Managing Your Red Team Operations with GHOSTWRITER

SO-CON 2020

Introduction

- Christopher Maddalena \ *@cmaddalena*
  - Managing Consultant at SpecterOps
  - Creator & Principal Developer of Ghostwriter
- Not Speaking:
  - Andrew Chiles \ *@andrewchiles*
    - Technical Director at SpecterOps
  - Daniel Heinsen \ *@hotnops*
    - Sr. Consultant at SpecterOps

Mini Agenda

- Ghostwriter Basics
- Wrangling Information
- Managing Infrastructure
- Activity logging
- Generating reports
- Q & A

What is Ghostwriter?

- Your team's dedicated scribe
- Manages essential assessment data
- Monitors and tracks infrastructure
- Provides reporting capabilities

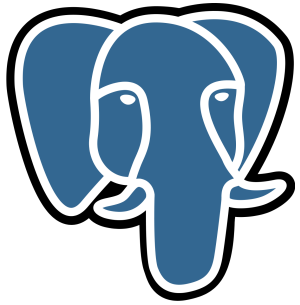
Ghostwriter v2.0 Release

AVAILABLE NOW

- New for SO-CON!
- This marks a new feature in v2.0

Ghostwriter Tech Stack

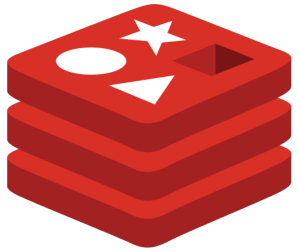
PostgreSQL



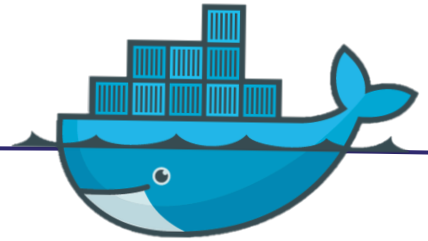
Django 3

Python 3.8

AMQP



HTTPS and Websockets



Docker

Managing Information

Using Ghostwriter to Distribute Project Information

Organizing Information

- Statement of Work
- Rules of Engagement
- Assessment Objectives
- Operator Assignments
- Call Notes

