

Incident Response Playbooks

A New Open Source Resource

Bio

Mathieu Saulnier

Tech Director, Advanced Security
at Syntax(.com)

Core Mentor @BlueTeamVillage

Threat Hunting
Adversary Detection

Talks at : Derbycon, SANS, BTV,
NorthSec, SecTor & BSides

@ScoubiMtl



Agenda

How it Started

Current Free Playbooks

Our Hybrid Format

Our Current Playbooks

How to Contribute



Disclaimer



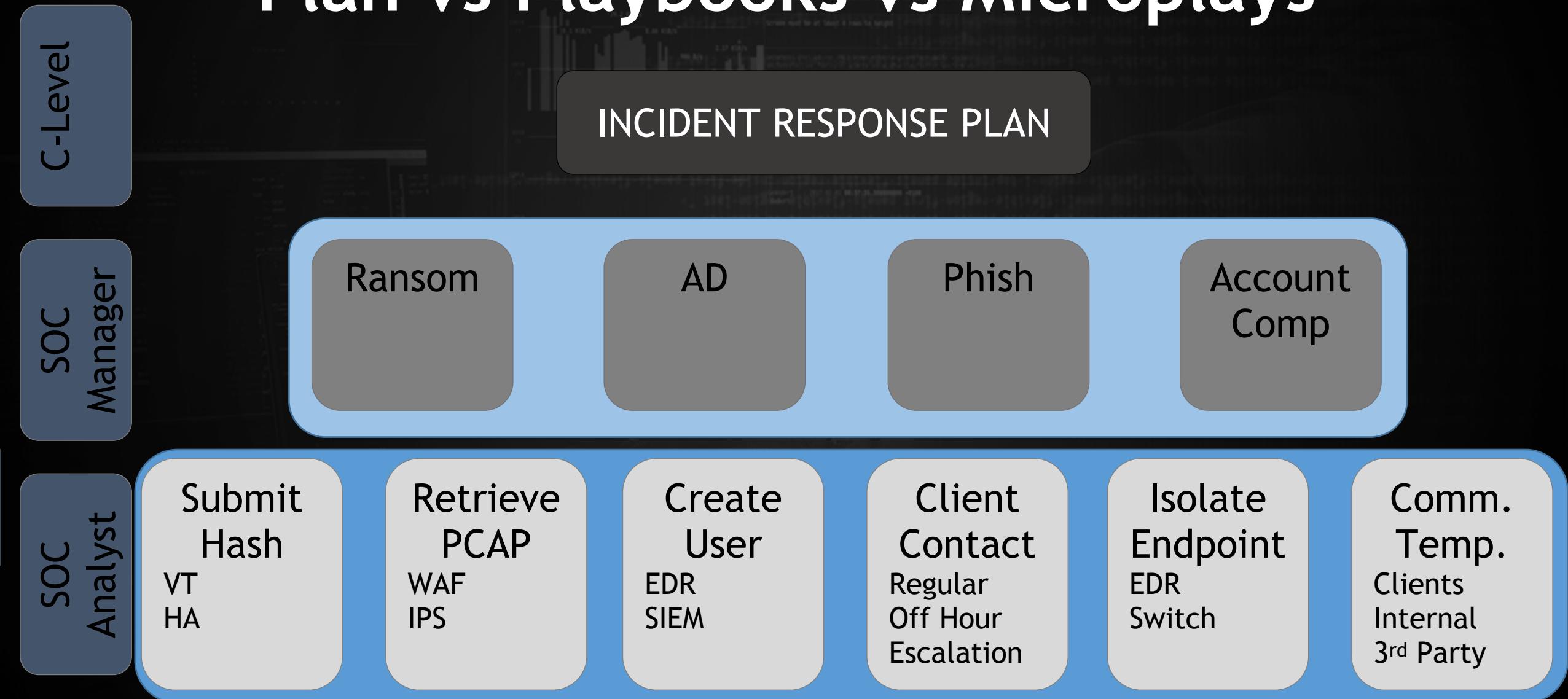
How it Started

New Position at Syntax



They Wanted Someone to Own IR
Hired July 2020
Asked Questions
SOC Analysts
SOC Management
Higher Management
Security Vendors
IR Plan
IR Playbooks
Microplays / WI

