DevSecCon

SCOUTSUITE

Scout Suite – A Multi-Cloud Security Auditing Tool Workshop

Xavier Garceau-Aranda
Senior Security Consultant, NCC Group

London | 14-15 November 2019

Introduction

Scout Suite (https://github.com/nccgroup/ScoutSuite) is an open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments:

- Using the APIs exposed by cloud providers, Scout Suite gathers configuration data for manual inspection and highlights risk areas.
- Rather than going through dozens of pages on the web consoles, Scout Suite presents a clear view of the attack surface automatically.

The following cloud providers are currently supported:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Alibaba Cloud (alpha)
- Oracle Cloud Infrastructure (alpha)

Project Details

- Formally known as Scout2 (https://github.com/nccgroup/Scout2)
  - Most of the tool has since been refactored to handle the multi-cloud paradigm elegantly.
- Released under the GNU General Public License v2.0
- Has received contributions from over 24 developers
- Additional details can be found at https://github.com/nccgroup/ScoutSuite/wiki

The Multi-Cloud Paradigm

With the steady rise of cloud adoption, many organizations find themselves splitting their resources between multiple cloud providers.

The main reasons for this are:

- Cost
- Familiarity
- Offering
- Resilience

While the readiness to deal with security in cloud environments has been improving, the multi-cloud paradigm poses new challenges.

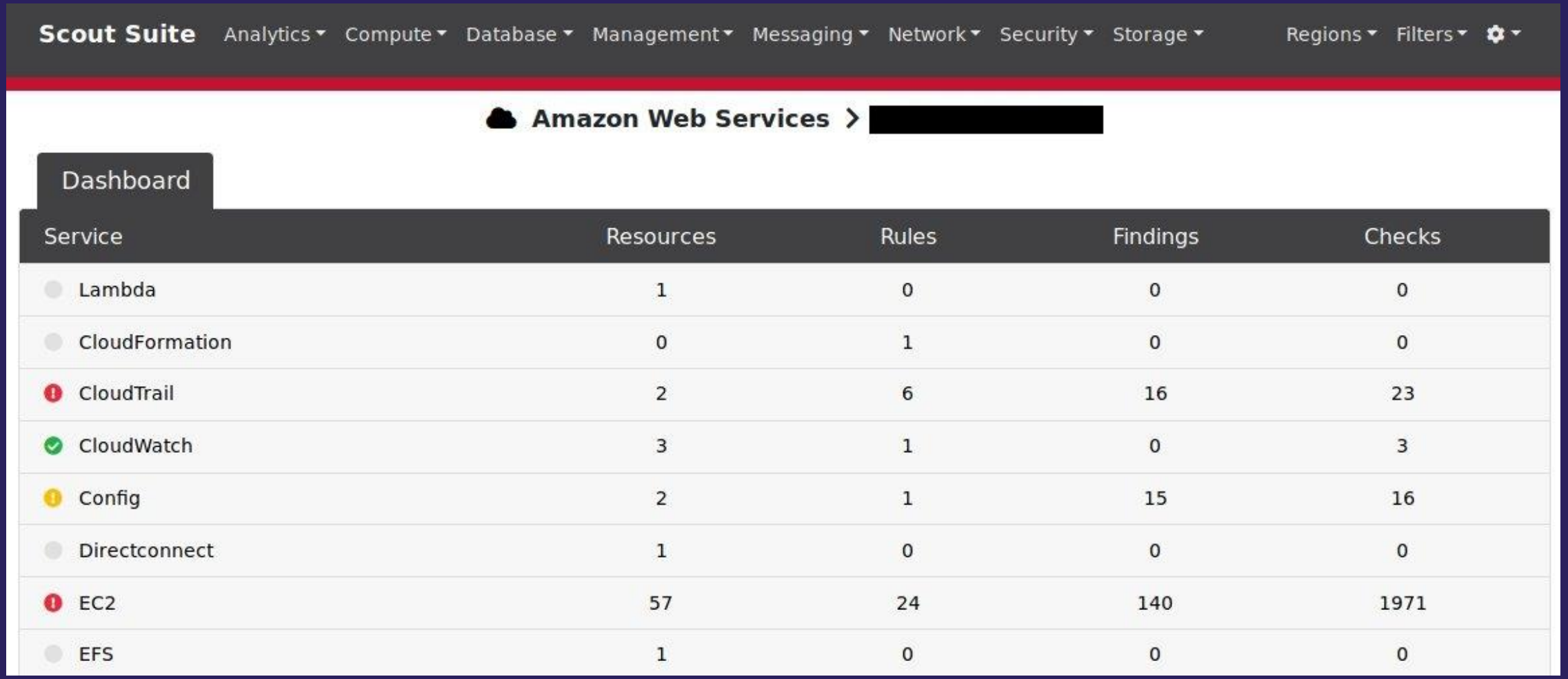
Cloud Provider Similarities – Offering

- “Everything” as a Service: IaaS, PaaS, SaaS, CaaS, FaaS, …
- Regions, Virtual Private Clouds (VPCs), Resources
- Identity and Access Management
  - Users, Groups
  - Programmatic identities (Roles/Service Principals/Service Accounts)
  - Policies, Permissions