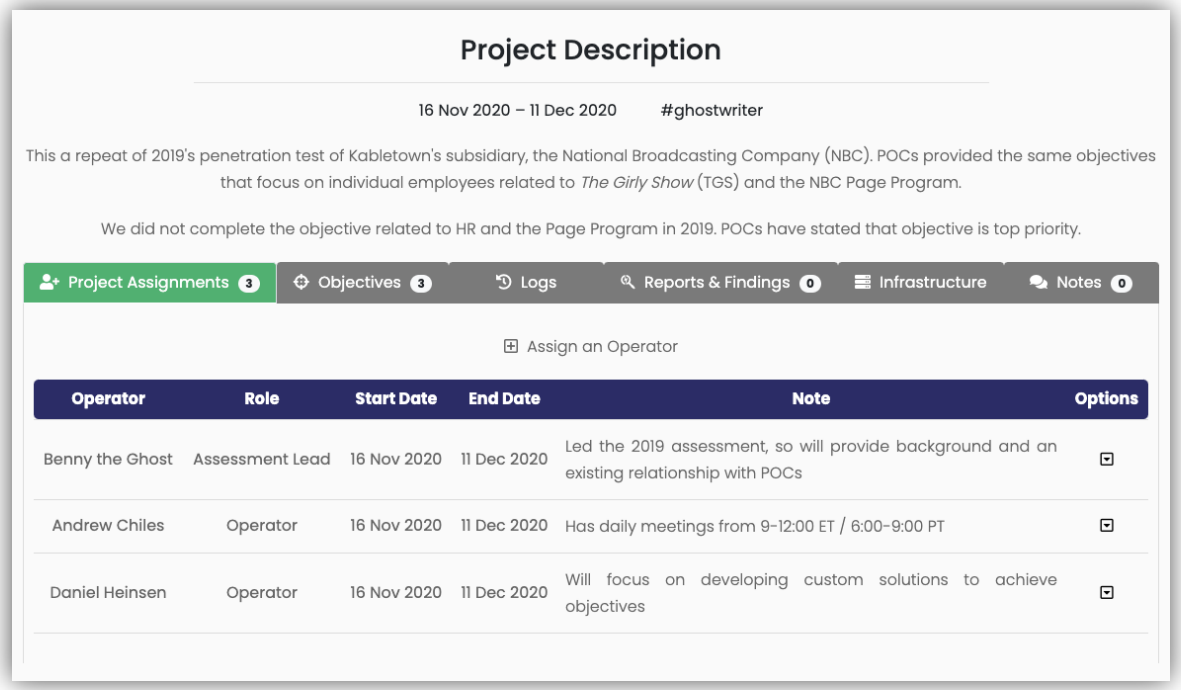
Build a Knowledge base

- Project information is only valuable if it is:
  - Readily accessible to all
  - Organized and consistent
  - Consolidated
  - Linked and tagged

Build a KNOWLEDGE BASE, not a filing cabinet

Developing a Project Dashboard

- Hub for execution information
- Linked for situational awareness
- One place for:
  - Project statuses
  - Access to activity logs
  - Infrastructure tracking



Tending to Your Flock

Being a Good Infrastructure Shepherd

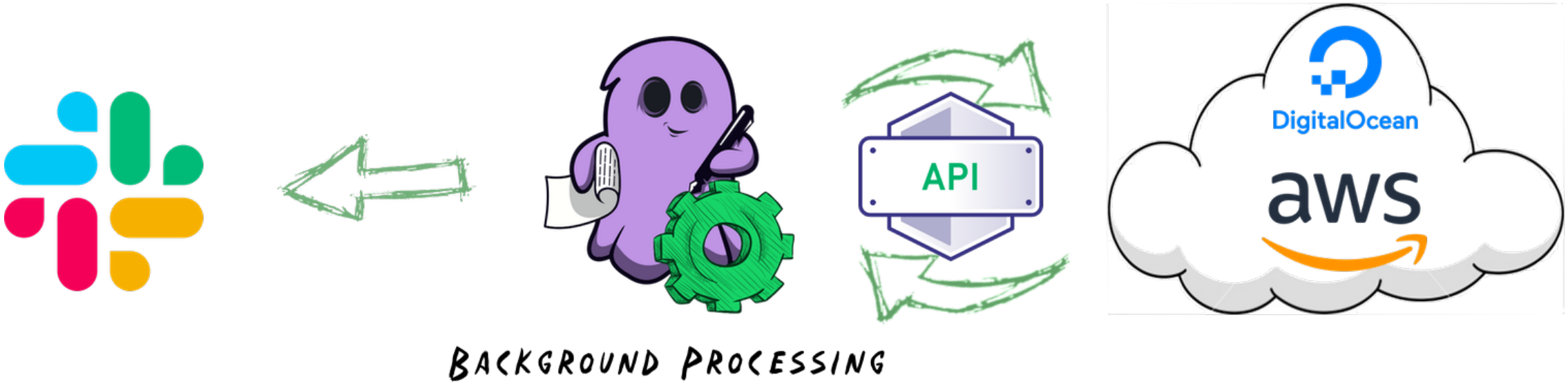
Managing Infrastructure

- Be a good shepherd
- Projects depend on it
- The effects outlast the project
- Must be *consistent*

Keep Tabs on All Your Assets

- Domains
- Servers you own
- Servers in the cloud
- CDN endpoints
- Cloud storage (Coming Soon)

Ghostwriter’s Eyes on the Sky



Overwatch & Logging

Keeping an Eye on OPSEC & Activity

New Asynchronous Events

- Support for Websockets
- Global messaging and alerting
- Groundwork for the REST API

