The Human Perspective

Security Automation and Orchestration

» TABLE OF CONTENTS «

01. Are security automation and orchestration the same?

Recently, we attended a CISO roundtable where the topic of discussion centered around security automation and orchestration. One of the questions that was asked was - “What is the difference between security orchestration and automation?”. Nobody had a concrete answer. The best answer was - “Orchestration” is a sexier word for “Automation”.

Since these terms are pretty hot right now and are used almost interchangeably,we did some research with the goal of defining three different terms - “Security Automation”, “Security Orchestration” and “Security Workflow”. We sent a bunch of emails, made lots of phone calls to customers, prospects and colleagues and read whatever material was available out there. Some highlights of the research include: -

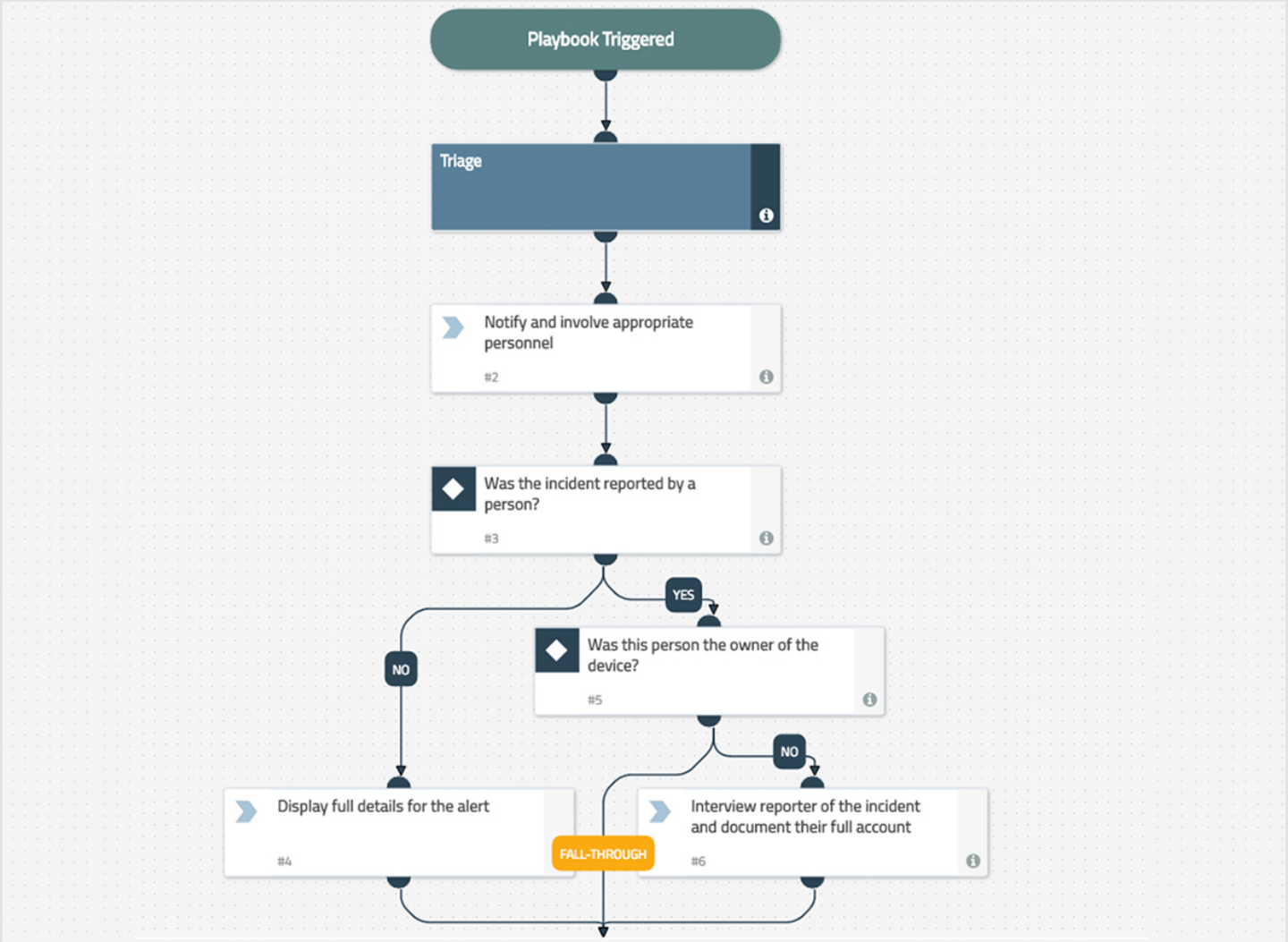
1. None of the customers and prospects clearly see the difference between automation and orchestration. They all understand the value that products in this space intend to deliver but the crowded market and the buzzword bingo that we are all part of result in a lot of confusion.

