

Managing Your Red Team Operations with *GHOSTWRITER*

SO-CON 2020

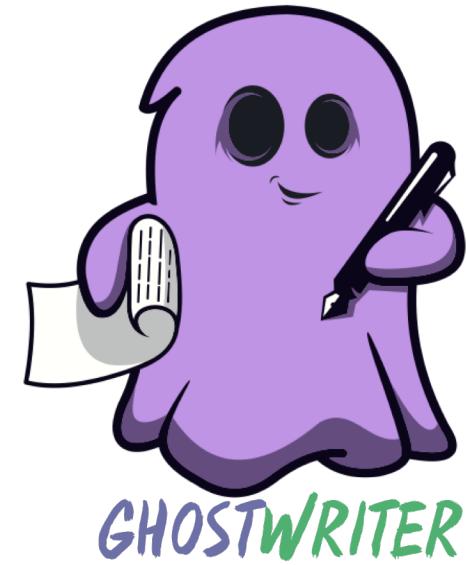
Introduction

- 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

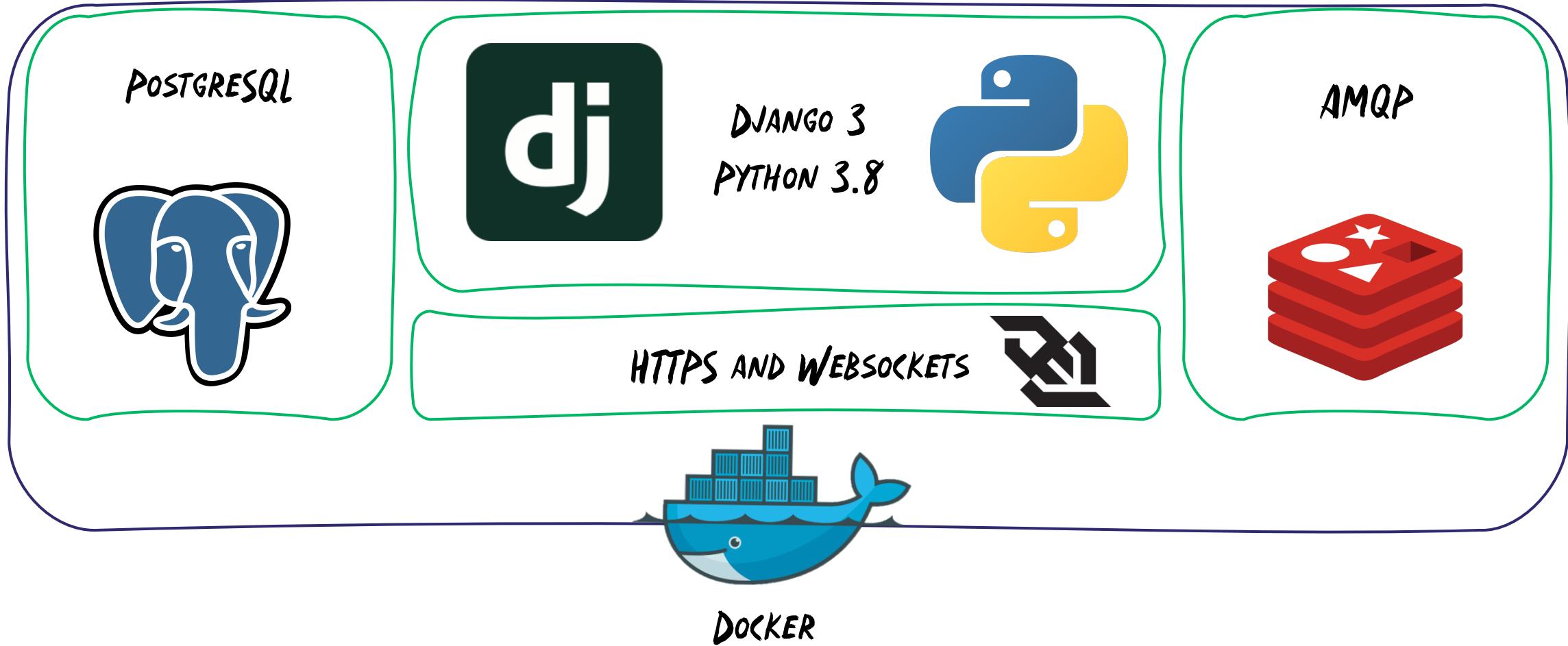
AVAILABLE NOW

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





Ghostwriter Tech Stack



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

Project Description

16 Nov 2020 – 11 Dec 2020 #ghostwriter

This is a repeat of 2019's penetration test of Kabletown's subsidiary, the National Broadcasting Company (NBC). POCs provided the same objectives that focus on individual employees related to *The Girly Show* (TGS) and the NBC Page Program.

We did not complete the objective related to HR and the Page Program in 2019. POCs have stated that objective is top priority.

Project Assignments	Objectives	Logs	Reports & Findings	Infrastructure	Notes
3	3		0		0

Assign an Operator

Operator	Role	Start Date	End Date	Note	Options
Benny the Ghost	Assessment Lead	16 Nov 2020	11 Dec 2020	Led the 2019 assessment, so will provide background and an existing relationship with POCs	<input type="checkbox"/>
Andrew Chiles	Operator	16 Nov 2020	11 Dec 2020	Has daily meetings from 9-12:00 ET / 6:00-9:00 PT	<input type="checkbox"/>
Daniel Heinsen	Operator	16 Nov 2020	11 Dec 2020	Will focus on developing custom solutions to achieve objectives	<input type="checkbox"/>

Tending to Your Flock

Being a Good Infrastructure Shepherd

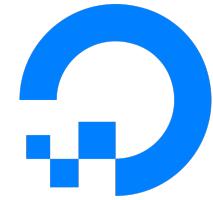
Managing Infrastructure

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



Keep Tabs on All Your Assets

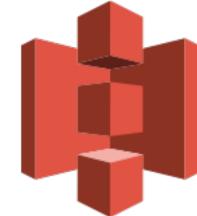
- Domains
- Servers you own
- Servers in the cloud
- CDN endpoints
- Cloud storage (Coming Soon)