Cloud Provider Similarities – Risks

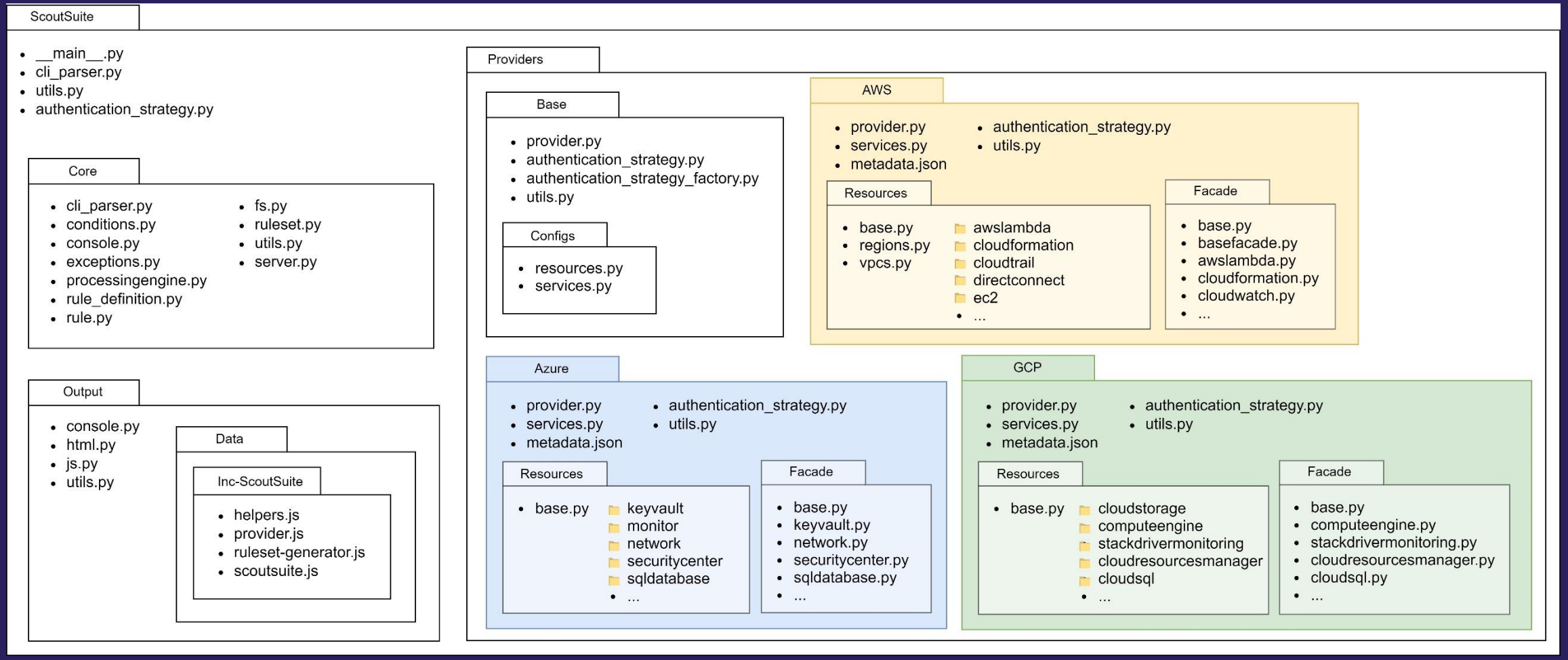
- Access Controls
  - Credential Leaks & Privilege Escalation
- Publically Accessible Resources
  - Virtual Machines, Databases, Storage Buckets, etc.
- Development practices
- Incident Response & Disaster Recovery

Scout Suite – Demo



Service	Resources	Rules	Findings	Checks
Lambda	1	0	0	0
CloudFormation	0	1	0	0
CloudTrail	2	6	16	23
CloudWatch	3	1	0	3
Config	2	1	15	16
Directconnect	1	0	0	0
EC2	57	24	140	1971
EFS	1	0	0	0

Scout Suite – Architecture



Scout Suite – Provider Support

- Amazon Web Services
  - 25 services & >130 rules
- Microsoft Azure
  - 6 services & ~30 rules
- Google Cloud Platform
  - 7 services & ~30 rules
- Alibaba Cloud
  - 6 services & ~20 rules
- Oracle Cloud Infrastructure
  - 3 services & ~10 rules

Scout Suite – Advanced Features

- Findings & Rulesets
  - https://github.com/nccgroup/ScoutSuite/wiki/HowTo:-Use-with-a-custom-ruleset
- Exceptions
  - https://github.com/nccgroup/ScoutSuite/wiki/HowTo:-Create-and-use-a-list-of-exceptions
- Exporting Results
  - https://github.com/nccgroup/ScoutSuite/wiki/HowTo:-Exporting-and-Programmatically-Access-of-Scout-Suite-Data

DevSecCon

SCOUTSUITE

Workshop Time!

