Security Automation for Phishing Alerts

Automating triage and incident response of phishing alerts

Manual Work

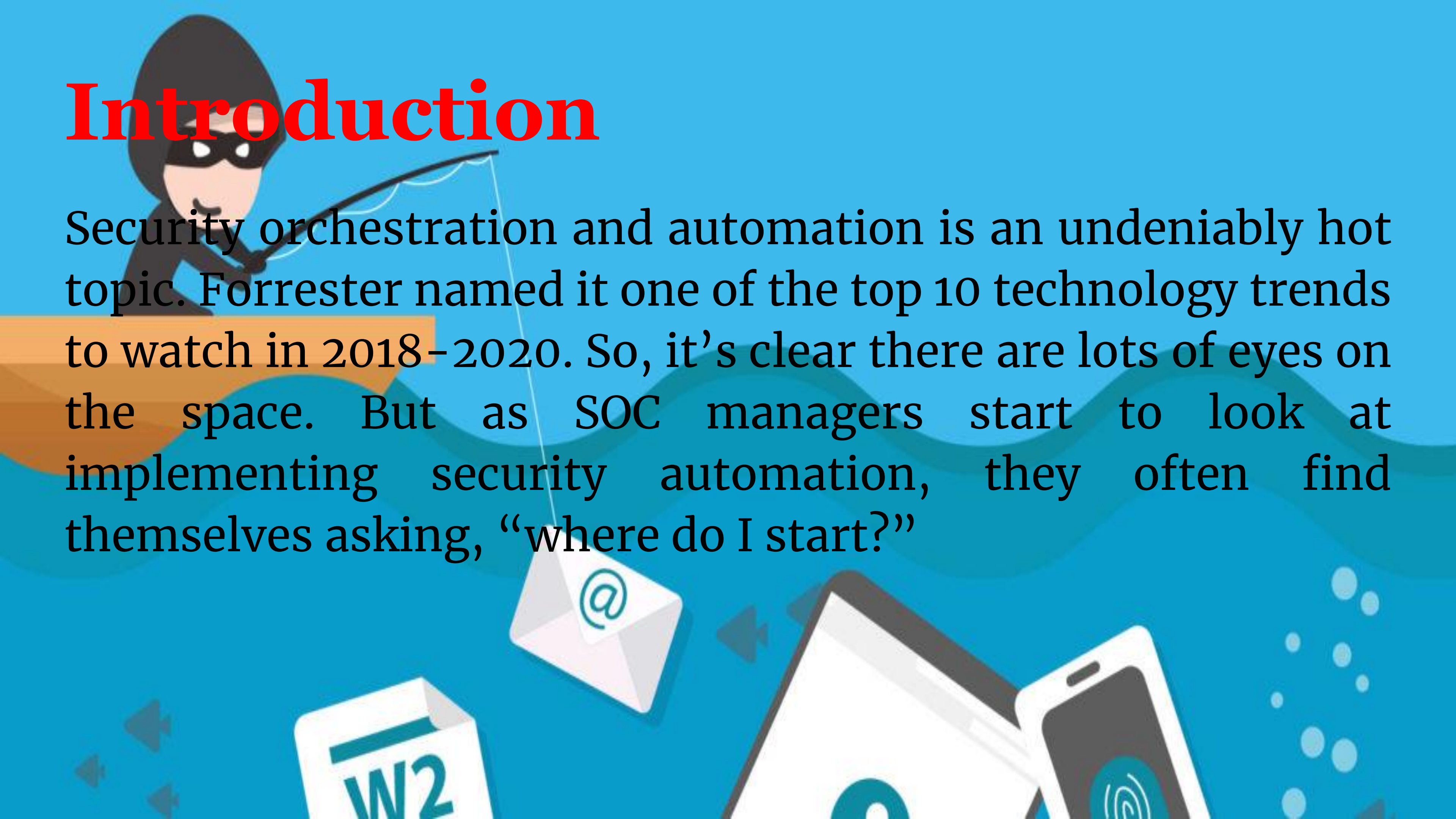
Fast Response

Low Alert Fidelity

User Involvement

Introduction

Security orchestration and automation is an undeniably hot topic. Forrester named it one of the top 10 technology trends to watch in 2018-2020. So, it's clear there are lots of eyes on the space. But as SOC managers start to look at implementing security automation, they often find themselves asking, "where do I start?"