2. The customers have separate requirements or wishes in this space. Some requirements that we had encountered earlier came up again.

02. Automation, Orchestration and Workflow Requirements

REQUIREMENT 1: PROCESS WORKFLOW

Customers, like most of us, have a need for order. When it comes to problem solving, order means consistency, repeatability and predictable results. They would like to have a system where they can see all of their processes be documented and tracked. This is not about integration with any security tools at all. Customers have had playbooks (or runbooks) which document the best practices and steps for each type of incident. For example, what to do when a ransomware incident is reported? Such a playbook can have steps that are very technical in nature like “check whether the encrypted file types are of a known ransomware type?” or the steps can be procedural like “call your legal and PR teams and get them ready for the bad news”. Here is an example of pure process workflow.



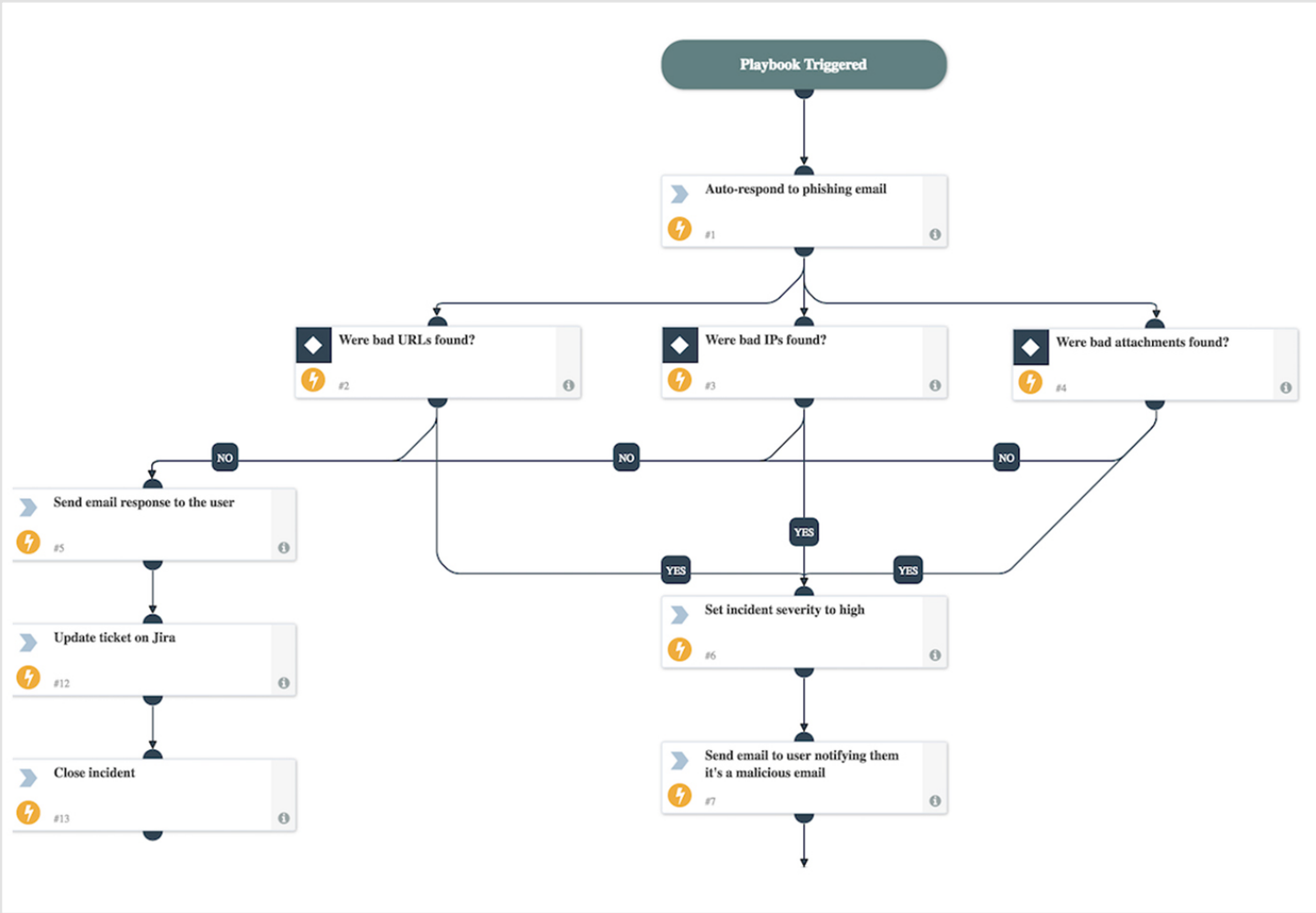
REQUIREMENT 2: TASK AUTOMATION

Customers have a large volume of security alerts spewing out of their SIEM or being generated by other security tools in their network. Security Operations Centers (SOCs) and specifically Incident Response Analysts are tasked with reviewing, understanding and dispensing with these alerts. With an increasing flood of alerts, they can't keep up. They need a way to be able to automate response and resolution of these alerts/tasks. Additionally, resolution usually requires integrating with various security tools and being able to take actions across those security tools like "hunt for a hash", "ban an IP", "check reputation of a url" etc. These actions can be triggered by an analyst or triggered when a new artifact is added to the incident. Notice that at its core this kind of automation does not include context sharing across different products in the same playbook. These are primarily "fetch" tasks and serve to gather information and evidence to support eventual resolution.

REQUIREMENT 3: PLAYBOOK AUTOMATION

SOC teams would like to create a sequence of the security automation tasks so that these tasks can be performed in a logical sequence with chained data flow. For example, in the initial phase of the phishing incident example below, triage includes steps like reputation checks for IPs and hashes across different threat intelligence feeds, hunting for the malicious IPs across the enterprise environment etc.

If the system can support sequencing of security automations then the system can be used to perform incident prioritization or detecting false positives etc. Notice that playbook automation is a "sequence of task automation with conditional logic".



