File Analysis with TruffleHog

Identify, Assess and Report Credential Leakage with TruffleHog

Tim Coakley
Senior Security Solutions Architect

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

PROFI
TRUFFLEHOG

Creator: Dylan Ayrey

TruffleHog is a security assessment tool that performs assessments of git source code repositories looking for high entropy strings and secrets.

TRUFFLEHOG

Easy to operate command line tool

Scalable, assess single or multiple git repositories

OpenSource License

Available to download on GitHub

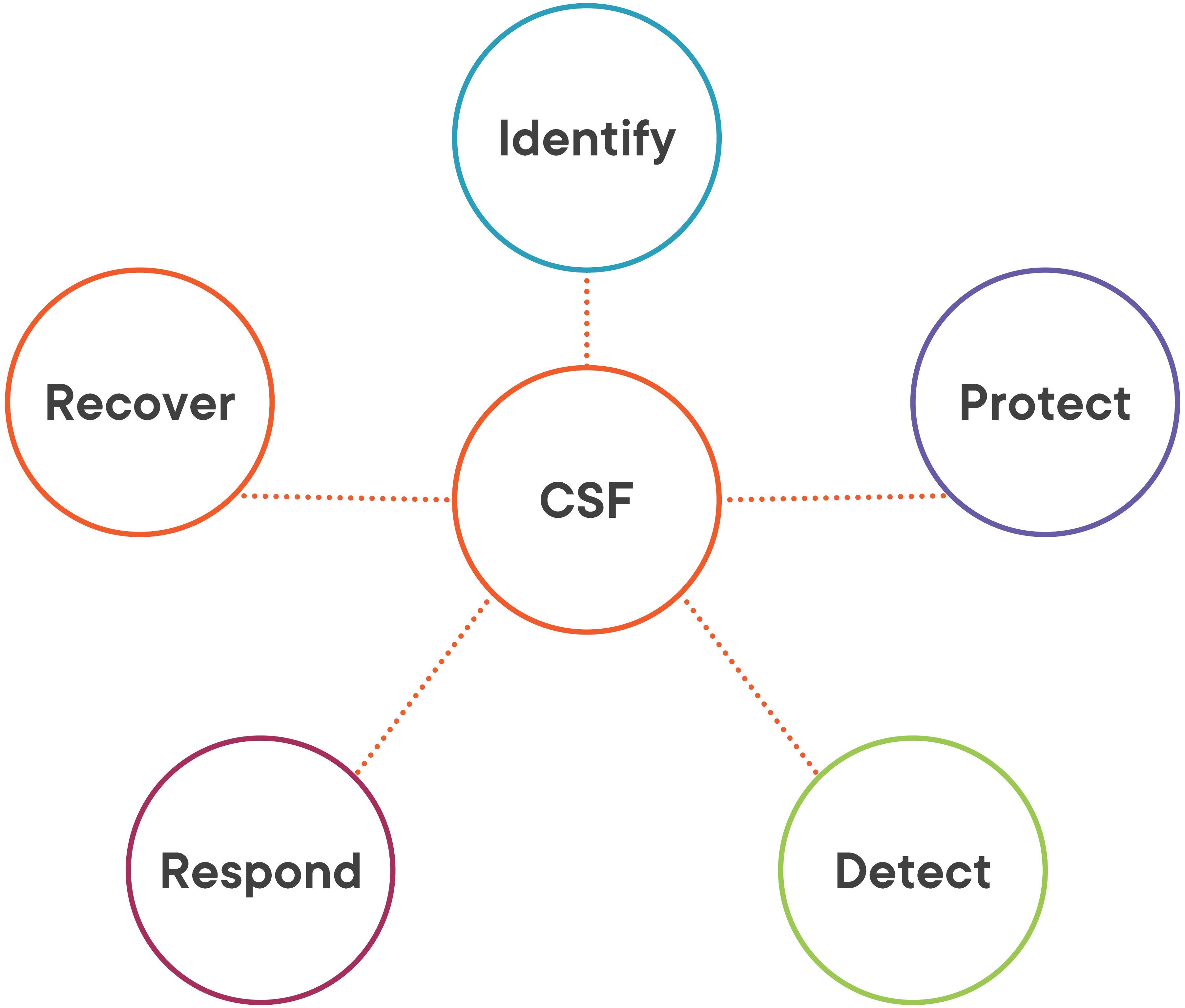
Includes default and custom checks

Automated or manual reporting

Search for high entropy strings or custom regex searches

Flexible reporting onscreen or to file

NIST Cybersecurity Framework



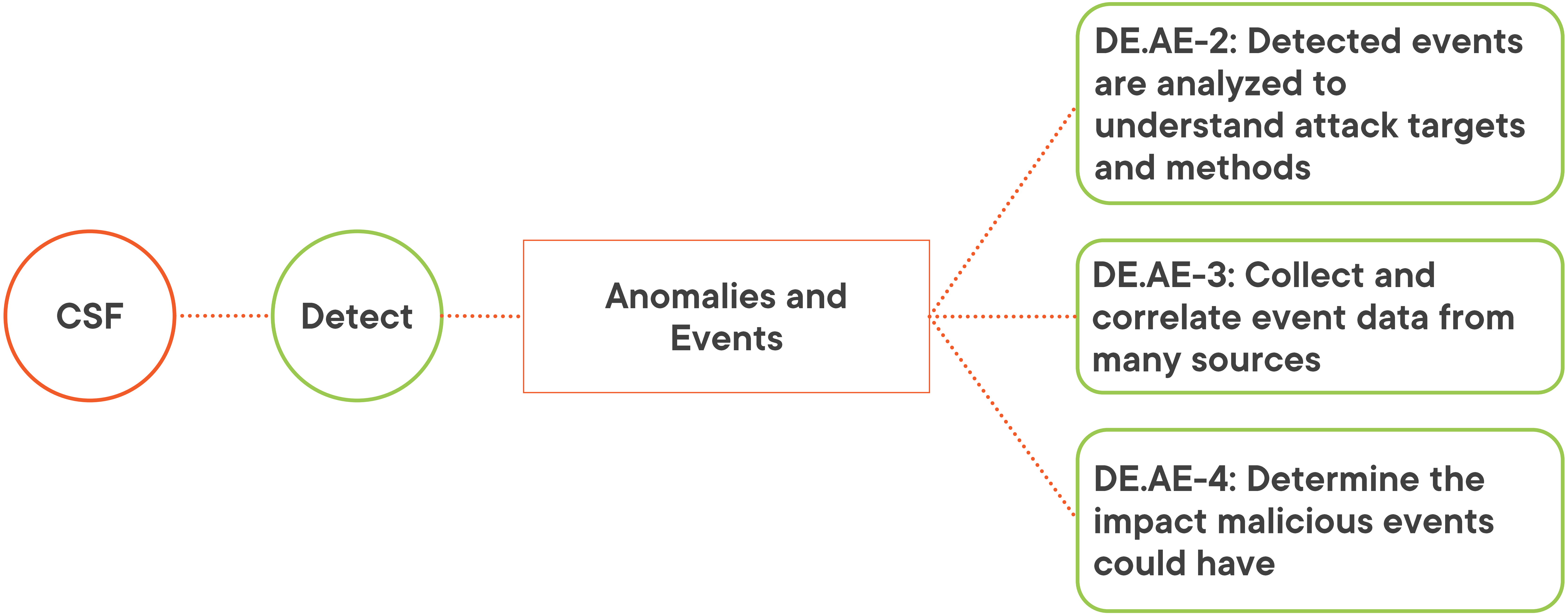
NIST Cybersecurity Framework

CSF

Detect

Anomalies and Events

NIST Cybersecurity Framework



CSF

Detect

Anomalies and Events

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.AE-3: Collect and correlate event data from many sources