All Security Alerts

Welcome to the first of our four-part blog series where we will take a look at the steps to automate some of the most common SOC processes. We will provide practical guides to automating steps that are part of managing, investigating and responding to alerts related to:

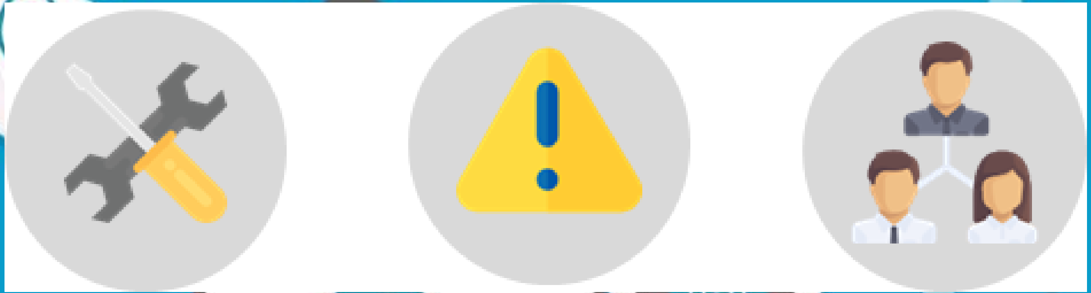
- Phishing
- Malware
- DLP
- Account misuse

Security Automation

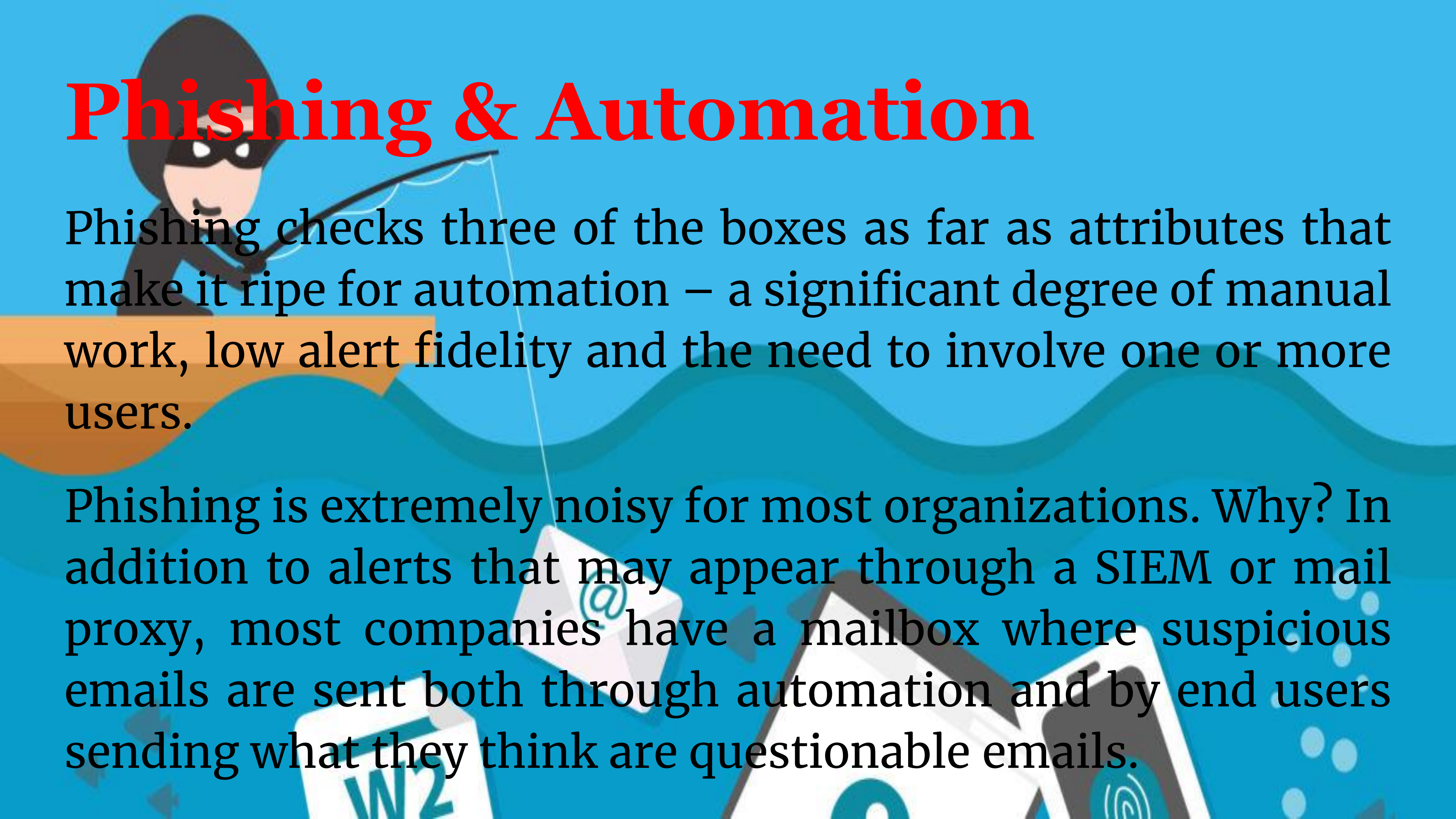
Finding opportunities for automation in a SOC isn’t hard; multiple areas can benefit substantially from it. Anything that involves a lot of manual work, requires fast response, has low alert fidelity and/or requires involving an end user is a prime candidate for security automation. Automating tasks that fit these categories can save precious security analyst time that can be refocused on higher value activities like threat hunting and…gasp!…actual analysis.

