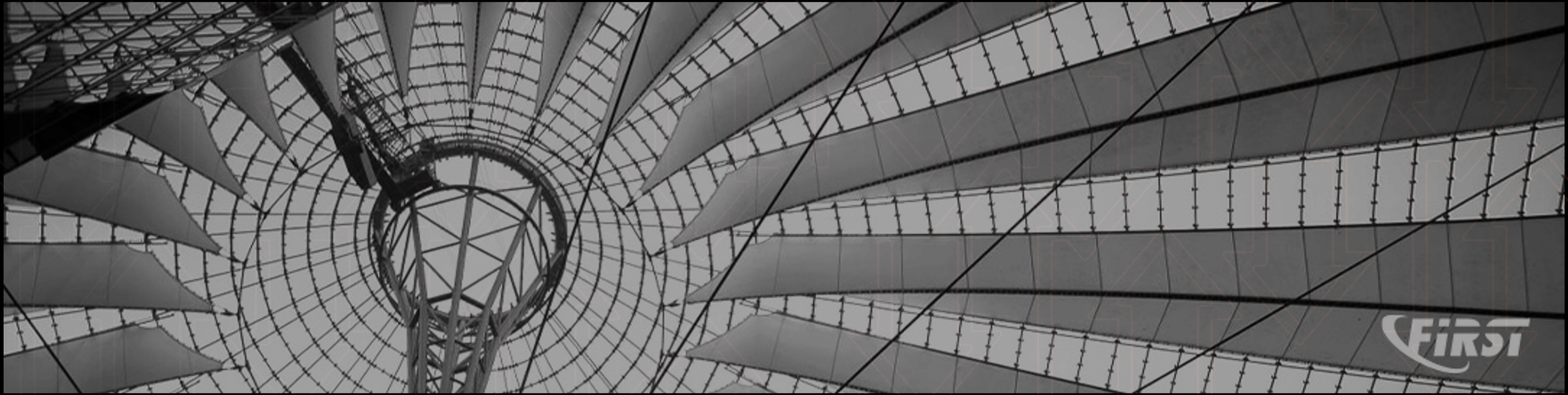
ticura

How much Alert Fatigue is actually Threat Intel Fatigue?

2023-11-08 Markus Ludwig TLP:CLEAR



We all know what fatigue is, don’t we?

“Fatigue in a medical context is used to cover experiences of low energy that are not caused by normal life.”

https://en.wikipedia.org/wiki/Fatigue

“The term alert fatigue describes how busy workers (in the case of health care, clinicians) become desensitized to safety alerts, and as a result ignore or fail to respond appropriately to such warnings. This phenomenon occurs because of the sheer number of alerts, and it is compounded by the fact that the vast majority of alerts generated by CPOE systems (and other health care technologies) are clinically inconsequential—meaning that in most cases, clinicians should ignore them.”

