A Walk Through Logs Hell

Xavier Mertens - TF-CSIRT - Malaga 2020
<profile>

<name>Xavier Mertens</name>

<nick>xme</nick>

<jobs>

<day>"Cyber" Security Freelance</day>

<night>SANS ISC Handler, Blogger, Hacker</night>

</jobs>

<![CDATA[

https://xavier.mertens.consulting
https://blog.rootshell.be
https://isc.sans.edu
https://www.brucon.org

]]>

</profile>
The Idea

“One thing is for sure—you will make mistakes. Learn to learn from them. Learn to forgive yourself. Learn to laugh when everything falls apart because, sometimes, it will.”

— Vironika Tugaleva, The Art of Talking to Yourself
Log Management 101

“Log management comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.)”
(source: Wikipedia)

It covers:
Log collection
Centralized log aggregation
Long-term log storage and retention
Log rotation
Log analysis (in real-time and in bulk after storage)
Log search and reporting.
How is Your SIEM-Fu?
Sounds Familiar?

“We can ingest 15K EPS!”

“Our SIEM indexes 30GB/day”

“Our SOC gets 250 alerts/day”
The Story of the Manager...

Every morning, a Manager visited the SOC...

M: “Mornin’ No incident? Everything is fine?”

S: “Nothing, sir! All green!”

M: “Do I have to be happy or scary?”
The Logs Dilemma

Opportunistic

vs.

Use Cases
The Logs Dilemma

<table>
<thead>
<tr>
<th></th>
<th>“Opportunistic” Approach</th>
<th>“Use Case” Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>“Everything” is logged</td>
<td>Business oriented</td>
</tr>
<tr>
<td></td>
<td>Ideal for DFIR</td>
<td>Control of resources</td>
</tr>
<tr>
<td></td>
<td>Ideal to hunt</td>
<td>“ROI” reachable</td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>Consumes a lot of resources</td>
<td>Missing logs</td>
</tr>
<tr>
<td></td>
<td>Constant flood of events</td>
<td>Impression to be blind</td>
</tr>
<tr>
<td></td>
<td>“A needle in a haystack”</td>
<td>“Slow” start</td>
</tr>
<tr>
<td></td>
<td>Need constant fine-tuning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>False impression of security</td>
<td></td>
</tr>
</tbody>
</table>
Best of Both Worlds

- Start with a few use cases
- Add more use cases
- Get more resources
- Hunt & React

Learn the tool

Demonstrate to the management

Log more and more
It’s not a tool,
It’s a process...
Ready to dive?

Challenge

Accepted
Bad Stories

All described stories have been anonymised but have been faced in real environments...

No SIEM was harmed in the making of this slide deck! ;-)
#1 Nothing in place

Yes, it still happen in 2019...

No logs?

💡 Microsoft solution for free, ELK, Splunk
#2 Know your tools

Be sure to know what is logged, when and how

Example: A firewall in a company logged only dropped connection

💡 RTFM!
#3 Don’t trust Sysadmins

Do not let Sysadmins decide what they will log and send to your SIEM. Rogue Sysadmins could alter logs at source.

💡 Get the management support with you.
Logs value may change in time.

If you filter today, you may miss some logs tomorrow.

Depending on the business, new compliance requirements.
#5 Log Yourself

Be sure to avoid events generated by your log management platform to be indexed!

💡 You may explode your license or storage :)

💡 Use a management network for your platform flows.
#6 OSI Layer 4

Routing might have an impact (vpn), firewalls,

Docker network tool over Splunk VLAN
#7 Wrong index

A classic one...

Events sent to the wrong index

💡 The “default” index should not receive any event and, if it’s the case, an alert could be generated.
#8 Default Config

Default configuration applied will never return relevant information.

Ex: $VENDORS sell “PCI compliancy packages”

💡 You need to apply some “tags” to your assets.
“No, we don’t use IPv6!”

IP addresses decoded with `\d{1,3}.\d{1,3}\.\d{1,3}\.\d{1,3}/`

Then you start seeing this in logs:

```
2605:a601:ac73:9000:843a:14cf:73fa:a2d7 - - [11/Nov/2019:19:50:56 +0100] "GET /feed/ HTTP/1.1" 304 4953 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Thunderbird/68.1.1 Lightning/68.1.2"
```
A cluster of appliances had its configuration not synced
#11 Search loops

Create an alert when a term is seen
#11 Search loops

Edit Alert

- **Settings**
  - **Alert**
    - Mail from: be
  - **Description**
    - Optional
  - **Search**
    - index=syslog host=marge:be
  - **Alert type**
    - Scheduled
    - Real-time
    - Run every hour
    - At: 0 minutes past the hour
  - **Expires**
    - 24 minutes past the hour
- **Trigger Conditions**
  - **Trigger alert when**
    - Number of Results: greater than 0
  - **Trigger**
    - Once
    - For each result
  - **Throttle**
    - Off
- **Trigger Actions**
  - + Add Actions
  - When triggered
    - Send email
      - **To**: xavier(rootshell.be)
      - **Priority**: Normal
      - **Subject**: Splunk Alert: $name$
      - **Message**: The alert condition for "$name" was triggered.

Save
#12 Gaps in Logs

💡 Create an alert when a gap is detected
After an upgrade (scheduled by the owner of the application), the API used to collect events changed.
$VENDOR decides to re-assign old event ID’s to new events!
#15 Lack of CIM(1)

src_ip != source != scrip != ip

This is common issue when you deploy apps or collectors from 3rd parties

(1) Common Information Model
#17 SOC Fatigue

Too much false positives generate a fatigue that reduce the SOC capabilities to react.
NOT SURE IF LISTEN TO TOO BAD EXAMPLES OR WE'RE ALL DOOMED
Rule #1

Most of the time, issues will be discovered when you need to investigate...

Implement rules to perform self-monitoring

Example: to detect gaps
Rule #2

Implement test scenarios to validate your use cases!
Rule #3

In your playbook, reserve some time to review and update rules
Sigma to the Rescue

title: Cobalt Strike DNS Beaconing
status: experimental
description: Detects suspicious DNS queries known from Cobalt Strike beacons
references:
  - https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
author: Florian Roth
date: 2018/05/10
logsource:
category: dns
detection:
  selection:
    query:
      - 'aaa.stage.*'
      - 'post.1*'
  condition: selection
falsepositives:
  - Unknown
level: high
Use-Cases Reverse Engineering
Thank You!

Question?