DigitalOcean



Amazon
EC2



amazon
S3



Ghostwriter's Eyes on the Sky



BACKGROUND PROCESSING

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





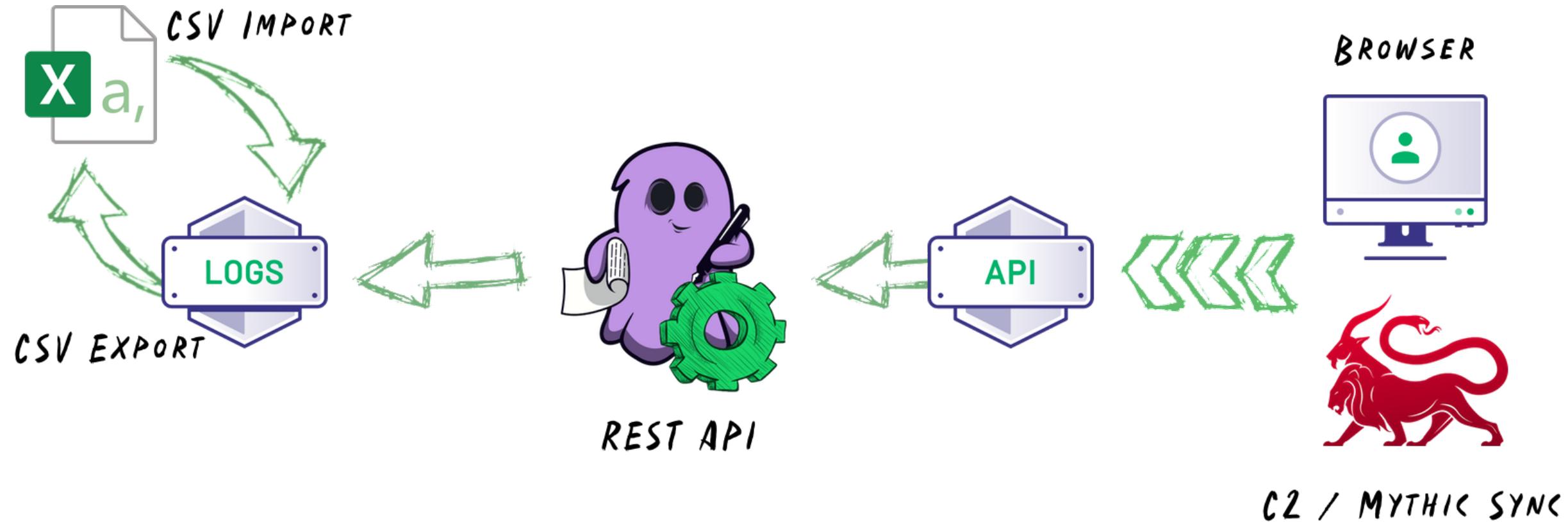
Activity Logs & You

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





Automated Logging

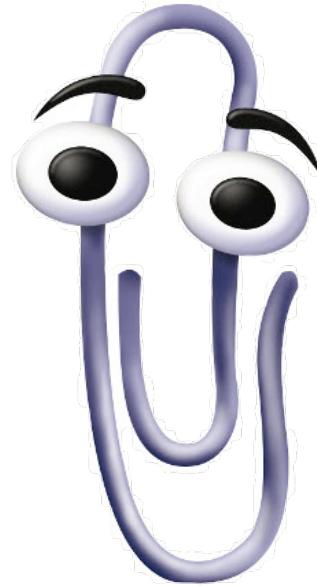


Leveling-up Reporting

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



It looks like you're trying to write some sort of cyber report.

Curate Your Findings

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

The screenshot shows a user interface for managing security findings. At the top, there is a search bar with a magnifying glass icon and the placeholder "Enter partial title...". Below the search bar are several filter buttons: Critical, High, Medium, Low, Informational, Cloud, Host, Mobile, Network, Physical, Web, and Wireless. There are also "Filter" and "Reset" buttons. A note below the filters says, "Click the icon to add a finding to the current report displayed at the top of the page." The main area is a table with the following data:

Severity	Type	Title	Add to Report	Edit Finding
Critical		.Terrible..Horrible..No.Good..Very.Bad.Vulnerability		
High		Application.Vulnerable.to.Surprise.Attacks		
Medium		Insecure.Service.Permissions		
Low		Default/Guessable.Login.Credentials		
Informational		User.Enumeration.is.Possible		

