

# A Walk Through L<sup>o</sup>g<sup>s</sup> 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>
```



Follow  
me!



# 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?





# S😺ounds 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 L<sup>o</sup>gs Dilemma

Opportunistic

vs.

Use Cases

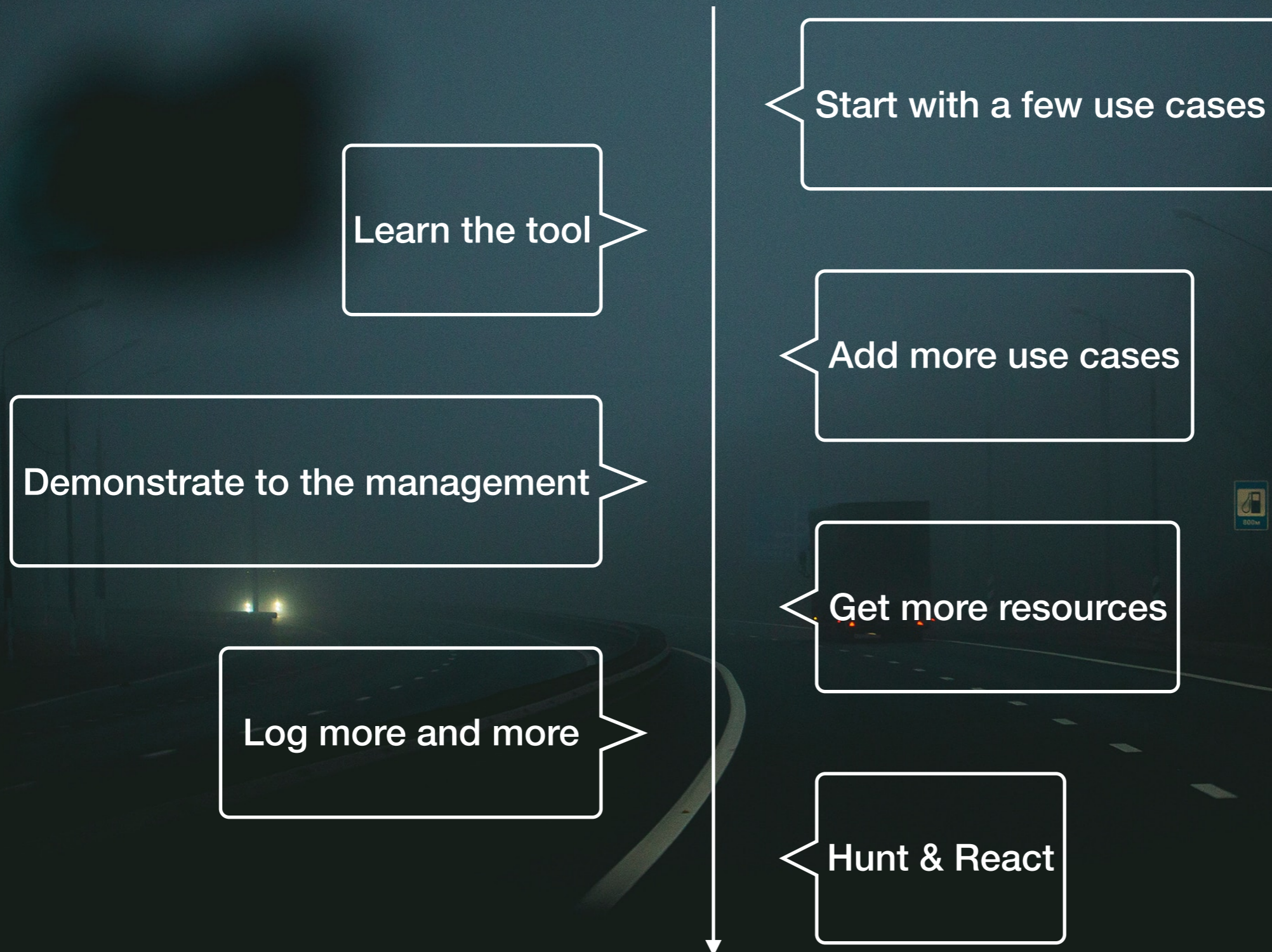


# The L<sup>o</sup>gs Dilemma

	<b>"Opportunistic" Approach</b>	<b>"Use Case" Approach</b>
<b>Pro</b>	<ul style="list-style-type: none"><li>● "Everything" is logged</li><li>● Ideal for DFIR</li><li>● Ideal to hunt</li></ul>	<ul style="list-style-type: none"><li>● Business oriented</li><li>● Control of resources</li><li>● "ROI" reachable</li></ul>
