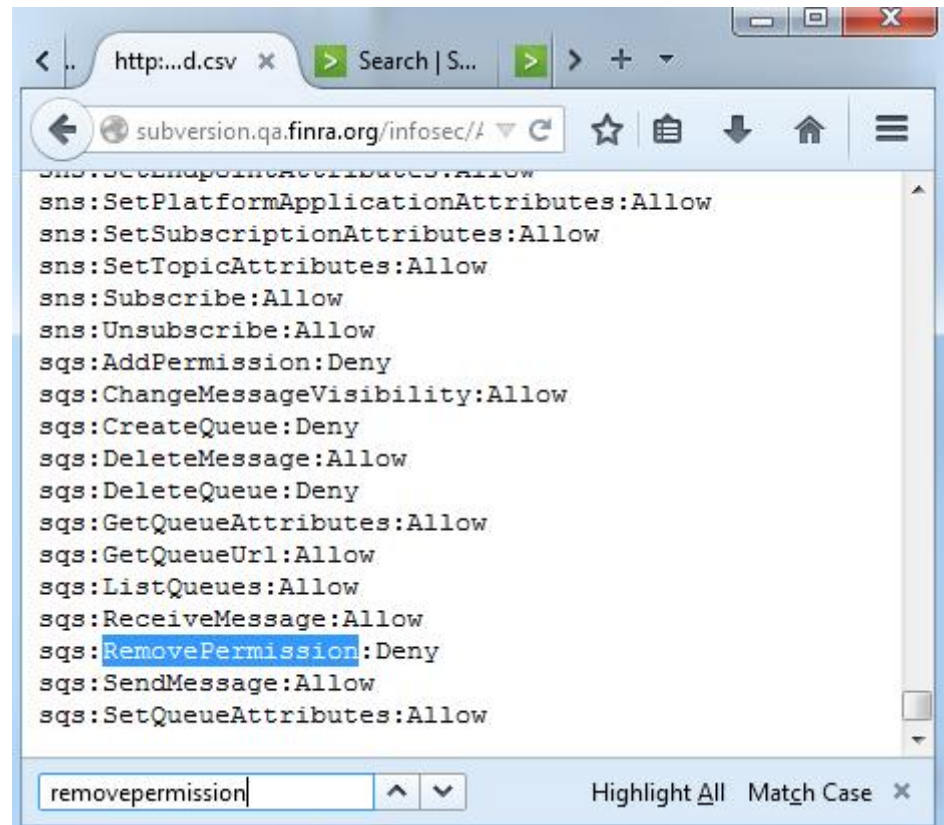


FINRAnet Home x infosec - Revision 1... x +

subversion.qa.finra.org/infosec/APPL/A

infosec - Revision 19: /APPL/AWS COMPLIANCE/Development

- ..
- [priv aws APP dev d.csv](#)
- [priv aws APP devops d.csv](#)
- [priv aws appseceng d.csv](#)
- [priv aws auditor d.csv](#)
- [priv aws billing d.csv](#)
- [priv aws cloudets d.csv](#)
- [priv aws cmbuild d.csv](#)
- [priv aws compliance d.csv](#)
- [priv aws devtools d.csv](#)
- [priv aws identityprovisioning d.csv](#)
- [priv aws management d.csv](#)
- [priv aws monitoring d.csv](#)
- [priv aws networkengineering d.csv](#)
- [priv aws operationscenter d.csv](#)
- [priv aws releasedeployment d.csv](#)
- [priv aws securityprovisioning d.csv](#)
- [priv aws svctools d.csv](#)



http...d.csv x Search | S... x +

subversion.qa.finra.org/infosec/A

```
sns:SetPlatformApplicationAttributes:Allow
sns:SetSubscriptionAttributes:Allow
sns:SetTopicAttributes:Allow
sns:Subscribe:Allow
sns:Unsubscribe:Allow
sqs:AddPermission:Deny
sqs:ChangeMessageVisibility:Allow
sqs:CreateQueue:Deny
sqs>DeleteMessage:Allow
sqs>DeleteQueue:Deny
sqs:GetQueueAttributes:Allow
sqs:GetQueueUrl:Allow
sqs:ListQueues:Allow
sqs:ReceiveMessage:Allow
sqs:RemovePermission:Deny
sqs:SendMessage:Allow
sqs:SetQueueAttributes:Allow
```