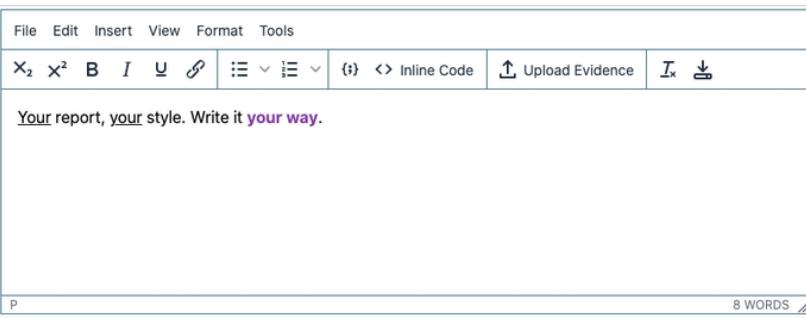


Collaborative Reporting

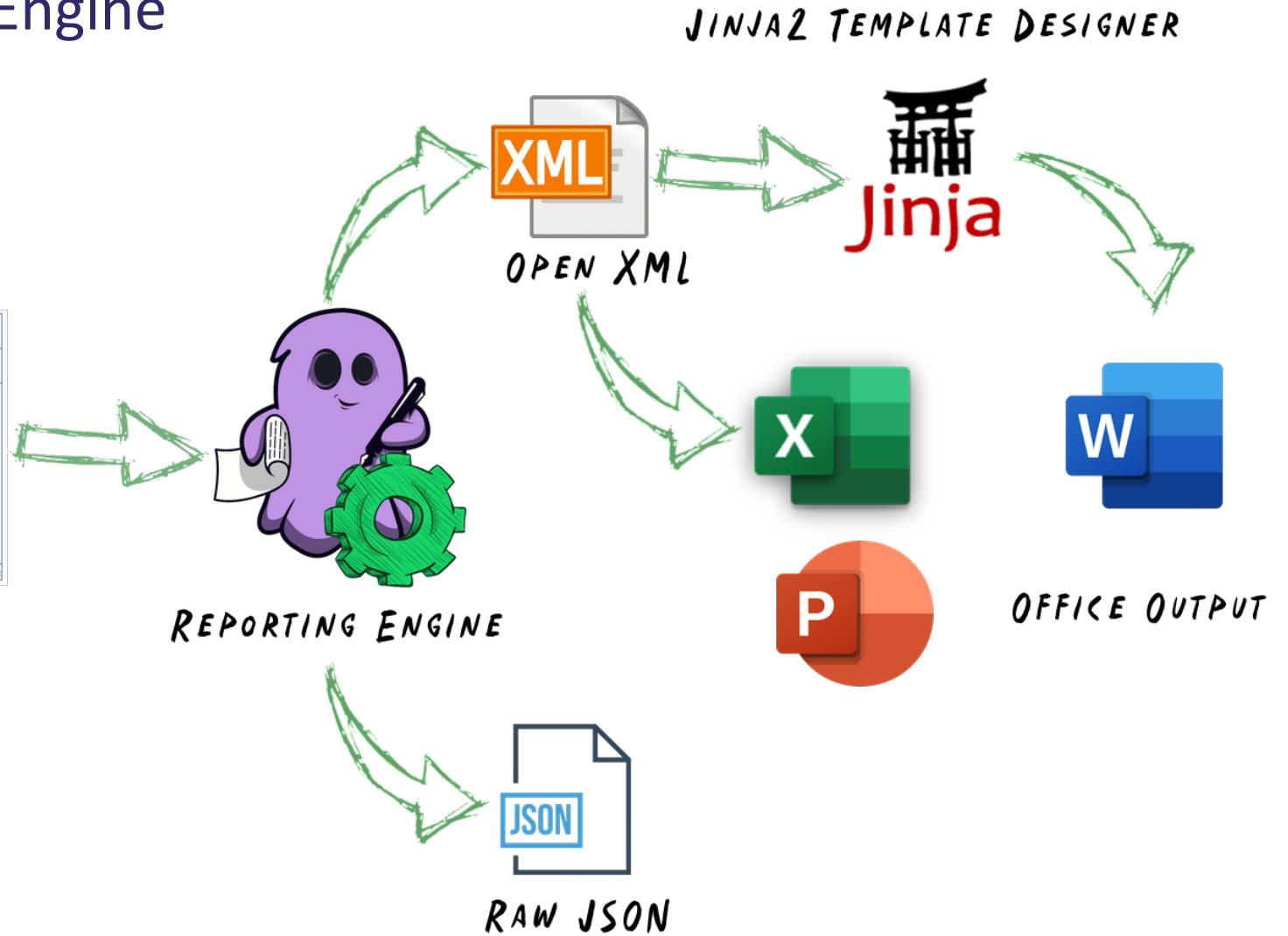
- Simple management
- Organize with drag n' drop
- Assign tasks to the team
- Attach evidence files

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

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	<input type="checkbox"/>
Ready	docx	Default.Word.Template	--	<input type="checkbox"/>
Ready	pptx	Default.PowerPoint.Template	--	<input type="checkbox"/>



