

# Cloud Infrastructure Analysis with Scout Suite

---



**Guillaume Ross**

SECURITY RESEARCHER & PRODUCT MANAGER

@gepeto42 [caffinessecurity.com](http://caffinessecurity.com)







Creator: NCC Group

---

Scout Suite is an open source multi-cloud security auditing tool, which allows you to assess the security posture of cloud environments, producing reports highlighting risky configurations. It is meant to be run as a point-in-time tool, taking a snapshot of the current security configuration of a cloud environment.





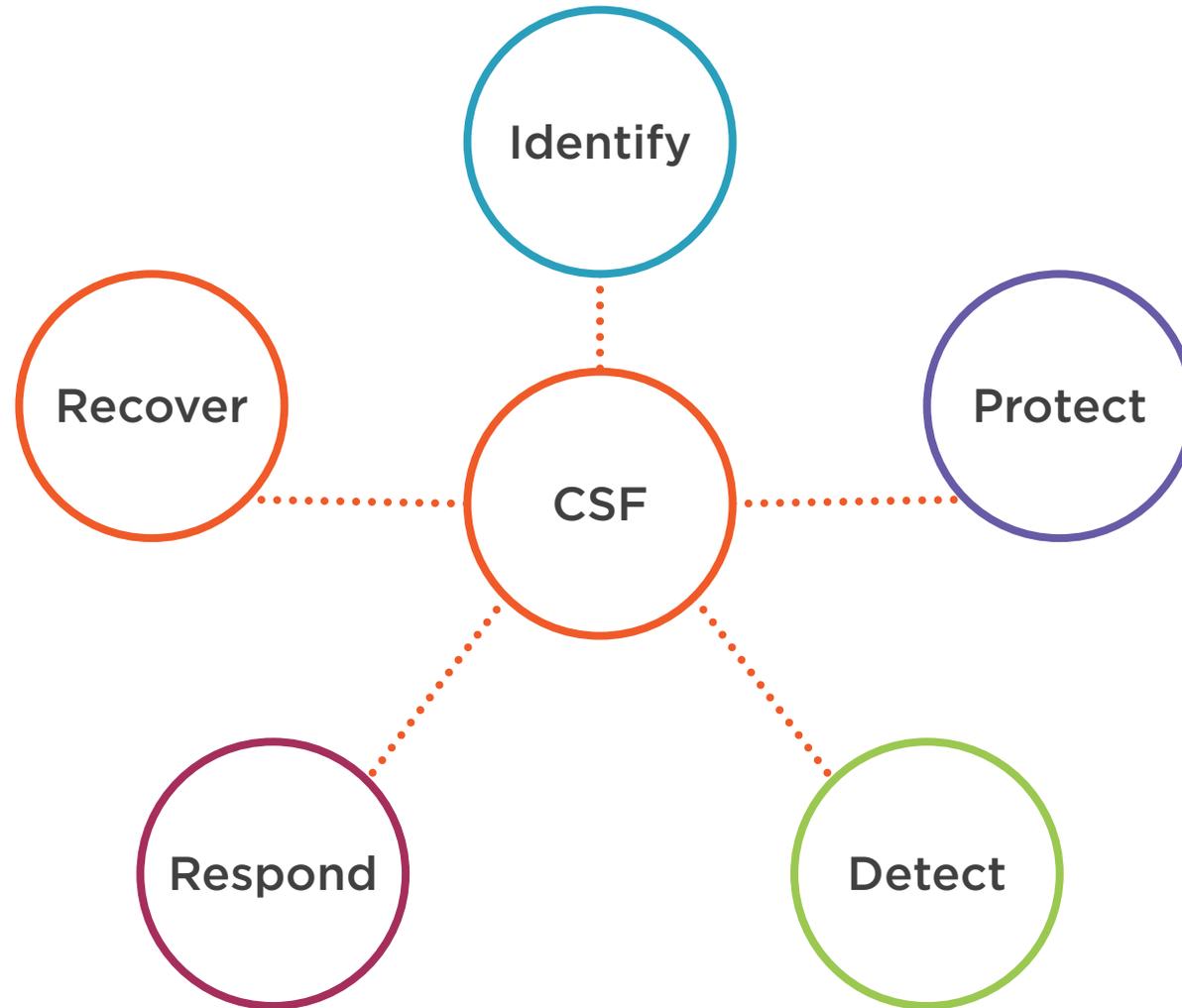
Scout Suite is a Python tool you can execute from any system able to connect to your cloud environments.