<b>Con</b>	<ul style="list-style-type: none"><li>● Consumes a lot of resources</li><li>● Constant flood of events</li><li>● "A needle in a haystack"</li><li>● Need constant fine-tuning</li><li>● False impression of security</li></ul>	<ul style="list-style-type: none"><li>● Missing logs</li><li>● Impression to be blind</li><li>● "Slow" start</li></ul>

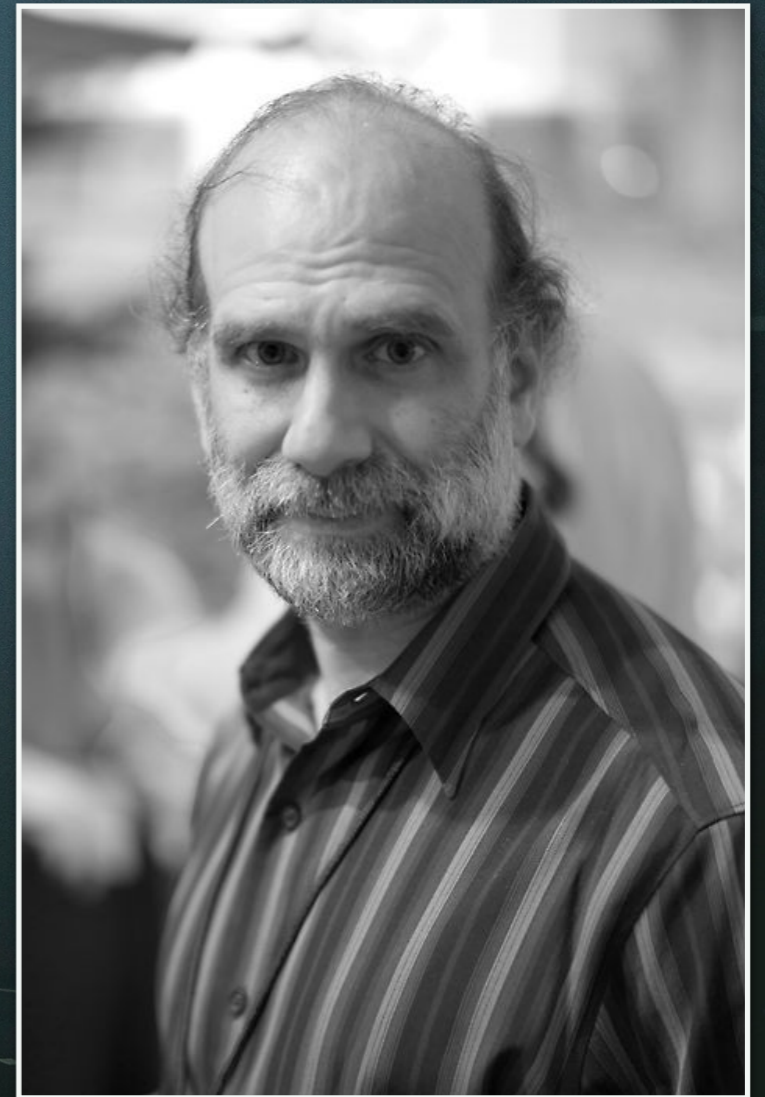


# Best of Both Worlds





It's not a tool,  
It's a process....





Ready to 😊 dive?





# Bad St☺ories

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 N<sup>o</sup>thing 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 D<sup>o</sup>n'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.



# #4 T🐱day != T🐱m🐱rr🐱w

Logs value may change in time.