Download slides from https://bit.ly/34Zpqnk

Download reports from https://bit.ly/32PD8HQ

Scenarios

Google Cloud

DevSecCon

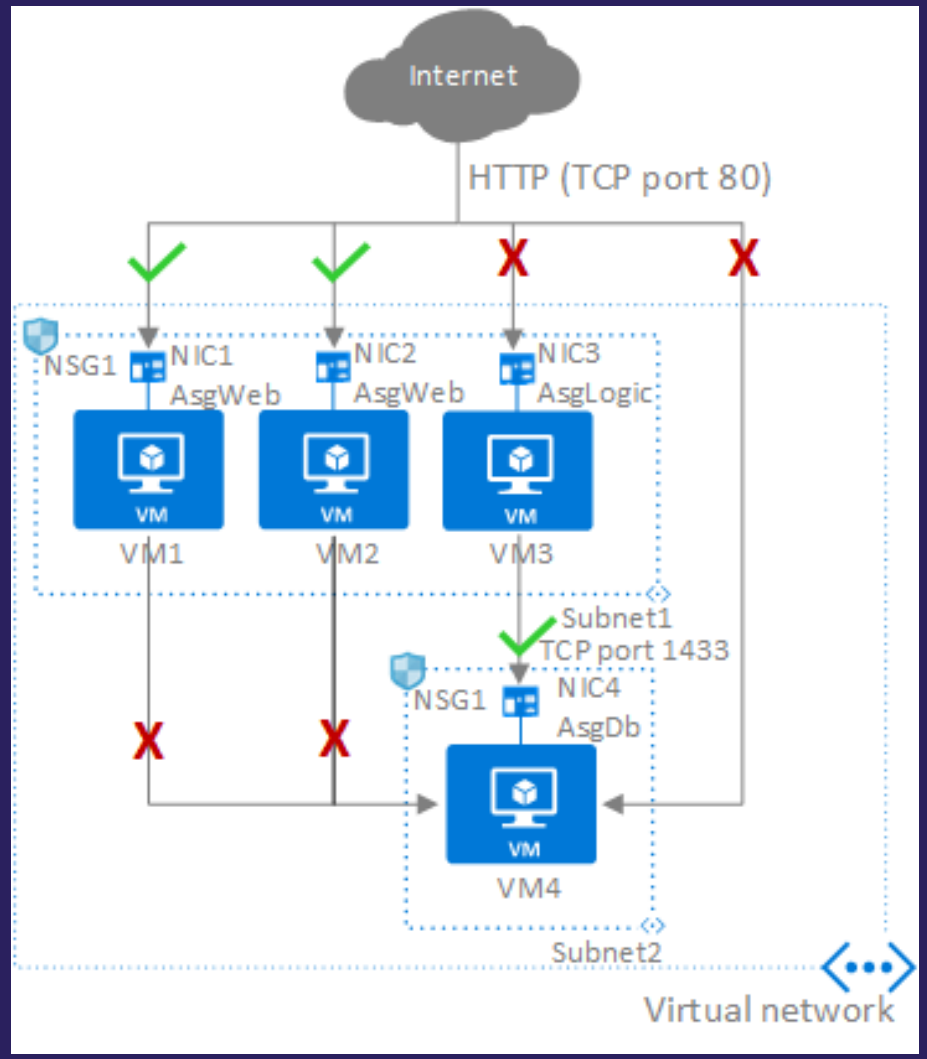
SCOUTSUITE

Azure – Exposed Virtual Machines

Azure – Security Groups

- Network Security Groups
  - Allow filtering network traffic to and from Azure resources in an Azure virtual network.
  - A network security group can be associated to a network interface, the subnet the network interface is in, or both.
- Application Security Groups
  - Allows for the grouping of Virtual Machines logically, irrespective of their IP address or subnet assignment within a Virtual Network.
  - Allows the application-centric use of Network Security Groups.

Azure – Exposed Virtual Machines



DevSecCon

SCOUTSUITE

GCP – Storage Buckets

GCP – IAM Members

In Cloud IAM, you grant access to members. Members can be of the following types:

- Google Account
- Service account
- Google group
- G Suite & Cloud Identity domains
- “allUsers”
  - Special identifier that represents anyone who is on the internet, including authenticated and unauthenticated users.
- “allAuthenticatedUsers”
  - Special identifier that represents all service accounts and **all users on the internet who have authenticated with a Google Account**.