It can be downloaded at <https://github.com/nccgroup/ScoutSuite>

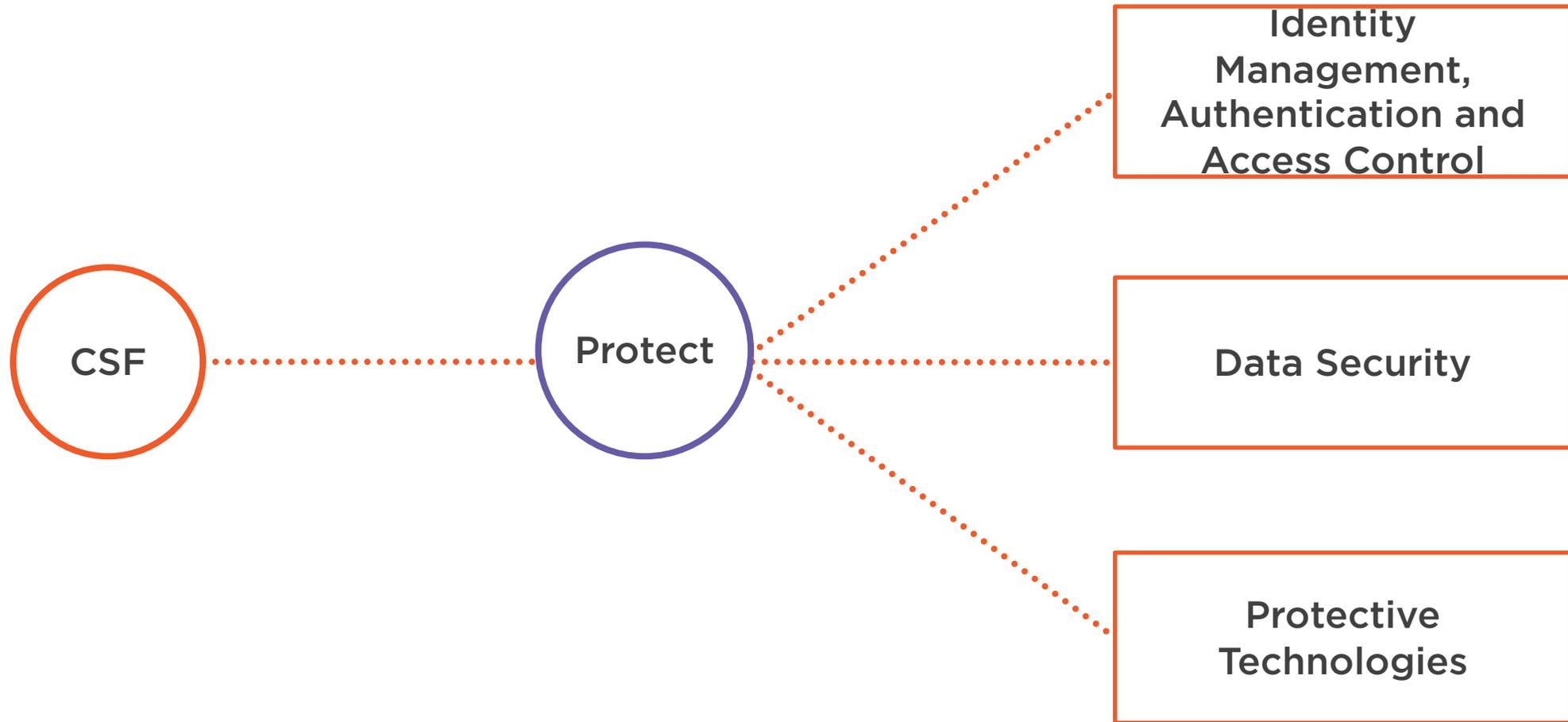
Not only is it open source and very easy to use, but it supports most IaaS vendors with many different security checks.