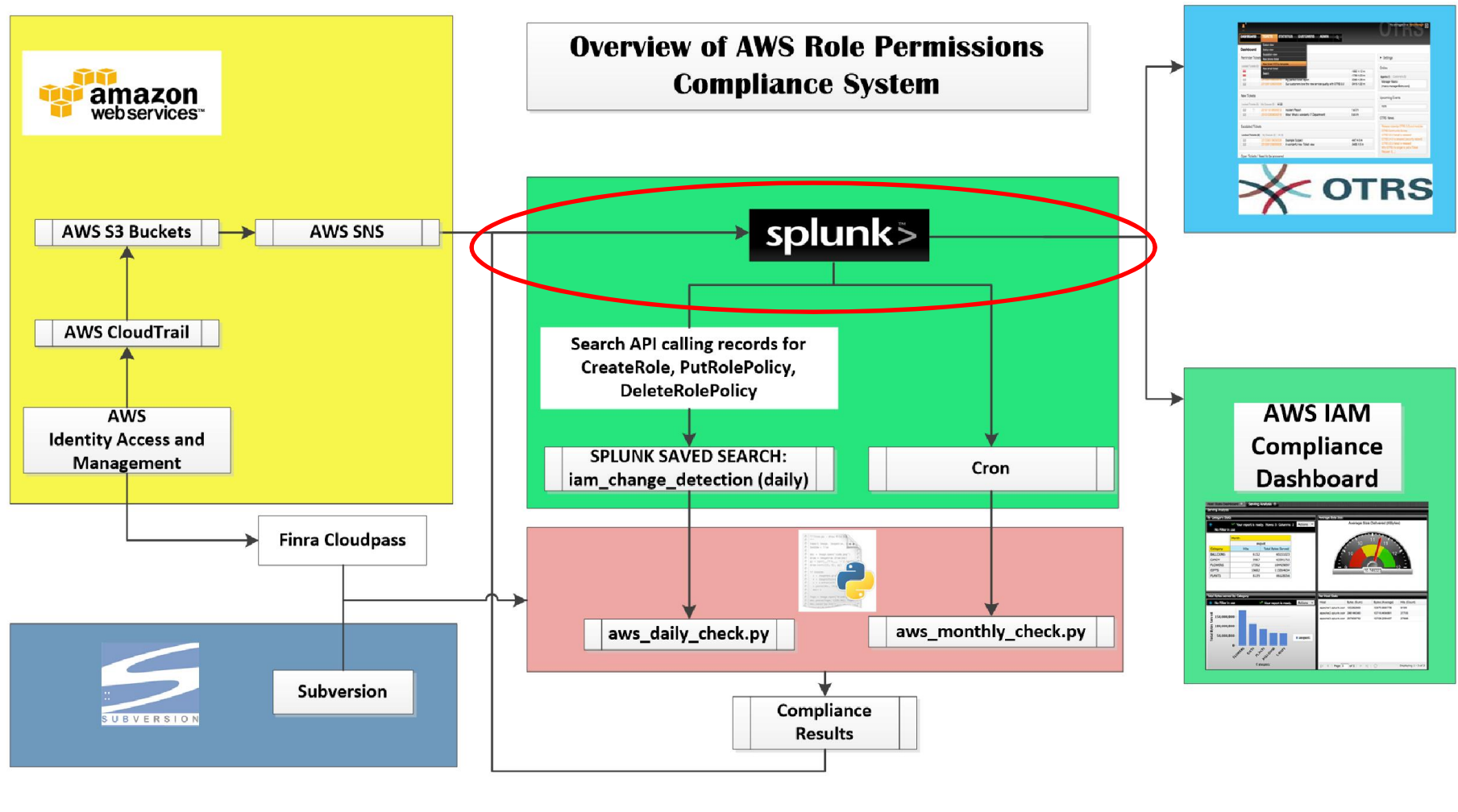
removepermission ^ v Highlight All Match Case x

COMPONENTS – Python Scripts

The screenshot displays the Splunk Search & Reporting interface. The search bar contains the query: `index=compliance sourcetype=aws-compliance Environment=Development Status=NonCompliant Observed=allow`. The results show 1,619 events from 7/30/14 12:00:00.000 AM to 8/6/14 12:03:19.000 AM. The interface is set to 'List' view with 20 items per page. The first three events are visible, each with a detailed event log. The first event, at 8/4/14 2:31:28.358 PM, shows an API call to `RemovePermission` for the role `priv_aws_cloudets_d` on the `sqs` service. The second event, at 8/4/14 2:31:28.357 PM, shows an API call to `AddPermission` for the same role and service. The third event, at 8/4/14 2:31:28.294 PM, shows an API call to `ListSigningCertificates` for the role `priv_aws_cloudets_d` on the `iam` service. The left sidebar shows the 'Selected Fields' list, including `AccountID`, `API`, `AWS_ROLENAME`, `Category`, `CloudProvider`, `Environment`, `GoldSource`, `index`, `Observed`, `PolicyName`, `RoleName`, `Service`, `Severity`, `sourcetype`, and `Status`.

