



WRITING EFFECTIVE TRIAGE NOTES IN THE SOC

THE IMPORTANCE OF CLARITY, ACTIONABILITY,
AND LEADERSHIP SUPPORT

Abhishek Tripathi



AGENDA

Who am I?

What is an alert?

Triaging an alert?

Templating an alert?

Communicating with the Leadership

Questions?



ABHISHEK TRIPATHI

- Working in Cyber Security filed for last 7+ years in Security Operations
- <https://www.linkedin.com/in/atripathi0001/>
- <https://keybase.io/abhishektripathi>

WHAT IS AN ALERT?

NIST SP 800-150 defines alert as “a brief, usually human-readable, **technical notification** regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.”

In simple words, for a Security Operations Center, it’s **a trigger that matches a condition on a security tool** and needs to be looked at or triaged.

TRIAGING AN ALERT

An alert triage needs to answer **WHO, WHAT, WHEN, WHERE,** and **WHY?**

- ✓ **Who** was involved in the incident – user, account ?
- ✓ **What** triggered the alert – malware being downloaded, malicious URL click, vulnerability exploited?
- ✓ **When** timestamp when the alert occurred, not triggered, *timeline*?
- ✓ **Where** did the alert trigger - file path, hostname?
- ✓ **Why** the incident happen, *root cause*?

TEMPLATING AN ALERT TRIAGE

To maintain the **consistency** and make the process **repeatable**, its important to template it.

Root cause

- *Why did the alert trigger?*

Summary

- *Details of who, what, where, and why?*
- *Summarize the event that took place, add analysis even if it did give results.*

Mitigation/Remediation

- *Give outlines for remediation or mitigation*
- *URL block, patch, etc.*

Analysis

- *Detailed analysis contains logs, links to the OSINT*

COMMUNICATING WITH THE LEADERSHIP

It is important that we communicate **clearly with actionability** to the leadership for their support.

Examples of root cause that **drives** strategic leadership actions:

- User clicked a malicious link → the end users need training
- A vulnerability was exploited → Patch is needed, review path process
- An unsecure protocol was used e.g., ftp → Review application using unsecure protocol

A series of white, overlapping geometric lines and polygons on a black background, located on the left side of the slide.

QUESTIONS?

A series of white, overlapping geometric lines and polygons on a black background, located on the left side of the slide.

THANK YOU