THREATQUOTIENT™

5 Steps to Making Better Security Decisions

www.threatquotient.com

Contents

The Goal is Effective Response

Every Security Operations Center (SOC) and Incident Response (IR) team wants to make better decisions faster with respect to security operations, vulnerability management and incident response. To do this, many organizations are bringing in more data feeds — both threat and vulnerability — and investing in analytic behavioral detection tools. Unfortunately, this is not driving improved decision making. Instead, it is burying staff under data. The end-result is declining decision-making capability due to alert fatigue.

In this report, we define a process for making better decisions faster, first by addressing alert fatigue to make better decisions, and then by introducing situational understanding to make these decisions faster.

More Data ≠ Better Decisions

SOC and IR teams are struggling to keep up with the pace of security operations due to data overload and the resulting onslaught of critical alerts. For example, three-quarters of security team members participating in a 2017 EMA study "felt overwhelmed by the volume of alerts."[1] Yes, machine learning and artificial intelligence are helping to weed out ancillary alerts. But the expanding threat landscape spurred by moves to the cloud, IoT, and new development methodologies such as microservices and continuous integration/continuous deployment (CI/CD) is exacerbating the critical alert count. The deluge of critical alerts is driving alert fatigue.

Alert Fatigue = Bad Decisions

Alert fatigue is when analysts are so overwhelmed with high priority alerts that they can no longer process them and may even start ignoring them. In fact, the same EMA study reports that 42 percent of security professionals say their organization ignores a significant number of security alerts due to the volume and more than 30 percent say they ignore more than half their alerts.[2] Though rampant in SOC and IR organizations, this is not unique to information security. Healthcare faces similar challenges, primarily from electronic health record (EHR) systems. The alert volume can be overwhelming to the point where some physicians are turning off the feeds. In one instance, this could have been a fatal move when doctors "ignored relevant information about how a patient might respond to a drug, because it appeared alongside heaps of superfluous notifications … Consequently, the patient received medication that induced a potentially lethal reaction."[3]

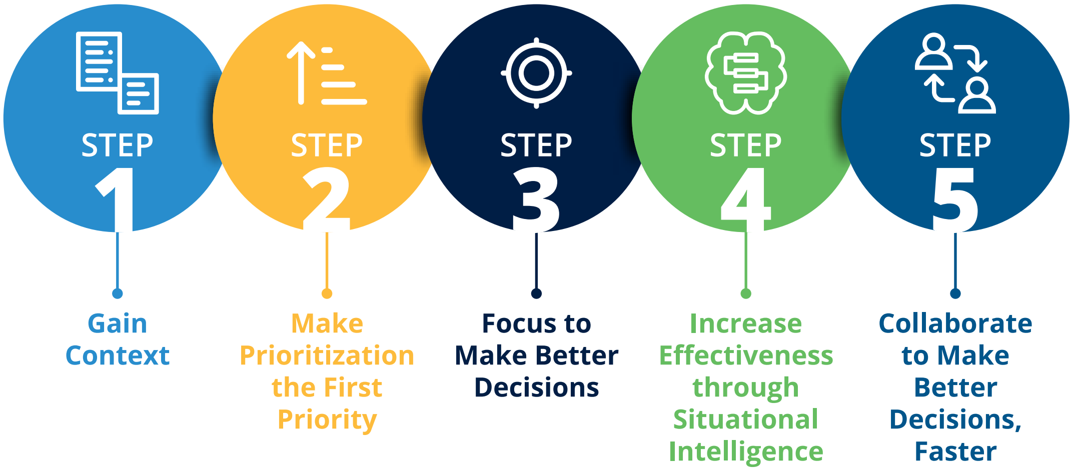
[1] David, Monahan, "A Day in the Life of a Cyber Security Pro," EMA.

[2] Ibid.

[3] Shefali Luthra, "Doctors are overloaded with electronic alerts, and that's bad for patients," *Washington Post*.