i	Time	Event
>	8/4/14 2:31:28.358 PM	[Time: 2014-08-04 14:31:28.358596 CloudProvider:AWS Category:IAM AWS_accountID:465257512377 Environment:Development Role_Name:priv_aws_cloudets_d API:RemovePermission Service:sqs GoldSource:explicitly deny Observed:allow Status:NonCompliant PolicyName:ETS-Core Severity:Low API = RemovePermission AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETS-Core RoleName = priv_aws_cloudets_d Service = sqs Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance
>	8/4/14 2:31:28.357 PM	[Time: 2014-08-04 14:31:28.357911 CloudProvider:AWS Category:IAM AWS_accountID:465257512377 Environment:Development Role_Name:priv_aws_cloudets_d API:AddPermission Service:sqs GoldSource:explicitly deny Observed:allow Status:NonCompliant PolicyName:ETS-Core Severity:Low API = AddPermission AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETS-Core RoleName = priv_aws_cloudets_d Service = sqs Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance
>	8/4/14 2:31:28.294 PM	[Time: 2014-08-04 14:31:28.294656 CloudProvider:AWS Category:IAM AWS_accountID:465257512377 Environment:Development Role_Name:priv_aws_cloudets_d API:ListSigningCertificates Service:iam GoldSource:explicitly deny Observed:allow Status:NonCompliant PolicyName:ETSRead Severity:Low API = ListSigningCertificates AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETSRead RoleName = priv_aws_cloudets_d Service = iam Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance

COMPONENTS – Splunk



COMPONENTS – Python Scripts

The screenshot displays the Splunk Search & Reporting interface. The search bar contains the query: `index=compliance sourcetype=aws-compliance Environment=Development Status=NonCompliant Observed=allow`. The results show 1,619 events from 7/30/14 12:00:00.000 AM to 8/6/14 12:03:19.000 AM. The interface includes tabs for Events (1,619), Statistics, and Visualization. A table of results is shown with columns for Time and Event. A sidebar on the left lists fields, with a red box highlighting the 'Selected Fields' section.

Selected Fields

- # AccountID 1
- a API 15
- a AWS_ROLENAME 14
- a Category 1
- a CloudProvider 1
- a Environment 1
- a GoldSource 1
- a index 1
- a Observed 1
- a PolicyName 13
- a RoleName 14
- a Service 5
- a Severity 1
- a sourcetype 1
- a Status 1

Interesting Fields

i	Time	Event
>	8/4/14 2:31:28.358 PM	[Time: 2014-08-04 14:31:28.358596 CloudProvider: AWS Category: IAM AWS_accountID: 465257512377 Environment: Development Role_Name: priv_aws_cloudets_d API: RemovePermission Service: sqs GoldSource: explicitly deny Observed: allow Status: NonCompliant PolicyName: ETS-Core Severity: Low API = RemovePermission AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETS-Core RoleName = priv_aws_cloudets_d Service = sqs Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance
>	8/4/14 2:31:28.357 PM	[Time: 2014-08-04 14:31:28.357911 CloudProvider: AWS Category: IAM AWS_accountID: 465257512377 Environment: Development Role_Name: priv_aws_cloudets_d API: AddPermission Service: sqs GoldSource: explicitly deny Observed: allow Status: NonCompliant PolicyName: ETS-Core Severity: Low API = AddPermission AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETS-Core RoleName = priv_aws_cloudets_d Service = sqs Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance
>	8/4/14 2:31:28.294 PM	[Time: 2014-08-04 14:31:28.294656 CloudProvider: AWS Category: IAM AWS_accountID: 465257512377 Environment: Development Role_Name: priv_aws_cloudets_d API: ListSigningCertificates Service: iam GoldSource: explicitly deny Observed: allow Status: NonCompliant PolicyName: ETSRead Severity: Low API = ListSigningCertificates AWS_ROLENAME = cloudets_d AccountID = 465257512377 Category = IAM CloudProvider = AWS Environment = Development GoldSource = explicitly deny Observed = allow PolicyName = ETSRead RoleName = priv_aws_cloudets_d Service = iam Severity = Low Status = NonCompliant index = compliance sourcetype = aws-compliance