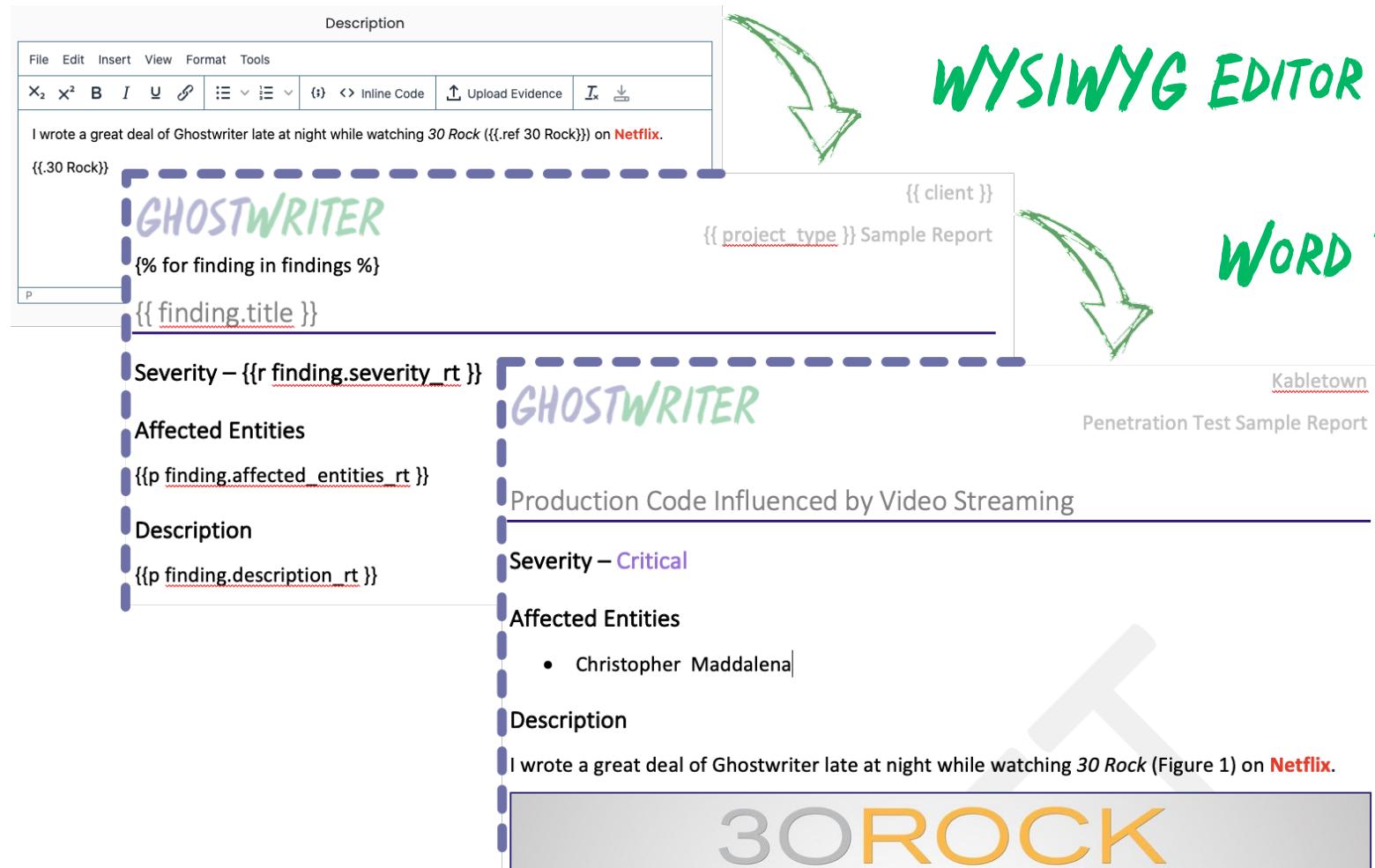
You Can Be a Reporting Ninja2

- 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

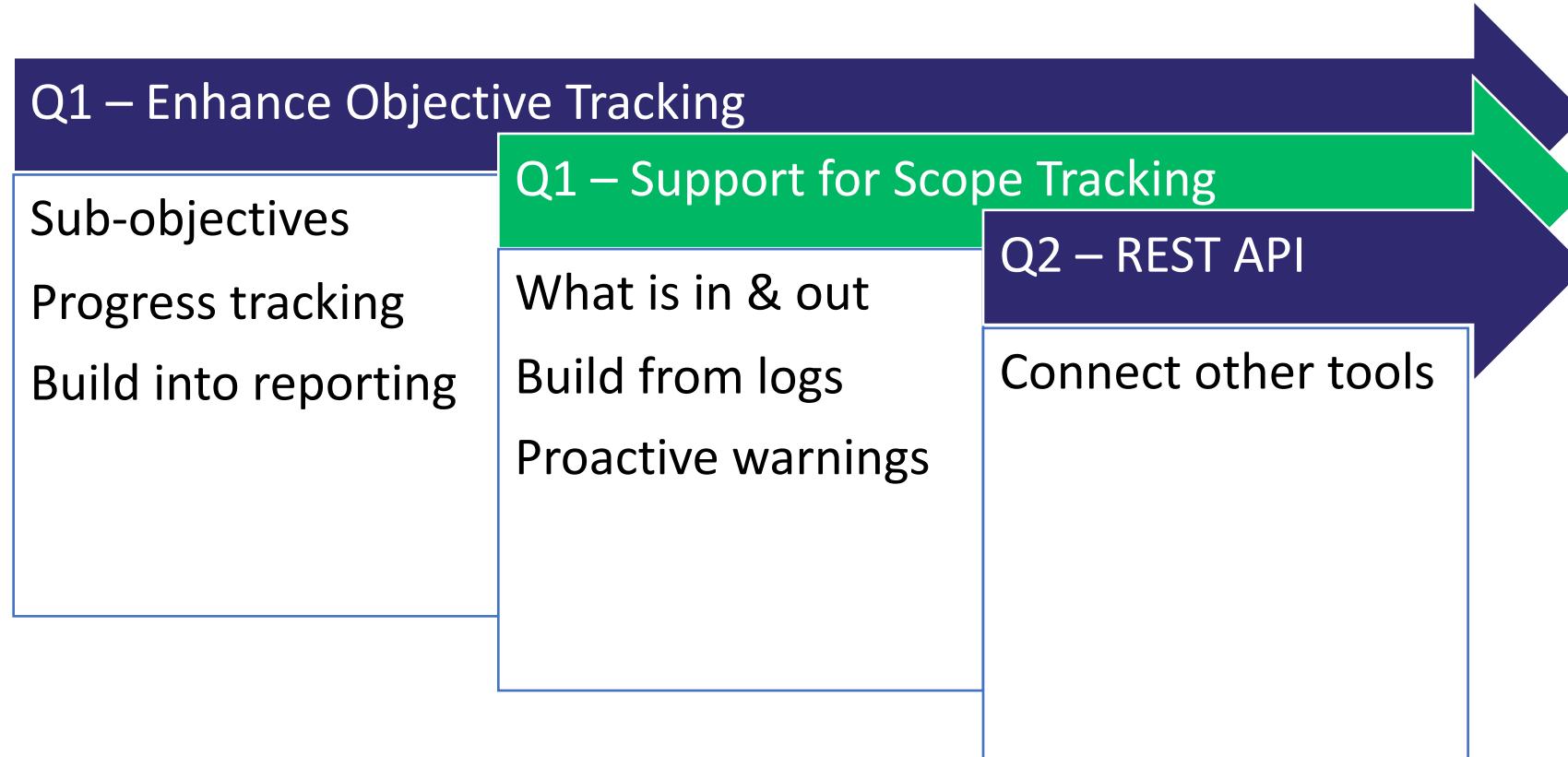
The screenshot shows a linter interface with the following sections:

- Warning**:
To correct these issues, make changes and re-upload this template
- Warning**: Undefined variable: project_end
- Warning**: Undefined variable: project_start
- Success**:
Template passed all linter checks, but try using it for a report to test it
- Template CHANGELOG**:
 - 05 November 2020
Fixed incorrect placeholders statements

A green hand-drawn style arrow points from the "Success" section down towards the changelog.

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