ANALYTICAL THINKING FOR SOC ANALYSTS

Topic: Mental Models for Better Investigations

---

1. Why analytical thinking matters in SOC

A SOC analyst's main job is NOT just clicking alerts.
The real work is:

- collecting raw data
- adding context
- analyzing behavior
- forming a hypothesis
- validating with evidence
- reporting facts clearly

Good decisions come from **structured thinking**, not guessing.

---

2. Key mental models learned today

These mental models help avoid bias, panic, and wrong conclusions.

Hanlon's Razor – "Not everything bad is malicious"

Meaning:
Many alerts come from **human mistakes or misconfigurations**, not attackers.

Before assuming attack:

- check user actions
- check IT changes
- check VPN/device behavior
- check password issues

Use this to **stay calm and logical**.

Ockham’s Razor – “Start simple first”

Meaning:
The simplest explanation is often correct.

Example:
Failed login attempts may just be:

- wrong password
- expired credentials
- MFA failure

Start with simple causes → move to complex only if needed.

This saves investigation time.

Begging the Question – Avoid circular reasoning

Wrong thinking:

“This alert is malicious because the tool flagged it.”

Correct thinking:

- alert
- evidence
- validation
- conclusion

Tools **raise suspicion**, they don’t prove truth.

Cognitive Bias – Your brain can mislead you

Common biases in SOC:

- confirmation bias → only looking for evidence that supports your idea
- anchoring bias → sticking to your first assumption
- availability bias → thinking something is common because you saw it recently

How to reduce bias:

- check multiple data sources
- ask “what else could explain this?”
- get a second opinion when unsure

Good analysts stay **neutral and evidence-driven**.

Falsification – Try to prove yourself wrong first

Instead of:

“I think it’s malware. I’ll prove it.”

Ask:

“If this is NOT malware, what would I expect to see?”

Test alternative explanations.
If they fail, confidence increases.

This prevents tunnel-vision.

---

3. How these models work in a real alert

Example alert: unusual login from new country.

Correct investigation flow:

- maybe VPN or travel? (Hanlon)
- start with simple checks (Ockham)
- don’t assume because tool alerted (no circular logic)
- avoid bias — collect objective logs
- test different explanations (falsification)

Result: decisions are **calm, logical, documented**.

---

4. Key Takeaways

- Tools show data — **thinking finds truth**
- Don’t assume attack too early
- Evidence > assumptions
- Always question yourself
- A SOC analyst is part detective, part scientist

Analytical discipline protects organizations just as much as technology.