The world is how we shape it

sopra steria

Communication between **SOC and Executives**

Why security fails at the language layer –
and how to fix the signal before it reaches the boardroom

Security fails at the language layer

It’s the exhausted brain and the emotional awareness

01 **The SOC speaks in alerts, packets and probabilities.**
Technical truth that doesn’t translate.

02 **The board speaks in risk, revenue, and reputation.**
Business truth that doesn’t wait.

03 **The communication chain loses quality and accuracy.**
Breaches not in the firewall; in the translation

It’s 03:00 AM. Your SOC just detected something …

9 AM, CEO arrives and asks:

« Are we okay? »

sopra steria

Four acts

Each one a piece of the same communication chain

I

THE GAP

Why SOC and CxO talk past each other.

II

THE COST

What happens when the signal get lost.

III

THE HUMAN

Framing, bias, and the dopamine loop.

IV

THE REBUILD

A maturity path from plug-in to delivery.

I.

THE GAP

When analysts speak Wireshark and executives hear white noise.

sopra steria

A new incident appear

THE ANALYST

Lateral movement detected

- Ps Exec from ADMIN$ share.
- Suspicious parent-child process tree.
- T1021.002 – SMB/Windows admin Shares.

Confidence: 87%. Dwell: 14 min.

THE BOARD

Is the business at risk?

- Will we make earnings?
- Is customer data exposed?
- Do we have to disclose?

How long until we recover?

Same incident. Different words.

Both are accurate. Only one causes a decision for executives.

THE ANALYST REPORT

Lateral movement detected

"We're seeing Powershell execution with encoded payloads on three endpoints – hash matches a known Cobalt Strike beacon. Likely T1059.001 with T1071.

I've isolated the hosts and pulled memory."

THE SAME THING, TRANSLATED

Is the business at risk?

"Someone just tried to plant a remote-control tool on three of our laptops. We caught it in minutes. No data left the company.

We want 48h to confirm how they got in."

Precision doesn’t equal clarity.

WHAT THE SOC PERCIEVES

A technically perfect report.

- 42 IOCS. 7 TTPS. 3 kill-chain stages.
- Full MITRE ATT&CK mapping.
- 12 pages of packet captures.

Sent at 04:17. Read at 10:34.

WHAT THE BOARD NEEDS

Three answers. Thirty seconds.

- What happened?
- What’s the exposure?
- What do you need from us?

Delivered before the next meeting.

Data lives in three states.

Show the wrong state to the wrong audience – and you create chaos.

TACTICAL	OPERATIONAL	STRATEGIC
Raw & granular	*Contextual*	*Financial*
• IPs, hashes, registry keys • Tools, queries, signatures • Speaks in log lines	• TTPs, campaigns, kill chains • Queue, SLA, trends • Speaks in dashboards	• *Loss, ROI, regulatory exposure* • *Board-ready narrative* • *Speaks in consequences*
→ **machines & Analyst/Engineers**	→ **SOC teams & Managers**	→ **C-suite & Board**

From trenches to boardroom, we lose 98% of the signal

Every handoff is a translation that costs fidelity – *every translation is a chance to lose the truth or distort the decision.*

Fidelity: **100%**	Fidelity: **20%**	Fidelity: **2%**
Raw telemetry *High-volume, ambiguous*	**Triaged alerts** *Summarized, prioritized*	**Board-ready brief** *Decision-grade, business framed*
• 2847 alerts today, 12 analyzed • Host beaconing to an IP every minute • Possible C2 over DNS	• One possible intrusion. Two unknowns. • Investigating workstation in Sales • ETA on triage: 4 hours	• *Suspected breach. Sale system at risk.* • *Exposure up to 8MNOK. Decision needed* • *Recommend: Isolate, call IR*

Speak money. Even Once.

Cyber Risk Quantification *(CRQ)* turns vulnerabilities into financial exposure.

25MNOK → 0.5MNOK

Current annual exposure → MFA rollout. ROI: 50 : 1

sopra steria

II.

THE COST

What happens when the signal get lost.

We don’t fix the garbage

We just buy bigger trucks.

TREATING THE SYMPTOM

Volume as proof of work

- Hire more L1s.
- Buy more AI.
- Bigger queues. Faster closes.

“We handled 12 000 alerts this week.”

TREATING THE DISEASE

Signal as proof of value

- Tune the detection rules.
- Kill the 90% false positives.
- Give analysts time to think and analyze.

“We stopped 3 attack that would have mattered.”

In medicine, the senior does triage

In cybersecurity, we hand it to the newest hire.

EMERGENCY RESPONSE (ER) MEDICINE

- ❑ Veran nurse at the front door.
- ❑ Senior physician for ambiguous cases.
- ❑ Interns in the back, learning.

Diagnosing severity is the hardest skill.

THE STANDARD/MODERN SOC

- ➢ Junior L1 at the front door.
- ➢ Limited time per alert – queue size enormous.
- ➢ Seniors hidden behind an escalation queue.

… We're shocked when they miss the coronary.

Pattern complacency & Symbolic analysis

When normal is the warning

Pattern Complacency: Same alert, every day.