GCP – Storage Buckets Access Control Options

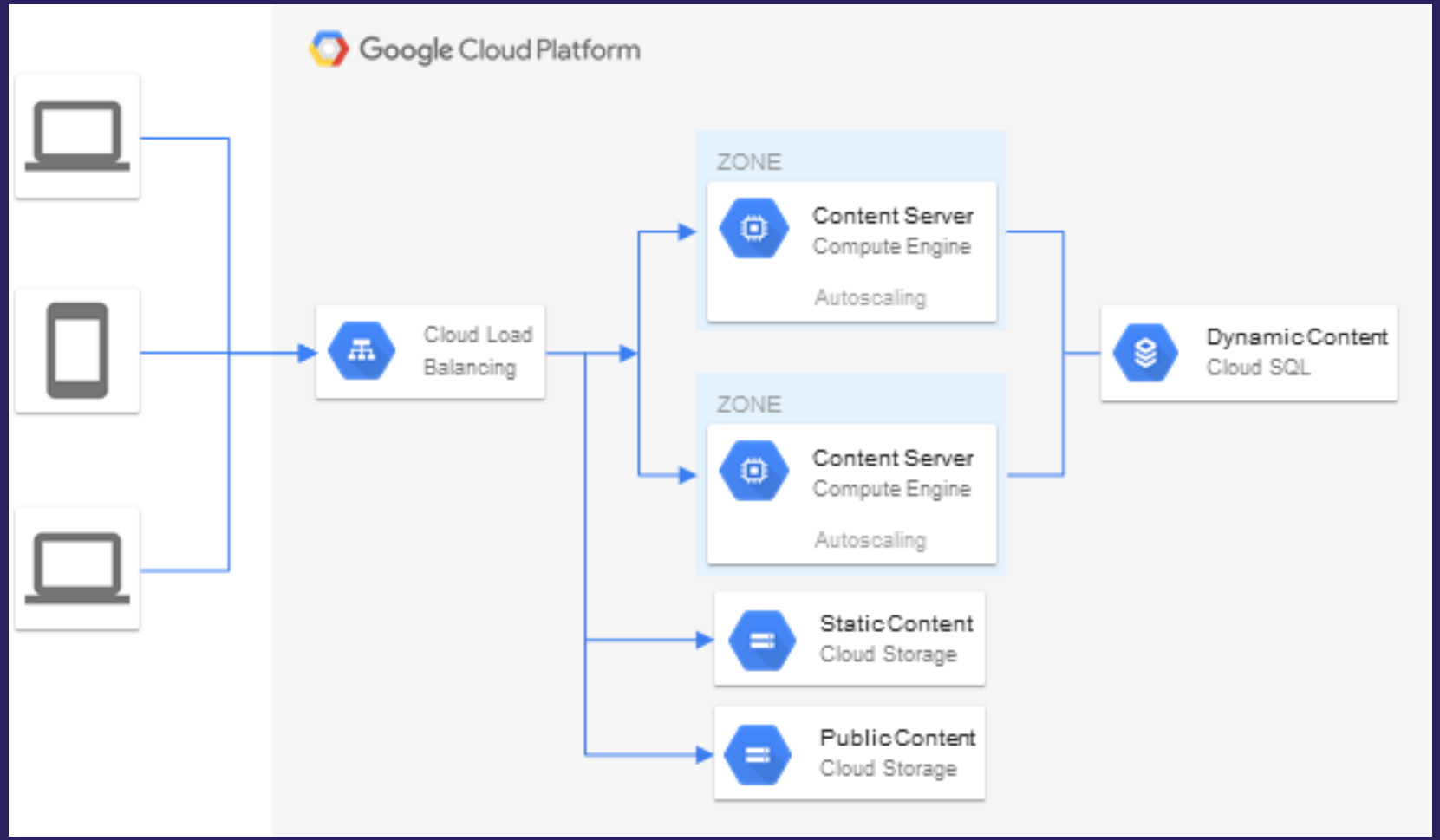
Cloud Identity and Access Management (Cloud IAM) permissions

Grant access to buckets as well as bulk access to a bucket's objects. IAM permissions give you broad control over your projects and buckets, but not fine-grained control over individual objects.

Access Control Lists (ACLs)

Grant read or write access to users for individual buckets or objects. In most cases, you should use IAM permissions instead of ACLs. Use ACLs only when you need fine-grained control over individual objects.

