

# Cloud Infrastructure Analysis with Prowler

---

Identify, Assess, and Report Cloud Security Threats with Prowler

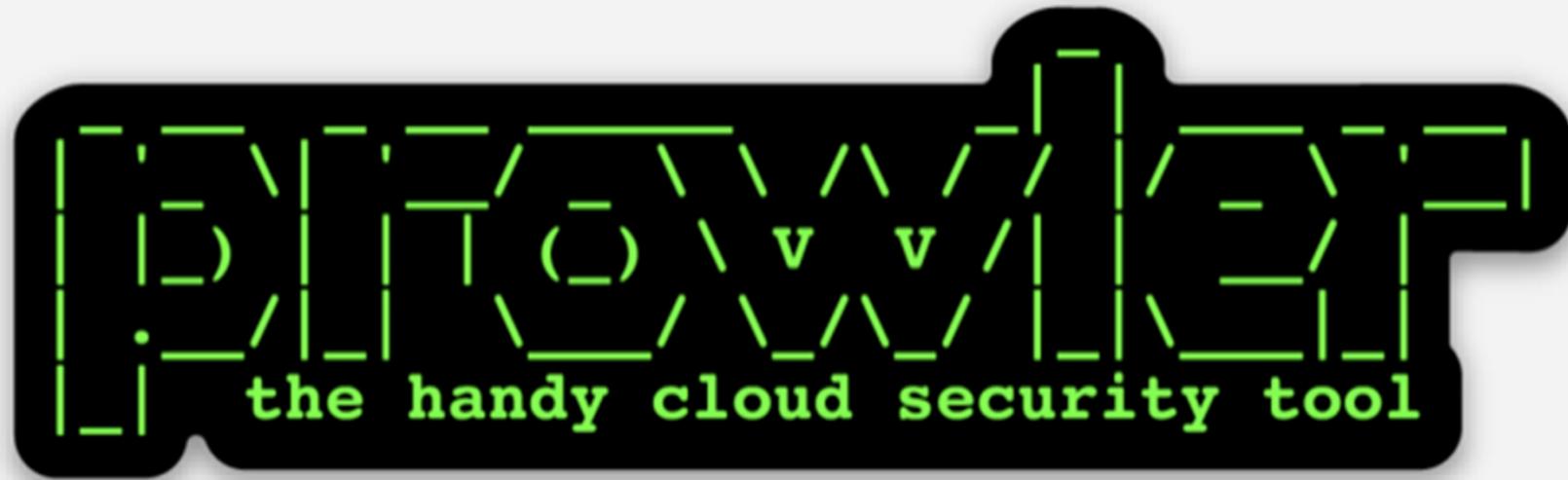


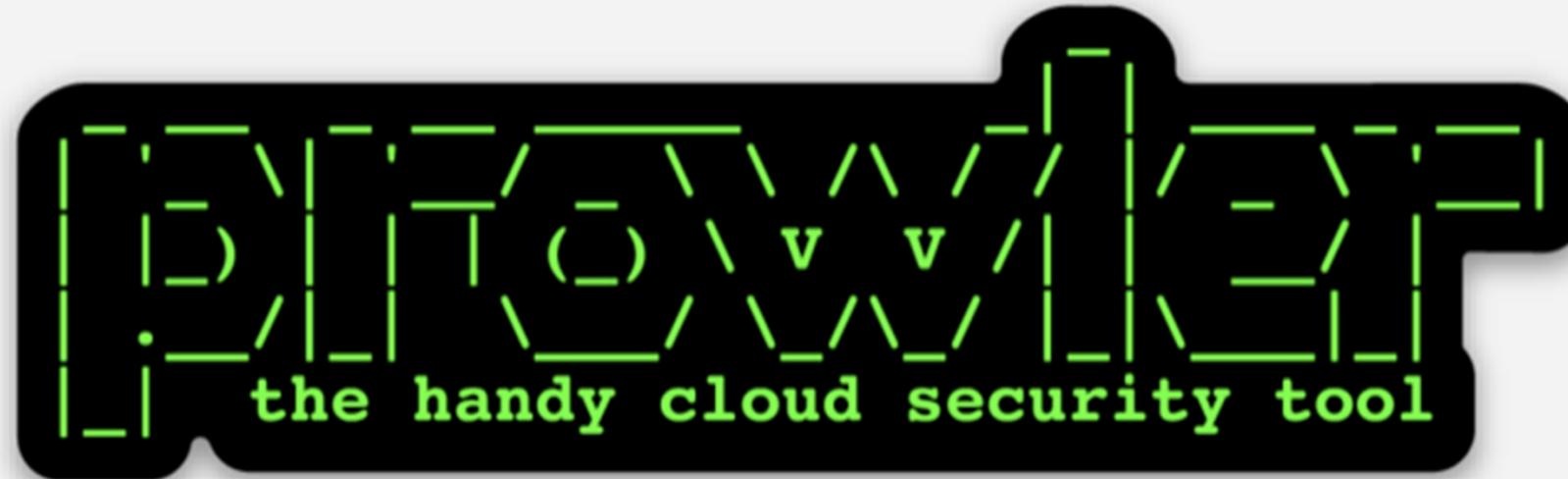
**Tim Coakley**

Senior Security Solutions Architect

<https://www.linkedin.com/in/timcoakley/>