- High volumes of false positives cause cognitive fatigue, leading analysts to dismiss potentially critical threats as "as expected". Yesterday's suspicious behavior becomes normalized into today's baseline.

- After two weeks, the team calls it "expected". After four weeks they stop analyzing it.

Symbolic Human Analysis: Ambiguous context, risk profiling.

- The pressure to "clear the queue" forces analysts into symbolic human analysis – merely checking boxes and passing information up the chain without taking the time to understand the true risk profile. The human becomes a router, not an analyst.

- The analyst is not taking the context into consideration. The brain is overworked and applies shortcuts.

Seven days of “as expected,”

Example case study of one week of ransomware attack.

DAY 1

Unusual login from VPN.

“As expected – we see this weekly.”

DAY 4

PowerShell on a file server

“As expected – admin tooling.”

DAY 7

1,400 files encrypted

“Oh.”

The reports are beautiful

The numbers tell a story that’s almost true

99.4%

Closure rate

8,400 alerts this month

Page 7

50 high-severity alerts for *impossible travel*

All closed: "expected behaviour”

If it’s truly expected – why are we alerting on it at all?

sopra steria

Three numbers. None of them answer “are we okay?”

If you can’t translate them, someone else will – and they’ll be wrong.

MTTD

Mean time to Detect

- Measured in minutes
- Reported as a win
- Doesn’t tell you what you missed

→ **181 days**

MTTR

Mean time to Respond

- Measured in hours
- Includes the wrong incident
- Average hides the outlier

→ **60 days**

DWLL

Dwell time

- *Measured in days*
- *The only number attacker cares about*
- *The one the board doesn’t see*

→ **241 days**

III.

THE HUMAN

Framing, bias, and the dopamine loop.

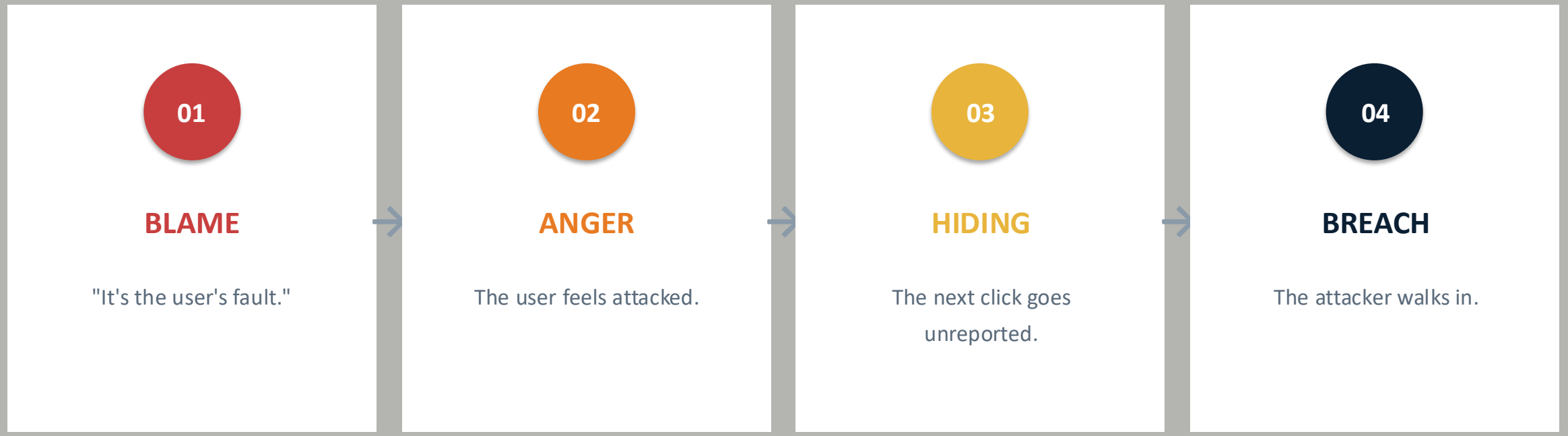
Framing chooses the emotion; *Emotion chooses the action*

	BLAME	THREAT	ADVOCACY	ASSURANCE
Framing	"Users clicked the link."	"They'll hit us next."	"We stopped it in time."	" Here's what we learned."
Emotion	• **ANGER**	• **FEAR**	• **PRIDE**	• **HOPE**
Action	• *Punish the outgroup*	• *Seek protection*	• *Defend status*	• *Steady participation*

sopra steria

“The user is the weakest link.”

Tell people they’re a threat, and they start acting like one.



The analyst isn’t lazy. They’re human.

Their brain is doing exactly what it is meant to do – take shortcuts under pressure.

CONFIRMATION

You see what you expect to see.

If yesterday’s alerts were benign, today’s alerts look benign too.

ANCHORING

The headline and first number wins.

The alert arrives as “low severity”. The analyst rarely changes it.

AVAILABILITY

Recent beats important.

Whatever we saw yesterday feels more likely than the quiet outline.

ACH: starve the dopamine loop.

Analysis of Competing Hypotheses

THE DOPAMINE TRAP

One hypothesis. Fast conclusion.