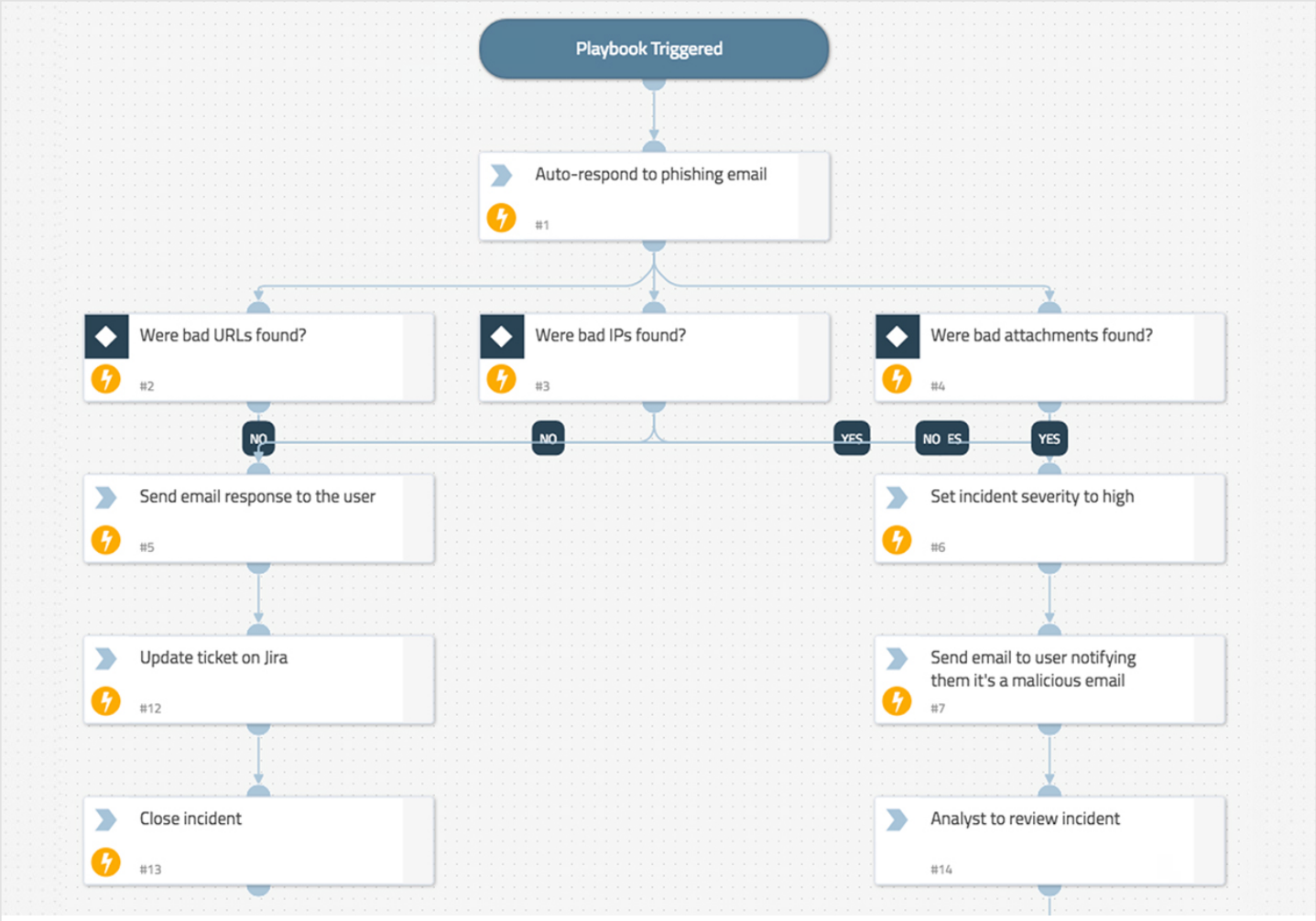
03. Real Life Security Operations - Security Orchestration

In a real life security incident, SOC teams require all of the above in a complicated mix and match scenario. Most of the vendors in this space have failed to deliver a solution that encompasses the whole of security operations. It is not about simply automating individual security tasks, nor about creating a playbook of security tasks with logic. It is about weaving the human analyst into the middle of these workflows and playbooks.

Let's walk through a scenario for a ransomware investigation. Typically, such an investigation will start with a simple malware alert from a SIEM or an employee calling about the problem. The following steps need to be done:

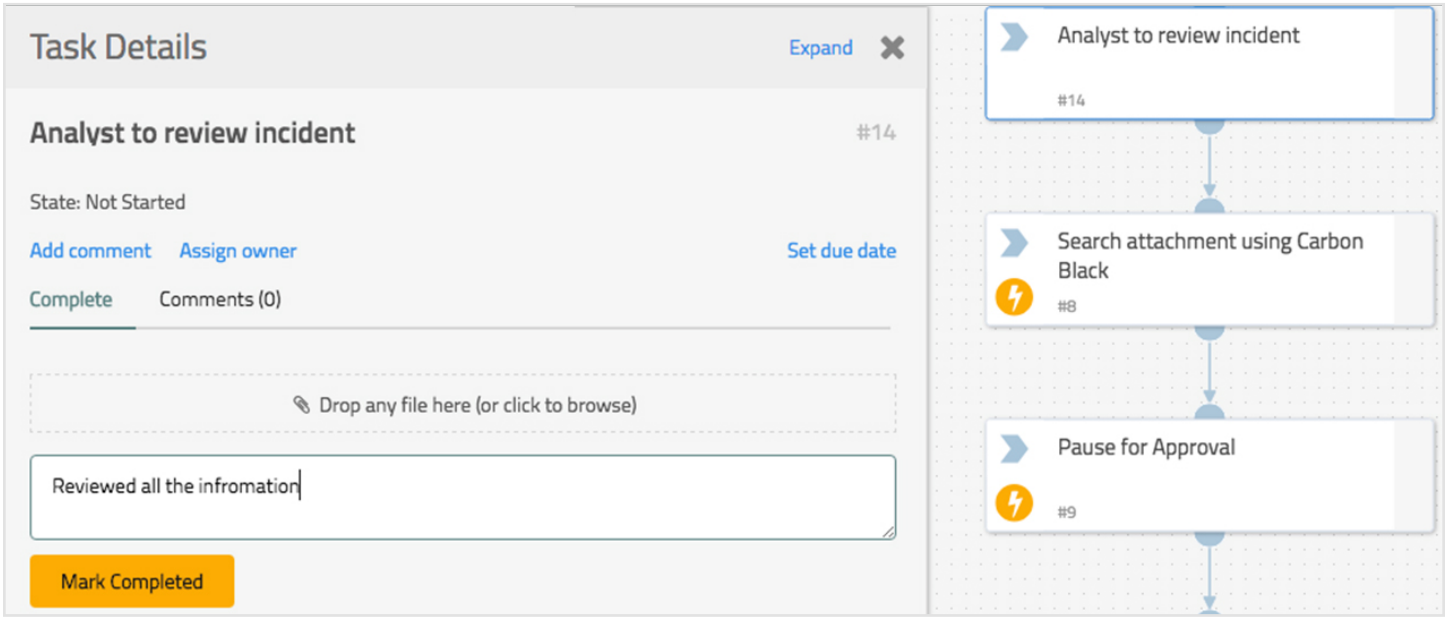
Step 1: Automate the enrichment:

Get more details about the compromised system or user using Active Directory, Asset