COMPONENTS – Splunk

■ Severity of Incidents

➤ Factor I : Environment (Development, QC, Production)

- ❖ e.g. : The noncompliance in Production is more severe than in Development

➤ Factor II : Noncompliant incident type (Type I, Type II)

- ❖ Type I : A role has been granted access to an API for which it should not have access
- ❖ Type II : A role has not been granted access to an API for which it should have access
- ❖ Severity of Type I noncompliance is higher than Type II noncompliance

➤ Factor III : API capabilities

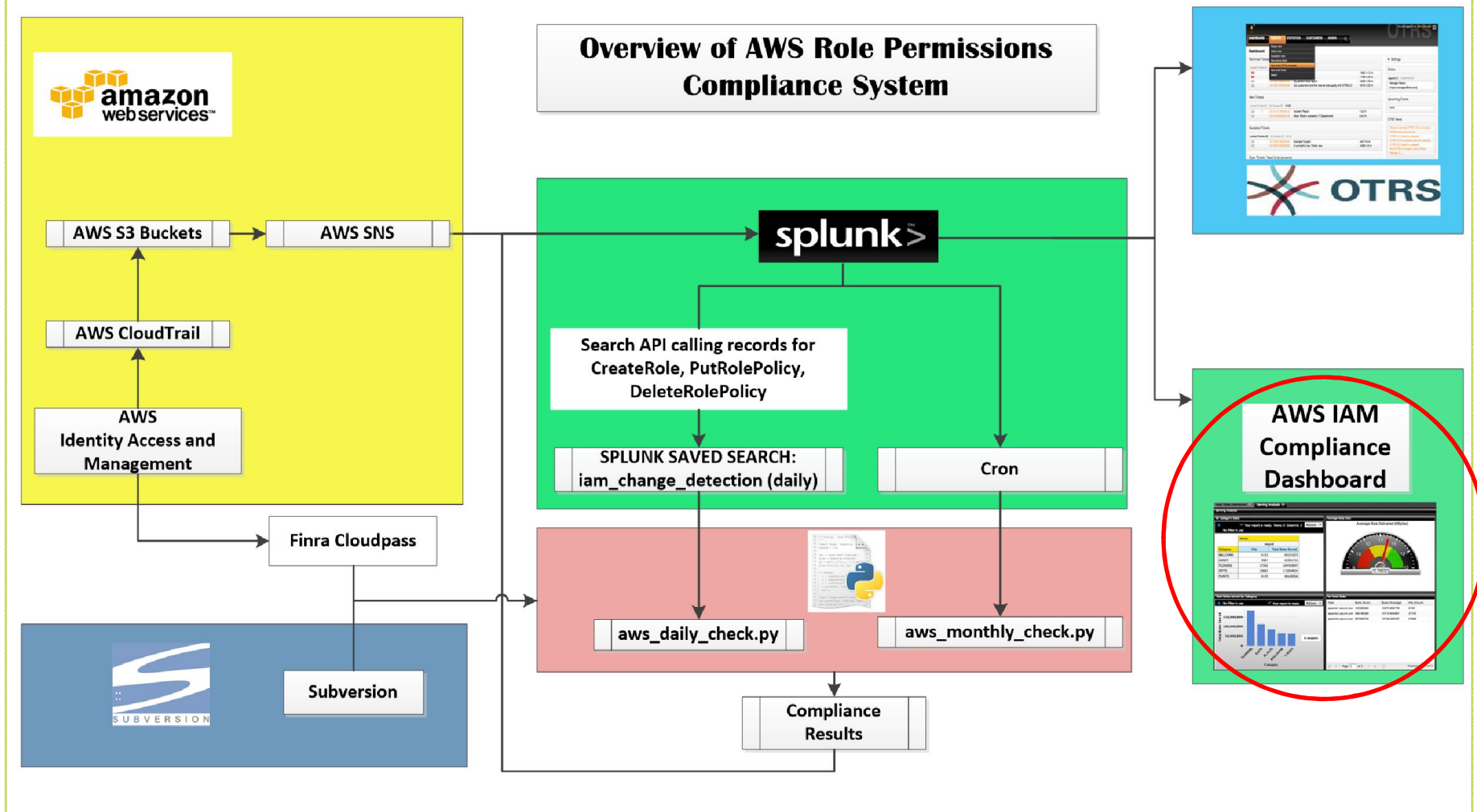
- ❖ e.g. : S3:ListBucket, S3>CreateBucket
Severity of S3:ListBucket noncompliance is higher than S3>CreateBucket