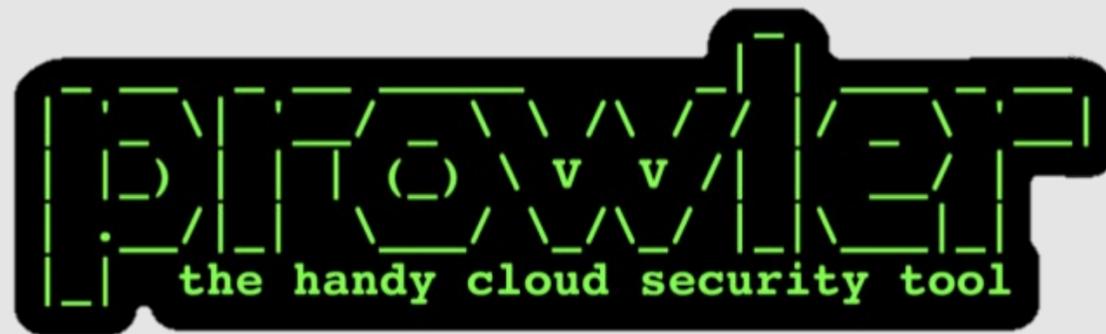


Creator: Toni de la Fuente



**Prowler is a security assessment tool that performs assessments of AWS cloud environments against AWS security best practices, audit, incident response, hardening and forensic readiness with over 100 different checks.**