If you filter today, you may miss some logs tomorrow

Depending on the business, new compliance requirements





# #5 L🐱g Y🐱urself

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 😺 SI 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 C<sup>o</sup>nfig

Default configuration applied will never return relevant information.

Ex: \$VENDORS sell "PCI compliancy packages" 

💡 You need to apply some "tags" to your assets.



# #9 Bad Decoders

"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"



# #10 Misc🐱nfiguration🐱n

A cluster of appliances had its configuration not synced





# #11 Search | 😺😺 ps

Create an alert when a term is seen






# #11 Search | ps

### Edit Alert

**Settings**

Alert **Mail from .be**

Description

Search .be"/>

Alert type  Scheduled  Real-time

Run every hour ▾

At  minutes past the hour

Expires  hour(s) ▾

**Trigger Conditions**

Trigger alert when

Trigger  Once  For each result

Throttle?

**Trigger Actions**

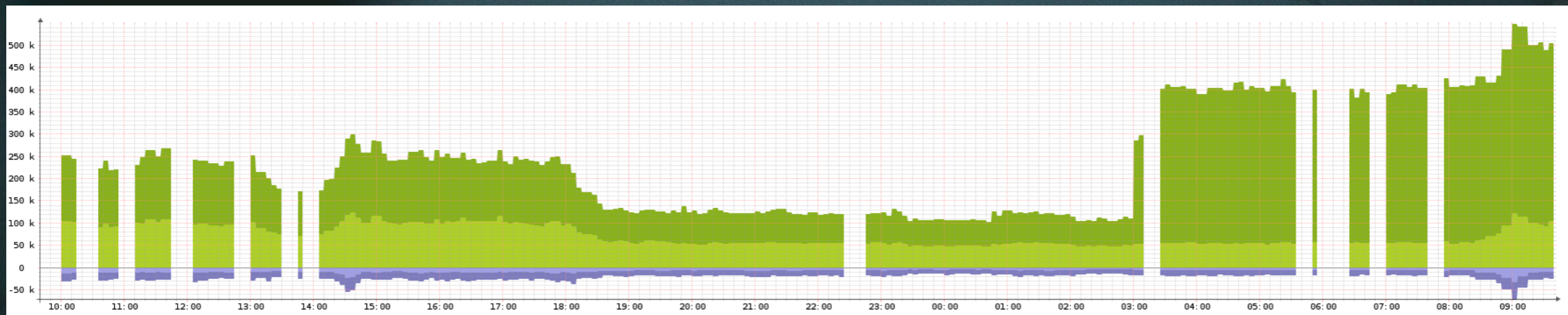
+ Add Actions ▾

When triggered

Send email	<input type="text" value="xavier@rootshell.be"/>	Comma separated list of email addresses. <a href="#">Show CC and BCC</a>
Priority	<input type="text" value="Normal ▾"/>	
Subject	Splunk Alert: <b><input type="text" value="\$name\$"/></b>	The email subject, recipients and message can include tokens that insert text based on the results of the search. <a href="#">Learn More</a>
Message	The alert condition for ' <b><input type="text" value="\$name\$"/></b> ' was triggered	



# #12 Gaps in Logs 🐱



💡 Create an alert when a gap is detected



# #13 Upgrades

After an upgrade (scheduled by the owner of the application), the API used to collect events changed.





# #14 Reused Event ID's

\$VENDOR decides to re-assign old event ID's to new events!