Plan vs Playbooks vs Microplays



Why IR Playbooks are Important

You don't plan while under stress

Improvisation will leave stones unturned

Might pull it off a few times if you have a large team

Do you know who to contact

For a DB compromised

At customer X

Current Free Playbooks



Société Générale

PDF

Windows Centric

More Procedure

No Edits in 5 Years

IRM

Preparation	1	Preparation	1	Containment	3
<p>Objective: Establish contacts, define procedures, gather information to save time during an attack.</p> <ul style="list-style-type: none">■ Create a list of all legitimate domains belonging to your company. This will help analysing the situation, and prevent you from starting a takedown procedure on a forgotten legitimate website.■ Prepare one web page hosted on your infrastructure, ready to be published anytime, to warn your customers about an ongoing phishing attack. Prepare and test a clear deployment procedure as well.■ Prepare takedown e-mail forms. You will use them for every phishing case, if possible in several languages. This will speed up things when trying to reach the hosting company etc. during the takedown process. <p>Internal contacts</p> <ul style="list-style-type: none">■ Maintain a list of all people involved in domain names registration in the company.■ Maintain a list of all people accredited to take decisions on cybercrime and eventual actions regarding phishing. If possible, have a contract mentioning you can take decisions. <p>External contacts</p> <ul style="list-style-type: none">■ Have several ways to be reached in a timely manner (24/7 if possible):<ul style="list-style-type: none">- E-Mail address, easy to remember for everyone (ex: security@yourcompany)- Web forms on your company's website (location of the form is important, no more than 2 clicks away from the main page)- Visible Twitter account■ Establish and maintain a list of takedown contacts in:<ul style="list-style-type: none">- Hosting companies- Registry companies- E-Mail providers■ Establish and maintain contacts in CERTs worldwide, they will probably always be able to help if needed. <p>Raise customer awareness</p> <p>Don't wait for phishing incidents to communicate with your customers. Raise awareness about phishing fraud, explain what phishing is and make sure your customers know you won't ever ask them for credentials/banking information by e-mail or on the phone.</p>	1	<p>Objective: Raise business line awareness</p> <p>People in business lines must be aware of phishing problems and consider security as a priority. Therefore, they should apply good practices such as avoid sending links (URL) to customers, and use a signature stating that the company will never ask them for credential/banking information online.</p>	1	<p>Objective: Mitigate the attack's effects on the targeted environment.</p> <ul style="list-style-type: none">■ Spread the URL of the attack in case of a phishing website. Use every way you have to spread the fraudulent URL on every web browser: use the options of Internet Explorer, Chrome, Safari, Firefox, Netcraft toolbar, Phishing-Initiative, etc. <p>This will prevent the users from accessing the website while you work on the remediation phase.</p> <ul style="list-style-type: none">■ Spread the fraudulent e-mail content on spam-reporting websites/partners.■ Communicate with your customers. <p>Deploy the alert/warning page with information about the current phishing attack.</p> <p>In case you are impacted several times a week, don't always deploy an alert/warning message but rather a very informative phishing page to raise awareness.</p> <ul style="list-style-type: none">■ Check the source-code of the phishing website.<ul style="list-style-type: none">- See where the data is exported: either to another web content you cannot access (a PHP script usually), or sent by e-mail to the fraudster.- Watch how the phishing-page is built. Do the graphics come from one of your legitimate website, or are they stored locally? <p>If possible, in case the graphics are taken from one of your own websites, you could change the graphics to display a "PHISHING WEBSITE" logo on the fraudster's page.</p>	3