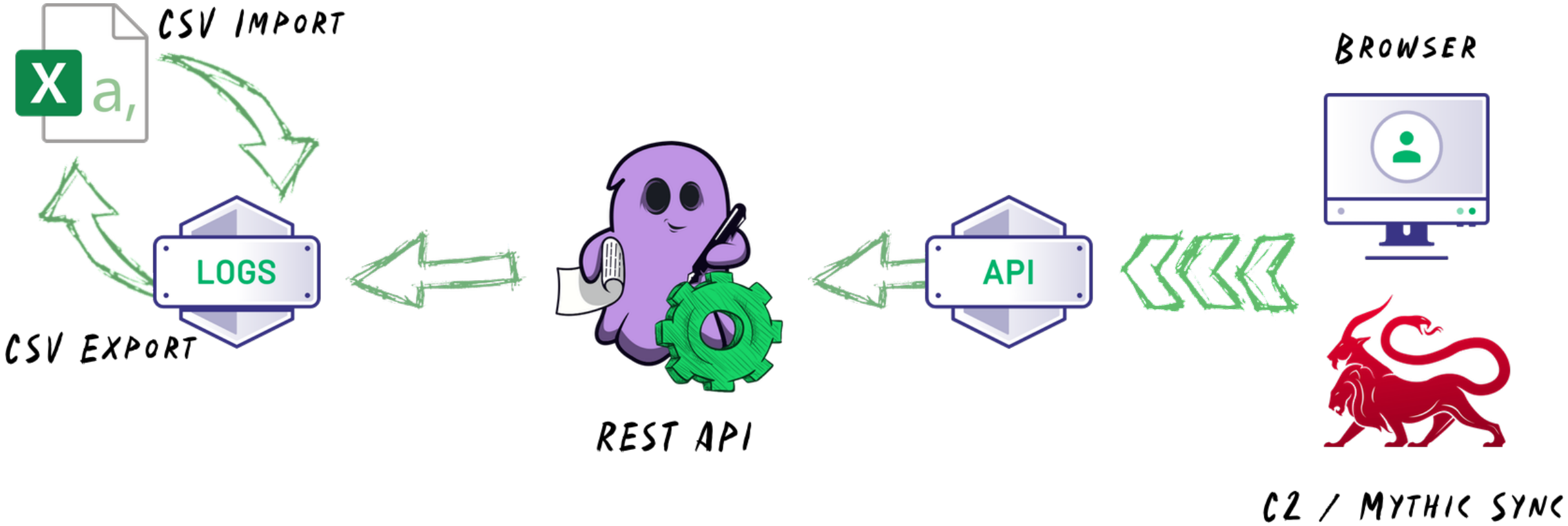
Watching Your Back

- Leverage historical data
- Basic sanity checks
- Catch avoidable OPSEC blunders