**Easy to operate command line tool**

**Scalable, assess single or multiple AWS accounts**

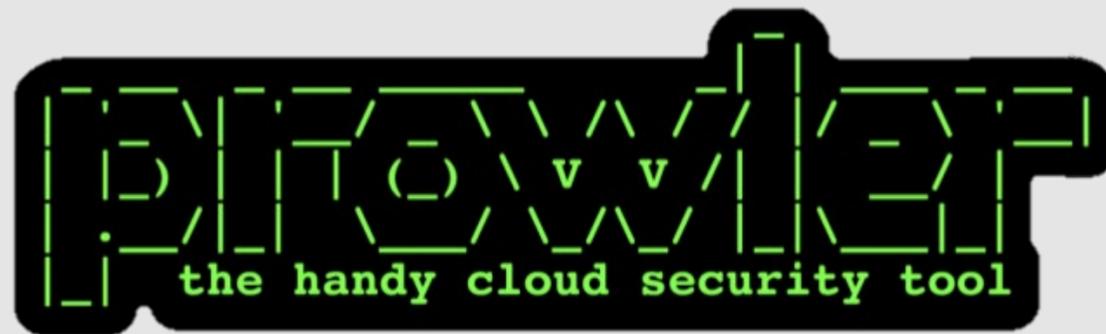
**Apache 2.0 Opensource License**

**Available