# #15 Lack of CIM<sup>(1)</sup>

```
src_ip != source != scrip != ip
```

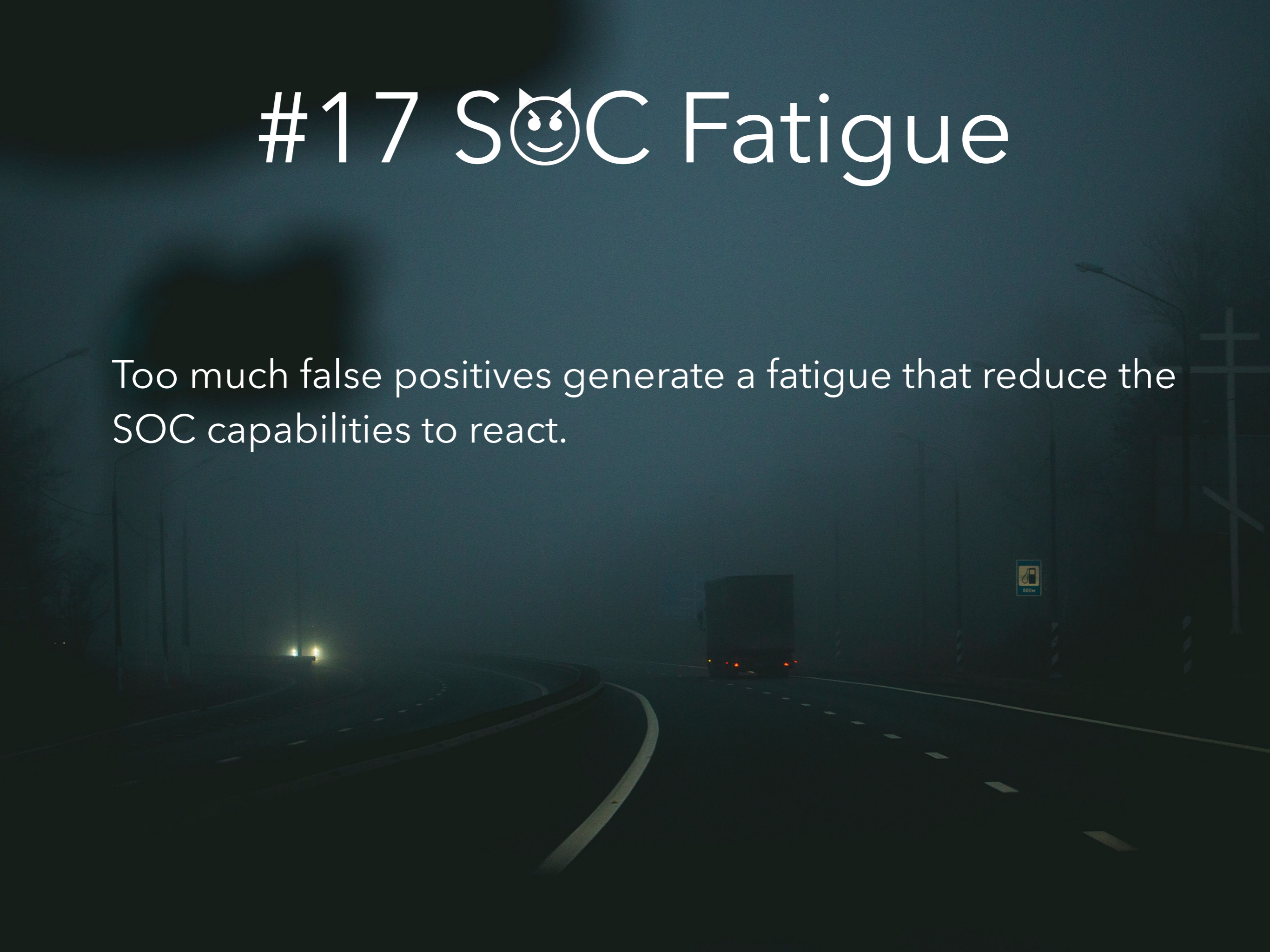
This is common issue when you deploy apps or collectors from 3rd parties

<sup>(1)</sup> Common Information Model



# #17 S☺C Fatigue

Too much false positives generate a fatigue that reduce the SOC capabilities to react.





Enough?





# Guid 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



# Guid Rule #2

Implement test scenarios to validate  
your use cases!