Activity Logs & You

- Need to answer questions
- Need to deconflict
- Tool logging can fail

Automated Logging

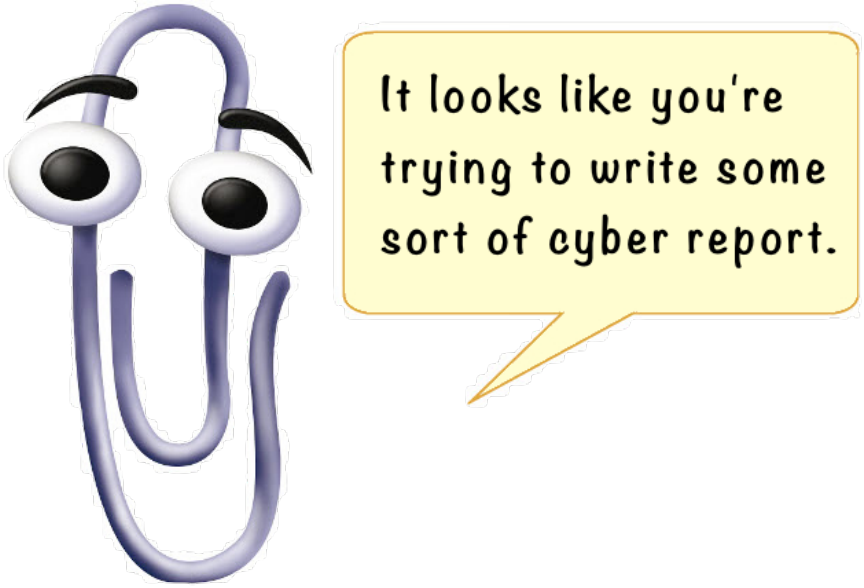


Leveling-up Reporting

Enable Operators to Focus on the Technical Details

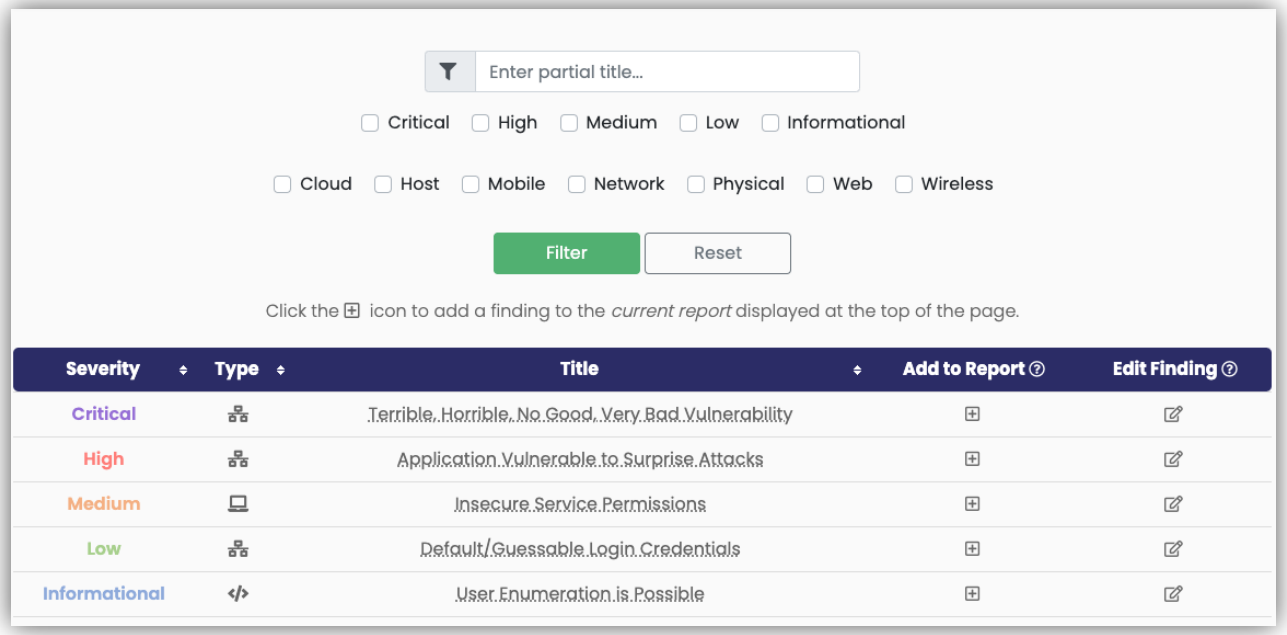
Building Reports Efficiently & Consistently

- Maintain template reports
- Maintain a finding library
- Maintain a style guide
- Maintain consistency