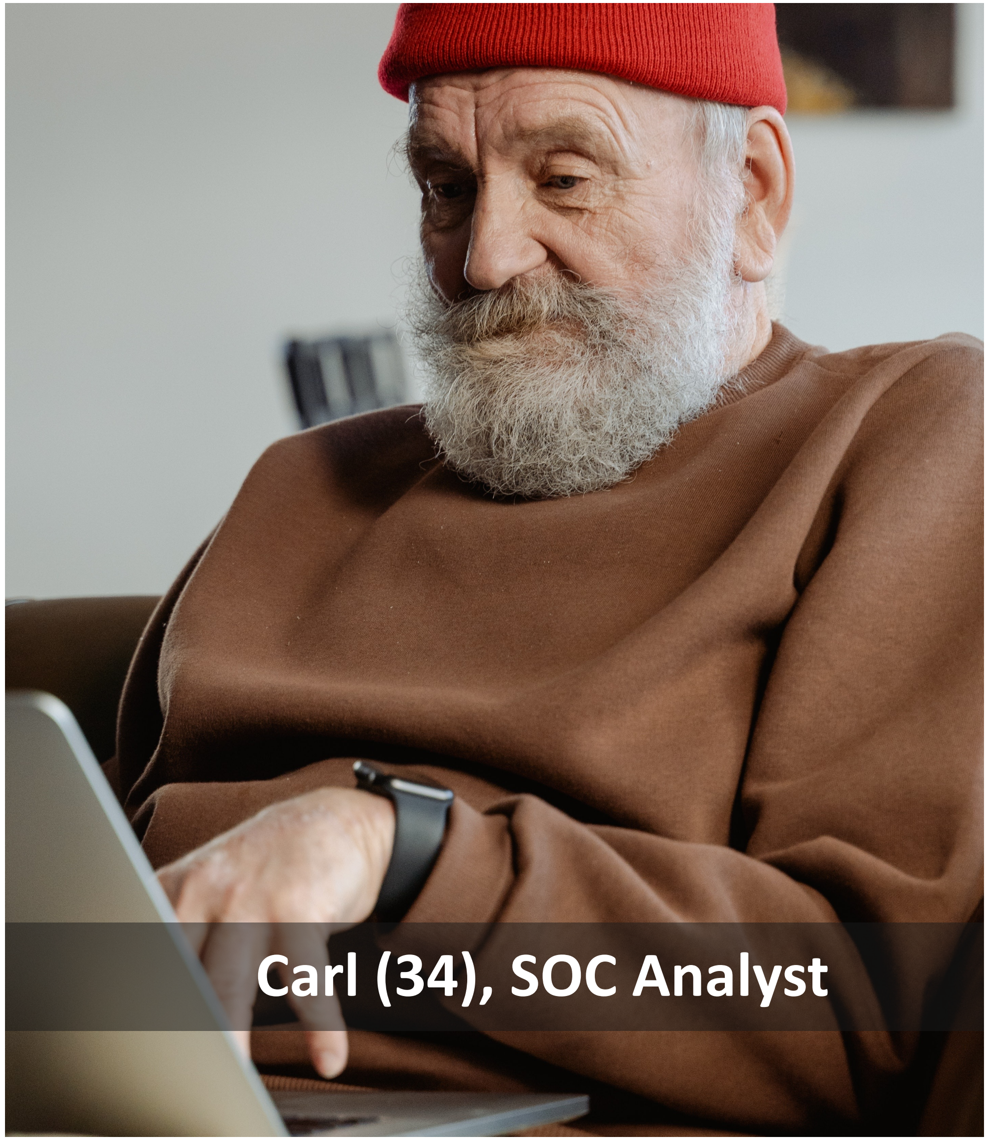
https://psnet.ahrq.gov/primer/alert-fatigue

Alert fatigue – so what?

25 % of analysts work time is wasted with false alerts *

80 % of cybersec professionals feel some level of burnout *

2.7M is the gap of cybersecurity professionals worldwide *



Carl (34), SOC Analyst

* External information sources in Appendix SOURCES

ticura

Who’s to blame?

Default or outdated alert rules *

Malfunctioning software / hardware / people *

Irrelevant, redundant or misinterpreted data **

20 % of all alerts are false positives *

40 % of all alerts are low priority *

* External information sources in Appendix SOURCES

Why's of “Threat Intel Fatigue”

Universe of Threat Intel is overwhelming

- No visibility of everything
- Not enough time to evaluate and measure
- Too dynamic

Overloaded teams give up trying to keep up, precursor of alert fatigue!

One-fits-All

- Average overlap:

Phishing URLs:	31%
Spam IPs:	11%
Anonymisation IPs:	72%
C2 IPs :	19%
Malware Downloads URLs:	7%

- Every use case / team / environment is different

Once picked ...