to download on GitHub**

**Over 100 different assessment checks**

**Flexible reporting onscreen or as files**



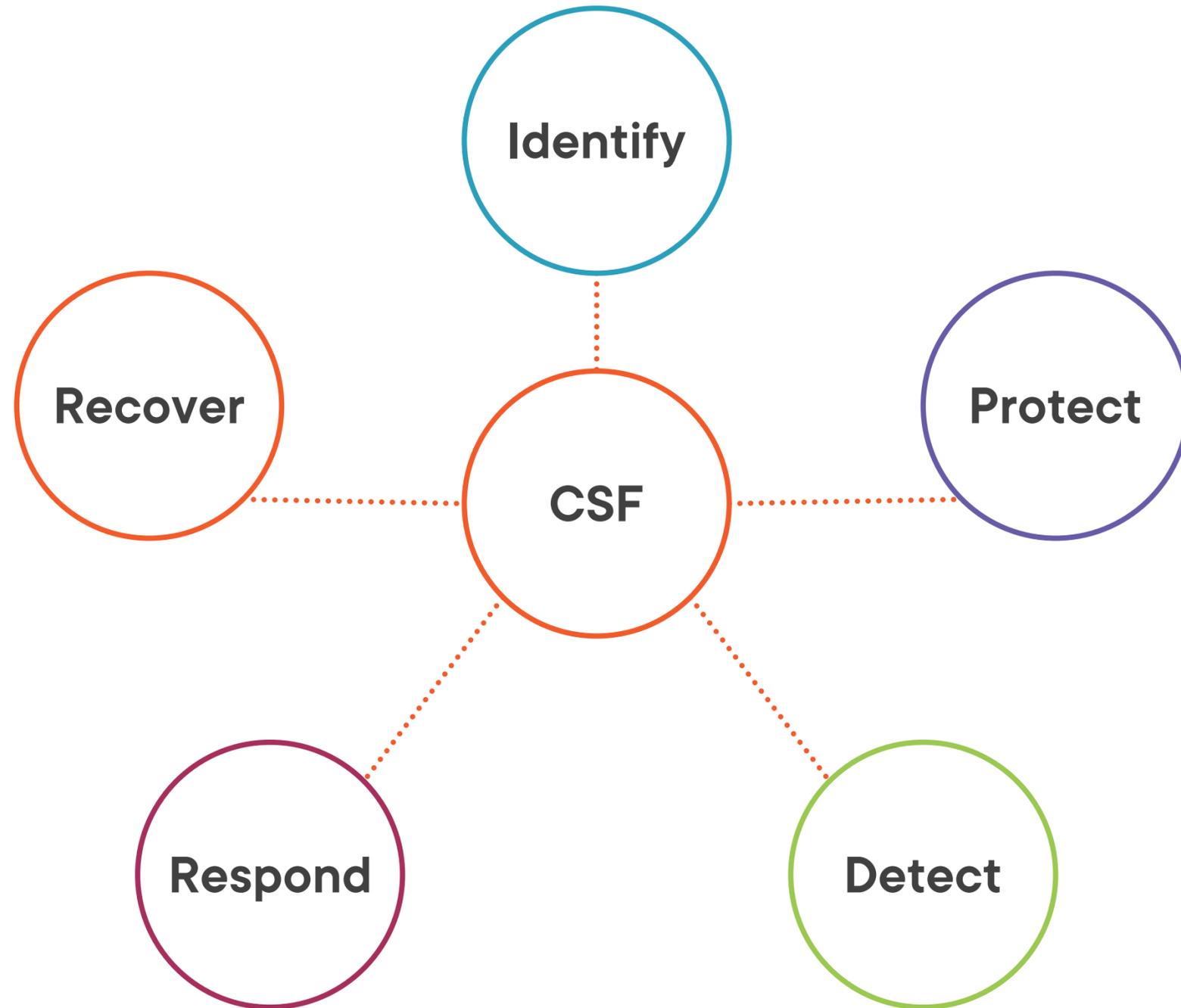


