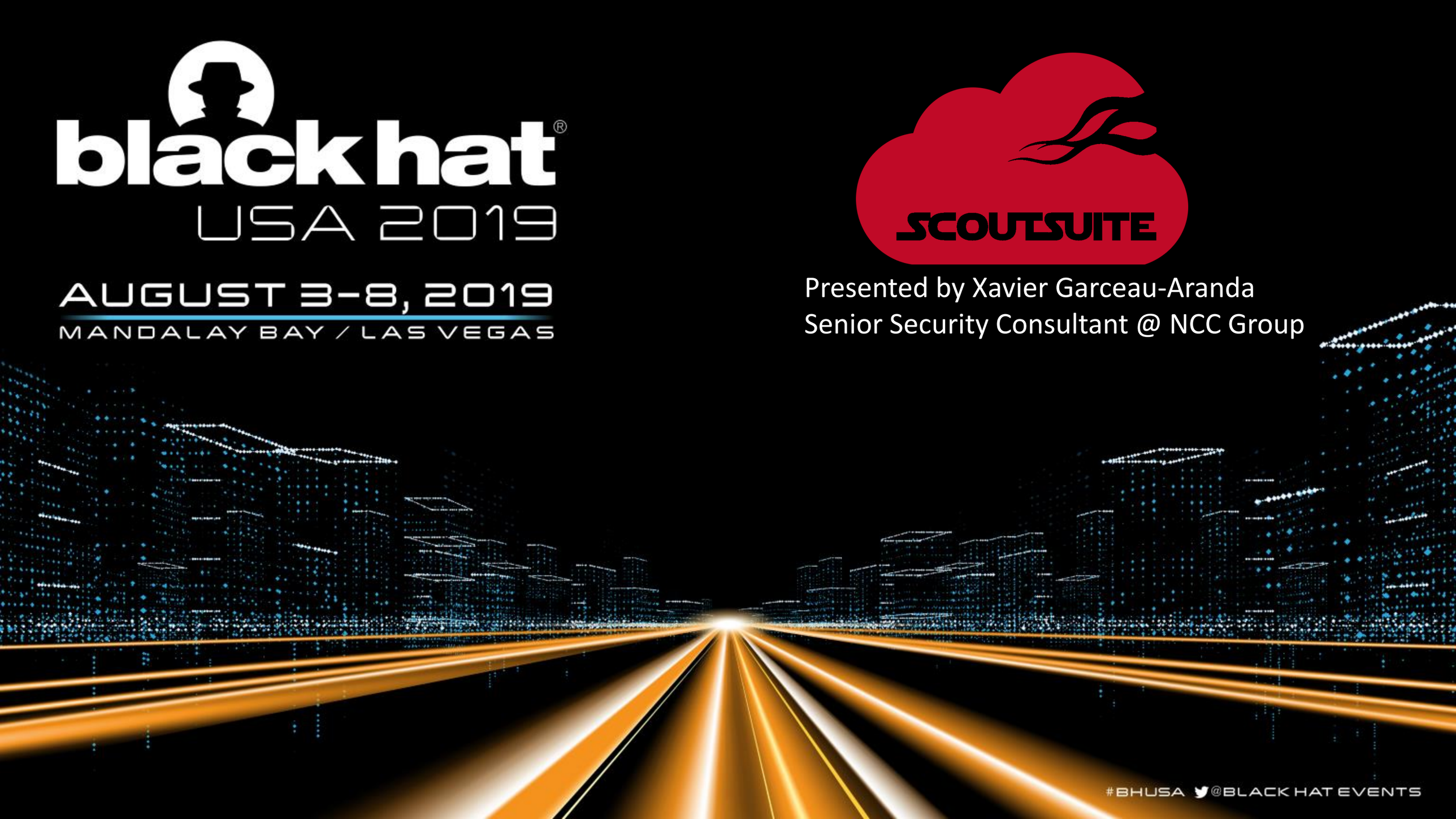

black hat
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
SCOUTSUITE
Presented by Xavier Garceau-Aranda
Senior Security Consultant @ NCC Group
#BHUSA @BLACK HAT EVENTS

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. This has in turn allowed adding support for Azure, Google Cloud Platform and however many more cloud providers.
- 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 native environments has been improving, the multi-cloud paradigm poses new challenges.

