SAPPAN: Standardization of cybersecurity playbooks

Martin Zadnik

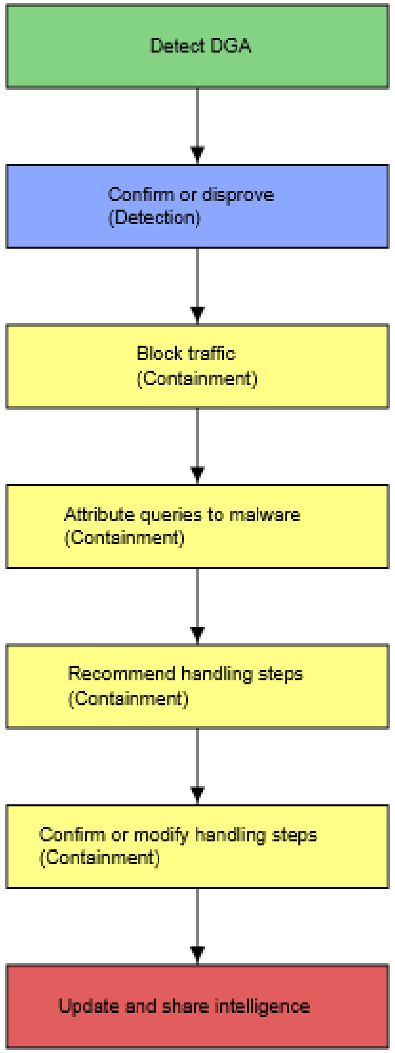
CESNET

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833418

Playbooks intro

- The response handling information captures guidelines for the particular phase in incident handling life cycle (preparation, analysis, containment, post-incident) and the particular threat/attack/incident. The guidelines are often documented as playbooks that are high-level human-readable, written in plain text without structure.

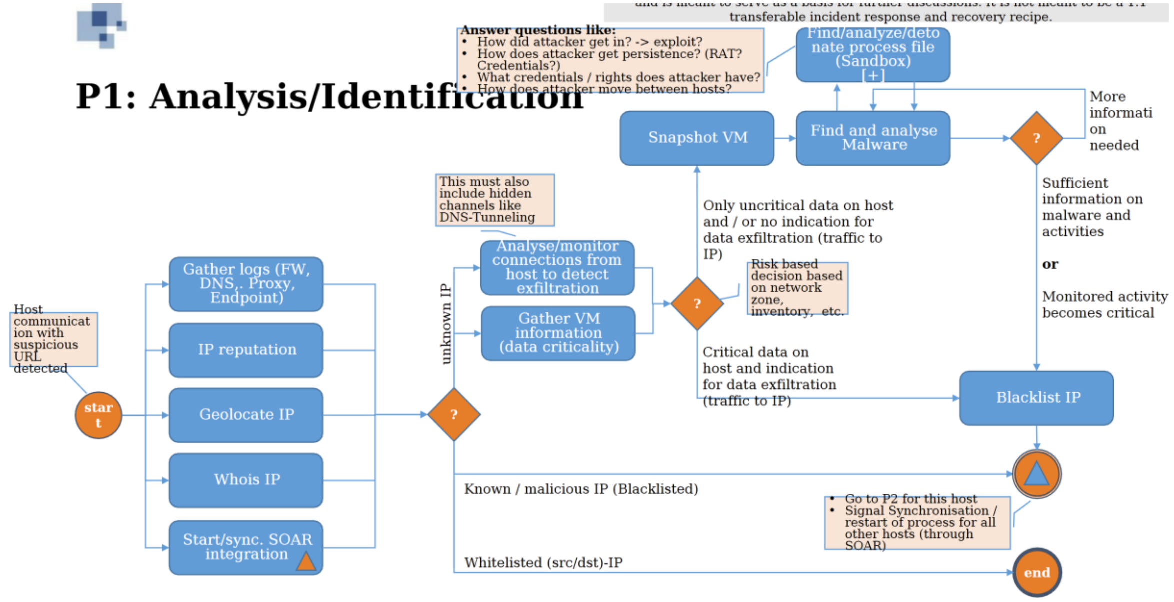
- One of the SAPPAN goals was to give structure to playbooks to make them machine-readable and actionable.


Detect DGA
Confirm or disprove (Detection)
Block traffic (Containment)
Attribute queries to malware (Containment)
Recommend handling steps (Containment)
Confirm or modify handling steps (Containment)
Update and share intelligence

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

SAPPAN playbook

- SAPPAN created its standard to capture cybersecurity response and recovery actions 1/2021
- Approximately at the same time we discovered there is Technical Committee CACAO under OASIS introducing its standard for cybersecurity playbooks



and is meant to serve as a basis for further discussions. It is not meant to be a 1:1 transferable incident response and recovery recipe.

P1: Analysis/Identification

Answer questions like:
• How did attacker get in? -> exploit?
• How does attacker get persistence? (RAT? Credentials?)
• What credentials / rights does attacker have?
• How does attacker move between hosts?
Find/analyze/detonate process file (Sandbox) [+]
Snapshot VM
Find and analyse Malware
?
More information needed
Sufficient information on malware and activities
or
Monitored activity becomes critical
This must also include hidden channels like DNS-Tunneling
Analyse/monitor connections from host to detect exfiltration
Gather VM information (data criticality)
Only uncritical data on host and / or no indication for data exfiltration (traffic to IP)
?
Risk based decision based on network zone, inventory, etc.
Critical data on host and indication for data exfiltration (traffic to IP)
Blacklist IP
Host communication with suspicious URL detected
start
Gather logs (FW, DNS,. Proxy, Endpoint)
IP reputation
Geolocate IP
Whois IP
Start/sync. SOAR integration
unknown IP
?
Known / malicious IP (Blacklisted)
• Go to P2 for this host
• Signal Synchronisation / restart of process for all other hosts (through SOAR)
Whitelisted (src/dst)-IP
end

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Sharing playbooks

- We got in touch with the CACAO TC
- Discussed our next goal to share the playbooks
- Proposed an implementation of playbook representation in MISP
- After fine-tuning details we pushed the cybersecurity playbook object data model in MISP repository with positive reaction from A. Dulanoy (CIRCL.LU)
- Joint paper describing our effort
  - Mavroeidis, V. et al: On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418