GCP – Storage Buckets



DevSecCon

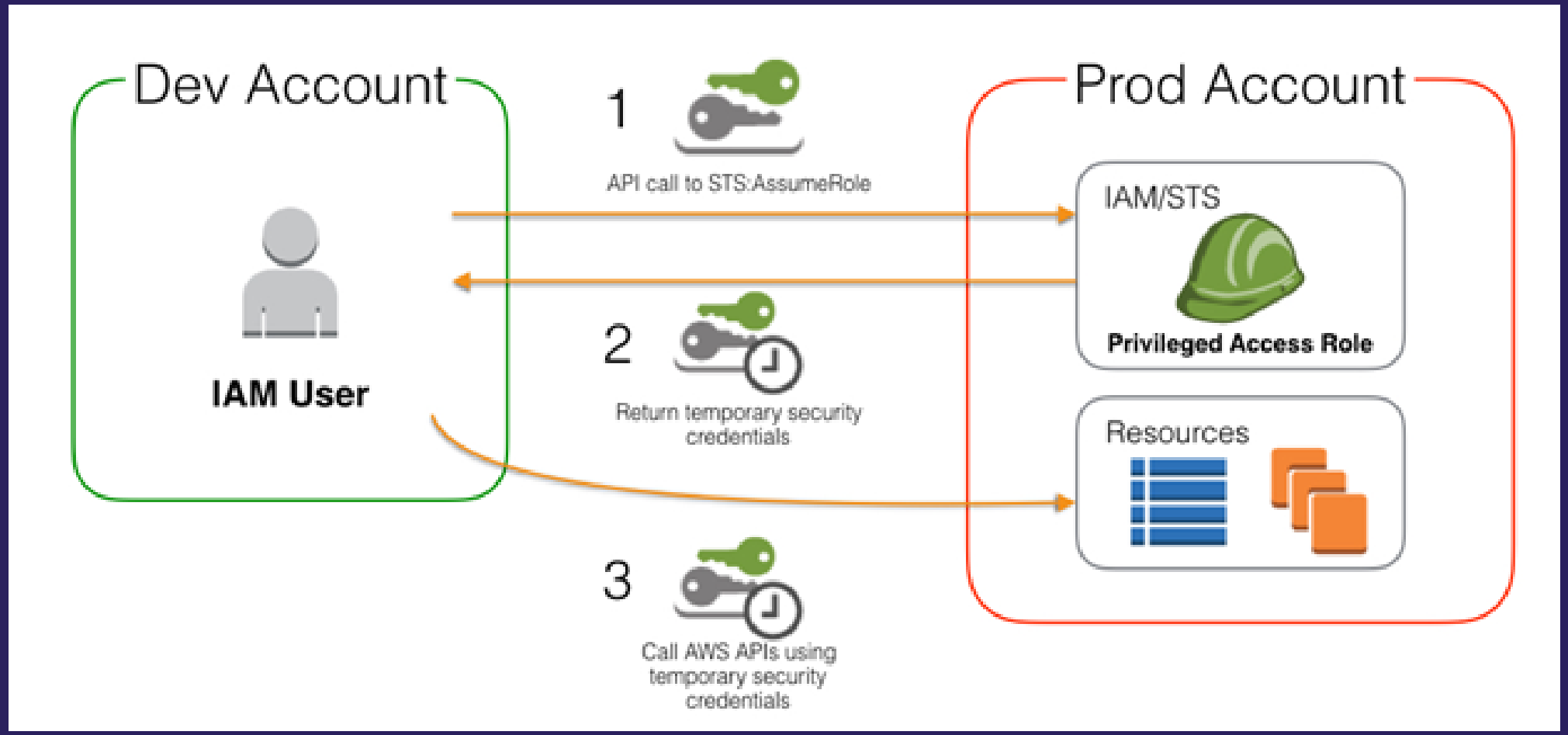
SCOUTSUITE

AWS – Privilege Escalation

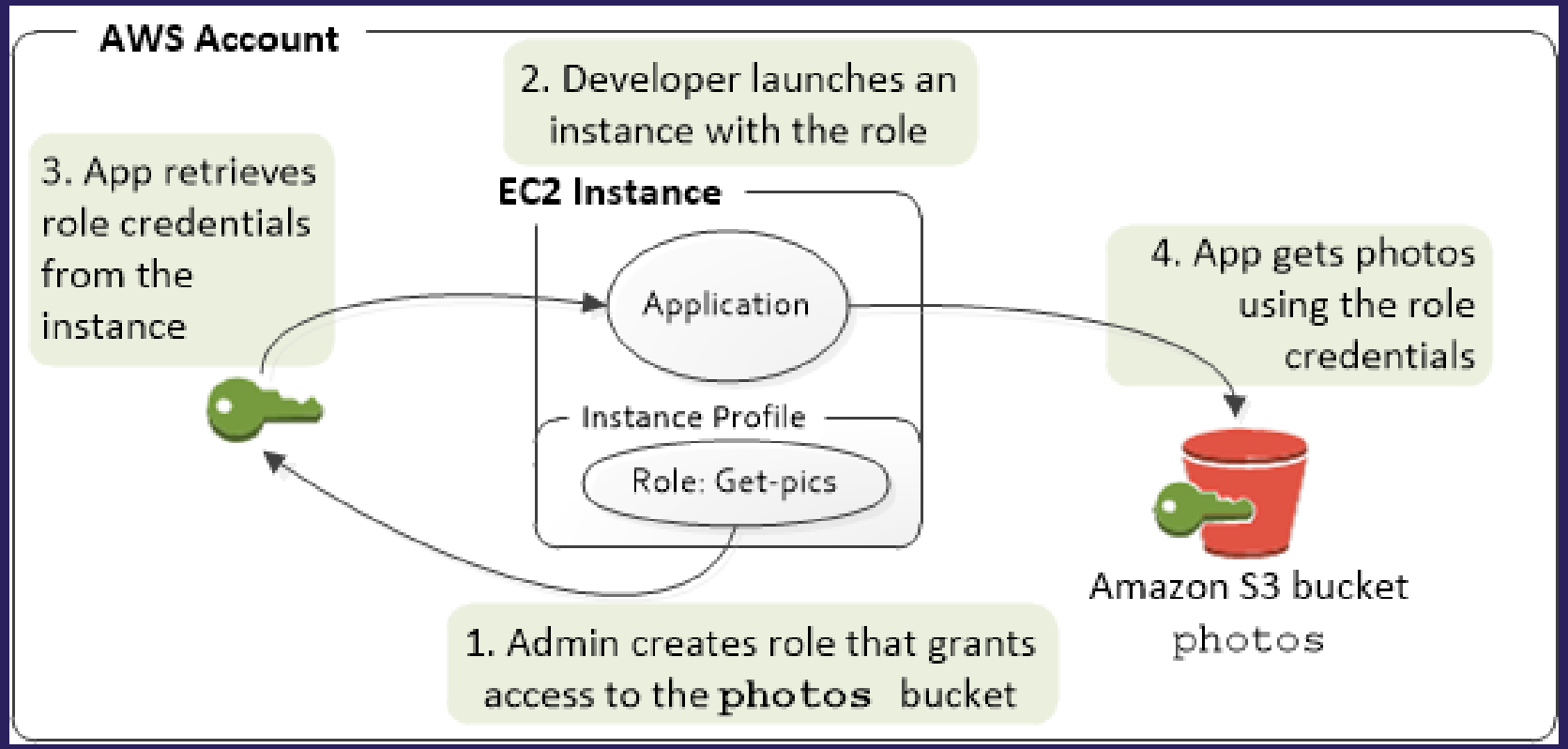
AWS – Privilege Escalation through IAM Permissions

- Creating a new policy version, or setting the default policy version to an existing version
  - An attacker with the `iam:CreatePolicyVersion` permission can create a new version of an IAM policy that they have access to. This allows them to define their own custom permissions.
  - An attacker with the `iam:SetDefaultPolicyVersion` permission may be able to escalate privileges through existing policy versions that are not currently in use.
- Creating a new user access key
  - An attacker with `the iam:CreateAccessKey` permission can create new access keys belonging to another user.
- Attaching a policy to a user, group or role
  - An attacker with the `iam:AttachUserPolicy`, `iam:AttachGroupPolicy` or `iam:AttachRolePolicy` permissions can escalate privileges by attaching a policy to a user, group or role that they have access to.
- Adding a user to a group
  - An attacker with the `iam:AddUserToGroup` permission can use it to add themselves to an existing IAM Group in the AWS account.