Cloud Provider Similarities

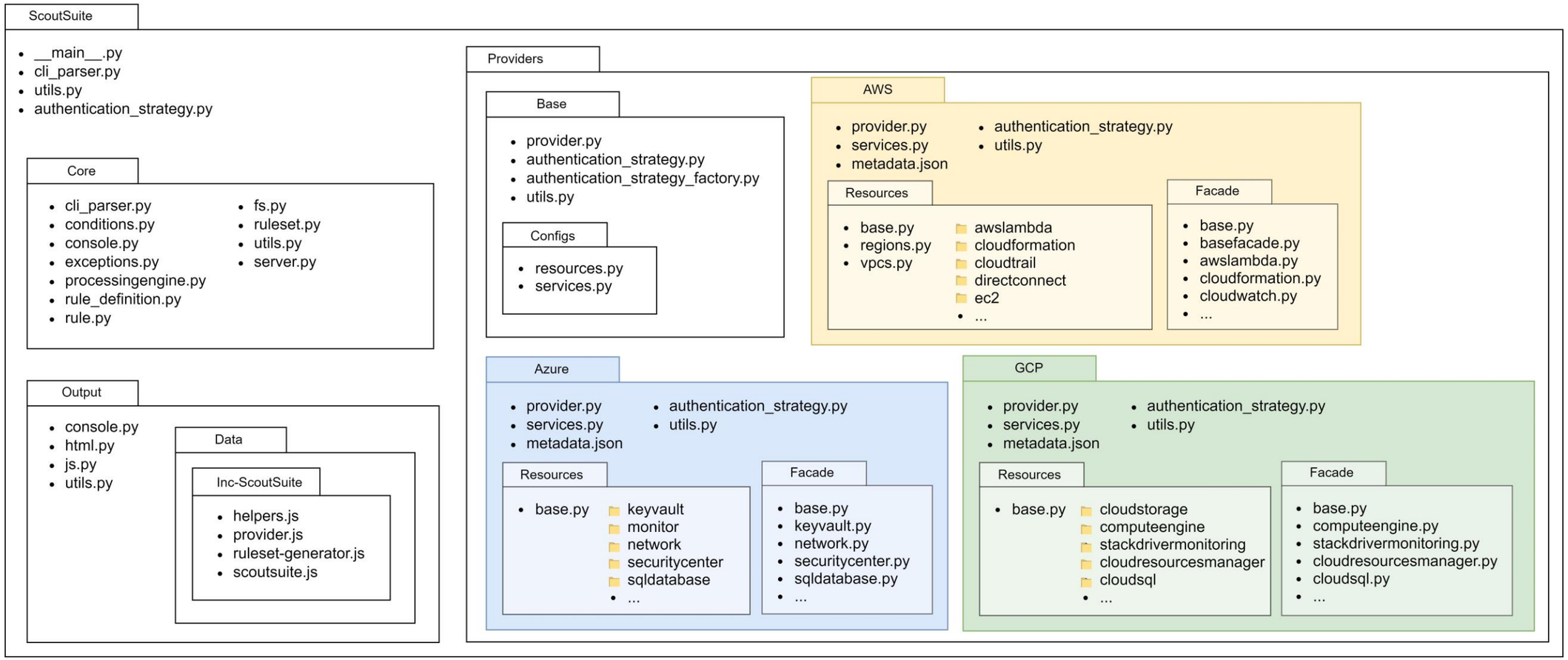
Offering:

- Identity and Access Management – Users/Groups, Roles/Service Principals/Service Accounts & Policies/Permissions
- Regions, Virtual Private Clouds (VPCs) & Resources
- IaaS, PaaS & SaaS offerings

Risks:

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

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

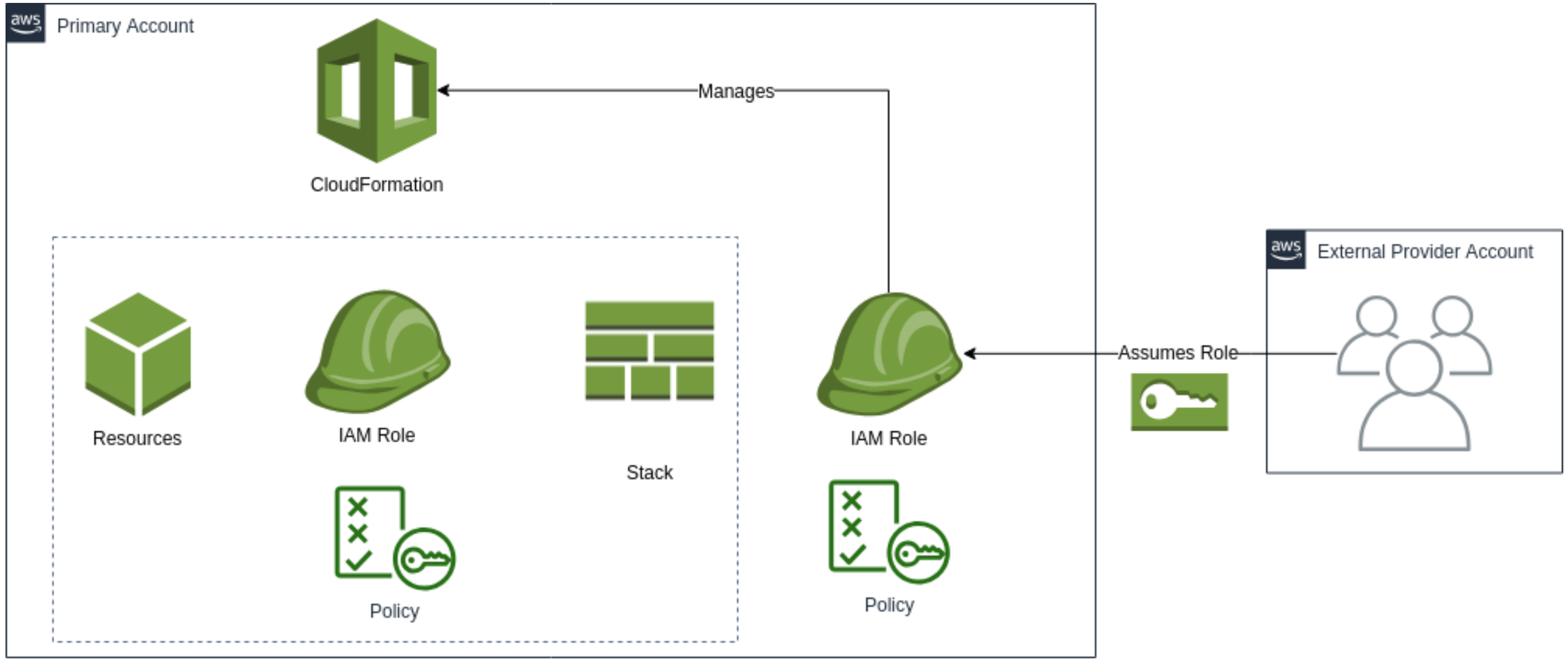
Scout Suite – Advanced Features

- 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
- Exports to CSV & JSON
- Report Parsing
  - https://github.com/nccgroup/ScoutSuite/wiki/HowTo:-Exporting-and-Programmatically-Access-of-Scout-Suite-Data