Why Phishing

A seemingly simple but malicious email can be the prelude to a more sinister threat. In fact, 91% of cyberattacks start with a phishing email. Also, phishing is arguably the top attack vector, accounting for 90-95% of all successful cyber attacks world wide. Because a phishing email can lead to a much larger attack, phishing alerts demand the utmost attention.



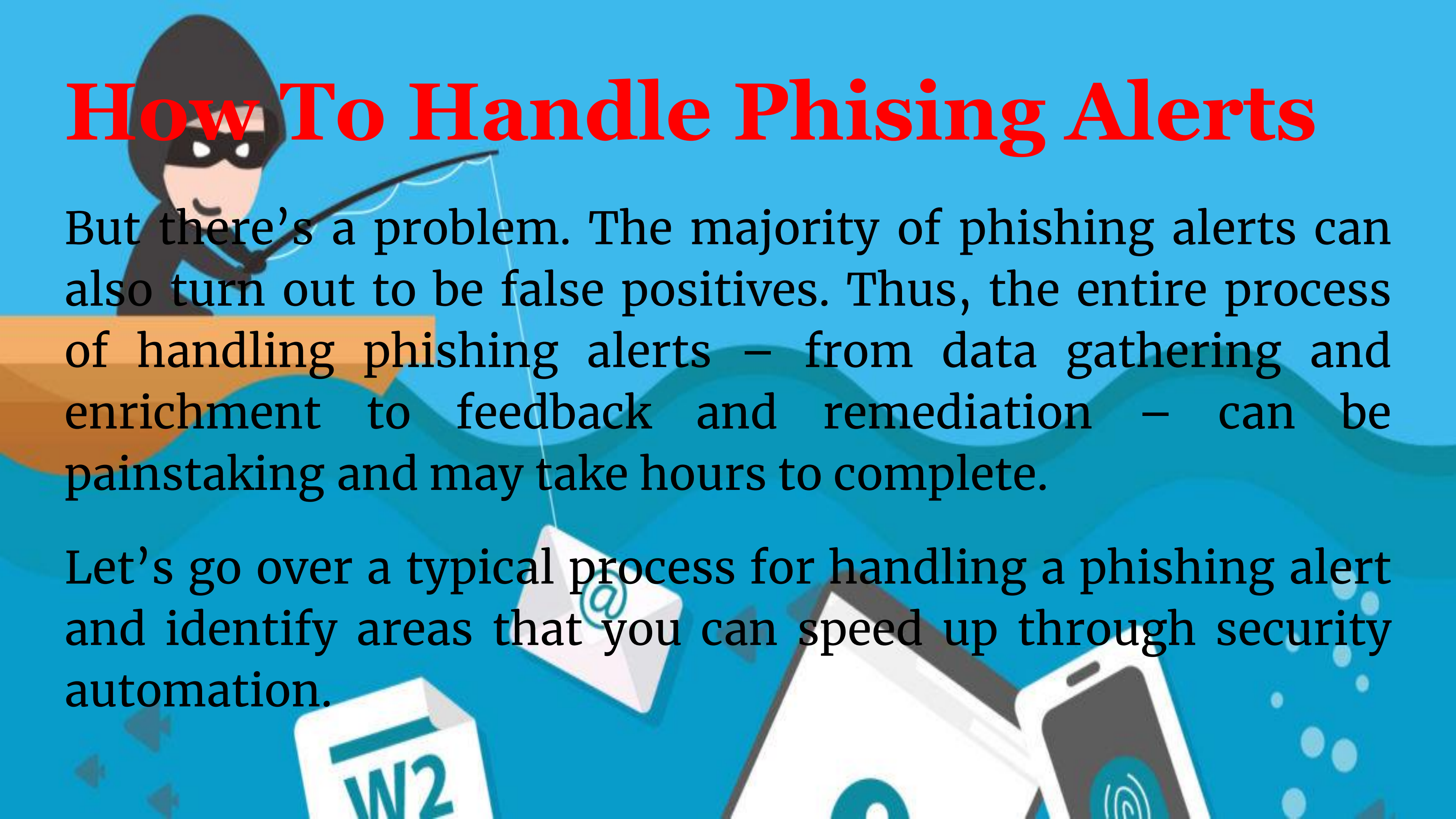
Phishing & Automation



Phishing checks three of the boxes as far as attributes that make it ripe for automation – a significant degree of manual work, low alert fidelity and the need to involve one or more users.

Phishing is extremely noisy for most organizations. Why? In addition to alerts that may appear through a SIEM or mail proxy, most companies have a mailbox where suspicious emails are sent both through automation and by end users sending what they think are questionable emails.

How To Handle Phising Alerts



But there’s a problem. The majority of phishing alerts can also turn out to be false positives. Thus, the entire process of handling phishing alerts – from data gathering and enrichment to feedback and remediation – can be painstaking and may take hours to complete.

Let’s go over a typical process for handling a phishing alert and identify areas that you can speed up through security automation.