AWS – Roles & Role Assumption



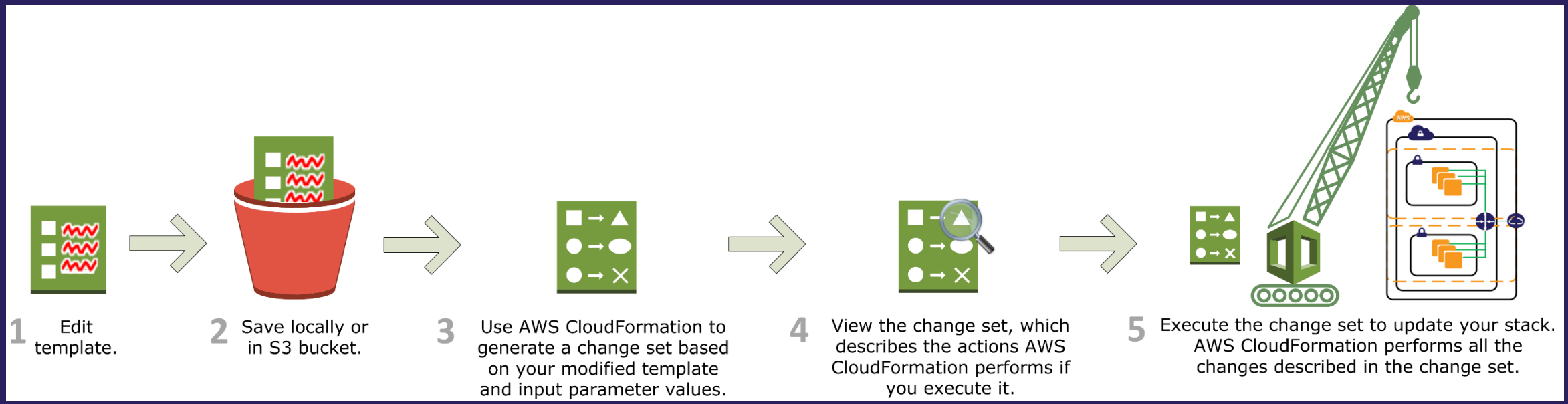
AWS – Service Roles



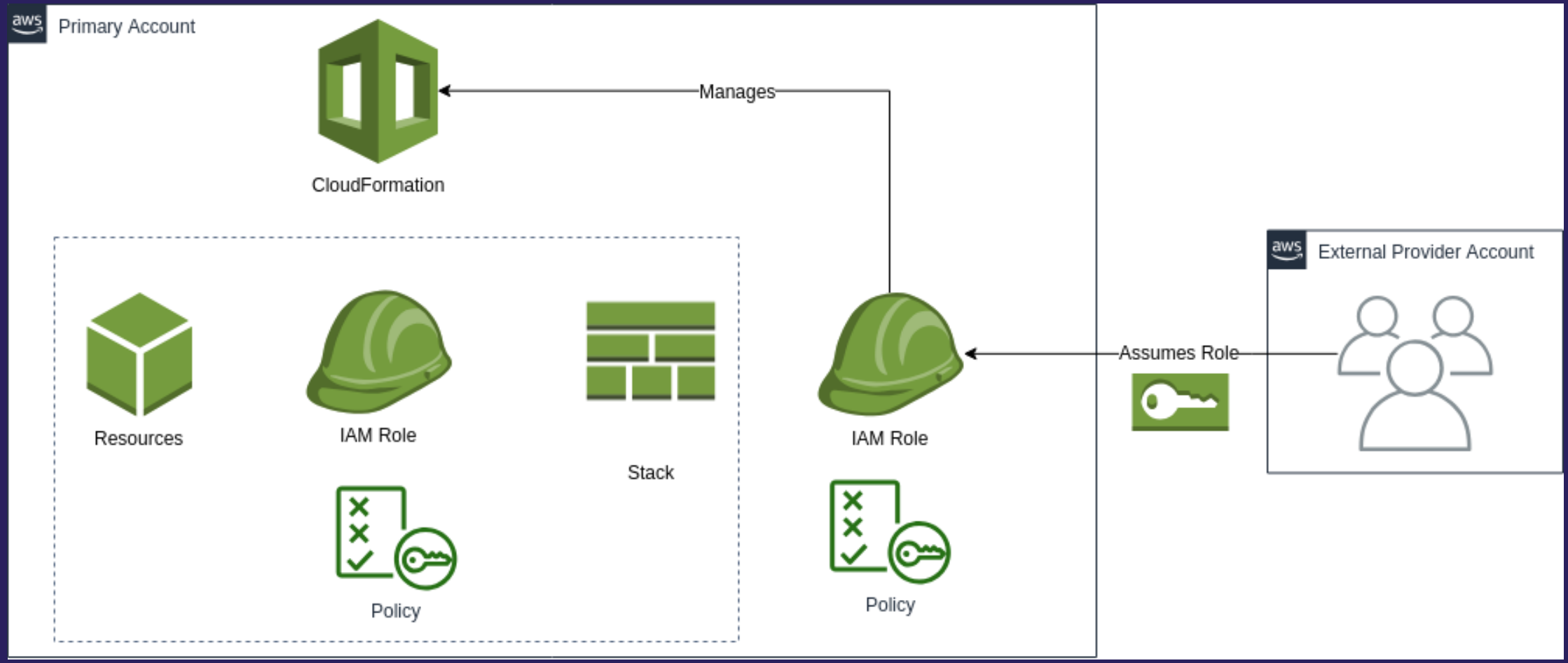
AWS – Privilege Escalation through Compute Services

- Creating an EC2 instance with an existing service role
  - An attacker with the `iam:PassRole` and `ec2:RunInstances` permissions can create a new EC2 VM instance that they will have access to (e.g. through SSH) and pass an existing service role to it.
  - They can then login to the instance and obtain the associated temporary AWS keys from the instance's meta data, which gives them access to all the permissions that the associated service role has.
- Updating the code of an existing Lambda function with a service role attached
  - An attacker with the `lambda:UpdateFunctionCode` permission could update the code in an existing Lambda function with an IAM role attached so that it would perform actions on behalf of that role.
  - They would then need to wait for the function to be invoked if they were not able to do so directly.

