Leveraging SOAR to Combat Adversary Behaviors and Malware

In an era where cyber threats are increasingly sophisticated and numerous, having an efficient and effective response mechanism is crucial. The integration of Security Orchestration, Automation, and Response *(SOAR)* platforms into the cybersecurity ecosystem has made it possible for security teams to swiftly detect, investigate, and remediate potential threats. In this article, we will explore a playbook that outlines steps to combat malicious behaviors and malware, with the Endpoint Detection and Response (EDR) serving as the detection source.

The Power of SOAR Playbooks in Modern Cybersecurity Operations

The increasing complexity of the cyber threat landscape necessitates that security professionals leverage advanced technologies like SOAR to keep pace. With the integration of SOAR playbooks, organizations can benefit in various ways:

Efficiency and Speed: With manual processes, the time taken to detect, respond, and remediate threats can be lengthy. SOAR playbooks allow for rapid response, ensuring threats are contained before they escalate.

Consistency: Human error is a common concern in any manual operation. SOAR playbooks offer a consistent approach to threat detection and response, ensuring every incident is handled according to best practices.

Reduced Alert Fatigue: Security professionals are often inundated with countless alerts daily, leading to alert fatigue. By automating mundane tasks and filtering out false positives, SOAR playbooks ensure that teams can focus on more critical threats.

Integration Capabilities: One of the key strengths of SOAR platforms is their ability to integrate with other security tools, such as SIEM, EDR, and threat intelligence platforms. This ensures a holistic approach to security, where different tools can work in tandem under the guidance of a SOAR playbook.

Customization: No two organizations are the same, and neither are their security requirements. SOAR playbooks can be tailored to fit the specific needs and infrastructure of an organization.

Continuous Improvement: As threat actors evolve, so should our defense mechanisms. SOAR playbooks can be continually refined based on lessons learned from past incidents, ensuring the organization remains one step ahead of potential threats.

Combating Adversary Behaviors and Malware:

1. Detection and Ingestion

Source of Detection: The EDR system acts as the primary source of detection. EDR tools monitor endpoint activities and can detect potential threats based on behavior or known malicious indicators.

Data Ingestion into SOAR: Detected threats or anomalous behaviors are ingested into the SOAR platform. This can be achieved directly through connectors established between the EDR and SOAR or indirectly via a data lake.

2. Playbook Activation

Upon ingestion into the SOAR platform, the playbook tailored to handle malicious behaviors is triggered.

3. Suspicious File Retrieval and Analysis

The suspicious file that caused the detection is fetched from the EDR through a pre-configured integration for a more thorough analysis.

If the file is successfully downloaded:

- The file's hash is cross-referenced with various threat intelligence sources to determine if it is associated with any known threats.
- For a deeper dive, the downloaded file undergoes a sandbox analysis to evaluate its behavior in a controlled environment.
- Post-analysis, the downloaded file is safely deleted from the SOAR platform.

4. Decision-making and Response

The file's hash results, and the outcomes of the sandbox analysis are evaluated:

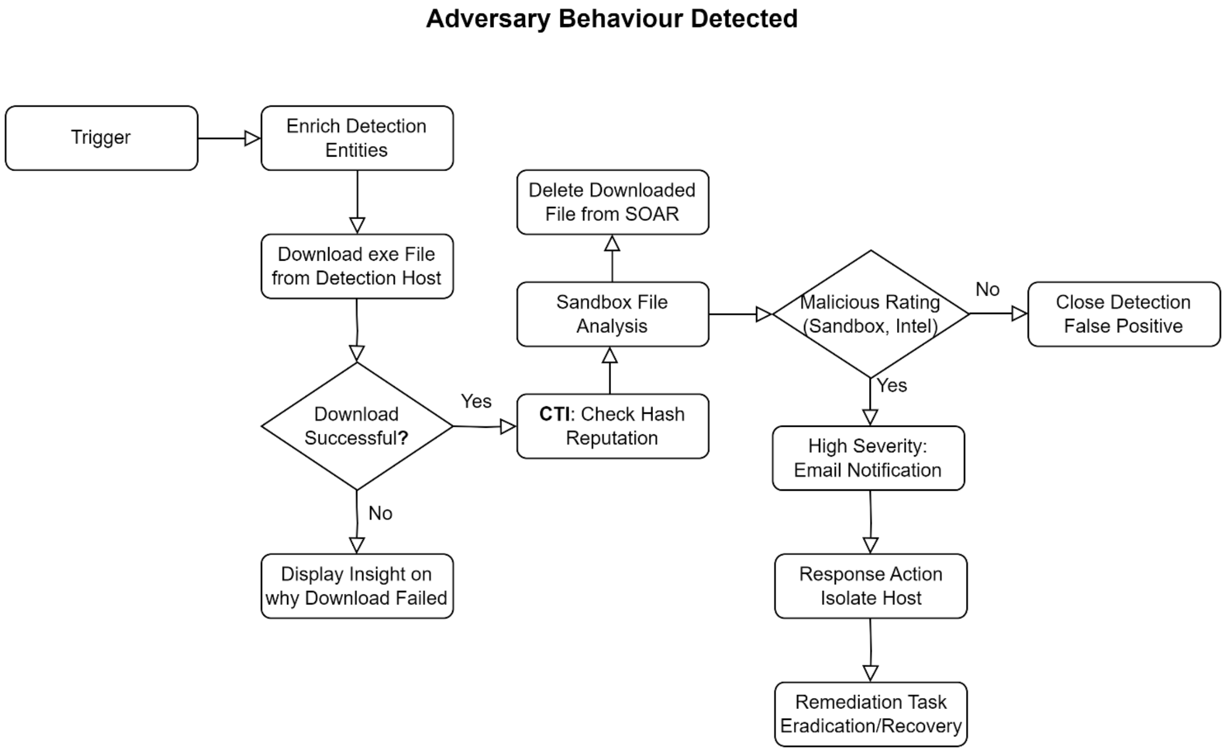
If found malicious:

- The threat's severity is elevated to "high."
- The Security Operations Center (SOC) team is promptly notified via email.
- The affected or "victim" host is isolated to prevent any potential spread of the threat.
- Remediation actions, including eradication of the malicious file and recovery processes, are initiated on the compromised host.

If deemed non-malicious:

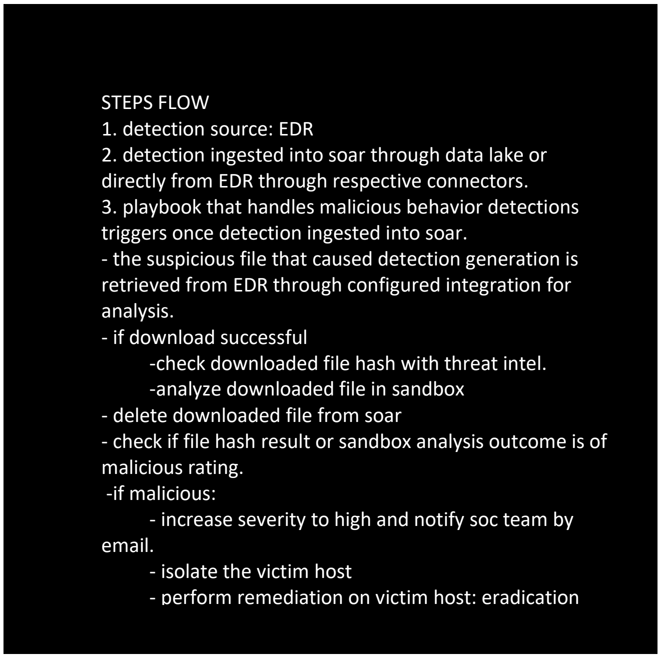
- The detection is archived as a false positive, and the alert is closed.

Below is an image of the playbook flow:


Adversary Behaviour Detected
Trigger
Enrich Detection Entities
Download exe File from Detection Host
Download Successful?
Yes
No
Display Insight on why Download Failed
CTI: Check Hash Reputation
Sandbox File Analysis
Delete Downloaded File from SOAR
Malicious Rating (Sandbox, Intel)
No
Close Detection False Positive
Yes
High Severity: Email Notification
Response Action Isolate Host
Remediation Task Eradication/Recovery

Conclusion:

In today's dynamic threat landscape, the integration of SOAR platforms can streamline and enhance the responsiveness of security operations. By employing tailored playbooks, like the one discussed, organizations can ensure they are better equipped to detect, analyze, and act upon cyber threats with agility and precision. Leveraging automation not only aids in reducing the workload of security professionals but also ensures a consistent and swift response to emerging threats.



STEPS FLOW
1. detection source: EDR
2. detection ingested into soar through data lake or directly from EDR through respective connectors.
3. playbook that handles malicious behavior detections triggers once detection ingested into soar.
- the suspicious file that caused detection generation is retrieved from EDR through configured integration for analysis.
- if download successful
    -check downloaded file hash with threat intel.
    -analyze downloaded file in sandbox
- delete downloaded file from soar
- check if file hash result or sandbox analysis outcome is of malicious rating.
 -if malicious:
    - increase severity to high and notify soc team by email.
    - isolate the victim host
    - perform remediation on victim host: eradication