Playbooks

By: Ryan Stewart

In the Security Operations Center (SOC) environment, diverse alerts ranging from web attacks to ransomware and phishing demand unique investigation methods. **Playbooks** are structured workflows specifically crafted for the effective and **consistent analysis** of alerts generated on platforms like SIEM or other security tools.

For instance, in the LetsDefend Monitoring page, initiating a ticket through the "Create Case" button automatically assigns a playbook. This streamlined process enables analysts to investigate alerts systematically by following the prescribed instructions.

Why are Playbooks Important?

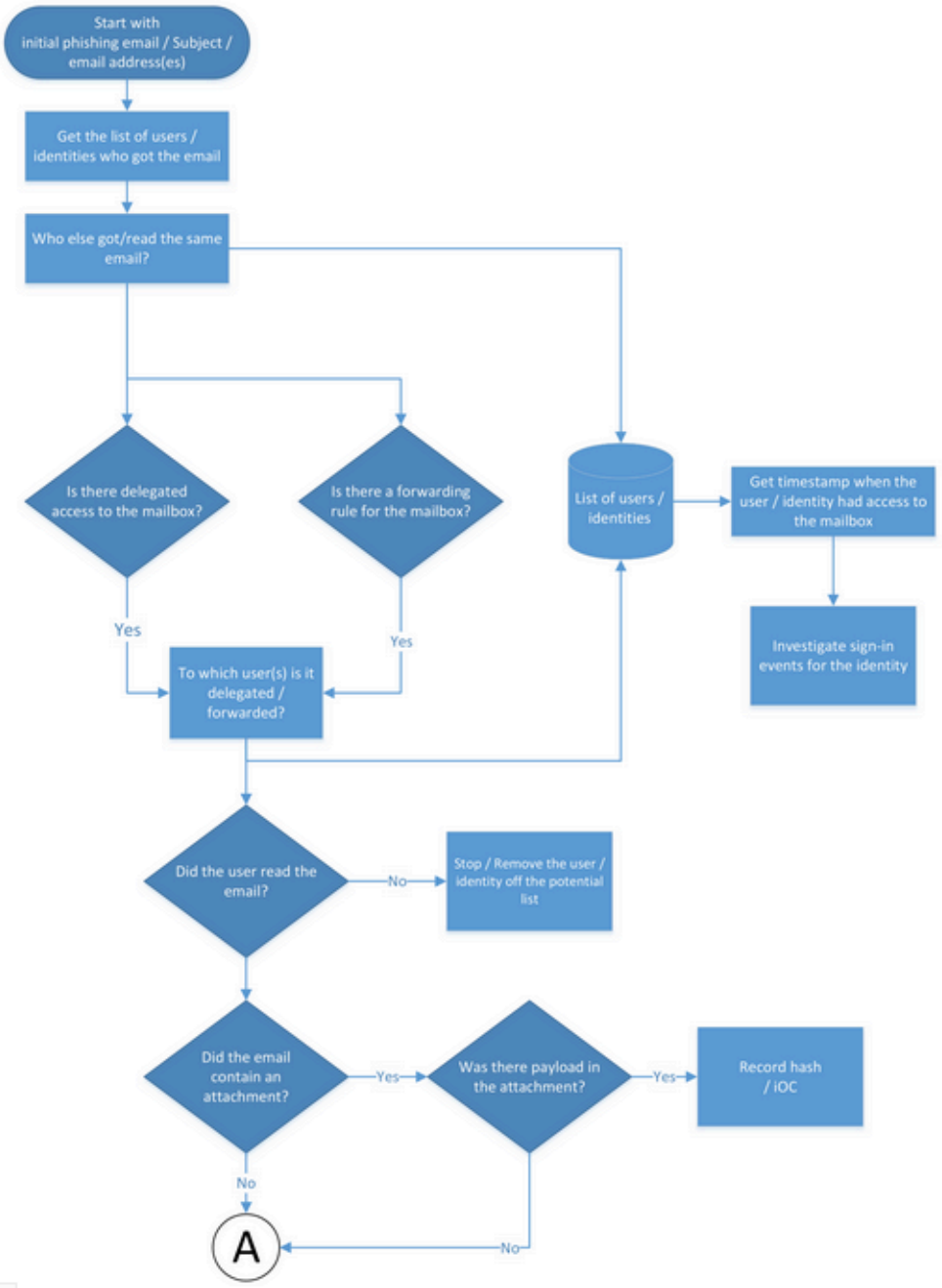
SOC analysts often encounter a multitude of alerts, each requiring a different response. Playbooks serve as **comprehensive** guides, offering step-by-step instructions for navigating the investigation process. This proves invaluable, especially for analysts who are relatively new to the SOC field.