- Set and forget
- Checkbox feature of solution

The More-the-Better Trap

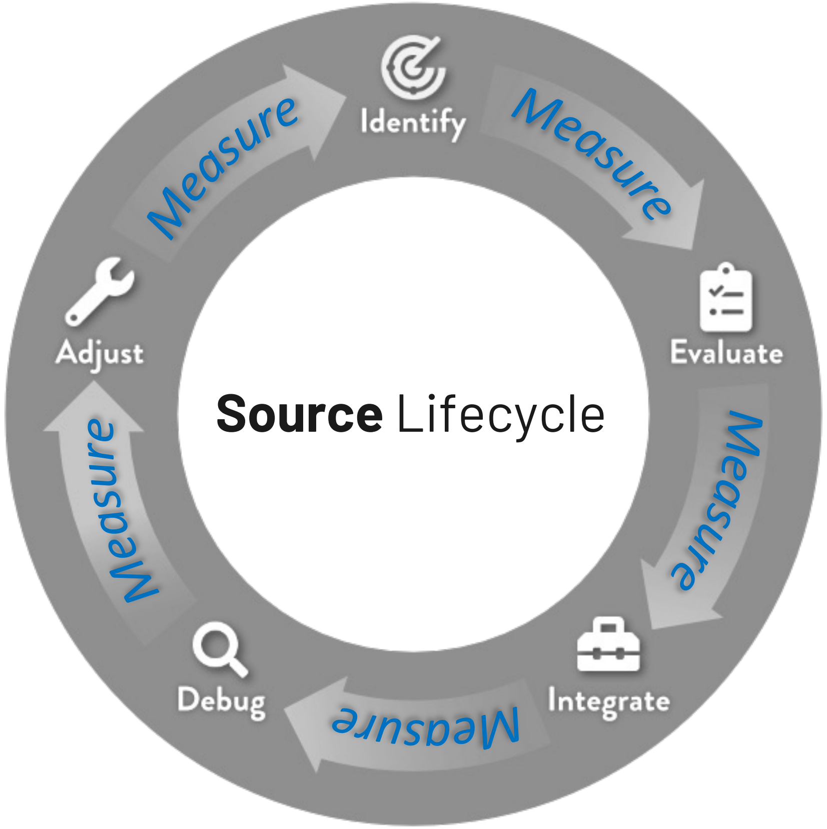
17	Sources are used on average
19 %	More potential noise per additional source
300 h	per source to evaluate, integrate, operate it
???	How much more can you keep up with?