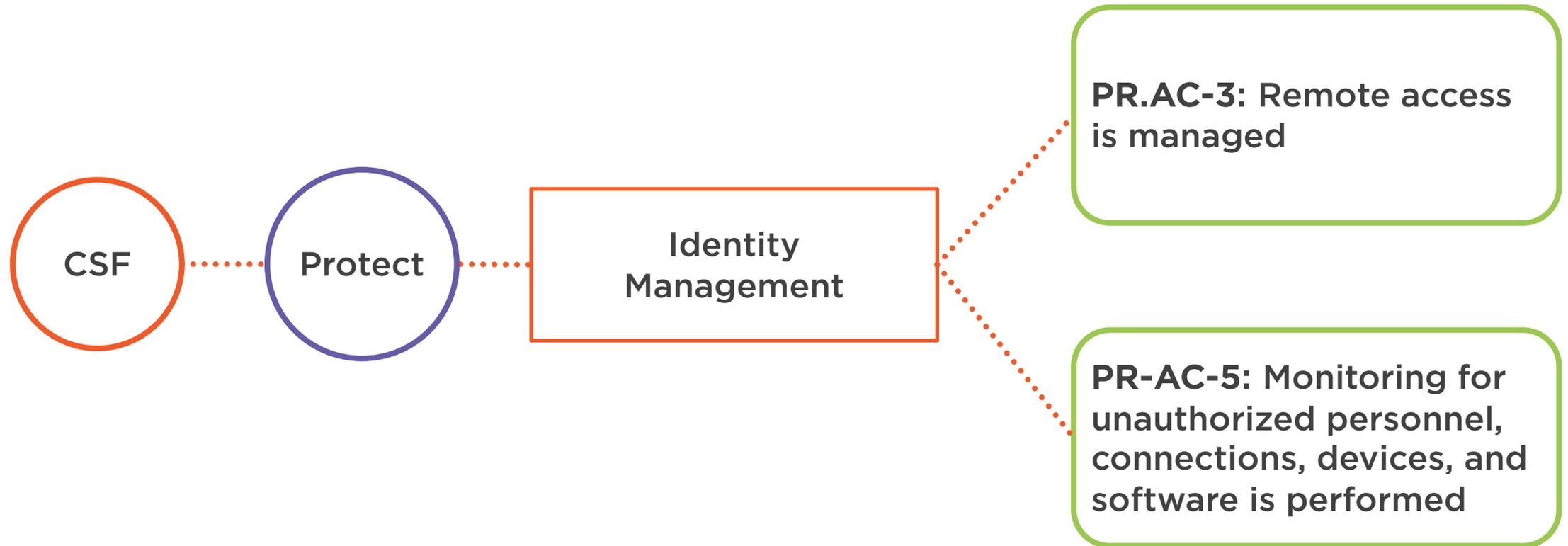
# NIST Cybersecurity Framework



# NIST Cybersecurity Framework



# NIST Cybersecurity Framework



# MITRE ATT&CK

## Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

File Analysis

Threat Intelligence

Incident Management



# MITRE ATT&CK

Data Type

Network Analysis

OS Analysis

Application Analysis

**Infrastructure Analysis**

File Analysis

Threat Intelligence

Incident Management

**T1078:**

Valid Accounts

**T1078.004:**

Cloud Accounts

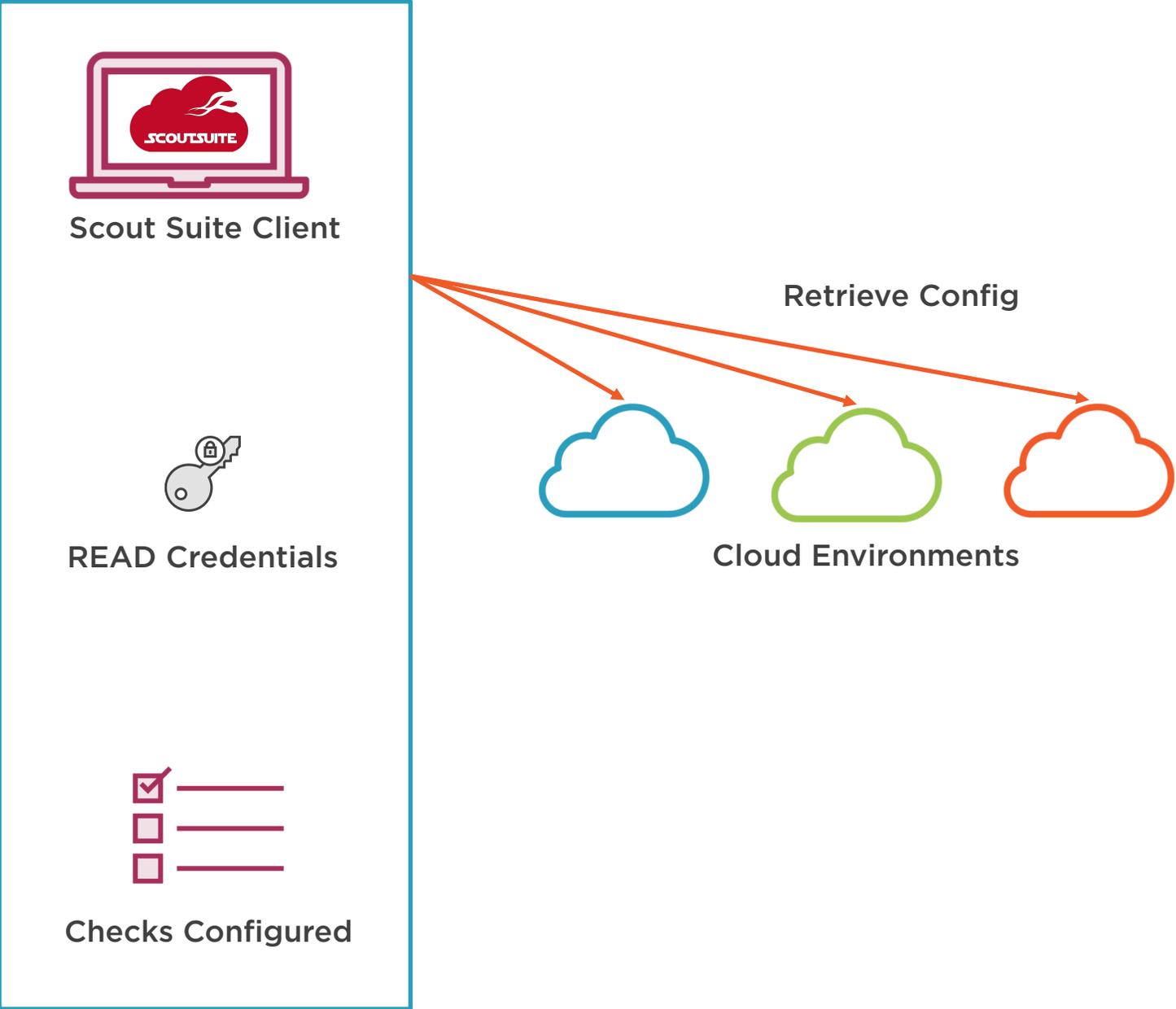
**T1538:**

Cloud Service  
Dashboard

**T1530:**

Data From Cloud  
Storage Object







Report



# Prerequisites

**A system with  
Python3 (Linux  
Recommended)**

**A few Python  
dependencies**

**An AWS  
environment to  
scan**



# Demo Place Holder

1. Python3 is required, along with the AWS CLI, and many other [dependencies](#).
2. We will use SadCloud to generate vulnerable AWS configurations (**do not use against a real environment**)
3. Set up access keys to AWS:  

```
export AWS_ACCESS_KEY_ID="accesskey"  
export AWS_SECRET_ACCESS_KEY="secretkey"  
export AWS_DEFAULT_REGION="us-east-1"
```
4. git clone <https://github.com/nccgroup/ScoutSuite.git>
5. python3 scout.py aws



# More Information

## Capabilities

Docker Container for Scout Suite

<https://github.com/nccgroup/ScoutSuite/wiki/Docker-Image>

Using Scout Suite with temporary credentials

<https://github.com/nccgroup/ScoutSuite/wiki/Amazon-Web-Services>

## Related Information

Cloud and Cloud Dashboard Security

<https://aws.amazon.com/security/>

### Pluralsight Resources

- Multiple Pluralsight Learning Paths
  - Links in links.txt
- Guillaume's Cloud Security Channel