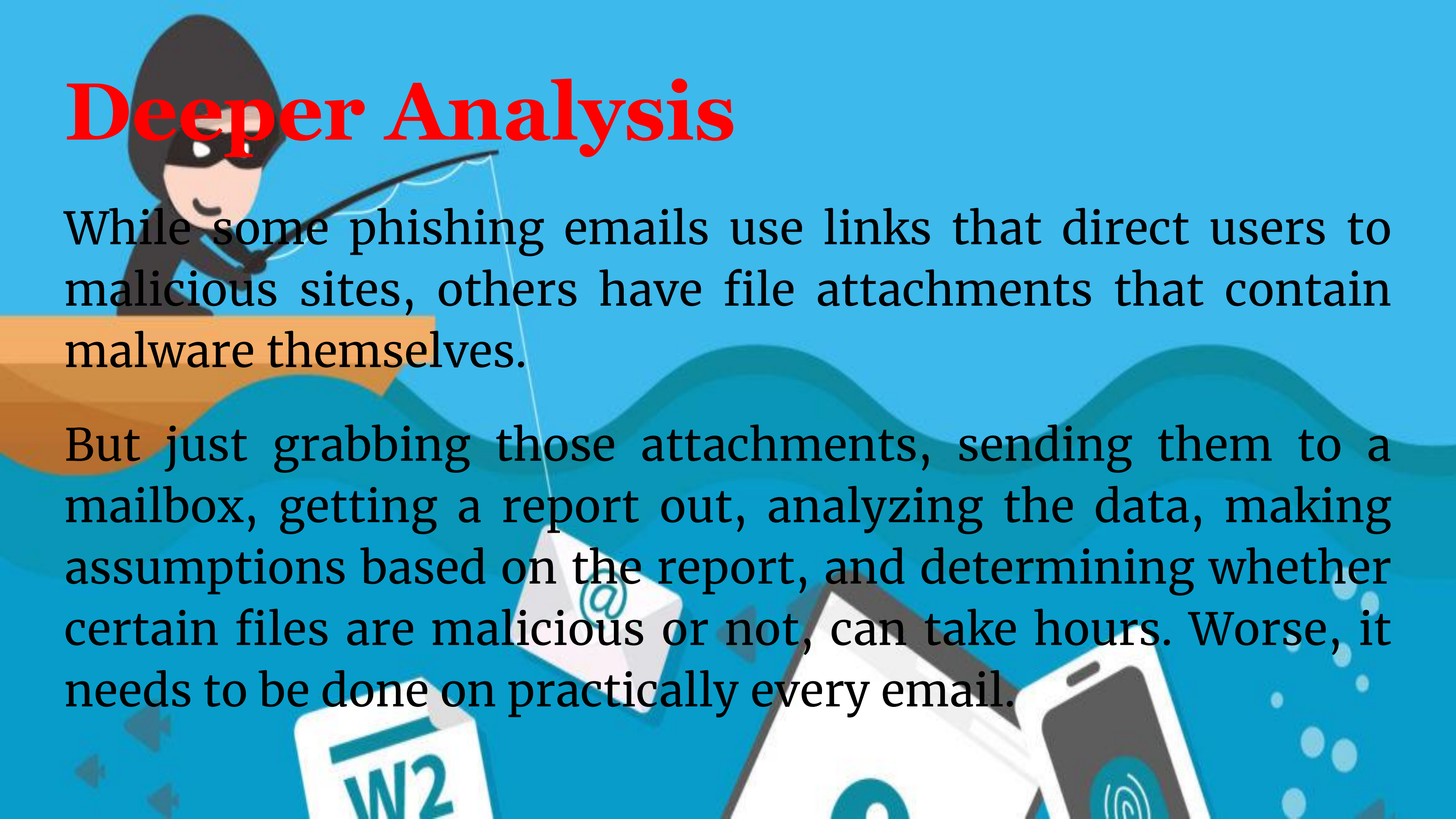
Data Gathering/Enrichment

The first step in handling phishing alerts is to gather information to make sure you have full context before making a decision based on those alerts. For instance, you might want to know the particular end user who was the source of the alert and what role he/she plays in your organization. So, if that user plays a key role – maybe in HR or Finance – then you might have a spear phishing attack on your hands.

