Whitepaper

Hidden Risk Caused by Your SOC's Alert Prioritization: A Primer for CISOs & CIOs

In the ever-evolving cybersecurity landscape, Security Operations Centers (SOCs) play a crucial role in identifying and mitigating potential threats. However, the effectiveness of a SOC depends on its ability to manage and analyze the influx of alerts. Some security leaders have had SOC alert prioritization decisions made for them. Others are dealing with decisions that were made so long ago, no one remembers how they came to be. While other leaders feel certain in their decisions — e.g. "I measure our reduction in false positives." — these decisions may in fact have a compounding effect on your organization's security.

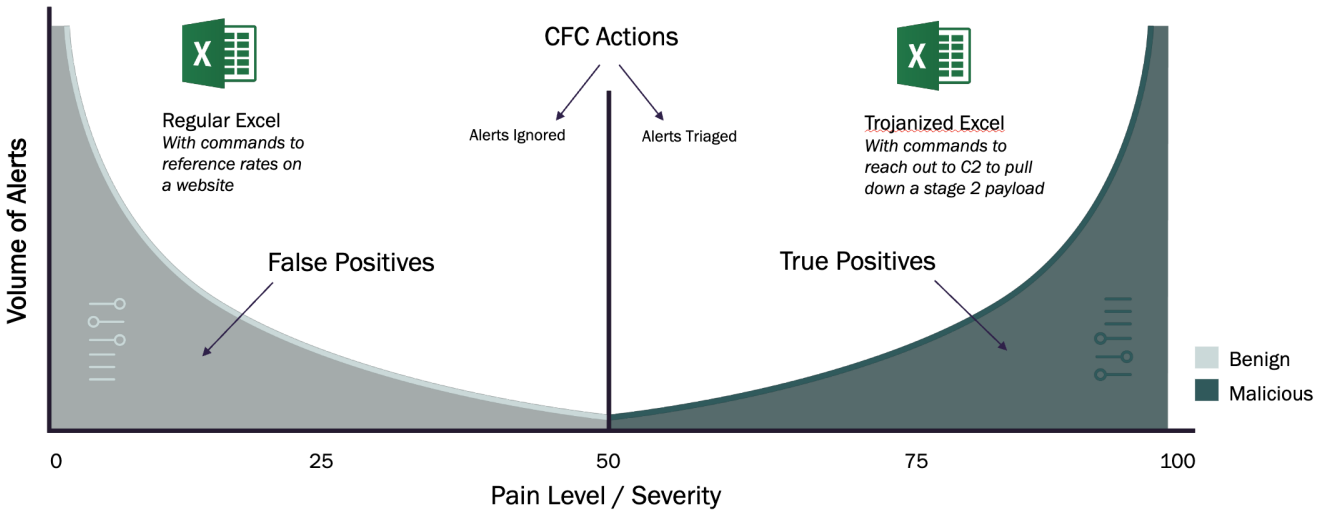
Let's dive deeper into key considerations for understanding and optimizing SOC performance.

Ideal State

For the purposes of reviewing the different models of alert detection and the inherent risks in those models, consider the following example.

> An organization has an Excel document reaching out to the Internet. There are both benign and malicious reasons why such a file would communicate online. A benign reason could be contacting legitimate sources to obtain something like the latest mortgage rates for calculations. A malicious reason might be that the document has been trojanized with an embedded macro that is reaching out to its command and control to download a stage one or stage two payload.

With this example in mind, let's explore how standard threat detection paradigms work. If alerts are generated on a pain level/security scale of 0 – 100, in an "ideal state," alerts with a severity level less than 50 would be considered benign, and anything above 50 would be considered to have at least some degree of maliciousness. In this ideal, it's very easy to sort the good from the bad - anything less than 50 the SOC can ignore and anything over 50 should be triaged.