databases etc. This can be a completely automated series of steps as shown below



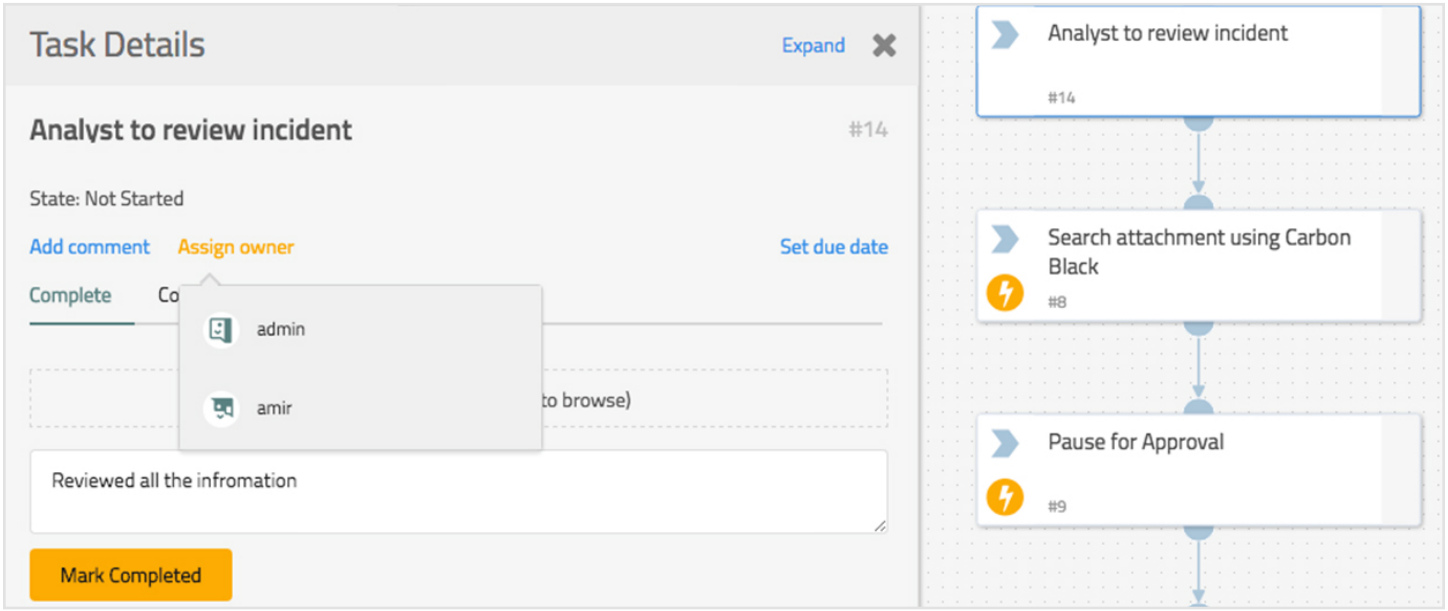
Step 2: Act on the information:

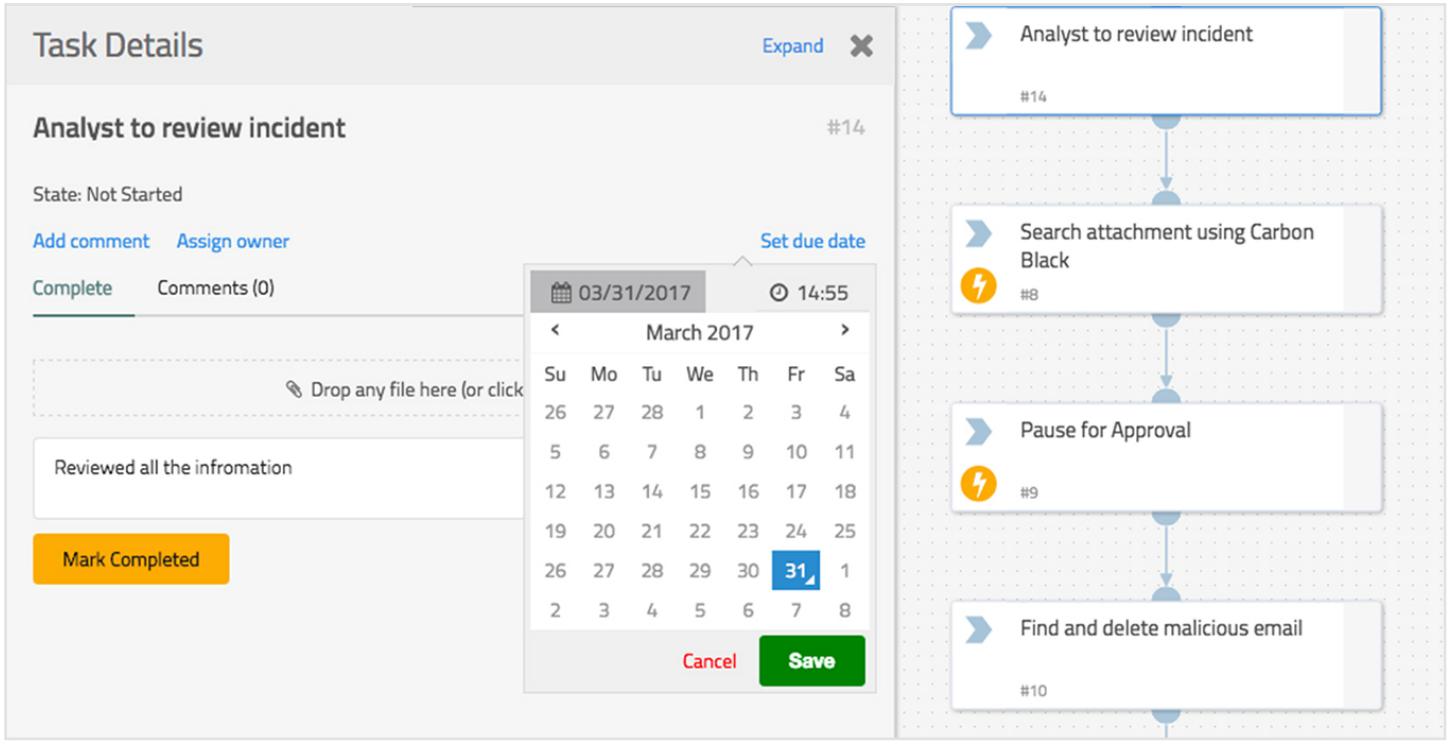
At this time, you might want an analyst to look at all the data and make decisions, maybe collaborate with peers, make comments on the task etc. Once all this is done, they can mark a task complete or assign it to another analyst.This step can have a lifecycle and timeline of its own.