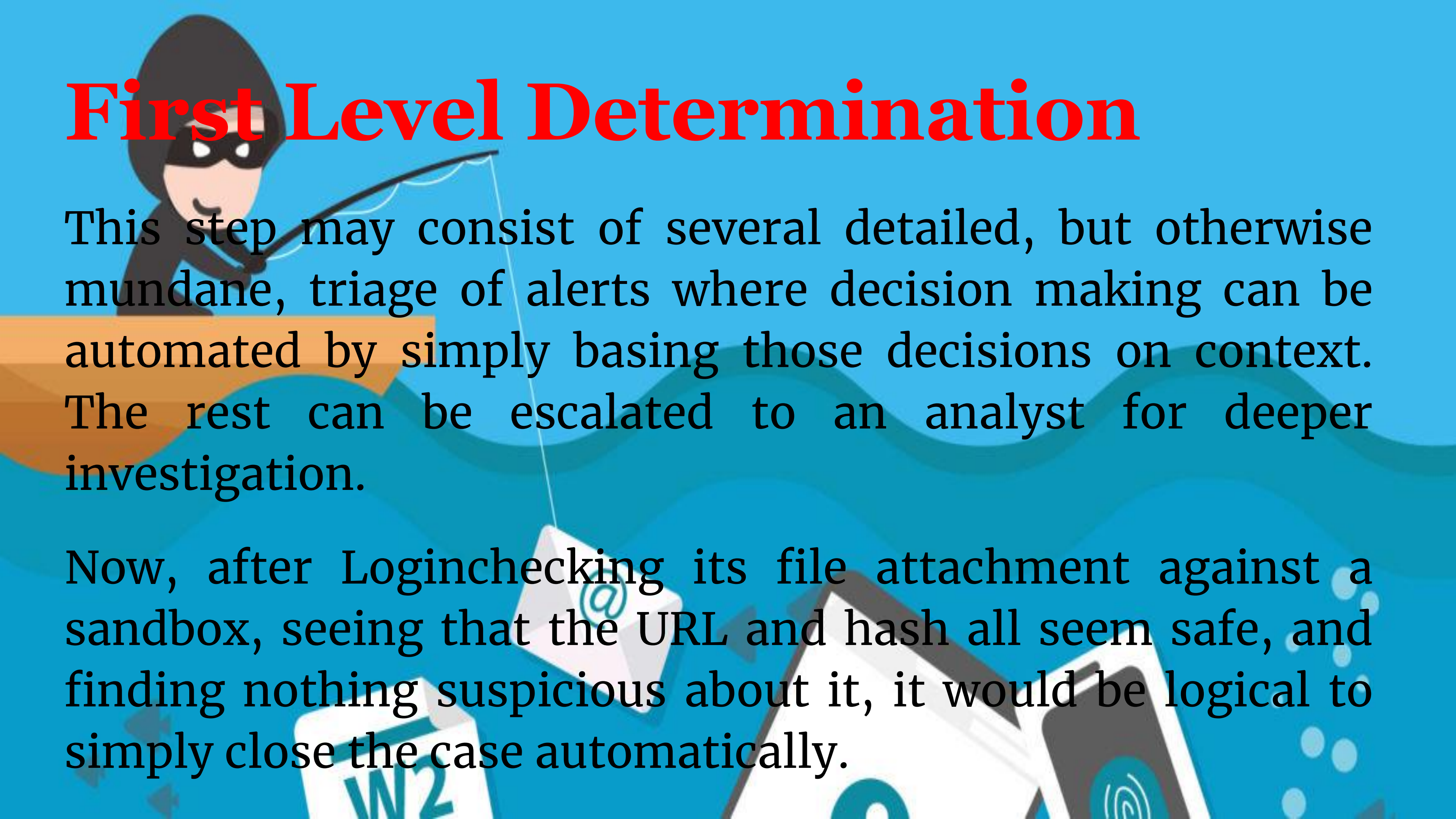
Deeper Analysis

While some phishing emails use links that direct users to malicious sites, others have file attachments that contain malware themselves.

But just grabbing those attachments, sending them to a mailbox, getting a report out, analyzing the data, making assumptions based on the report, and determining whether certain files are malicious or not, can take hours. Worse, it needs to be done on practically every email.