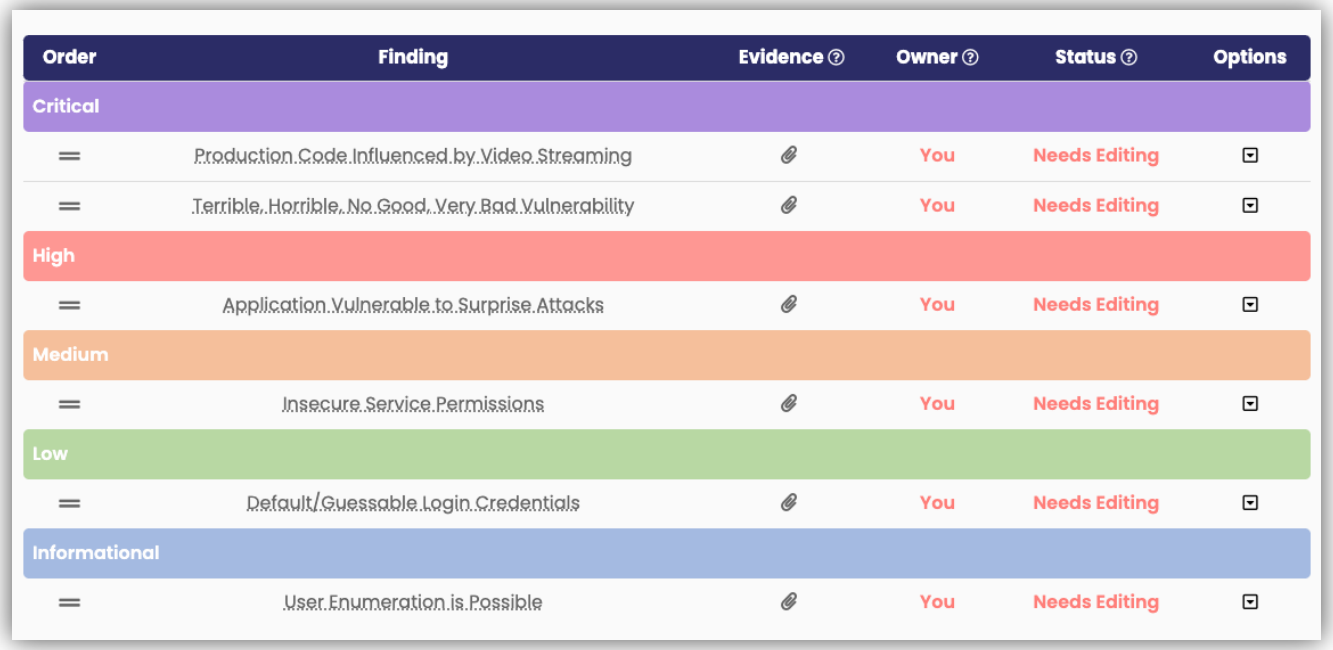
Curate Your Findings

- Maintain a master library
- Add styling and formatting
- Avoid copy/paste oversights
- Create copies for reports



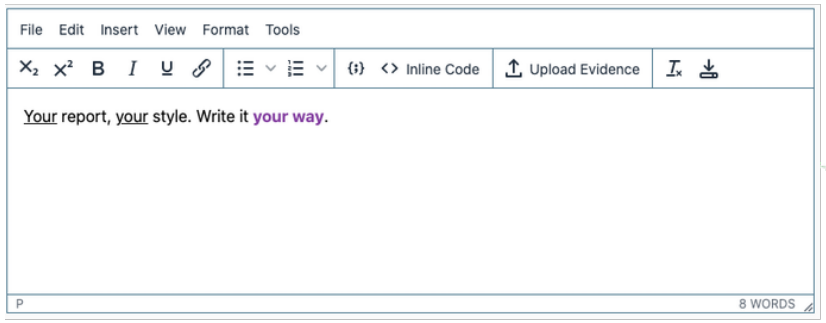
Collaborative Reporting

- Simple management
- Organize with drag n’ drop
- Assign tasks to the team
- Attach evidence files