COMPONENTS – Splunk

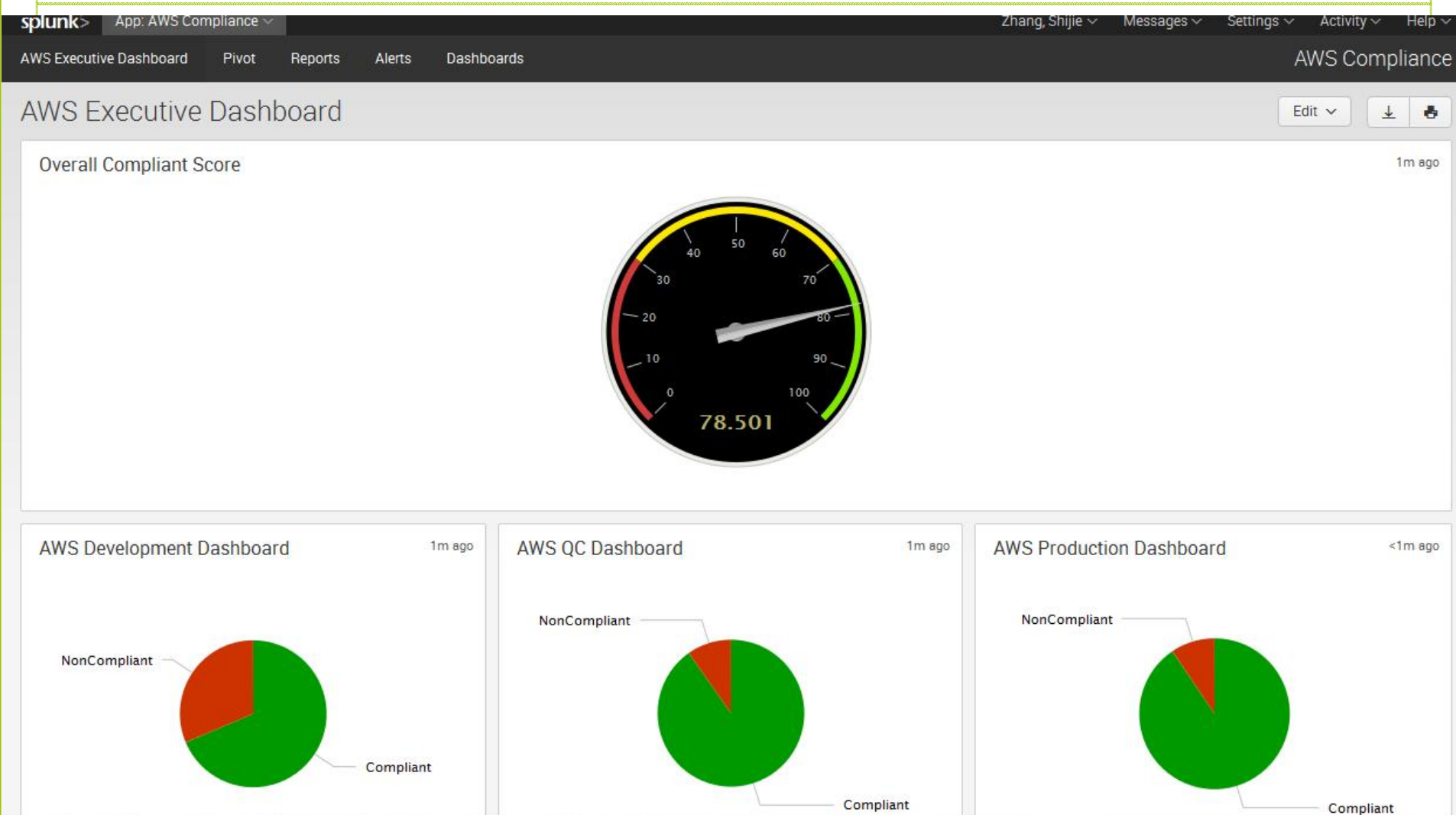
- Initial Rating Scale

SCALE	
HIGH	> 30
MEDIUM	26 to 30
LOW	0 to 26

COMPONENTS – Dashboard



COMPONENTS – Dashboard



AGENDA

■ How It Works

■ System Components

- Gold Source
- Amazon Web Services
- Developed Scripts
- Splunk
- AWS Compliance Dashboard

■ Demo

■ Summary

Summary

- **Accomplishments:**

 - Build an AWS Role Permission Compliance System**

- **Thanks to my boss, teammates and many other co-workers**

- **Questions and Comments?**