DE.AE-4: Determine the impact malicious events could have

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

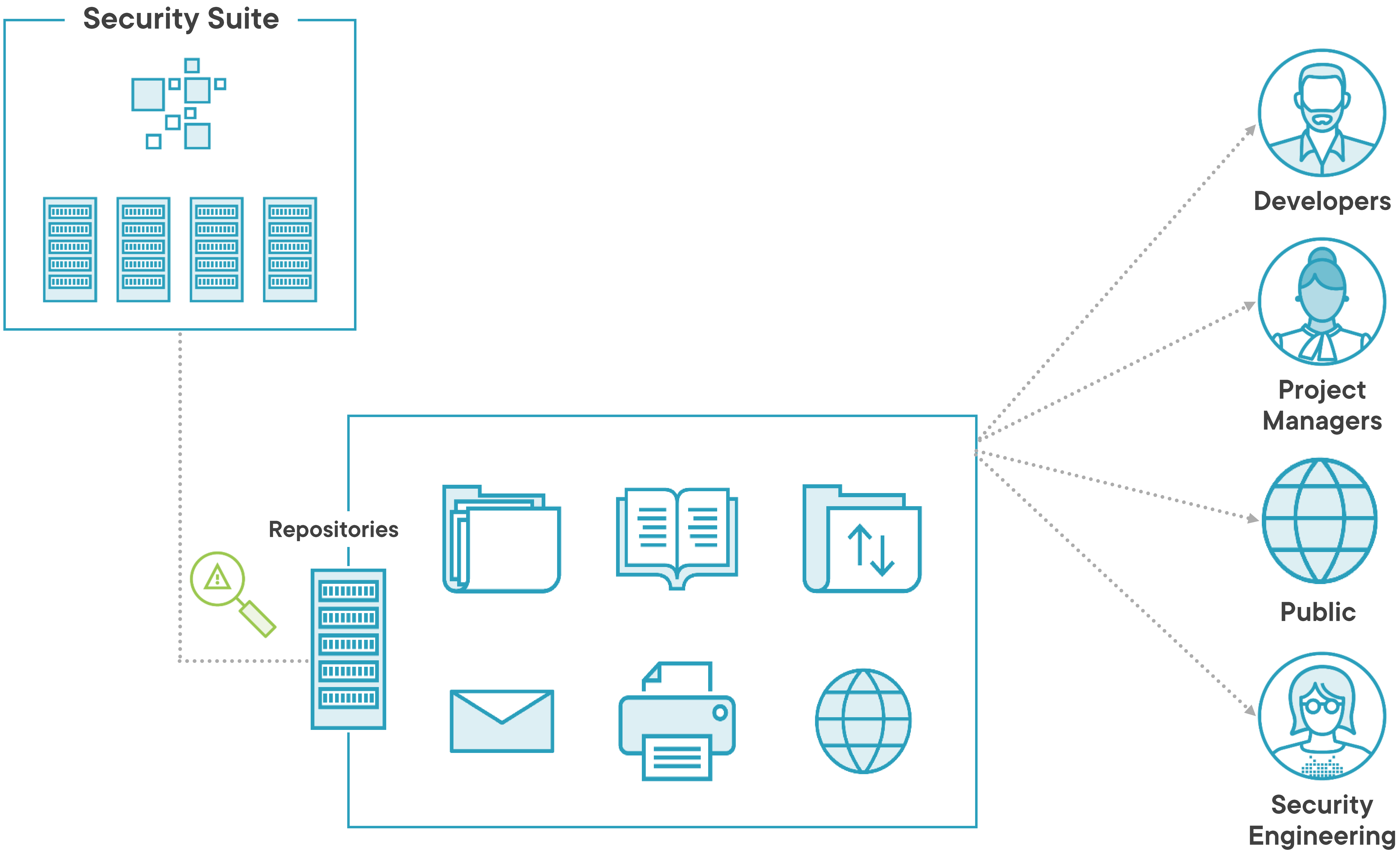
- Network Analysis
- OS Analysis
- Application Analysis
- Infrastructure Analysis
- **File Analysis**
- Threat Intelligence
- Incident Management

T1552:
Unsecured Credentials

MITRE SHIELD

T1552:
Unsecured Credentials

DTE0012 – Decoy Credentials: Create user credentials that are used for active defense. (DUC0084)



Security Suite

Repositories

Developers

Project Managers

Public

Security Engineering

Perform manual runs (security)

Perform automated runs (devops)

TruffleHog needs access to your git repositories to perform assessments.