Luckily, this was a wrong decision caught in time and the patient survived. Had the doctors been able to triage alerts (i.e., quickly discern alerts relevant to this specific child), they would have managed the data and avoided alert fatigue. Similarly, SOC/IR teams need alert triage to focus rapidly on the most pressing issue; addressing less urgent matters, later.

Making better decisions faster requires security teams to take five critical steps.



STEP 1
Gain Context

STEP 2
Make Prioritization the First Priority

STEP 3
Focus to Make Better Decisions

STEP 4
Increase Effectiveness through Situational Intelligence

STEP 5
Collaborate to Make Better Decisions, Faster

Step 1 — Gain Context

Alert triage reduces alert fatigue by facilitating quick differentiation of one high priority alert from another. The best method to achieve this differentiation is by incorporating contextual information. Having the right context empowers analysts to separate alerts carrying immediate risk from those that carry high risk, but they can address later.

The right context helps the SOC and IR teams separate the *possible* from the *probable*.

One of the best means to gain context is through aggregating and authenticating internal security indicators (indicators of compromise and event data) with external threat intelligence. Unfortunately, most organizations incorporate threat intelligence only after they classify an event as suspect.[4] We see this as a missed opportunity because threat intelligence provides valuable context long before an event is considered suspect. Or, put another way, incorporating context earlier in the analysis increases the likelihood of detecting suspect events, sooner. Examples of threat-based contextual intelligence include the origin of the data, the distribution method, the actors, the target victims, attack vectors, target data, etc.

The right context helps the SOC and IR teams separate the *possible* from the *probable*. Otherwise, everything is *possible* making all high priority alerts equal. For example, an anomalous outbound activity alert from a bank's development server is *possibly* malicious, requiring further investigation, regardless if this is a malicious or a benign event. In contrast, integrating threat intelligence that shows the IP addresses are command & control (C&C) sites explicitly targeting financial services organizations indicates this alert is *probably* a beacon requiring immediate blocking and incident response.

[4] Matt Bromiley, *The Show Must Go On! The 2017 SANS Incident Response Survey*, (SANS, 2017).

Step 2 — Make Prioritization the First Priority

Separating probable from possible via context enables analysts to discern one high priority alert from another, empowering them to prioritize. Prioritization is critical and to underscore this point, the National Institute of Standards and Technology (NIST) states in its *Computer Security Incident Handling Guide*, "prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process."[5] Prioritization applies to not just incident response, but all critical alerts. The ability to prioritize gives the analysts the breathing room necessary to focus on what matters, addressing the highest priority alerts first.

Step 3 — Focus to Make Better Decisions

Prioritization forms a foundation for focus. By reducing noise and providing a means to differentiate one high priority event from another, security analysts can focus without incurring alert fatigue. And, when analysts focus, they make better decisions.

Security operations is a team sport where addressing complex security incidents requires precise synchronization of multiple people working together.

However, security operations is a team sport where addressing complex security incidents requires precise synchronization of multiple people working together. Just because an individual analyst is focused and making better decisions doesn't mean the organization is *collectively focused* and making better decisions. If team members do not have the right information at the right time, then team decisions will not happen. Worse, decision making will stall.

For success, the team must be on the same page. Everyone must have the same understanding of the situation, the risks, the impacts and next steps. Team orchestration is not a trivial feat, and team coordination is a top challenge for security and risk managers. To address this, some organizations are instituting playbooks into their SOC and IR activities. These playbooks map out the critical steps to move from detecting a suspicious event to classification, analysis and response. A playbook is a flow model for executing repeatable steps along the path of incident response. These models are extremely helpful for mapping and in some cases automating various stages in the process. However, playbooks are static and limited in their ability to effect team decision making because they lack a key ingredient: real-time situational intelligence.

[5] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide*, 2012, Pub. SP800-61 Rev 2, Gaithersburg, MD.