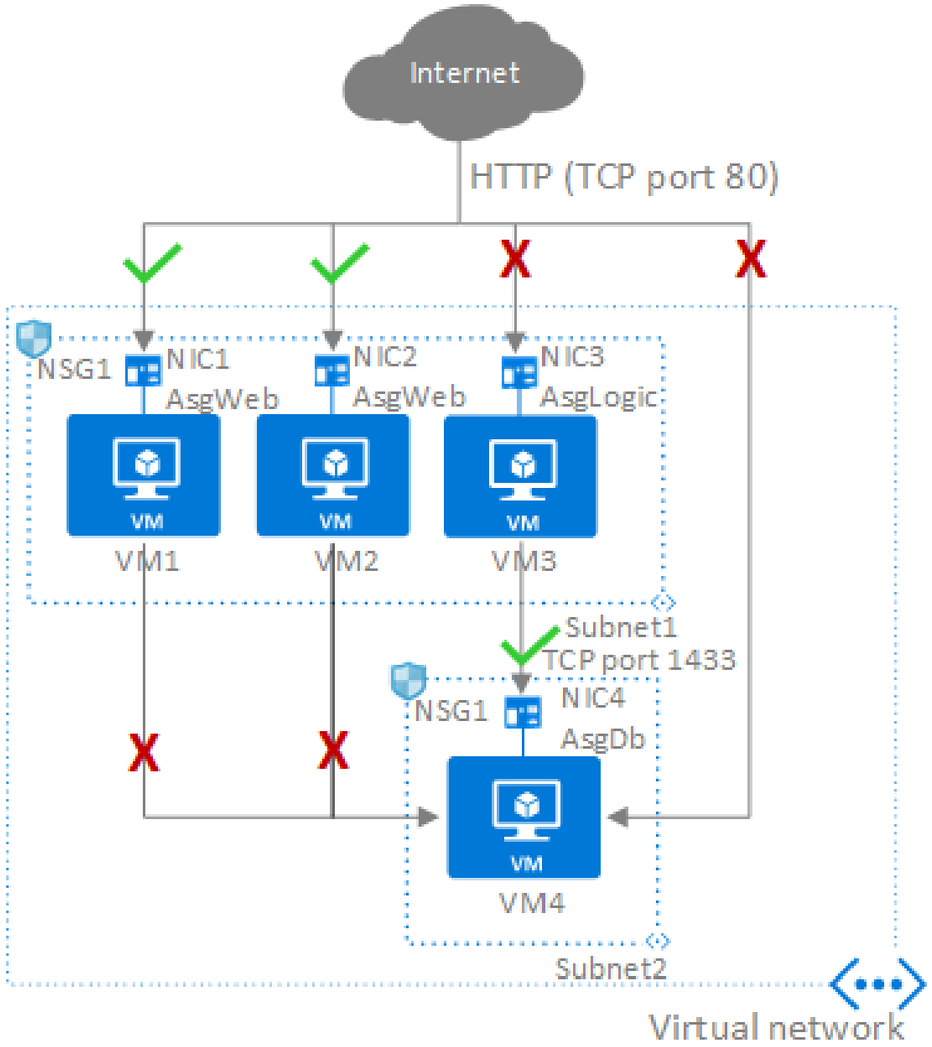
Scenarios

Google Cloud

Scenario – AWS: Privilege Escalation Vector

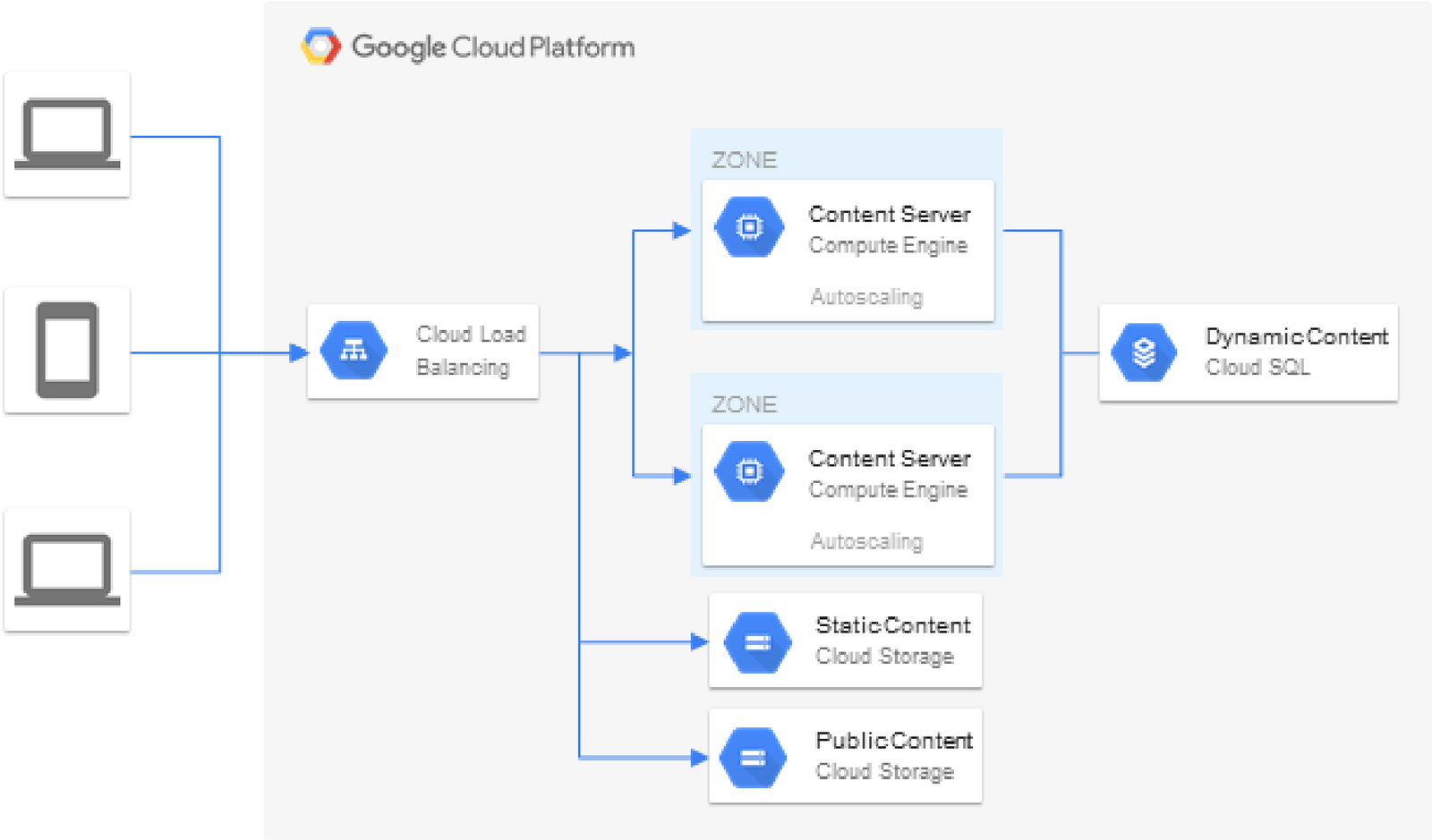


Scenario – Azure: Exposed Virtual Machines



SCOUTSUITE

Scenario – Google Cloud Platform: Storage Buckets



SCOUTSUITE

Going Forward

- Improve provider support
- Addition of a plugin system
  - Privilege escalation checks, identification of publically exposed instances, 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!

Special Mentions

Polytechnique Montréal

- Antoine Boisier-Michaud
- Michaël Sghaïer
- Rémi Pelletier
- Vincent Fortin
- Philippe Dugré

Matt Lewis, NCC Group

Loïc Simon, author of Scout2

SCOUTSUITE