The Need for Investigation Playbooks at the SOC

Matias Cuenca-Acuna
Ismael Valenzuela

SANS SOC Summit 2017 – Crystal City, VA
It’s play time! (it’s 5 o’clock somewhere…)
Was it the rope or the revolver?
How do we investigate in the SOC
SOC Investigations

• We have weapons
  • Host & network artifacts

• We have rooms
  • Systems, network segments

• We have suspects
  • Patient zero, threat actors
How do we investigate?

- Results of a survey conducted on 16 companies across US, LATAM and EUROPE
  - Up to weeks to make a conclusion.
  - 75% of the time spent on collecting data and 25% of the time spent on analyzing the data
  - 25% of alerts are never triaged and 1/4th of these return as severe or moderate incidents
  - Talent shortage

- What resources do we use to drive our analysis? How do they help with scoping or adding context to the investigations?
Response  Playbooks vs Investigation Playbooks

- As the SOC Survey indicates, when we use the word playbook we typically refer to:
  - A list of actions
  - That can be scripted / automated
  - That has an objective to contain or eradicate

- e.g. Abnormal nr. of outbound SMTP -> reset users’ pwd -> collect / review evidence

- What do we have to guide the investigation (analysis) phase?

Source: SANS SOC Survey 2017
Investigation Playbooks Today

- Embedded in Response Playbooks
- Expressed in terms of checklists and flowcharts describing actions
- Organizational culture and bias influences analysis
- Non-portable (e.g. include references to products & versions)
- Do not enable human-machine collaboration

Can this be improved?
Level setting: How do people investigate?

Being an expert investigator is about asking the right questions

- Related work
  - *How Analysts Approach Investigations* by Chris Sanders
  - *Analysis of competing hypotheses* by Dick Heuer (CIA)

Investigation playbooks should be about capturing questions & hypotheses

- Not a scripted set of procedures & actions
  - But they should lead to actions/procedures
- Questions are product/company independent

Playbooks should capture WHAT we need to ask not HOW to answer it

(i.e. a declarative versus a procedural approach)
Actions vs Hypothesis & "Clue-based" Questions

Traditional malware infection investigation:

- Review HTTP logs prior to infection
- Review AV logs
- Review DNS logs
- Collect evidence from this system
- Send sample to AV vendor
- ...

Hypothesis: there is no security threat, we cannot confirm malicious activity.

- Does the endpoint contain evidence of suspicious outbound network connections?
  - Does the endpoint connect to IPs or domains with bad reputation?
- Does the endpoint contain evidence of malware persistence?

No two investigations are identical to each other!
What is the best way to capture investigation playbooks?
Existing document formats fall short

- **.PDF**
  - Capture expert knowledge

- **.TXT**
  - Enable manageability & scale
  - Support scripting

- **.DOC**
  - Enable collaboration

- Wikis
Using Markdown to write investigation playbooks

Markdown (MD) is a plain-text format
- It allows to do basic text formatting
- It can be converted to HTML & PDF

We have extended markdown for iPBs
- Question numbering, hierarchy & order
- Question linking & PB modularity
- Tagging
- implementation & reference tracking
- Enable collaboration on Github
Checkout our spec on GitHub

https://github.com/Foundstone/InvestigationPlaybookSpec
Highlights of using markdown to capture investigation playbooks
Capturing sections & metadata

Playbook: Malware alert triage

**Elevator pitch**

This is a general playbook that explores the presence of malware and tries to answer basic questions like origin & spread of malware, evidence of activation, persistence, purpose (C2, ransomware, etc).

**Alerts captured**

Any alert signaling the presence of malware on an endpoint (for example, a firewall rule or heuristic detection).

**Investigation questions**

1. **There is no security threat, we cannot confirm malicious activity.**
   
i. Does the endpoint contain evidence of suspicious outbound activity?
   
   a. Did the endpoint connect to IP or domains with bad reputation?
Capturing questions

---

Investigation questions

1. *There is no security threat, we cannot confirm malicious activity*

   i. Does the endpoint contain evidence of suspicious outbound network connections?
      a. Did the endpoint connect to IP or domains with bad reputation?
      b. Is the endpoint establishing network connections in abnormal times?
      c. Does the endpoint present performance degradation or instability