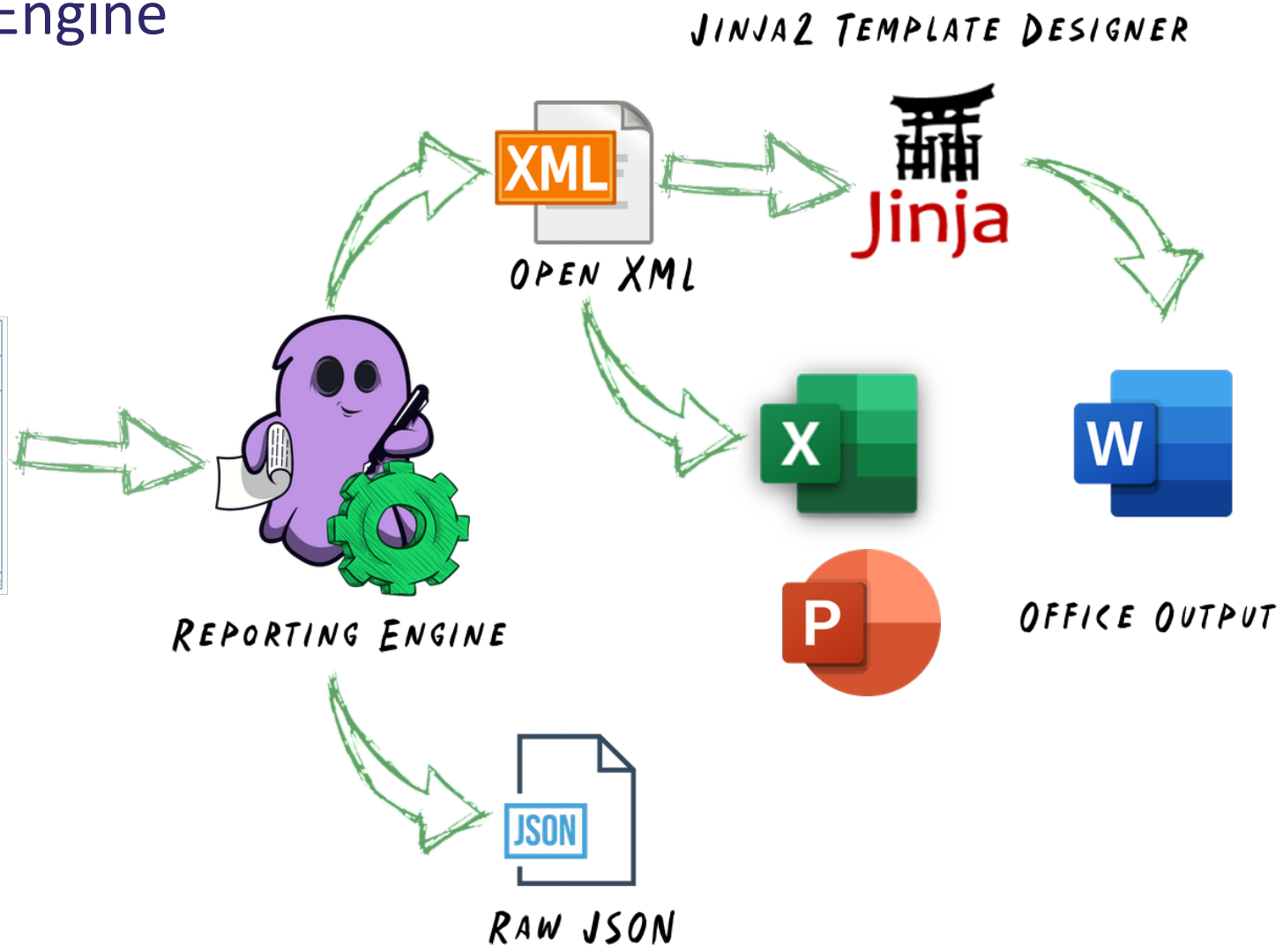


Order	Finding	Evidence	Owner	Status	Options
Critical					
=	Production Code Influenced by Video Streaming		You	Needs Editing	
=	Terrible, Horrible, No Good, Very Bad Vulnerability		You	Needs Editing	
High					
=	Application Vulnerable to Surprise Attacks		You	Needs Editing	
Medium					
=	Insecure Service Permissions		You	Needs Editing	
Low					
=	Default/Guessable Login Credentials		You	Needs Editing	
Informational					
=	User Enumeration is Possible		You	Needs Editing	