Gov.scot

Scottish Government

PDF

Reviewed in 2020

Overlap

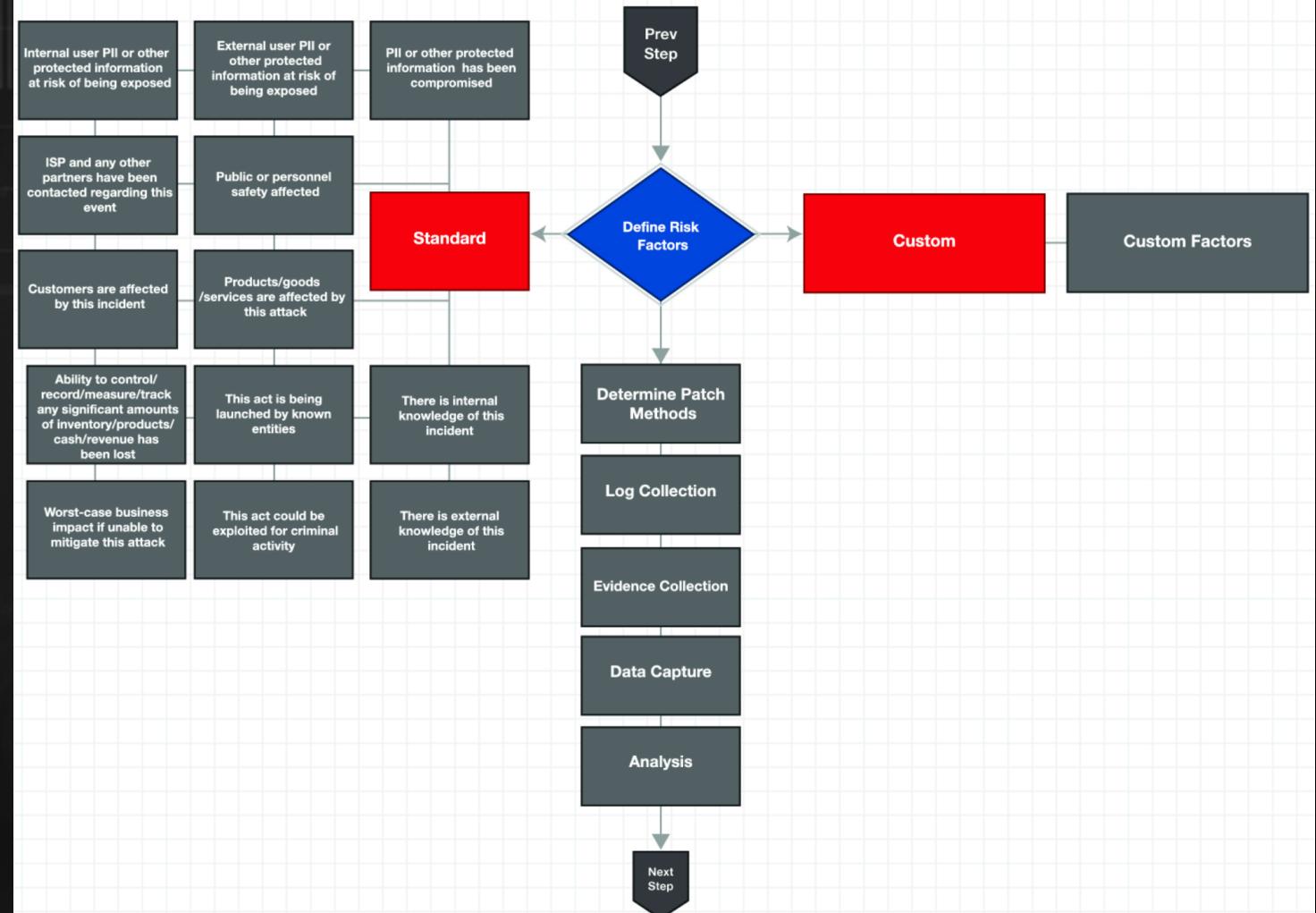
Workflow in the Annex

4. Analyse

Analysis Phase		
Phase objectives	Description	
Activity	Description	Stakeholders
Analyse the extent of the incident	The analysis phase has the following key objectives: <ul style="list-style-type: none">Analyse the cyber incident to uncover the scope of the attack;Identify and report potentially compromised data and the impact of such a compromise;Establish the requirement for a full forensic investigation;Develop a remediation plan based upon the scope and details of the cyber incident.	
	Activities may include, but are not limited to:	
	Engage technical staff from resolver groups.	<ul style="list-style-type: none">Information Security ManagerCore IT CIRTCIRT
	<p>Identify and research whether;</p> <ul style="list-style-type: none">Personal data is at risk (internal or external to the organisation);Other SENSITIVE data is at risk, <u>if so use the Data Loss Play-Book</u>;Public or personal safety is affected;Services are affected and what they are;You are able to control / record and measure critical systems;There is any evidence of who is behind the attack;There is internal knowledge behind the incident;The act could be exploited by criminals.	<ul style="list-style-type: none">Information Security ManagerCore IT CIRTCIRTResilience LeadBusiness Continuity LeadPolice Area Lead
	Determine patch methods.	<ul style="list-style-type: none">Information Security ManagerCore IT CIRT