First Level Determination



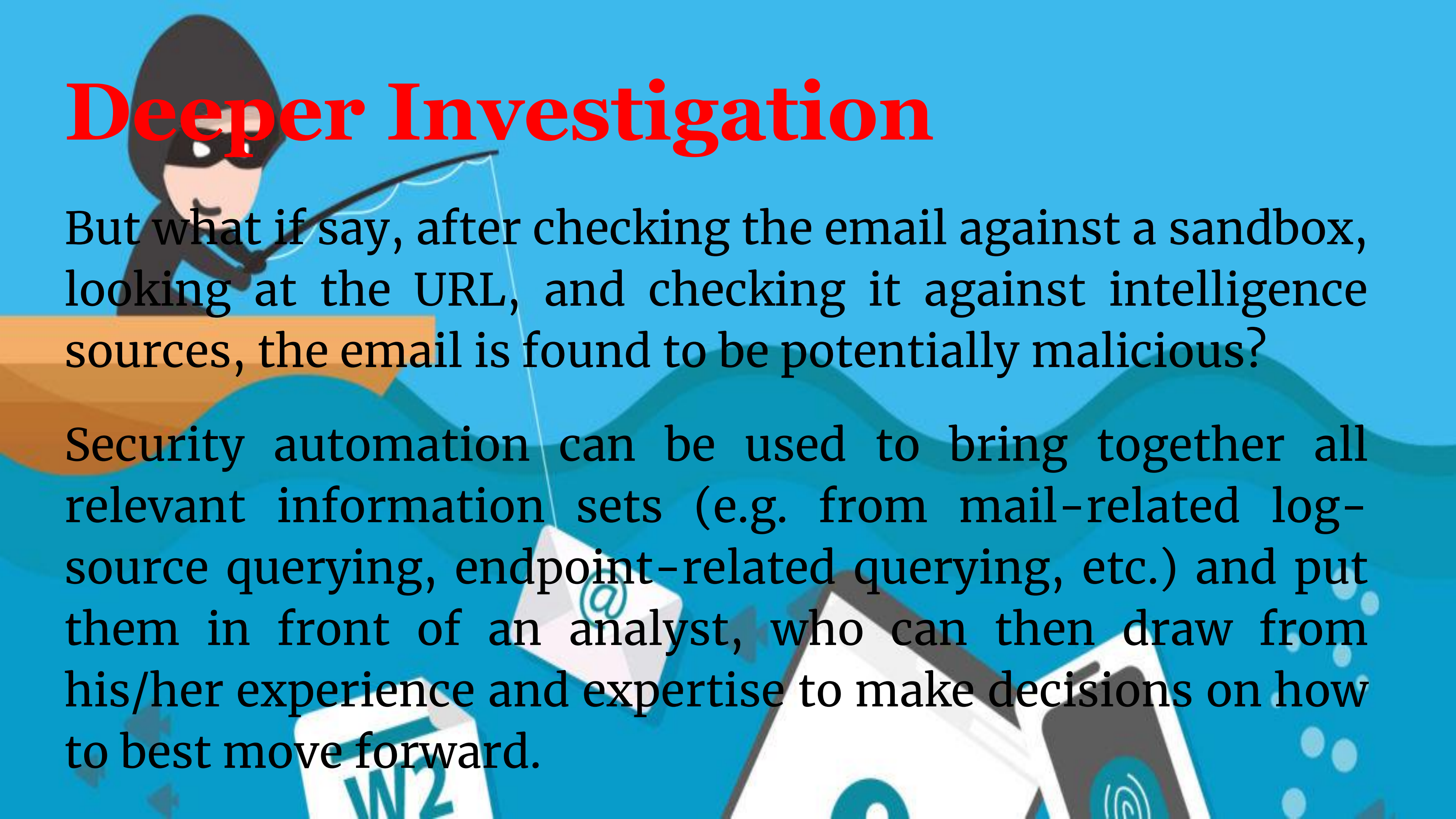
This step may consist of several detailed, but otherwise mundane, triage of alerts where decision making can be automated by simply basing those decisions on context. The rest can be escalated to an analyst for deeper investigation.

Now, after Loginchecking its file attachment against a sandbox, seeing that the URL and hash all seem safe, and finding nothing suspicious about it, it would be logical to simply close the case automatically.

Deeper Investigation

But what if say, after checking the email against a sandbox, looking at the URL, and checking it against intelligence sources, the email is found to be potentially malicious?

Security automation can be used to bring together all relevant information sets (e.g. from mail-related log-source querying, endpoint-related querying, etc.) and put them in front of an analyst, who can then draw from his/her experience and expertise to make decisions on how to best move forward.

