When Security Tools Become the Noise

By: Jaiz Anuar

12 April 2025 · Cybersecurity · Security Operations · 8 min read

Security Operations Centres were built to make threats visible. But for many teams, the problem is no longer visibility—it is noise.

Organisations cannot defend against threats they cannot see. For years, the cybersecurity industry responded in the same way: collect more logs, deploy more sensors, integrate more tools, generate more alerts, and build more dashboards.

The assumption seemed reasonable: more visibility leads to better security.

But many SOC teams today are discovering something unexpected. The problem is no longer visibility. The problem is noise.

The Modern SOC Has a Signal Problem

Most mature organisations now collect enormous amounts of security telemetry: endpoint detections, firewall logs, cloud activity, email events, identity anomalies, network traffic, threat-intelligence feeds, vulnerability findings, and application logs.

The SOC is no longer struggling to collect information. The SOC is struggling to understand which information actually matters.

Not every alert deserves investigation. Not every anomaly represents malicious activity. Not every suspicious event is a threat.

Yet analysts continue to spend countless hours reviewing events that ultimately lead nowhere.

Alert Fatigue Is More Dangerous Than It Looks

Alert fatigue is often treated as an operational inconvenience: too many alerts, too few analysts, not enough people, not enough budget.

But alert fatigue is much more serious than that. It changes behaviour.

The same alerts appear every day. The same investigations produce the same result: false positive, false positive, false positive.

Eventually, analysts become conditioned to expect that the next alert will also be harmless. That is when danger begins.

Attackers do not need security teams to ignore every alert. They only need security teams to ignore the right one.

The most dangerous alert in the SOC is often the alert that looks exactly like all the others.

More Detection Does Not Mean More Security

Cybersecurity teams have a habit of responding to incidents in predictable ways: add another detection rule, threat feed, dashboard, correlation use case, or tool.

The intention is good. The outcome is not always good.

Visibility increases. Complexity increases. Noise increases. Analyst workload increases. Meanwhile, detection quality may remain unchanged.

At some point, organisations need to ask an uncomfortable question: Are we detecting threats, or are we detecting activity?

A failed login is activity. A PowerShell execution is activity. A file download is activity. A new process is activity. None of these automatically represent risk.

SOC teams do not exist to collect interesting events. They exist to identify events that matter.

Every False Positive Has a Cost

False positives are often accepted as part of the job. To some extent, they are unavoidable. But they are not free.

Every false positive consumes analyst time, investigation effort, and operational focus. Every false positive slowly erodes trust in the detection platform.

Over time, this becomes dangerous. Analysts stop believing the alerts. Operations teams become frustrated by repeated investigations. Business teams become reluctant to engage.

Eventually, the tools themselves lose credibility. And once security tooling loses credibility, rebuilding trust becomes difficult.

This is no longer a technical issue. It becomes a governance issue.

Attackers Benefit From Noise

Security teams often assume attackers benefit from invisibility. That is true. But attackers also benefit from excessive visibility.

A SOC overwhelmed by alerts can become just as ineffective as a SOC with no monitoring at all. One suffers from blindness. The other suffers from distraction. Both create opportunity.

Experienced attackers understand this. They know that operating inside noisy environments makes detection harder.

The objective is not always to avoid detection completely. Sometimes it is simply to become one more alert in a queue of thousands.

The Objective Is Signal, Not Volume

Security operations should optimise for signal quality rather than event quantity.

Ten highly reliable alerts may provide more value than ten thousand low-confidence detections.

Achieving this requires difficult decisions. Some use cases need tuning. Some detections need retirement. Some telemetry sources contribute little operational value. Some integrations create more work than insight.

Removing a detection can sometimes improve security more than adding another one. That idea often feels uncomfortable, because many organisations still associate more data with greater maturity. Operational reality often suggests otherwise.

Mature SOC teams are not measured by how much they collect. They are measured by how effectively they respond.

AI Will Help, But AI Will Not Save Us

The industry is increasingly turning towards artificial intelligence: AI-powered XDR, AI-assisted triage, AI-generated investigations, and AI prioritisation engines.

These technologies have enormous potential. They may reduce analyst workload, improve prioritisation, and accelerate response times.

But AI cannot solve bad detection engineering. Poor-quality signals fed into intelligent systems still produce poor outcomes.

Artificial intelligence can amplify good processes. It can also amplify bad ones.

The objective should not be replacing analysts. The objective should be allowing analysts to focus on thinking rather than filtering.

Detection Engineering Is Becoming a Strategic Capability

The future SOC may look less like a monitoring centre and more like an engineering discipline: detection engineering, threat-informed defence, behaviour analytics, security telemetry architecture, and risk-based prioritisation.

The key question is no longer: “How many alerts can we generate?”

The better question is: Which alerts would we regret ignoring?

That single question changes the entire philosophy of detection.

The Bigger Lesson

Cybersecurity spent years trying to solve the visibility problem. Many organisations succeeded. Now they face a new challenge: how to create clarity from abundance.

Visibility without prioritisation creates noise. Noise creates fatigue. Fatigue creates blindness. And blindness creates opportunity.

Final Thought

The purpose of a SOC is not to collect alerts, operate dashboards, or produce impressive event volumes. The purpose of a SOC is to help organisations make good security decisions quickly.

Sometimes that means collecting more information. Sometimes it means ignoring more of it.

Because in cybersecurity, visibility without clarity can become its own vulnerability. And sometimes the biggest threat to detection is not the attacker. It is the noise surrounding them.

Question assumptions.

Share knowledge.

Build trust.