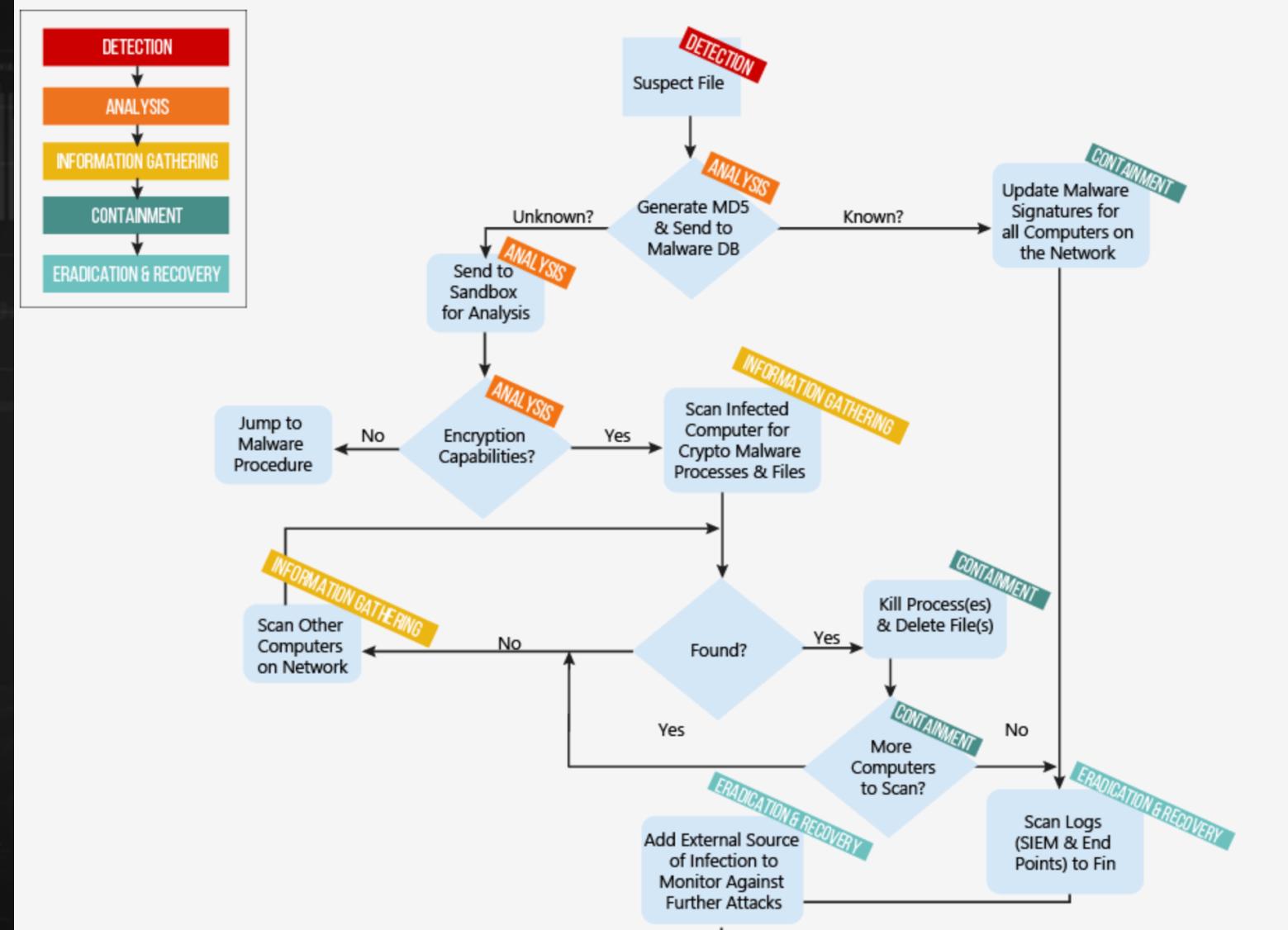
Incidentresponse .com

Consortium
PDF & Visio
9 Playbooks
All very similar
Flow chart



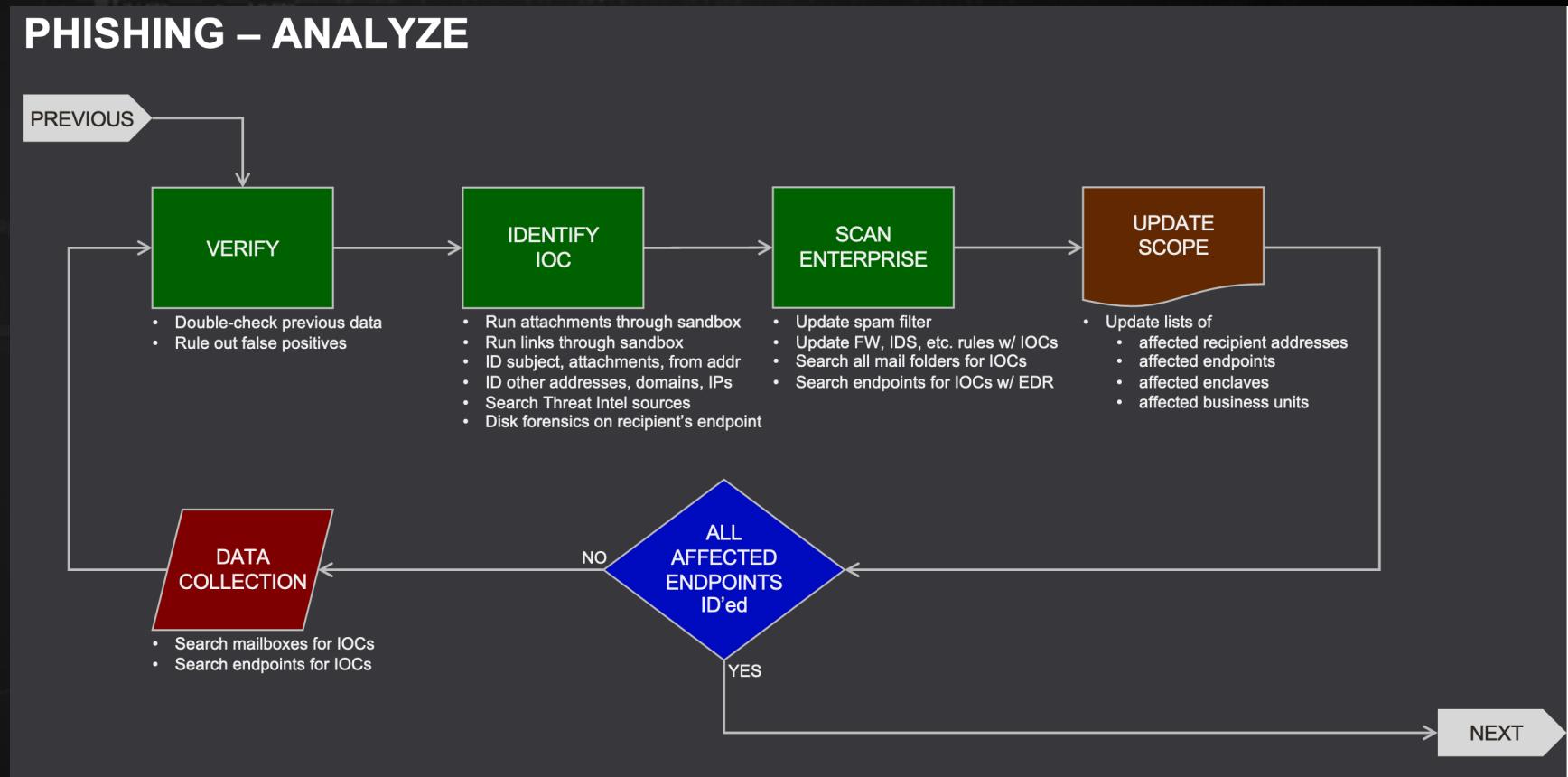
Ayehu.com

Part of Resolve (?)
Images
Limited Sample
High Level
Flow chart



Taksati

Chris Taylor
PowerPoint
Visio / Draw.io
Workflow with
details
Perfect level



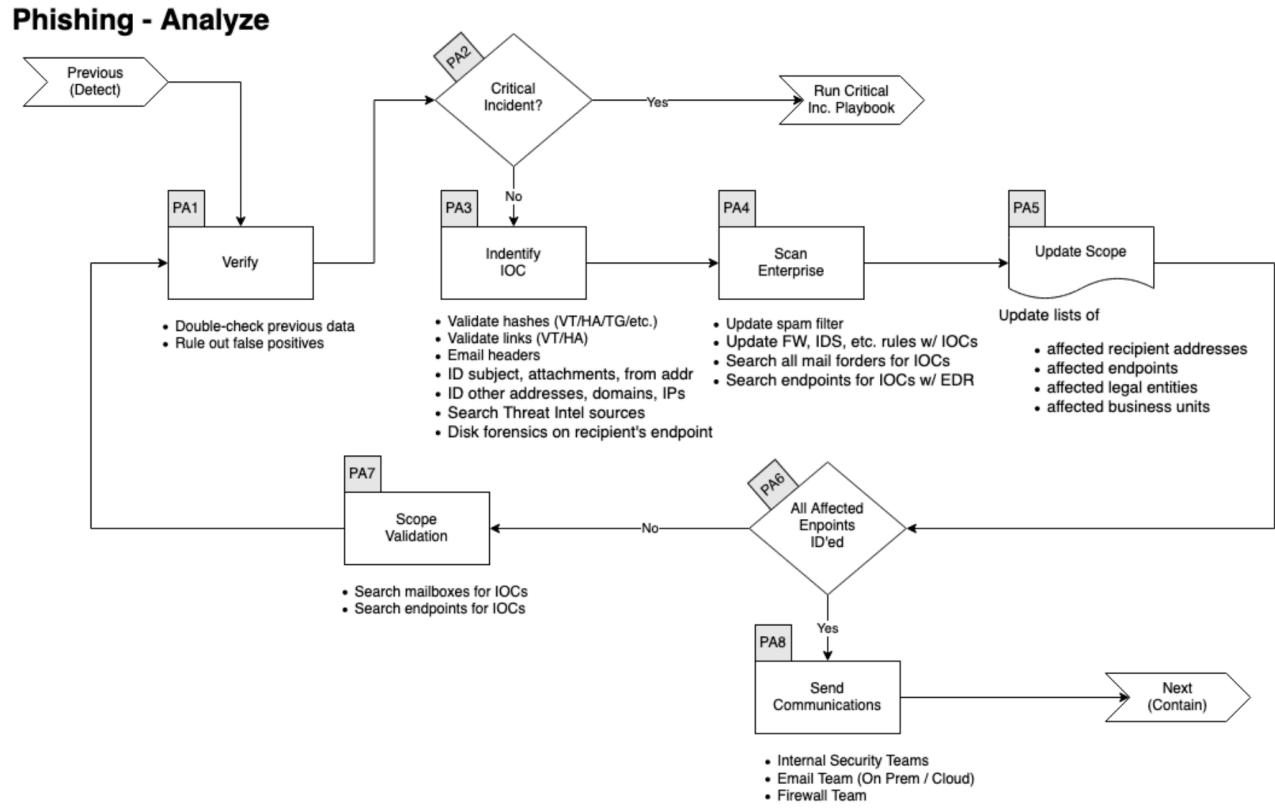




But there's Only
One

Syntax Playbooks

Git
Markdown / Draw.io
Open & Free
Easy to modify



Verify

▼ Expand/Collapse

In conjunction with a senior member of the ISOC

- Double check previous data
- Rule out False Positive

Identify IOCs

▼ Expand/Collapse

- Validate hashes
 - VirusTotal
 - Hybrid Analysis
- Validate links
 - VirusTotal
 - Hybrid Analysis
 - URLScan

@atc_project
Modular
Open Source
Framework
Lack real content

RE&CT

The screenshot shows the RE&CT web application. The top navigation bar is blue with the text "RE&CT". Below it is a dark sidebar with the following structure:

- INTRODUCTION**
 - RE&CT Framework (EN)
 - RE&CT Framework (RU)