* External information sources in Appendix SOURCES

ticura

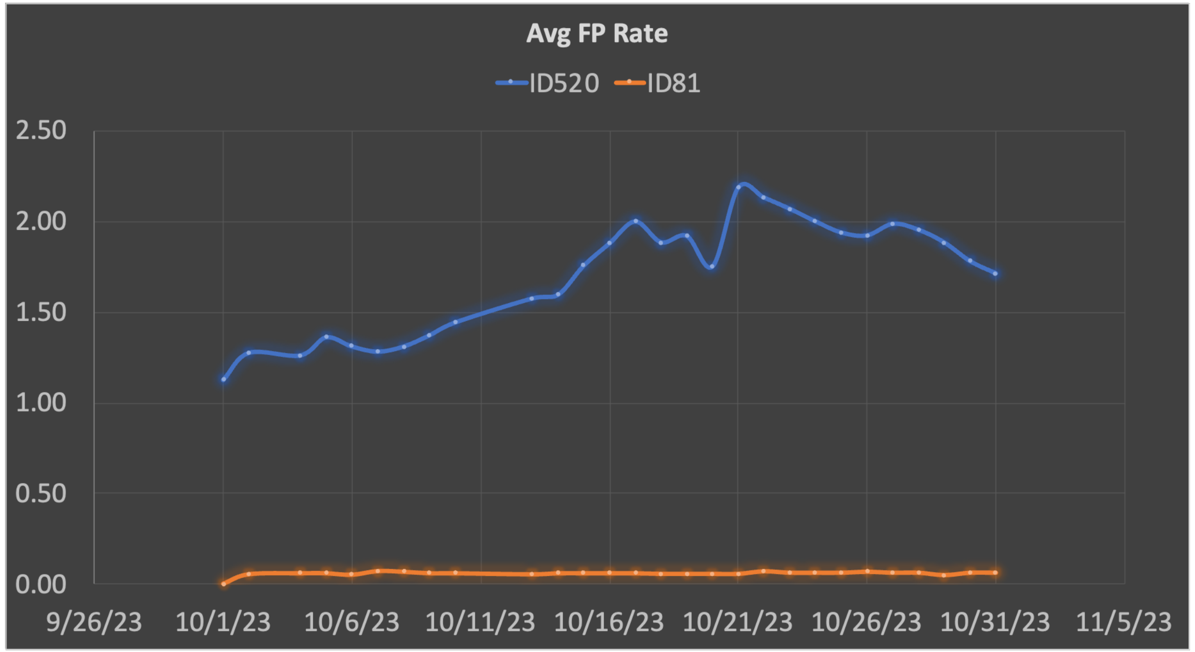
Awareness & Action vs Fatigue

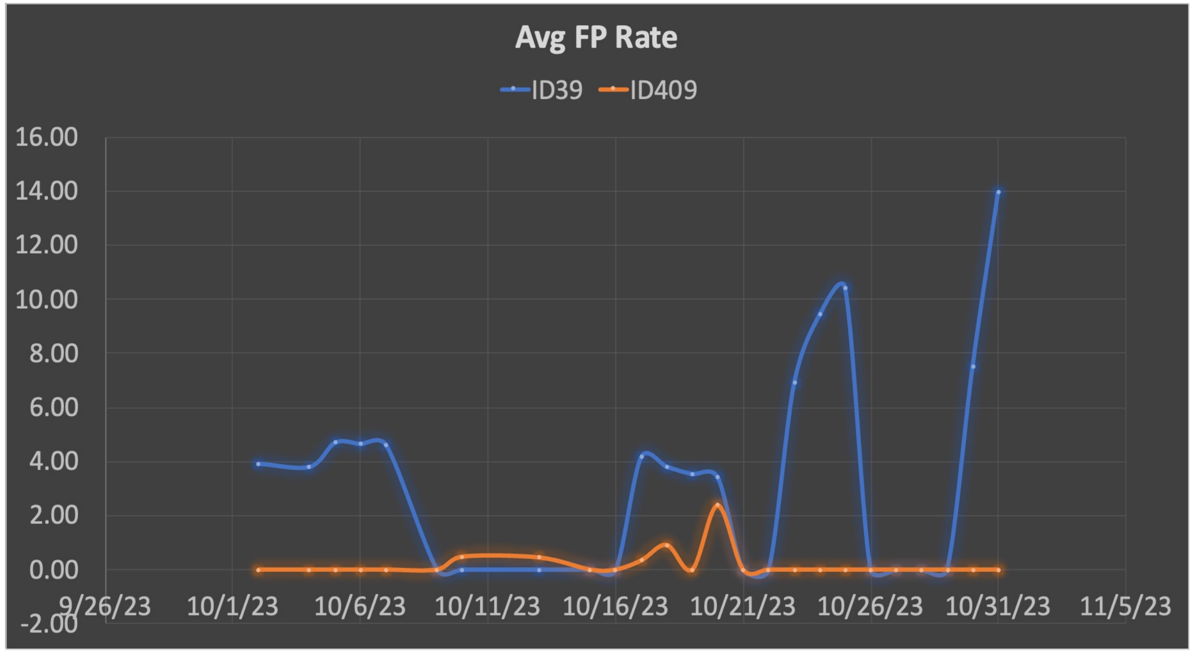
- Know the challenges in managing sources
- Measure at each step of the source lifecycle



* External information sources in Appendix SOURCES

Free your mind!