**Over 100 different assessment checks**

**Flexible reporting onscreen or as files**



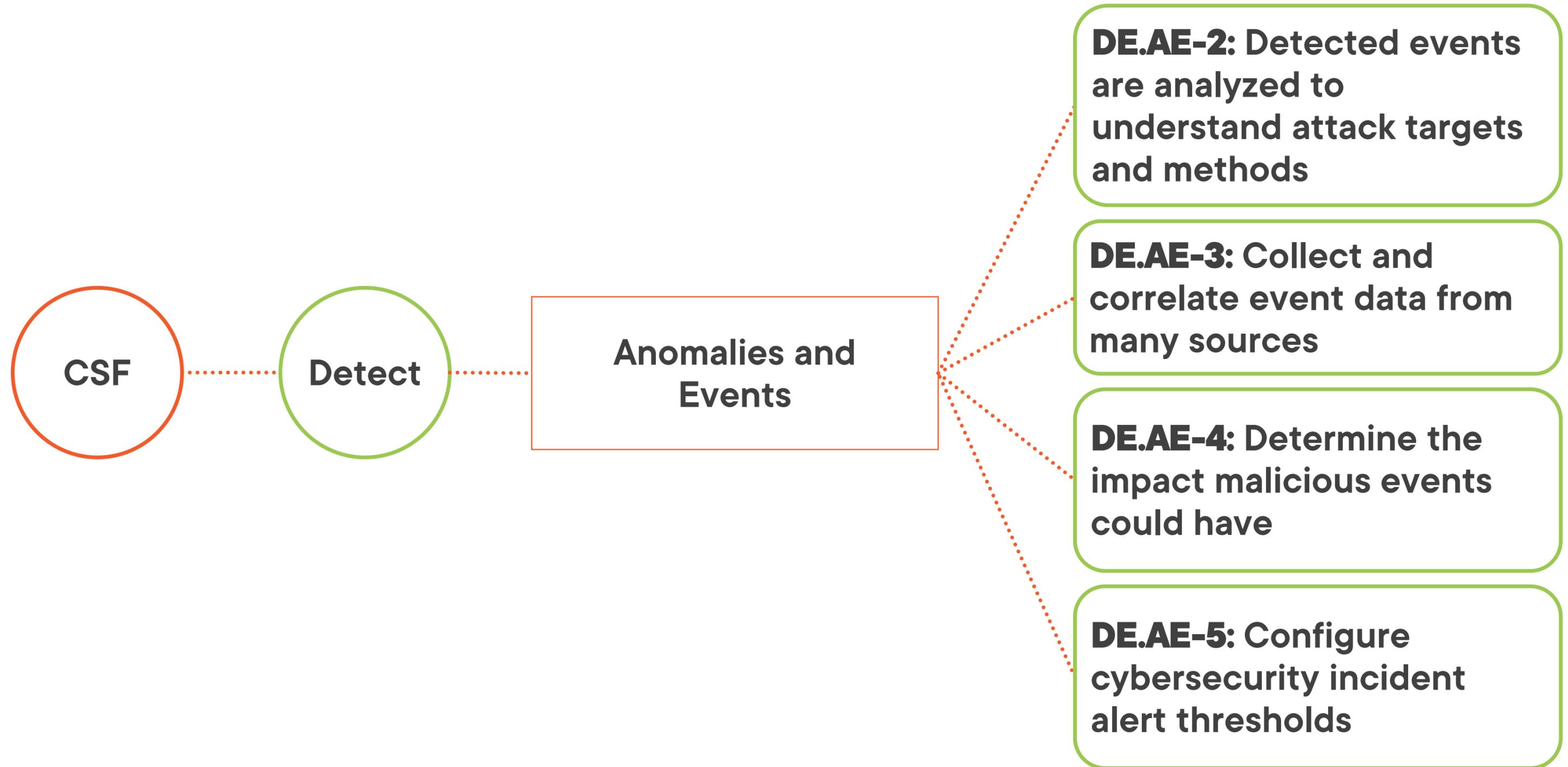
# NIST Cybersecurity Framework



# 