SIEM Tuning vs. Alert Fatigue: Finding the Signal in the Noise

By Lucio Rodrigues

🚀 Introduction

In the world of cybersecurity operations, data is both a weapon and a weakness. SIEMs (Security Information and Event Management systems) are crucial for aggregating and correlating security logs, but when left unoptimised, they can quickly become overwhelming.

This post explores the delicate balance between SIEM tuning and managing alert fatigue, and how mastering this balance separates noise from true threats.

🧾 Abbreviation Summary

ATT&CK - **A**dversarial **T**actics, **T**echniques & **C**ommon **K**nowledge

TTPs - **T**actics, **T**echniques, and **P**rocedures

SLA - **S**ervice **L**evel **A**greement

IP - **I**nternet **P**rotocol

YAML - **Y**et **A**nother **M**arkup **L**anguage

JSON - **J**ava**S**cript **O**bject **N**otation

SIEM - **S**ecurity **I**nformation and **E**vent **M**anagement

---

📌 Understanding Alert Fatigue

Alert fatigue happens when analysts are bombarded by excessive alerts. Many of them are false positives, redundant, or low priority. This cognitive overload causes critical alerts to be missed, leading to delayed response times or, worse, breaches that go unnoticed.

🧩 Why SIEM Tuning Matters

SIEM tuning is the process of configuring your SIEM to minimise noise, enhance fidelity, and prioritise meaningful alerts. This isn't about turning off alerts recklessly, it’s about using intelligence and context to optimise visibility.

Key Tuning Techniques:

- Suppressing known false positives
  (e.g., allow-listed IP ranges, scheduled vulnerability scans)

- Threshold-based tuning
  (e.g., only trigger after multiple login failures within a short time frame)

- Use Case Prioritization
  Aligning alerts with critical assets or known attacker TTPs (MITRE ATT&CK)

- Custom correlation rules
  Creating logic that ties multiple benign events together to surface malicious behavior

---

📉 The Cost of Not Tuning

Without tuning:

- SOC teams face analyst burnout
- False positives drown out real threats
- SLAs on incident response time deteriorate
- Attackers thrive in the noise

A misconfigured SIEM doesn’t amplify security signals, it buries them - leaving critical alerts lost in a sea of false positives.

🧠 My Experience & What I’ve Learned

Working through real-world labs, I’ve seen firsthand how raw logs create more confusion than clarity unless filtered and contextualised properly.

For example, in a Splunk-based simulation, I noticed hundreds of password spraying attempts coming from a single IP, but without tuning, the alert was buried among unrelated low-priority events. After configuring correlation rules and filtering redundant alerts, I was able to surface the actual threat in under a minute, rather than digging through layers of irrelevant noise.

🔧 Key Takeaways

It’s important to understand:

- SIEMs are not plug-and-play.
- Tuning is a continuous process, not a one-time setup.
- Great defenders don’t just react, they refine.
- Reducing alert volume is not about doing less, it’s about focusing on what matters more.

I am committed to building environments where signal intelligence drives response, and threats don’t get lost in the static.

Final Thoughts

SIEMs are powerful, but only as smart as the people behind them. I believe tuning is where strategy meets action, where defenders turn information into intelligence. It’s not glamorous work, but it’s the difference between a team that reacts late and a team that responds fast.

I’ve made it my goal not just to detect threats, but to refine *how* we detect them.