Step 4 — Increase Effectiveness through Situational Intelligence

There is a difference between getting everyone on the same page and making sure everyone has the information they need to do their job. For example, a threat analyst will be looking for information about active threats in the wild, known threats to the organization and all the unique indicators of the potential threat actor, with an emphasis on the Reconnaissance, Weaponization, Delivery and Exploit steps of the Cyber Kill Chain (CKC). Contrast this with an IR analyst focusing on Indicators of Compromise (IoC) related to Exploit, Installation, C&C and Actions on Objectives steps in the CKC. Both team members are working the same problem, but their intelligence needs are different, yet, related.

Situational intelligence gives the team member the actionable information they need to work more efficiently and effectively as part of a team effort.

We call this different, yet, related intelligence, situational intelligence: presenting the right information to the right person at the right time. Situational intelligence derives from bringing together the machine data generated by all the security devices (e.g., SIEM, IDS/IPS, endpoint, HIDS and FW) and integrating it with threat intelligence. The goal is to provide situationally relevant insights to the team member analyzing the data (i.e., related to the actual role of the team member). Situational intelligence gives the team member the actionable information they need to work more efficiently and effectively as part of a team effort.

When all team members have the right information at the right time, and the team is operating on the same page, we call this universal understanding. Universal understanding is a tipping point in team dynamics, when the team is operating at full effectiveness. Organizations must start tracking mean time to understanding (MTTU) as a critical SOC/IR metric. MTTU is the only metric focusing on team effectiveness and reducing it dramatically increases security operations effectiveness.

Step 5 — Collaborate to Make Better Decisions, Faster

So far, we have been discussing the mechanics of making better decisions. How do organizations make better decisions faster?

The conventional wisdom among SOC and IR teams is making faster decisions requires lowering mean time to detection (MTTD). Many organizations are investing in automation, artificial intelligence (AI) and machine learning with the goal of triggering alerts sooner, to reduce MTTD. For example, prioritizing alerts and scoring threat feeds might be perfect opportunities for automation.

Seamless Collaborative Workspace

However, simply because an alert triggers sooner (i.e., lower MTTD) does not mean the team is positioned to act faster. Accelerating critical decision making requires team collaboration. In the movies, we often see SOCs depicted as large facilities filled with screens and staff. Responding to events seems to happen magically: everyone needed to catch the threat actor is already in the room.

In the real world, SOC and IR teams are dispersed, sometimes globally. Plus, given the complexity of today's IT and security environments, team members typically require compartmentalized knowledge (e.g., server focus, endpoint focus, AppDev focus) to do their jobs.

A collaborative investigation workspace takes the playbook concept but makes it dynamic to reflect real-time team decision making and puts it into action through automation. The underlying framework and flow are laid out, tracking the actions and interaction of the team in real time. This is similar to how the sports commentator displays an instant replay, drawing the playbook moves (Xs, Os, and arrows) the team is going to make and then puts the play into action. Except this isn't instant replay; this is real time.

The seamless collaboration workspace enables team members to make better decisions, faster by providing:

- **Global view** — A universal perspective showing all teams and team members involved in the investigation and their activities, across the entire organization, divided by region or specialty focus
- **Focused knowledge** — Keeping the big picture in mind with consistent, shared global knowledge, while still supporting localized concentration. For example, having a perspective of the entire kill chain, while integrating threat intelligence to understand adversary motivation and goals, focusing specifically on the servers receiving the exploit
- **Test, then talk capability** — Team members can work through their hypotheses in parallel, test their theories, and then report to the broader team

Conclusion

Security teams are facing significant alert fatigue as they battle a continual barrage of high priority alerts. The expanding threat landscape and the increasingly dynamic nature of IT operations are the primary contributors to this alert escalation. The only way SOC and IR teams have a chance to overcome alert fatigue is to introduce threat intelligence to add context, which facilitates prioritization and triage.

Doing this helps to make better decisions, but the team also needs to be aligned and synchronized. This is challenging for many teams because they are dispersed and specialized. They need a consistent way in which to operate, so everyone is on the same page, while still focusing on their role in the decision-making process. Achieving this requires situational intelligence and working within a seamless collaborative environment. In the end, doing all the above positions teams for universal understanding which is the basis for making better decisions, faster.

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC. For more information, visit **www.threatquotient.com**.