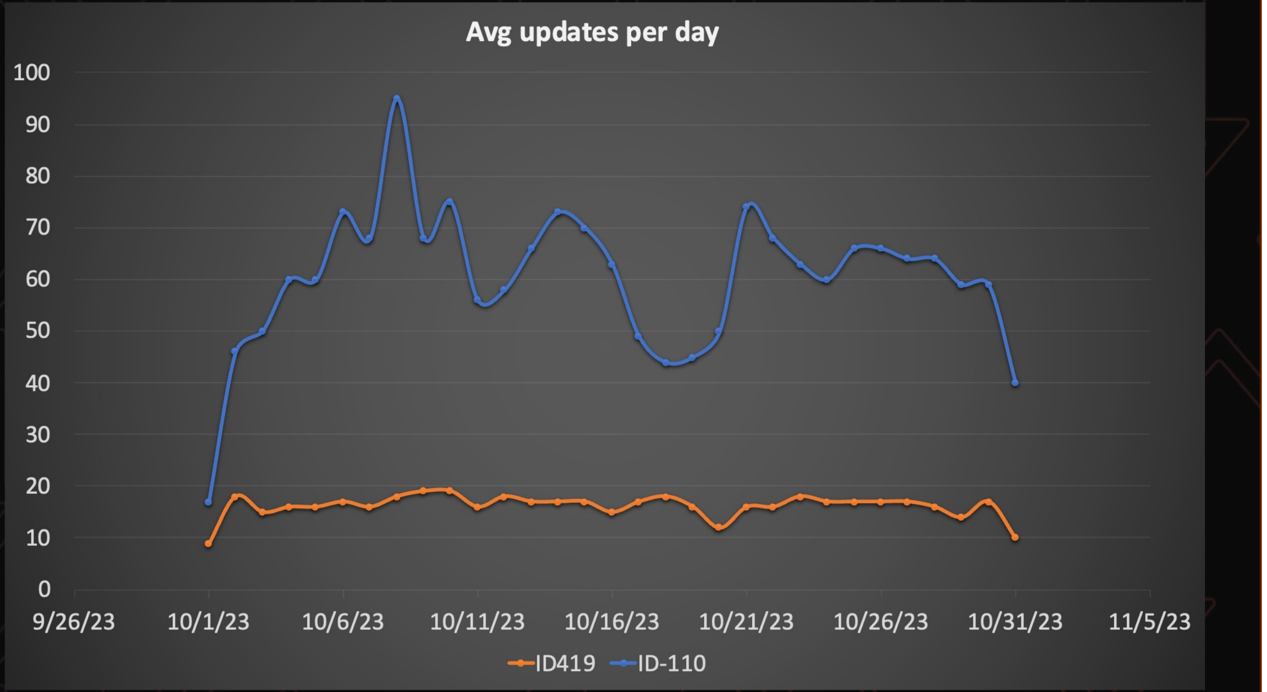
* External information sources in Appendix SOURCES