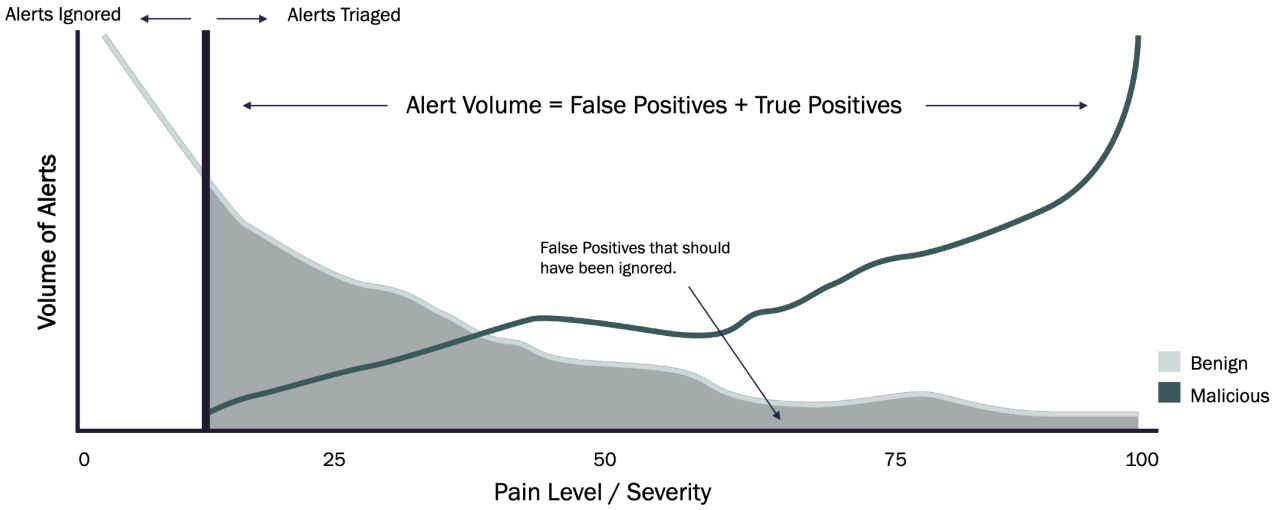


Unfortunately, this ideal doesn't represent the reality of the threat landscape in which cybersecurity professionals operate.

The "I Don't Want to Miss Anything" Approach

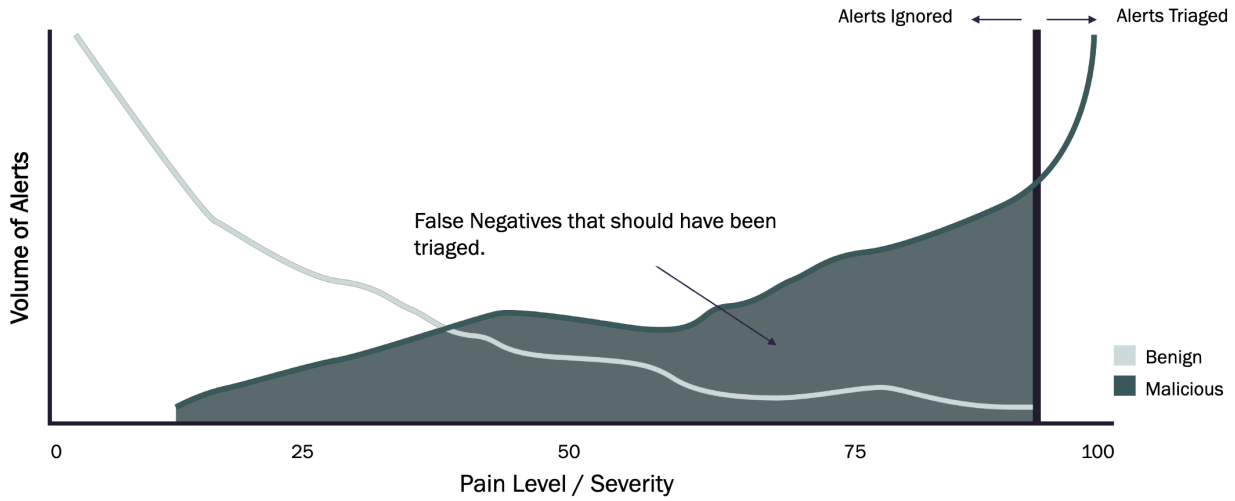
Different security leaders take different approaches in determining what alerts to ignore and what alerts to triage. One school of thought is, "I don't want to miss anything." It's understandable why a cybersecurity leader might think this way, and functionally this approach is easy to achieve. Operationally though, it is very difficult to accomplish.