# Git Rule #3

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



# Sigma to the Rescue

**title:** Cobalt Strike DNS Beaconsing

**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

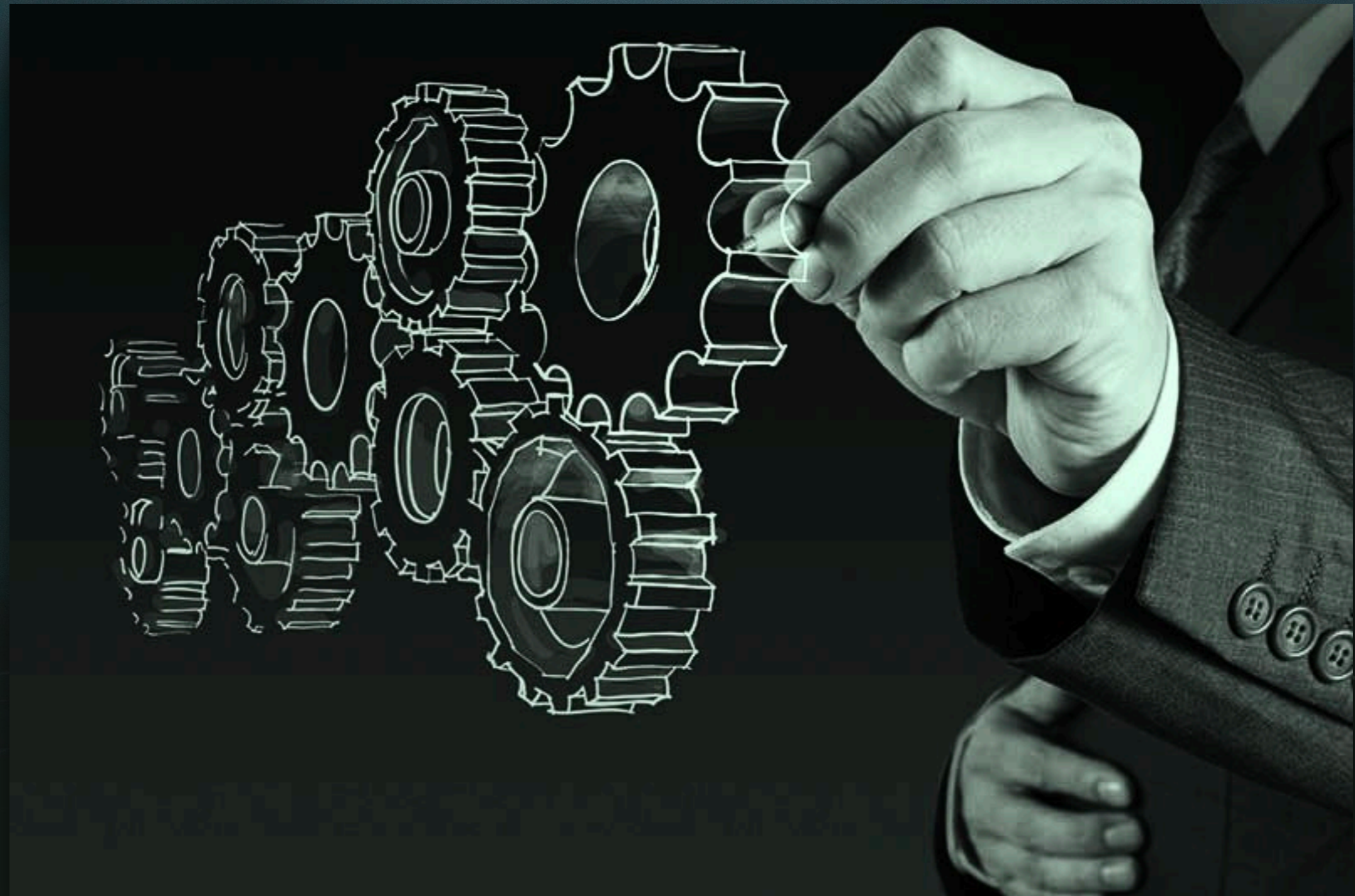
**falsepositives:**

- Unknown

**level:** high



# Use-Cases Reverse Engineering





Thank You!  
Question?