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

**T1562:**  
**Cloud Service Discovery**



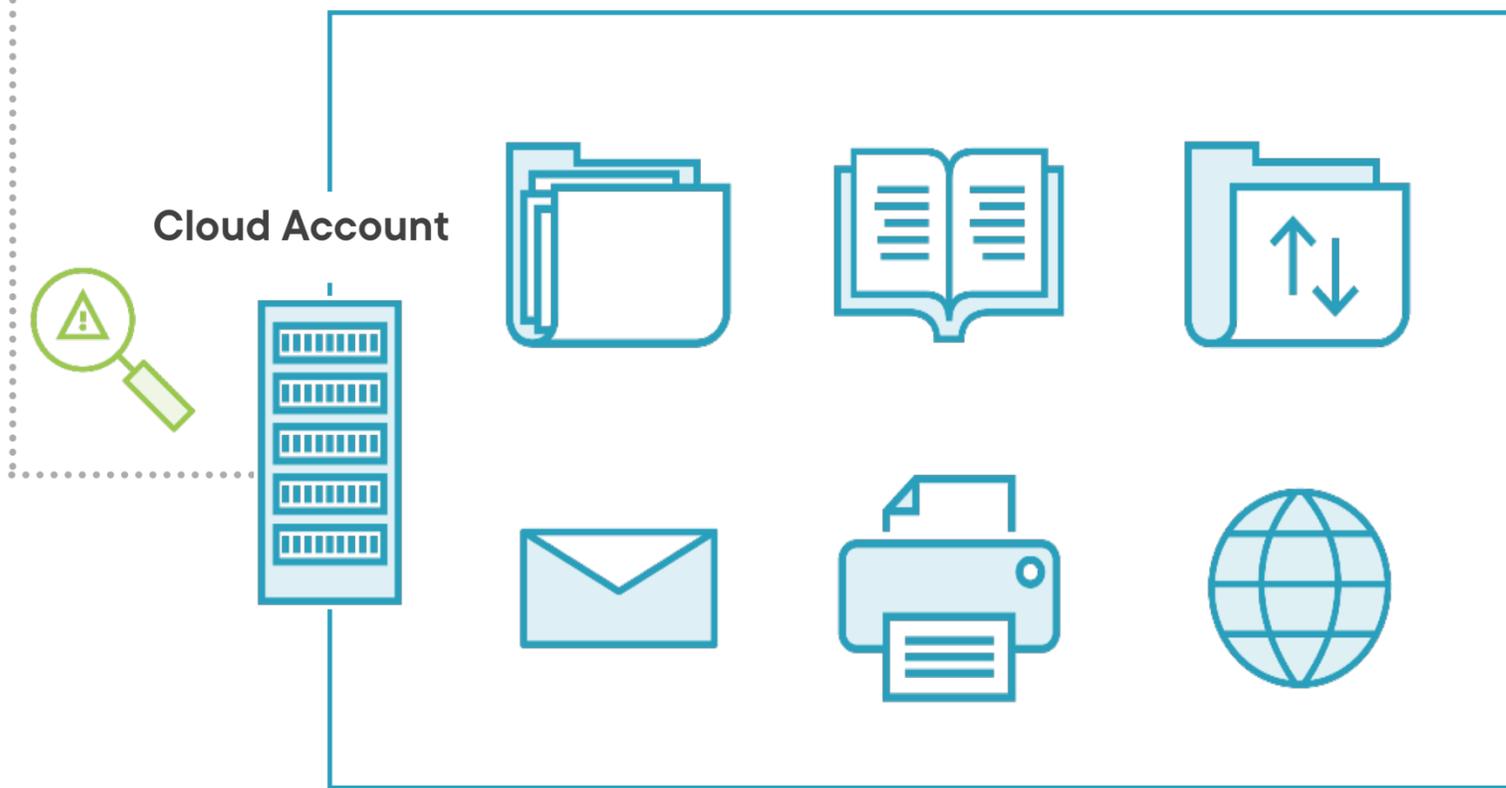
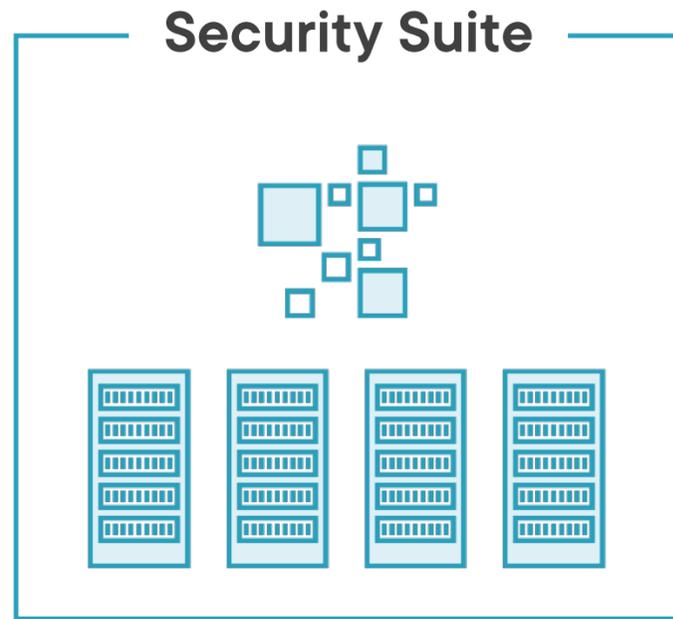
# MITRE SHIELD