1. Form a theory.
2. Look for evidence that proves it.
3. Get a dopamine hit on every match.
4. Ignores what contradicts.

"Fast. Closed. Potentially wrong."

THE ACH CIRCUIT BREAKER

Many hypotheses. Weighed evidence.

1. List ALL hypotheses first.
2. Build an evidence matrix.
3. Never ask "does this prove me right?"
4. Always ask "does this disprove any?"

"Slow Rigorous. True"

One alert. Four hypotheses. One matrix.

An alert shows massive data exfiltration followed by file encryption. Example 1

EVIDENCE	H1 BENIGN ADMIN	H2 MISCONFIG	H3 INSIDER	H4 INTRUSION
PsExec from admin host	+	+	–	+
Login at 03:00 local time	–	0	+	+
New service installed	–	+	0	+
Outbound to unknown IP	–	–	0	+
SCORE	**–2**	**+1**	**0**	**+4**

One alert. Four hypotheses. One matrix.

An alert shows massive data exfiltration followed by file encryption. Example 2

EVIDENCE	H1 BENIGN ADMIN	H2 MISCONFIG	H3 INSIDER	H4 INTRUSION
Files encrypted	+	+	+	+
Data leaving network	+	0	+	+
No ransom note observed	+	+	+	-
No C2 traffic observed	+	+	+	-
SCORE	+4	+3	+4	+2

IV.

THE REBUILD

A maturity path from plug-in to delivery

Three phases. One promise.

You do not try to catch advanced threat actors on day 10.

0 – 30 **STABILIZE**	30 – 90 **TRANSLATE/EQUILIBRIUM**	90+ **OPERATE/MATURE**
Noise reduction – stop the bleeding • Tune every rule. Define normal. Filter out the 90% garbage. • Run ACH on real cases • Define 3 exec-grade metrics • Brief the board in 5 lines	*Meaningful signal – build the bridge* • Alert volume becomes meaningful. IR is always-on – because it matters. • Shared vocabulary with Finance • Weekly one-page brief • Kill one report that nobody reads	*The norm – High ROI value* • *Low volume. High quality. Value shifts to hunting and architecture.* • *Narrative reviewed like code* • *Board-grade brief every cycle*

What a good exec brief looks like.

Same incident. Two ways to report it. Only one receives the correct response.

WHAT USUALLY GETS SENT

"Threat Intelligence Update"

- 47 IOCs blocked this week
- APT29 TTPs observed in sector
- 12 endpoints showing lateral movement indicators
- SIEM rule tuning in progress
- Recommend continued vigilance

The executive nods. Nothing changes.

WHAT SHOULD GET SENT

"An intrusion attempt was contained"

- **Impact**: 0 NOK – caught before data exfiltration.
- **Risk**: Similar attempts rising 30% quarter-on-quarter.
- **Ask**: Approve 0.5 MNOK for identity and phishing-resistant MFA.
- **ROI**: Prevents one 80 MNOK incident every 3 years.

The executives decides. Something changes.

What changes when we fix the language

BEFORE

Volume metrics.

MTTR: **8 hrs**

Alerts/week: **12,400**

Board engagement: **quarterly, reluctant**

AFTER

Outcome metrics.

Critical resolved: **< 30 min**

Incidents that mattered: **3/year**

Board engagement: **monthly, invested**

Stop measuring activity. Start measuring outcome.

Shifting the focus to be more risk-centered – enabling the business to grow.

STOP ✕

- ✕ Alert volume.
- ✕ Tickets closed this week.
- ✕ Tool coverage matrix.
- ✕ MITRE mapping completeness.
- ✕ “We investigated X events.”

START ✓

- ✓ Incidents that would have mattered.
- ✓ Decisions the board made differently.
- ✓ Treat analyst expertise as strategic asset
- ✓ Hours saved by killing bad reports.
- ✓ “We prevented X from reaching production.”

Five things to do Tomorrow – Human focused

01 **Kill one report nobody reads.**

If no-one asks about it for two weeks, it doesn't exist.

02 **Write a 5-line brief of today's posture.**

One page, three answers, one ask.

03 **Pick one recurring alert and ACH it.**

Four hypotheses. Score them. Publish.

04 **Sit with a user for 30 minutes.**

Not to train them — to listen.

05 **Ask your CEO one question.**

“What would you want to know at 3 AM?”

Tomorrow – SOC focused

The analyst speaks in outcomes, not alerts.

“We stopped one thing that mattered,” instead of “we closed 400 tickets.”

The exec asks better questions.

“What's the exposure?” replaces “Are the tools working?”

The board funds the fix, not the fear.

Budget follows the story, not the headline.

Monday feels different than Friday.

Less noise. More signal. Fewer surprises.

Am i actually analysing this – or is my brain just telling me it's « as expected » ?

Ask it at 3 AM. Ask it at 3 PM. Ask it in the board meeting.

sopra steria

If you forget everything else…

> *A SOC is a translation layer,*
> ***not an alerting machine.***

Every dashboard, every rule, every report – ask one question:

"Does this help the right human understand, at the right time?"

sopra steria

Q&A