Step 3: Collaborate on the information:

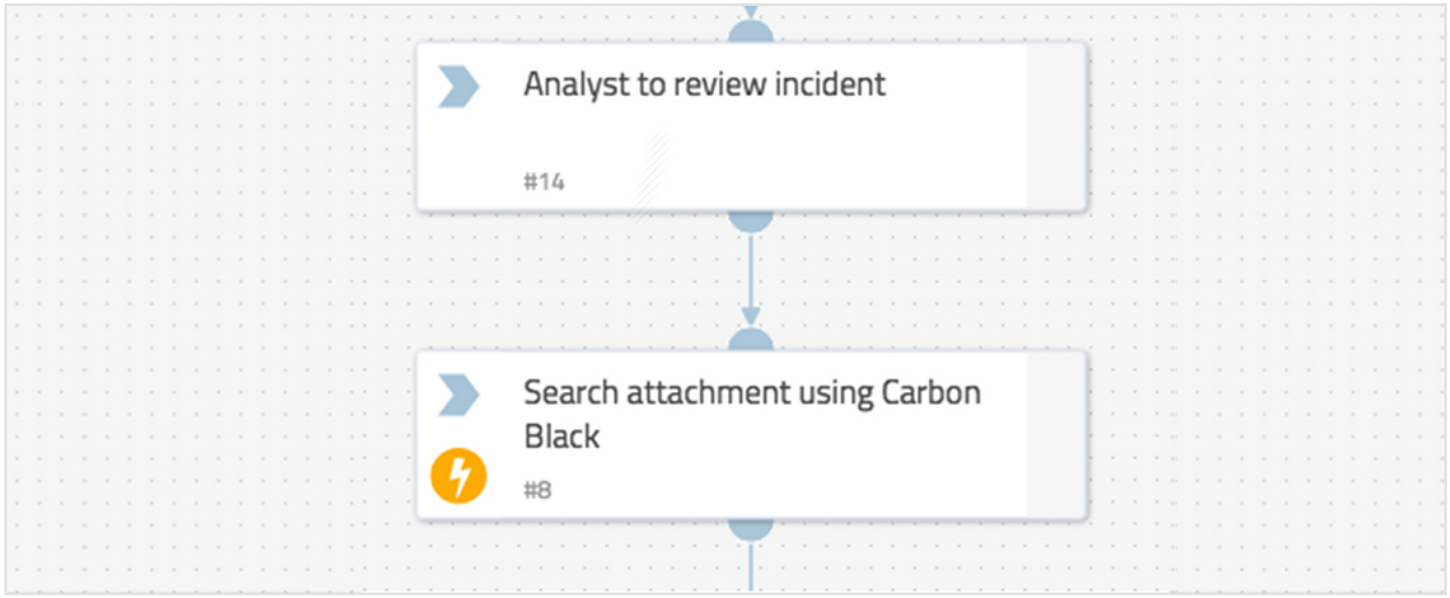
They might also want to assign a task to another analyst and set a due date. Once that task is completed, the playbook run continues.





Step 4: Automate the actions:

Playbook automation comes in play again here as it runs a series of tasks designed to fetch more data about the incident and contain the incident.



04. Summary

What looks like a simple four-step process can be very complicated and Step 2 and Step 3 can be repeated many times. This is real life security operations. In real life, automation and human tasks needs to be interweaved and work together in a seamless fashion. Automation and human process workflow when combined is essential to optimized security operations.

A comprehensive “Security Orchestration” platform should be able to automate security product tasks, create playbooks with complicated logic and be able to track and orchestrate tasks assigned to analysts. This is essential to streamlined security operations processes.

This is our definition of ‘Security Orchestration’ - like a conductor conducting a harmonious musical symphony. You need to make music. Not noise.