## T1526:

### Cloud Service Discovery

**DTE0014 – Decoy Network:** Create a target network with a set of target systems, for the purpose of active defense. (DUC0251)





**Colleagues**



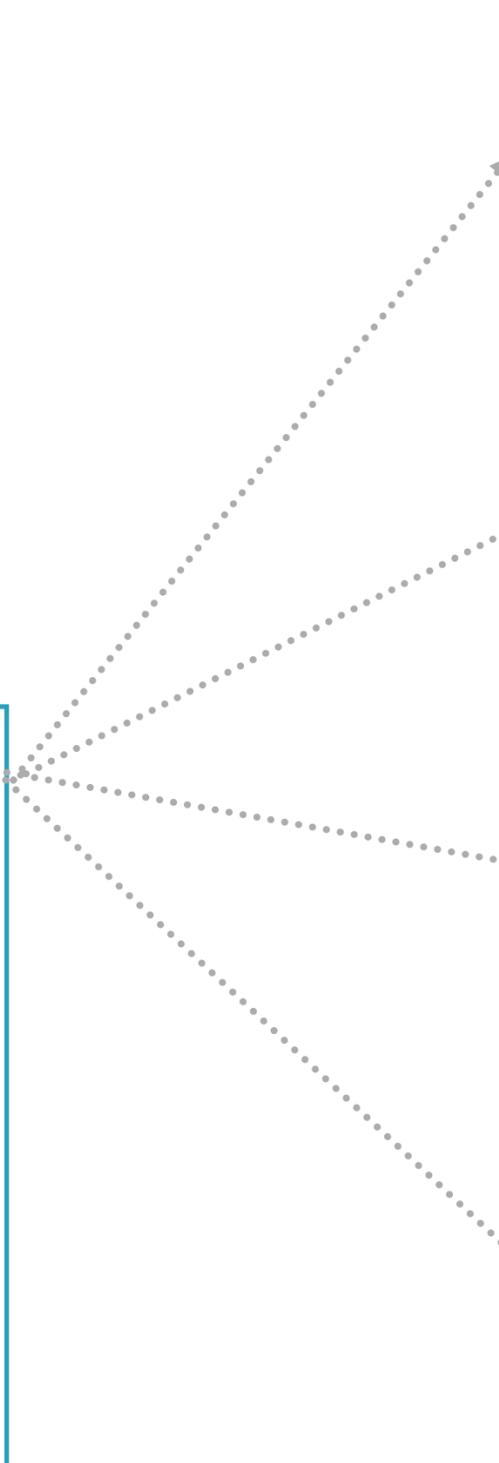
**Exec / VIP**

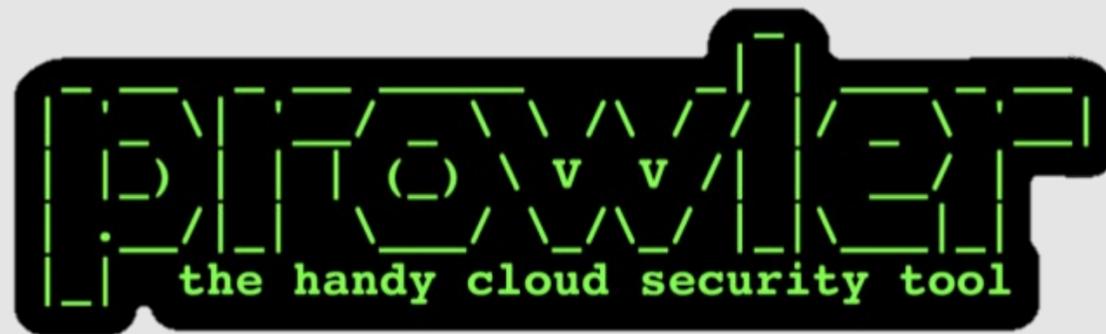


**Finance / HR**



**Engineering**

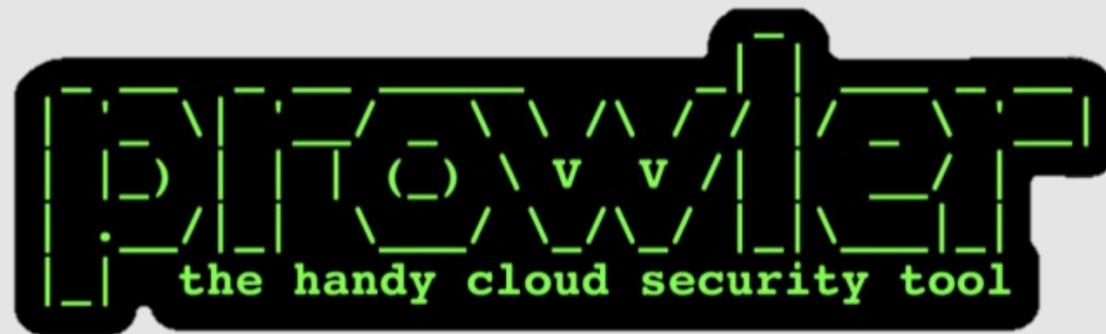




**Perform ad-hoc infrequent manual runs**

**Perform regular automated runs**





**Prowler requires a cloud account with the necessary access permissions. Installation details are available of the [Prowler GitHub page](#).**



# KEY TAKEAWAYS

## **Exposed Services**

**Develop ability to detect  
internet facing services**

## **Attacker Motivations**

**Understand attackers  
persistence**





## **Cloud Security**

**Is a challenging but rewarding  
experience**



## **Technology**

**Prowler is one of many tools that  
will aid the cybersecurity  
professional**