In the spirit of not missing anything, you begin to introduce alert fatigue into your SOC. Personnel become so overwhelmed with threat alerts that alert fatigue sets in, resulting in an increased risk of missing a viable security threat.



The "I Only Want High-Fidelity Alerting" Approach

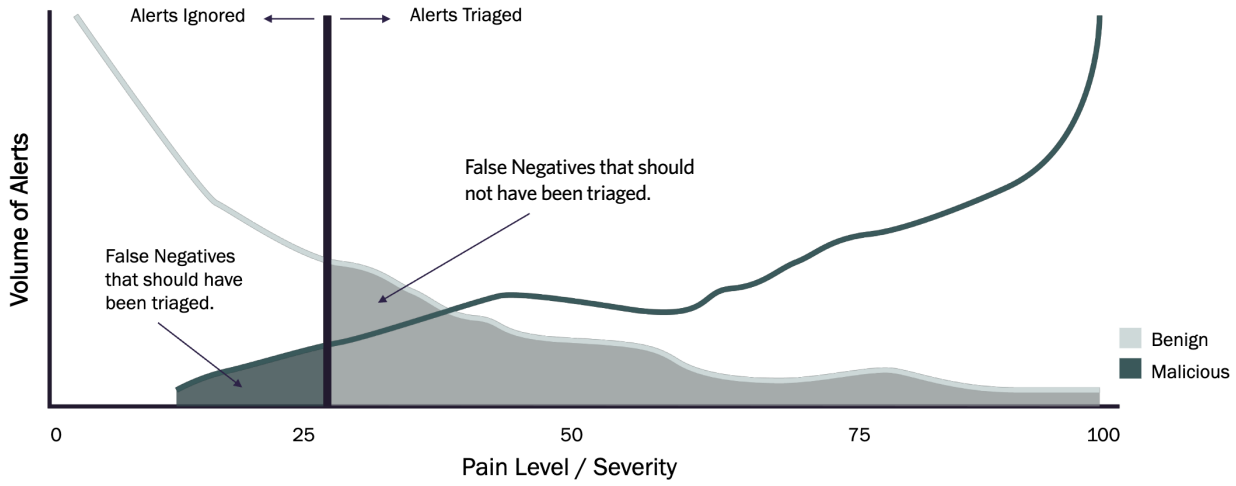
At the opposite end of the spectrum, and in an effort to mitigate the risk of analysts drowning in false positives, some cybersecurity professionals may move to the other end of the model in an effort to only achieve high fidelity alerts. In this approach, the number of false positives is decreased, reducing alert fatigue. However, there is an inherent risk in this model as well – an increased likelihood of false negatives in which a legitimate threat triggers an alert but is ignored in the interest of efficiency.



The DeepSeas Approach

The DeepSeas approach is one of balance. We look at where the lines of benign and malicious alerts converge and willingly introduce a moderate increase in false positives in order to decrease the likelihood of false negatives.

In an effort to mitigate any remaining false negative risk, DeepSeas implements what we call “control intelligence” or “control detections.” One example of control intelligence could be a Microsoft Office document coming through the detection apparatus, in which case we would sandbox that document to increase the likelihood of elevating the severity level in the event the document is malicious. This very basic example is one of many methods SOCs can use to reduce the risk of false negatives getting through the system.



Key Takeaways

At some point, every cybersecurity operation has had to make the choice of how it will approach alert prioritization. More often than not, we find that the decision was made so long ago nobody can recall how the decision was made or the implied risks.

Common phrases leaders should look out for from their SOC teams are:

- **“There are just so many alerts.”**
- **“We only have time to focus on the high-risk alerts.”**
- **“We are constantly battling alert prioritization.”**
- **“The detection tools need to be tuned better.”**

Giving direction to a SOC like, “I don’t want to miss anything,” or “I only want high-fidelity alerts,” is ripe with risk. The “I don’t want to miss anything” approach dramatically increases false positives; thereby increasing the likelihood of missing something due to alert fatigue. The “only high-fidelity alerting” approach has obvious repercussions of false negatives.

The good news is that there is a balance that can be achieved.

> “Giving direction to a SOC like, “I don’t want to miss anything,” or “I only want high-fidelity alerts,” is ripe with risk.”

Dive Deeper

deepseas.com