Ghostwriter's Reporting Engine



WYSIWYG EDITOR



Report Templates

- Create document templates
- Maintain consistency
- Share improvements and changes
- Reduce time spent on formatting

Status	Doc Type	Name	Client	Options
Ready	docx	Demo Template	Kabletown	
Ready	docx	Default Word Template	--	
Ready	pptx	Default PowerPoint Template	--	

You Can Be a Reporting Ninja2

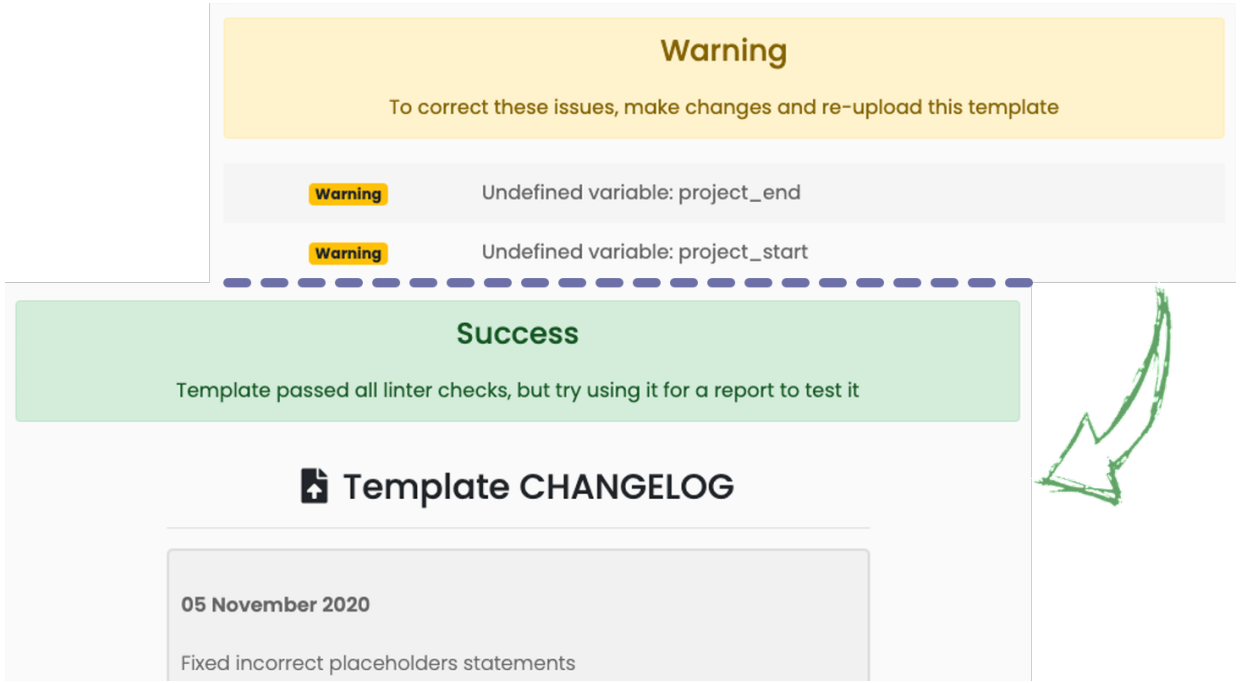
- Full templatization with Jinja2
- Custom variables and filters

```
{% for finding in report %}
    {{ finding.title }}
    …
{% endfor %}
```

