7 Basic Habits to Follow to Minimize False Positives

1

Be proactive

Be proactive in your threat-management approach. If all you do is wait for alerts and alarms to go off, you will spend more time chasing false positives than you will on identifying real threats.

2

Begin with the end in mind

Focusing on your end goal—the most relevant threats you want to detect—will help reduce false positives.

3

Prioritize high-risk alerts

Prioritization is one of the best tools a SOC can use to minimize time spent on false positives.

4

Think win-win

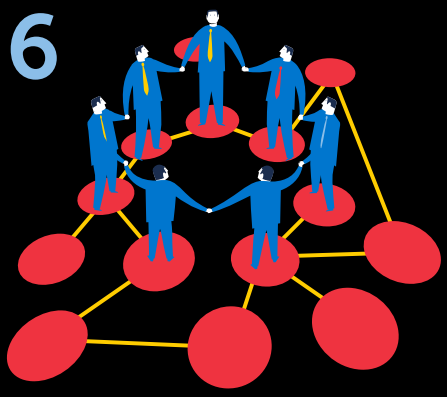
Choose collaborative intelligence sources that will bring different fidelity, relevance, and value to your security operations.

5

Seek first to understand

When implementing a tool, ensure that you fully understand why you're deploying it, rather than making assumptions about 'common' use cases, or worse...installing a tool with default settings.

6



Synergize

Use a set of clearly defined correlation rules and only send an alert to your work queue if all related correlation criteria are satisfied.

7

Sharpen the saw

Review all alerts and develop better alerting rules based on lessons learned.

To learn more, read the full blog post on the RSA Conference blog here:

How To Avoid Wasting Time On False Positives

RSAConference