Installation details are available on the TruffleHog GitHub page.

KEY TAKEAWAYS

Exposed Credentials

Develop ability to detect credentials and secrets

Attacker Motivations

Understand attackers techniques and persistence

Cybersecurity

Is a challenging but rewarding experience

Technology

TruffleHog is one of many tools that will aid the cybersecurity professional

The Dangers of Credentials in Code

Data Breaches

Lateral Movement

Privilege Escalation

Source Code in your Environment

Version Control

Package Management

Websites

File Sharing

Collaboration Tools

Commit History

Reasons credentials appear in Commit History

Developer

Correcting code, updates…

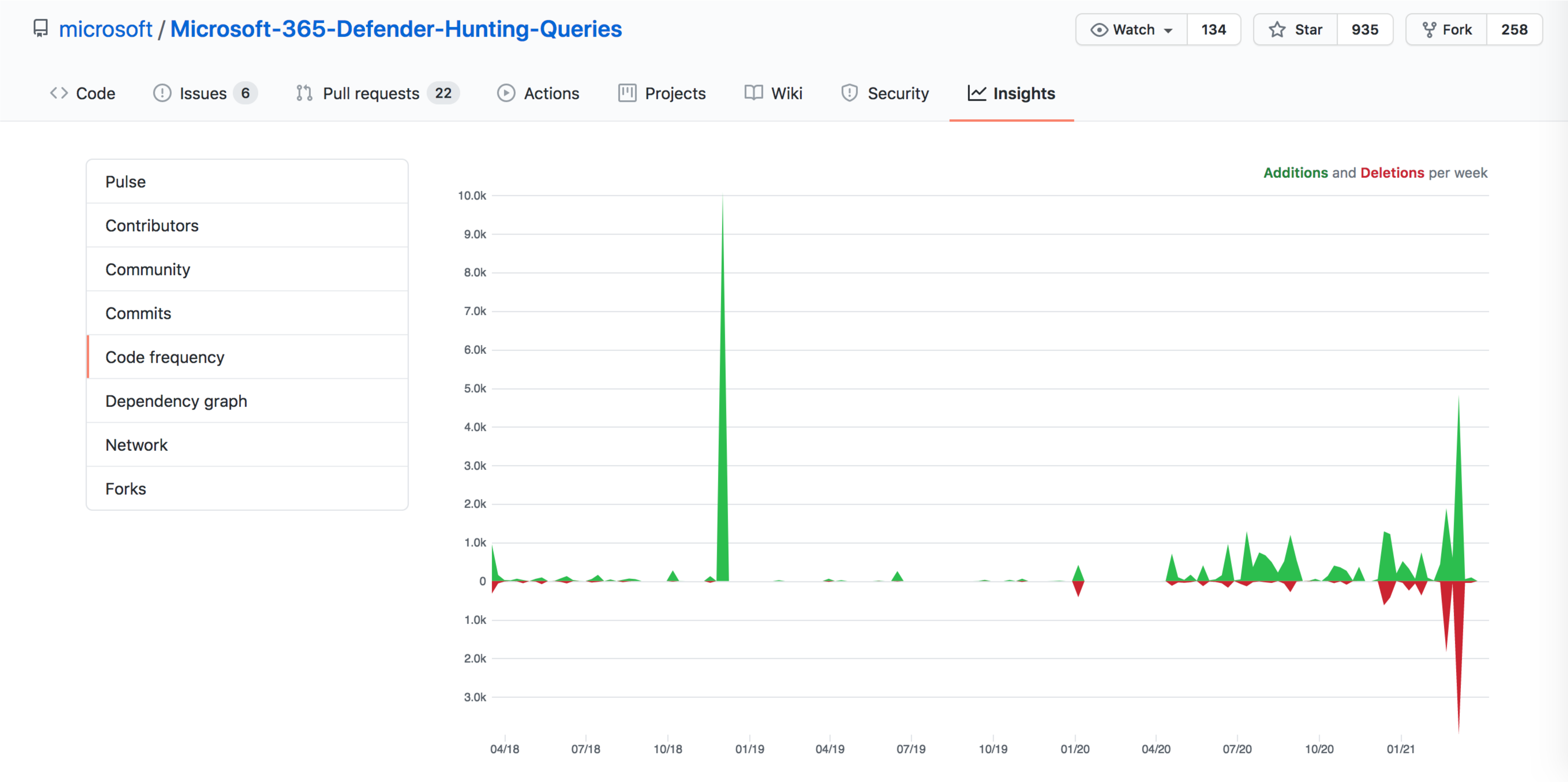
Legacy Features

Product updates, replacing old tech…

Code Reviews

Removing insecure code, dev notes…

Code Additions and Deletions



Preventing Exposed Credentials

Security Awareness

Code Reviews

Training

General Remediation Actions

Remove Code

Edit and remove credentials from code

Disable Credentials