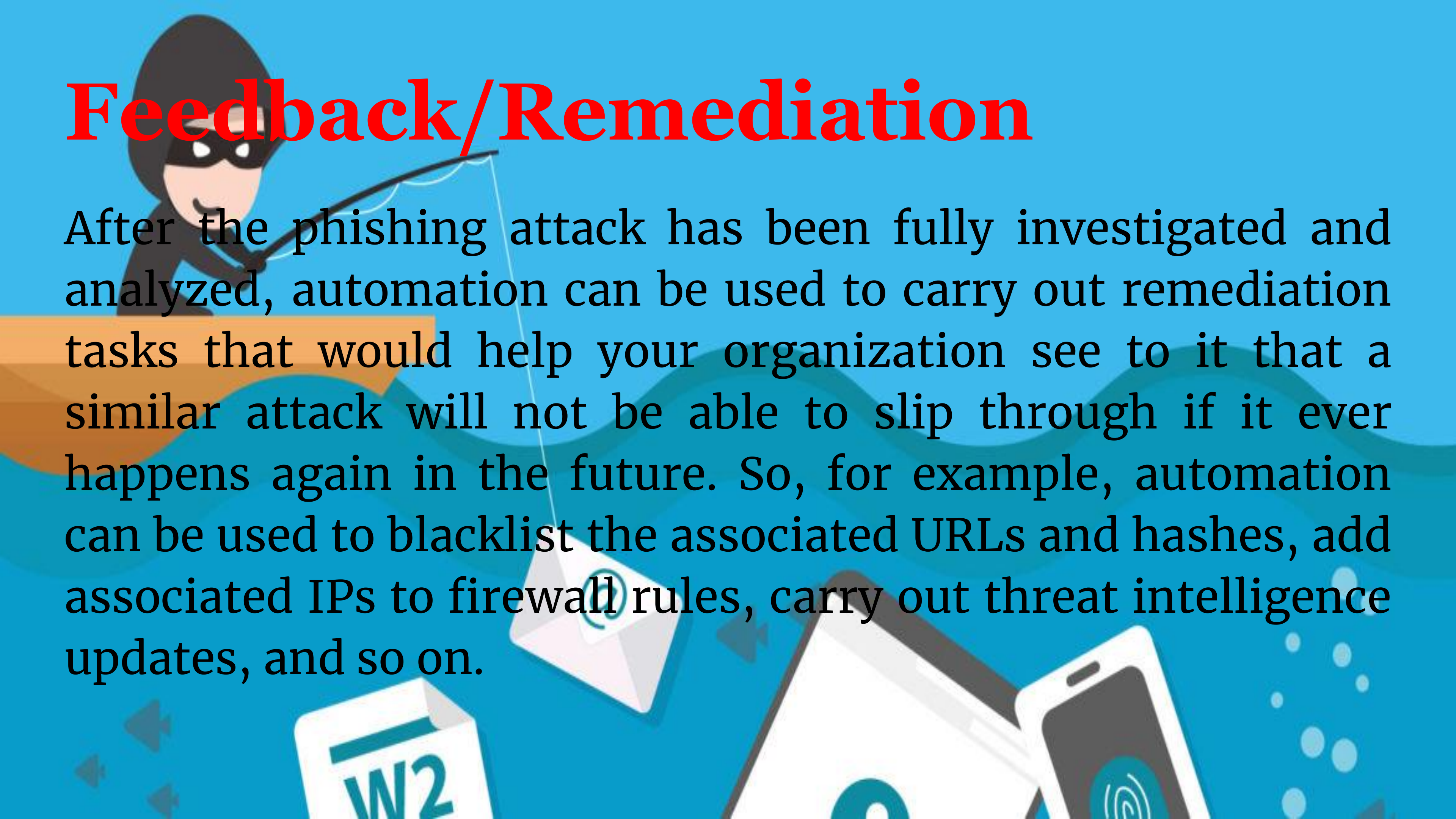


Escalation/Response Path

While this step may not be automated, as they require people to handle escalation and incident response, the next step can certainly be.

Feedback/Remediation

After the phishing attack has been fully investigated and analyzed, automation can be used to carry out remediation tasks that would help your organization see to it that a similar attack will not be able to slip through if it ever happens again in the future. So, for example, automation can be used to blacklist the associated URLs and hashes, add associated IPs to firewall rules, carry out threat intelligence updates, and so on.



Rules Of The Road

- Always automate data collection and enrichment
- Automate triage activities when possible
- Automation empowers (not replaces) human decision making
- Sensitive actions should be analyst assisted
- Embrace consistency…it’s value to security operations can’t be overstated