---

Implementation details

1. Did the endpoint connect to IP or domains with bad reputation?

   <details>
   <summary>Implementation</summary>

   * Use SIEM to get all the network accessed blocked by Web Gateway from the endpoint during the investigation window [[@UseSIEM, @Manual]"
   * Dump the endpoint [DNS cache using this tool](tools/ADDumper.bat) and check domains against VirusTotal [[@Manual]"

2. *Are there any red flags on the connection target?*

   [OutboundNetworkConnection/README.md#1.1]

3. Is the endpoint establishing network connections in abnormal times?

4. [Does the endpoint present performance degradation or instability](#1.3)

5. Is the network connection destination geo suspicious? [[SIEM has lists of corporate geos, we could check against those]"

---

Question links

---

Tagging

---

Question ID
Online collaboration using GitHub

We have tested this approach with 30+ interviews and 10+ experts!
Managing investigation playbooks using open source tools
Using static analyzers to sanitize playbooks

**Broken markdown**

1. Is the appliance in a good shape? [ ](# "IPS,Siem")

   1. Does the appliance have anomalies reporting alerts? [ ](# "IPS,Siem")

   warning Incorrect indentation before bullet: remove 2 spaces list-item-bullet-indent
   remark-lint  

**Broken links to questions**

./playbooks/OutboundNetworkConnection/README.md

17:6-17:101 warning Link to unknown heading or anchor in `../..//playbooks/Phishing/README.md`:

`2` remark-validate-links  remark-validate-links

**Terminology & text quality**

1. Are there multiple logon processes evidence? [ ](# "ePO,ForensicsTools, Logs")

   warning Hard to read sentence (confidence: 4/7) retext-readability
   retext-readability  

   warning Replace “multiple” with “many” multiple retext-simplify  

Managing playbooks using command line scripts

Find duplicate questions

```bash
fmcuenca$ find playbooks -iname README.md -exec ./tools/pbLint/questionDumper.pl {} \; | sort
...
Is there a running command trying to escalate privileges? playbooks/MalwareAlertTriage/README.md#3.4.2.1.3
Is there a server or critical infrastructure involved? playbooks/MalwareAlertTriage/README.md#4.1.1
Is there a server or critical infrastructure involved? playbooks/OutboundConnection/README.md#3.4.1
Is there an attacker with access to privileged accounts? playbooks/MalwareAlertTriage/README.md#3.4.2.1.4
```

Filter by tags

```bash
fmcuenca$ find playbooks -iname README.md -exec ./tools/pbLint/questionDumper.pl {} \; | sort | grep @IPS
...
Did the appliance register malware alerts? playbooks/TI/README.md#1.1.2.4 @EPO,@IPS
Did the frequency of alerts increased? playbooks/TI/README.md#1.1.1.2 @IPS,@SIEM
Is there evidence of some exploit kit? playbooks/TI/README.md#2.1.5 @IPS,@SIEM
```
Wrap up & takeaways

An expert is the one that asks the **right questions**

**Investigation** playbooks should provide those **questions**

**Static** documents are **not the right tool** to capture playbooks

**Markdown** adds little effort and has lots of upsides

- Reduces effort to write and maintain
- Enables collaboration
Call to action

Checkout our public playbook spec on GitHub:
https://github.com/Foundstone/InvestigationPlaybookSpec

Send us feedback!
- ismael_valenzuela@mcafee.com
- francisco_cuenca@mcafee.com

More on how to share the implementation of playbooks and analytics tomorrow!
The Need for Investigation Playbooks (iPB) at the SOC

As SOCs mature and start to formalize their operations, they typically focus on preparedness, escalation process and incident response plans. However, even with these plans in place, SOCs report that 25% of the alerts are not triaged and that investigations take too long. Why so? In many cases, this can be attributed to the lack of a standardized investigation process and community wide tools that can be applied consistently & repeatedly over time, preventing less experienced analysts and incident responders from doing their job effectively.

In this talk, Ismael Valenzuela (SANS Instructor, GSE #132 and Global Director of Foundstone Consulting Services), and Matias Cuenca-Acuna, (Principal Engineer at McAfee), will showcase how SOC investigations can be presented as an iterative process of postulating hypotheses and answering questions in the pursuit of an outcome. Using this approach, they will show how to use Markdown to capture investigation playbooks and how they should be structured so they can be effectively used by SOC analysts and incident responders.

Matias Cuenca-Acuna, Principal Engineer, McAfee

Ismael Valenzuela, SANS Certified Instructor, GSE #132; Global Director of Foundstone Consulting Services