AWS – CloudFormation (Infrastructure as Code)



AWS – CloudFormation Service Roles



AWS – Privilege Escalation through CI/CD

- An attacker with the `iam:PassRole` and `cloudformation:CreateStack` permissions would be able to escalate privileges by creating a template that will perform actions and create resources using the permissions of the role that was passed when creating the stack.
- An attacker with the `cloudformation:UpdateStack` permission would be able to escalate privileges by updating an existing stack with a template that will perform actions and create resources using the permissions of the role that was passed when creating the stack.

DevSecCon

SCOUTSUITE

Don’t use users where you can use roles.

Where you do use users, enable MFA.

Leverage policy conditions and follow the principle of least privilege.

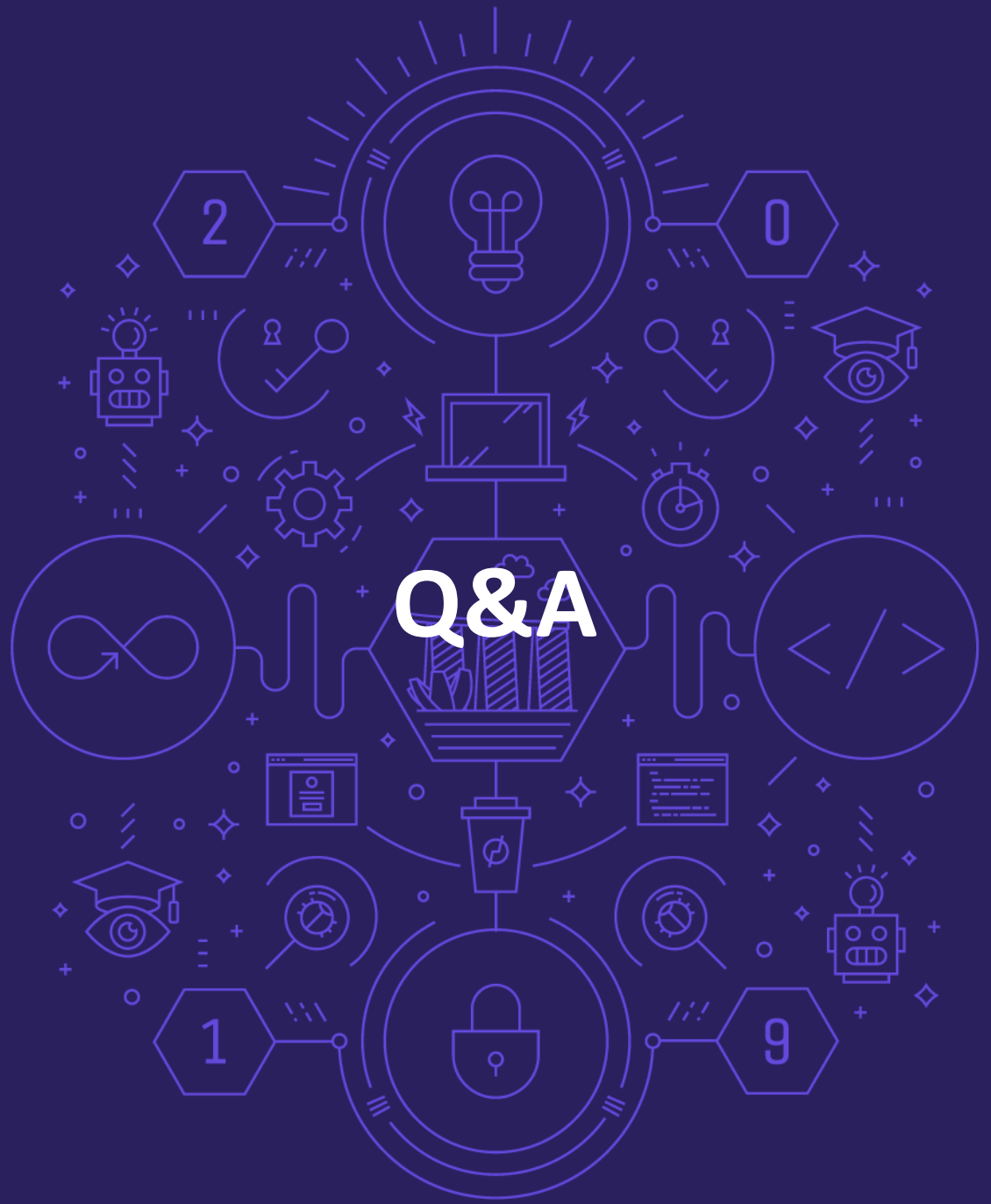
Going Forward

- Refactoring of the front-end as well as the storage implementation
- Improve provider & service support (forever…)
- Addition of a plugin system
  - Privilege escalation checks, identification of publically exposed instances, integration of third-party tools, etc.
- Integration with native security management solutions
  - AWS Security Hub, Azure Security Center, GCP Security Command Center

Contribute! The wiki (https://github.com/nccgroup/ScoutSuite/wiki) has everything you need to get started!

DevSecCon

SCOUTSUITE



Q&A