Beyond individual guidance, playbooks play a crucial role in **establishing consistency** within the team's analysis standards. For example, ensuring the verification of access to Command and Control (C2) sites/IP addresses is essential **after** analyzing malware. However, not all analysts may consistently perform this check, leading to inconsistencies in the team's work standards. The creation and adherence to playbooks are essential to ensure a **consistent level** of analysis standards across the entire team.

In the example below, you can explore **Microsoft's** published phishing playbook stream.

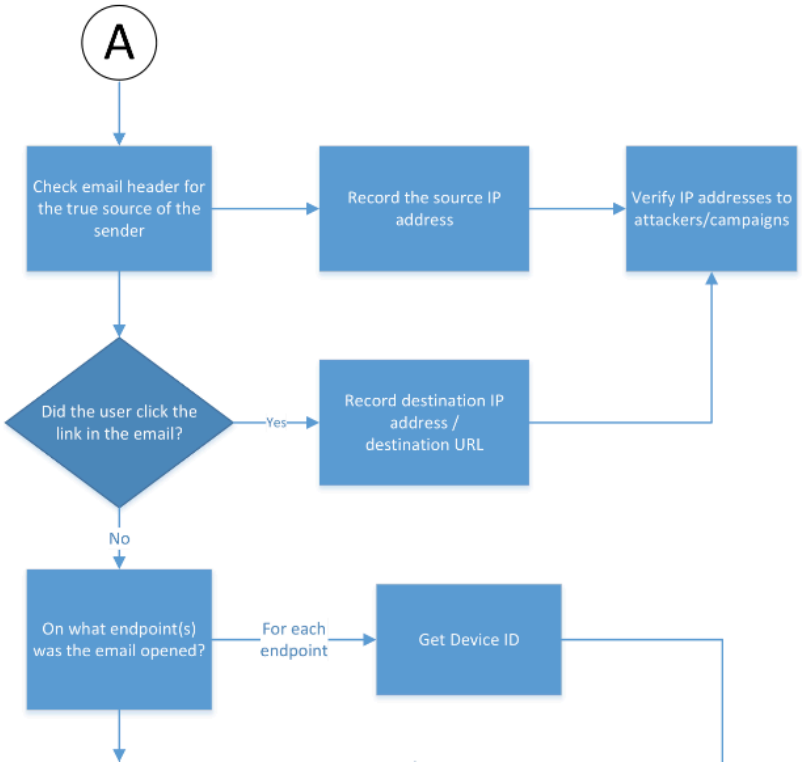
Incident response playbook: Phishing investigation (part 1)