- Response Stages**
 - Preparation
 - Identification
 - Containment
- Eradication**
 - RA4001: Report incident to external companies
 - RA4101: Remove rogue network device
 - RA4201: Delete email message
 - RA4301: Remove file
 - RA4501: Remove registry key
 - RA4502: Remove service
 - RA4601: Revoke authentication credentials
 - RA4602: Remove user account

Docs » Eradication » Response Actions » RA4501: Remove registry key

Title	Remove registry key
ID	RA4501
Description	Remove a registry key
Author	your name/nickname/twitter
Creation Date	YYYY/MM/DD
Category	Configuration
Stage	RS0004: Eradication
References	<ul style="list-style-type: none">https://example.com
Requirements	<ul style="list-style-type: none">DN_zeek_conn_log

Workflow

Description of the workflow for single Response Action in markdown format.
Here newlines will be saved.

Austin Songer

[github.com/austinsonger/
Incident-Playbook](https://github.com/austinsonger/Incident-Playbook)

Playbook for every MITRE
Technique

Exercise Scenarios that
can be used for training
purposes

Credential Access	T1110	Brute Force	Password Spraying	IaaS, Linux, Office 365, SaaS, Windows, macOS	User
-------------------	-------	-------------	-------------------	---	------

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Ensure that workstations and servers are logging to a central location
4. Verify that authentication attempts to systems and applications are being logged
5. Set up network segmentation and firewalls to limit access to systems and services
6. Make use of multi-factor authentication
7. Establish and enforce a secure password policy

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

TODO: Expand investigation steps, including key questions and strategies, for <Type of Incident>.

1. Monitor for:
 - a. Failed login attempts for default and common account names
 - b. Failed login attempts for the same account across multiple systems
 - c. Failed login attempts to multiple systems from the same source
2. Investigate and clear ALL alerts associated with the impacted assets

Demo Time!



gitlab.com/syntax-ir/playbooks/

Create a new Playbook

Folder & Files

To create a new Playbook:

- Create a new folder ex: IRP-DDoS
- Create a file called README.md inside your new folder
- Paste the content of IRP-TEMPLATE.md
- Replace the string -NAME- for your playbook name ex: DDoS in all the document
- Edit the sections.

Workflows

To create the Workflows

- Inside your new folder create a folder called Workflows
- Open the file WORKFLOW-TEMPLATE.drawio in [Draw.io](#)
- Save locally until you have completed all the tabs
- Once all the tabs/phases are completed, upload a copy to your new Workflows folder
- Use the File → Export as → PNG function of Draw.io to save each diagram phase separately
 - Make sure you Unchecked Include a copy of the diagram
 - Click Export
 - Save locally
- Upload each .PNG file to your new Workflows folder

Sub Folders

Products

This folder contains information about the various “commercial” products we use during an incident.

Tools

This folder contains information about the various free/online tools we use during an incident.