Disable accounts so they cannot be used

Review Settings

Secure the repo, set to private

Rotate Credentials

Changing a password from old to new

Incident Response

Manage security incidents

Public vs Private Repositories

Public

Open to the all, anyone with an Internet connection

Private

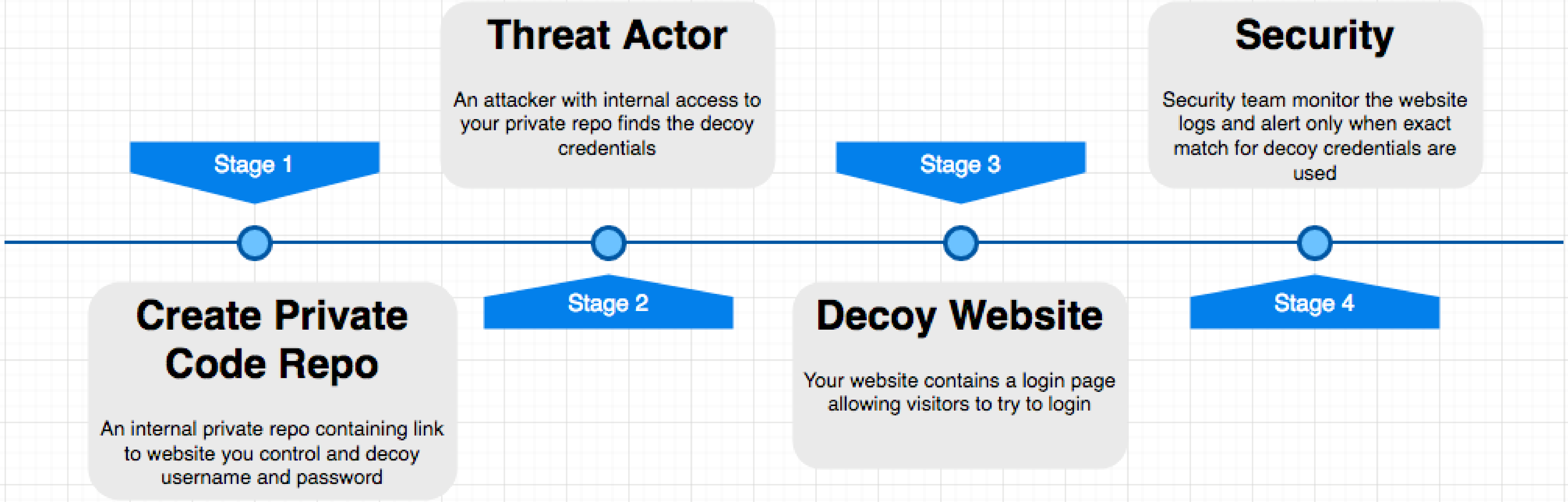
Restricted to organization members

Demo

Using decoy Credentials

Assessing for Credential Leakage

Active Defense



Stage 1

Create Private Code Repo

An internal private repo containing link to website you control and decoy username and password

Stage 2

Threat Actor

An attacker with internal access to your private repo finds the decoy credentials

Stage 3

Decoy Website

Your website contains a login page allowing visitors to try to login

Stage 4

Security

Security team monitor the website logs and alert only when exact match for decoy credentials are used

Demo

Custom search criteria using TruffleHog

Scenario: as a security engineer I want to detect Azure Storage Keys