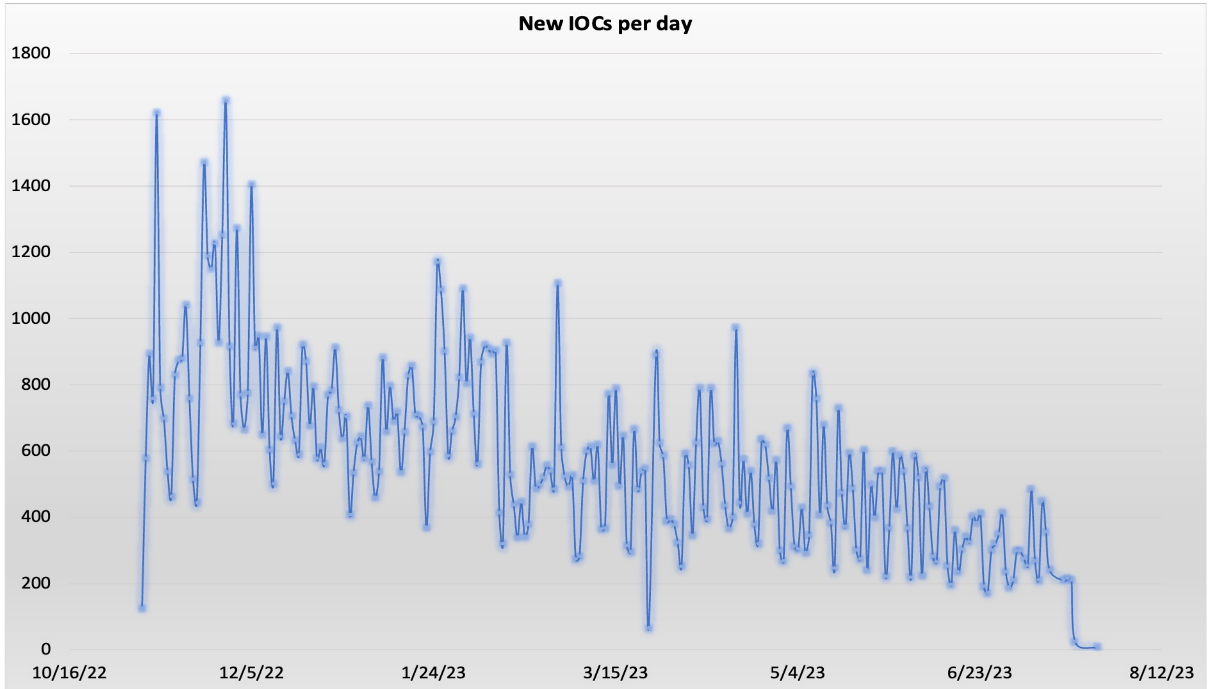
ticura

But ... where to start?

- What sources do you use today?
- Where do you use them for what?
- What can you measure quick & easy?