How To Contribute

Clone/Fork the Repo

Add, Modify Contents

Use Templates

Submit PR

Build Pipelines

CI/CD

Draw.io automation

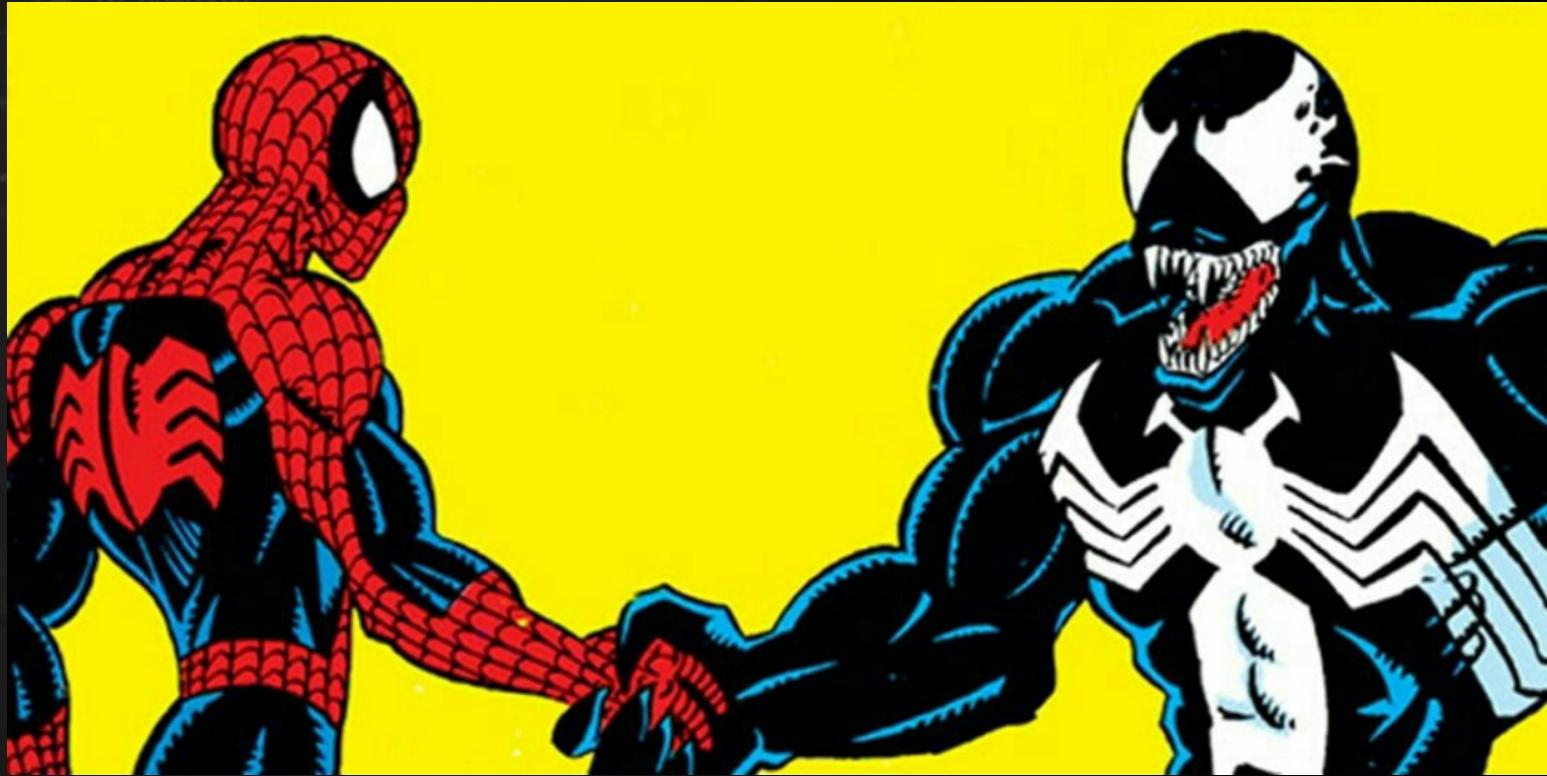
Become a Maintainer

Sharing is Caring

Let's play a game!

Rules

- Not your Employer
- The first that comes to mind



Stronger Together



Thank You!

Mathieu Saulnier
@ScoubiMtl