From WYSIWYG to Word

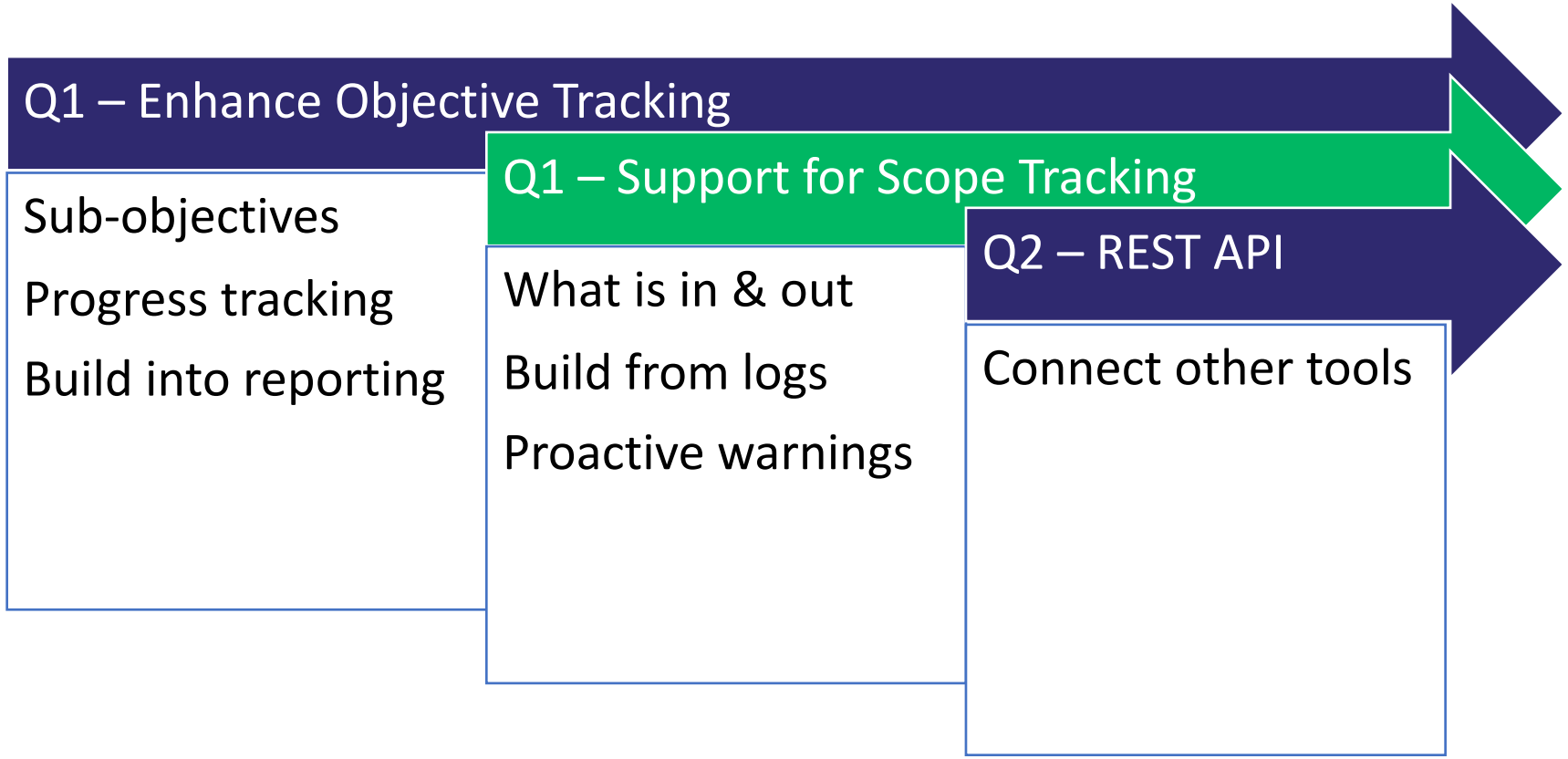
Template Linter

- Vet new templates with a linter
- Be warned of potential issues
- Understand the results
- Use *{% debug %}* to troubleshoot



Wrap-Up

Development Road Map



Wrap-up & Ghostwriter Resources

- Join us on Slack
  - *bloodhoundgang.herokuapp.com*
  - #ghostwriter & #reporting
- Remote Team Project Management
  - *getghostwriter.io/rtpm-presentation*

Thanks for Joining!

getghostwriter.io
@cmaddalena
#ghostwriter