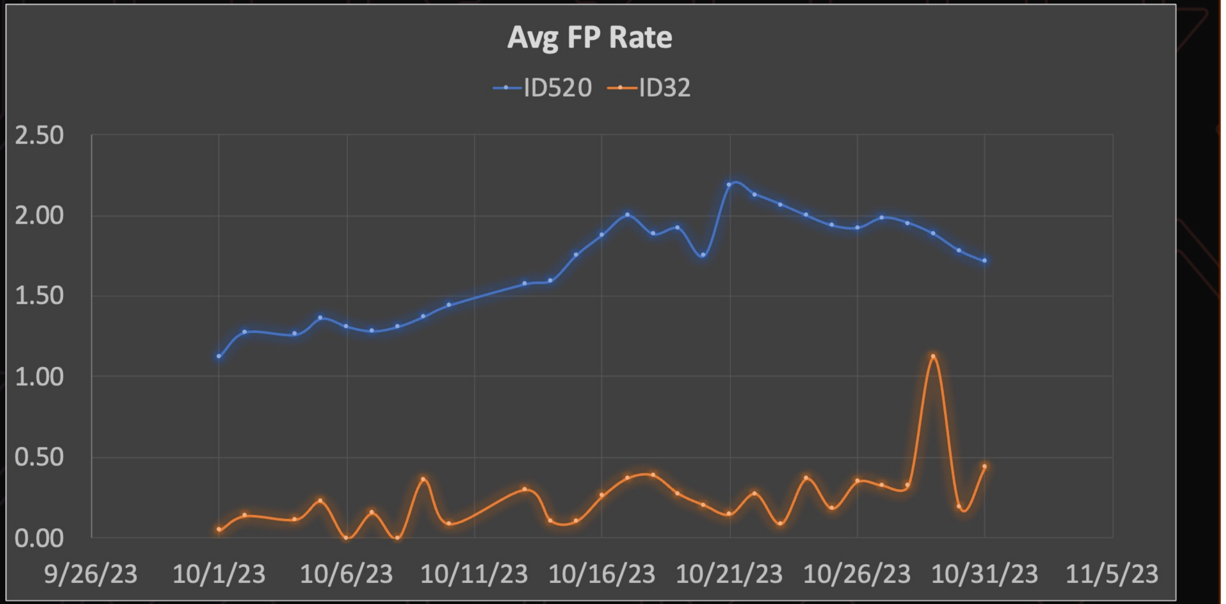
Lifecycle matters they said …

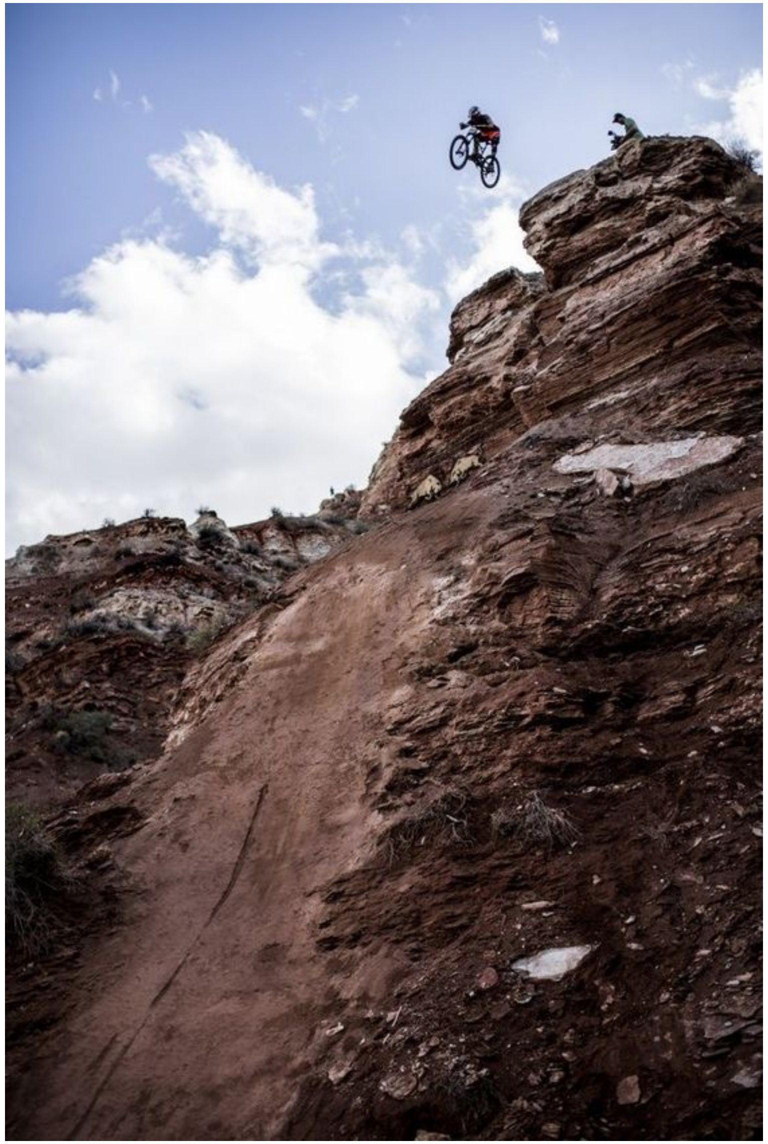




ticura

That can escalate quickly





ticura

Every beginning is hard

Start easy: Which use cases & sources, measure updates and volume / day

Improve: Measure false alerts, measure true positives, proactively adjust set of sources

Master it: Passive environment for continuous source evaluation, continuous scouting and adjustments,

....

Start easy, improve

- Tidying up vs. wasting your time
- Being aware and proactive eliminates fatigues!

Continuously, even if it’s boring.

Thanks

ticura

Ludwig-Erhard-Straße 4, D-34131 Kassel
https://ticura.io · info@ticura.io

Sources

- https://securityboulevard.com/2019/09/false-positives-and-negatives-the-plague-of-cybersecurity-software/#’
- https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021
- https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment
- https://resources.runpanther.com/hubfs/Marketing%20Materials/Reports/Life%20As%20A%20Security%20Engineer
- https://www.forrester.com/report/How-To-Integrate-Threat-Intelligence-Into-Your-Security-Program/RES160276
- https://purplesec.us/resources/cyber-security-statistics/#Cybercrime
- https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-
- 2021 of-business-investment
- https://www.atlassian.com/incident-management/on-call/alert-fatigue#How-to-avoid-alert-fatigue
- https://www.ibm.com/downloads/cas/5AEDAOJN
- https://www.helpnetsecurity.com/2019/08/29/soc-alert-overload/

- Memes from imgflip.com, quickmeme.com, knowyourmeme.com

*PLEASE NOTE: The referenced sources for statistics on false or low priority alerts provide a wide range, so we reference always the lowest of them.