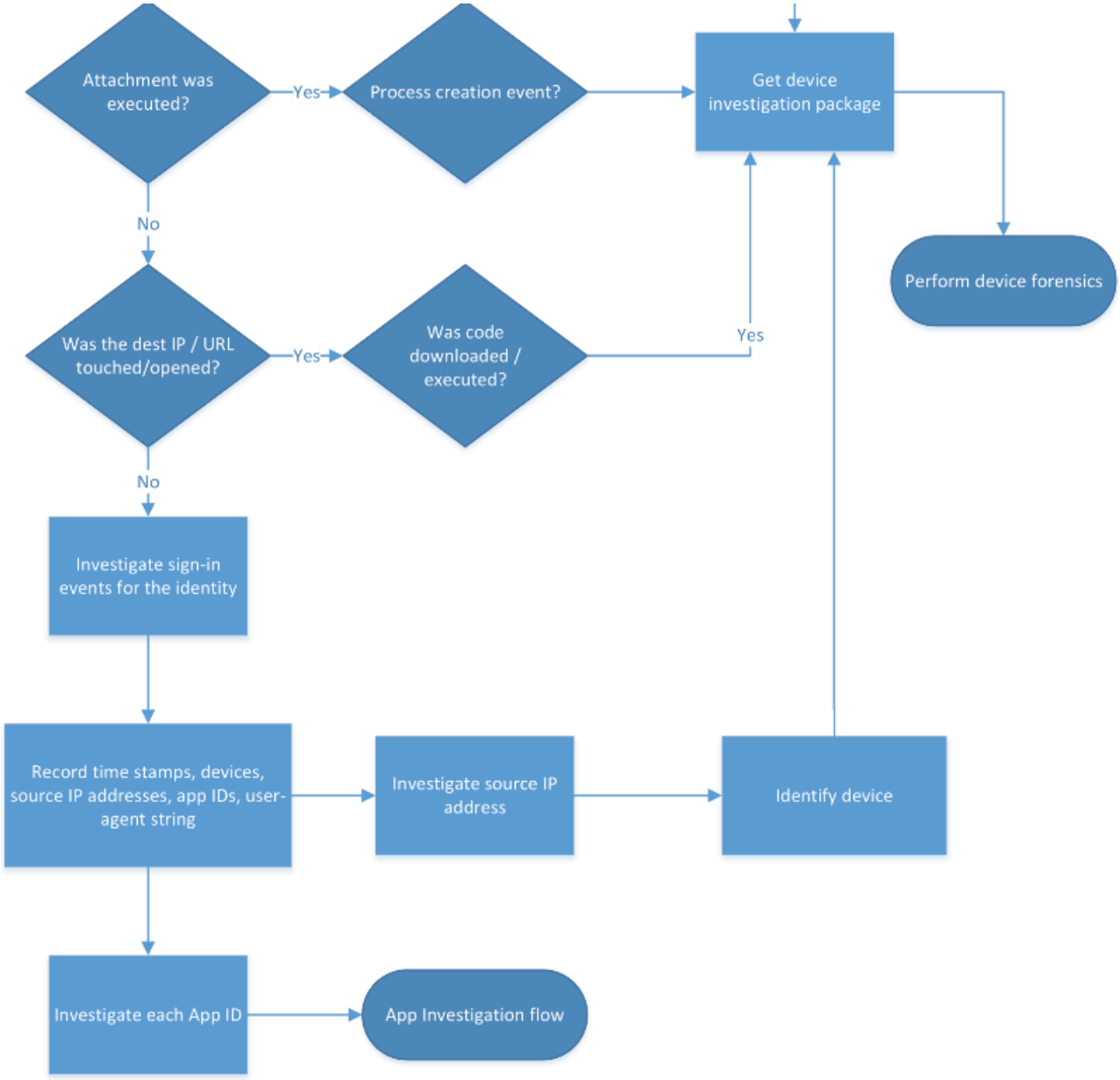
Microsoft



Incident response playbook: Phishing investigation (part 2)

Microsoft




Attachment was executed?
Yes
Process creation event?
Get device investigation package
Perform device forensics
No
Was the dest IP / URL touched/opened?
Yes
Was code downloaded / executed?
Yes
No
Investigate sign-in events for the identity
Record time stamps, devices, source IP addresses, app IDs, user-agent string
Investigate source IP address
Identify device
Investigate each App ID
App Investigation flow