noggin

Security

Authoritative Guide to Data Alerts

The importance of multiple data sources for situational awareness

Situational awareness, scholars and practitioners have argued, is critical to effective decision making. After all, it's situational awareness that ensures that response teams, whether in the command and control, emergency response, and/or cybersecurity settings, have sufficient perception of elements in the environment, comprehension of their meaning, and projection of their status into the future[i].

But as critical events themselves become more complex, achieving situational awareness has become more difficult.

Why's that? Simply put, teams can no longer rely on single sources of information to establish a complete picture of a fluid environment during a multi-dimensional crisis.

What do they need, instead?

Multi-source data points are needed to establish and heighten situational awareness, improve comprehension and perception, and support effective critical decision making. Properly integrated, multiple data sources offer the following benefits:

Better quality decision-making

Faster response time and minimized impact of critical events

More time for coordination

More consistent messaging to affected publics

Which data sources, though? Well, open and public data sources have provided the requisite information, to improve situational awareness before, during, and after critical events.

Through the medium of data alerts or automatic notifications, the following sources specifically have been among the most useful:

GeoRSS. Large-scale disasters require extensive amounts of geospatial information regarding regions affected, infrastructure, and resource requirements. As a result, GeoRSS feeds, live-web feeds that include geographic features and locations, have been added to existing feeds, enabling users to perform geographic searches and map information, to improve disaster response, boosting planning, response, collaboration, and communication efforts. This location content consists of basic geometries (e.g., geographic points, lines, and polygons of interest) and related feature descriptions[ii].

Weather forecasting. Weather forecasting data serves a similar function, frequently used to predict magnitude, location, timing, and even duration of potentially damaging events[iii].

Open-source data. Often inclusive of the above, open-source data is data that is openly accessible, exploitable, editable, shared by anyone for any purpose. Open-source applications (e.g., CDC, FEMA, HHS, and Frontline SMS) have been used successfully in emergencies and disaster recovery.

Challenges in maintaining situational awareness from multiple data alerts

Sure, the intelligence that comes from data alerts have been crucial when responding to critical events and other disruptions.

But stakeholders maintain there are important caveats – rather than information, it's the *right information*, delivered at the *right time*, that makes the difference.

To that end, serious challenges have emerged to impede the effectiveness of data alerts. And many have to do with the kind and quality of the alerts themselves.

The data in the alerts is often considered too granular to be actionable. Coming from noisy sources, the data is often wrong or misleading, leaving responders tilting at windmills or jumping at shadows.

One of the more acute challenges, though, is the frequency of data alerts. The increasing pace of automatic notifications has created alert fatigue.

What is alert fatigue?

Alert fatigue happens when an overwhelming number of alerts desensitizes responding individuals to individual alerts – even when those alerts carry valuable information.

The effects of alert fatigue were first studied in public healthcare after the introduction of clinical decision support systems.

As the name suggests, these systems were meant to aid in decision making in the clinical setting. Researchers subsequently noted that: "Despite their benefits, clinical decision support systems are sometimes criticized for issuing excessive alerts about possible drug interactions that are of limited clinical usefulness..."[iv]

The excessive warnings caused "alert fatigue"[v]. In the clinical setting, that meant that physicians, receiving too many alerts, were inadvertently ignoring individual alerts that turned out to be useful. The result was a diminution in effectiveness of the systems themselves with "adverse consequences for patients"[vi].

Cybersecurity experts, for their part, also picked up on alert fatigue. As in public healthcare, technology led to increasing numbers of alerts; the onset of COVID, in particular, exacerbated cyber risk, leading to a sharp rise in alerts[vii].

How bad has the issue become?

In 2021, the International Data Corporation (IDC) issued a report on the effects of escalating cyber alerts on cyber response.

The numbers weren't pretty. Surveyed staff reported spending more time (32 minutes) on alerts that turned out to be false leads than on actionable alerts[viii].

As a result, more than a quarter (27 per cent) of all alerts were ignored or not investigated in mid-sized corporations[ix]. Slightly larger organizations (1,500 to 4,999 employees) saw personnel ignore nearly a third of all alerts.

Beyond that, alert fatigue is also creating tail risk for recruitment and retention. Employees, particularly Security Operations Center (SOC) staffers, acknowledge not wanting the thankless task of wading through innumerable data alerts, many of which turn out to be false herrings.

Seeing this, employers have ramped up security spend on systems that produce even more alerts without having sufficient staff to triage actionable alerts. Risk, as such, has increased everywhere – remaining staff think alerts are false; and organizations risk more missed real alerts, slow response times, and potentially infected systems.

Digital technology solutions to the alert fatigue challenge

What can be done?

Just as the wrong technology can exacerbate alert fatigue, the right solution can mitigate these negative effects, ensuring that actionable data alerts get through in a format that incentivizes speedy triaging.

Indeed, the solutions that have gotten data alerts right (actionable alerts get through; false leads stay out) have managed to adopt the appropriate information management framework – a framework which suits all fields, not just as healthcare and cybersecurity.

They deploy information management frameworks (or triggers), leading to the following outcomes:

- Increased specificity of alerts which reduces inconsequential alerts
- Tiering of alerts by severity and priority, e.g., alerts are customized to notify workers in a particular way to help distinguish between alert types
- Consolidation of redundant alerts
- Rendering alerts more actionable, by eliminating vague alerts that take too much time and energy to triage
- Continuous review of the alerts program itself, to detect whether alerts have been missed, thresholds are too high or low, and/or if employees have become desensitized

The technical modality at play, here, includes powerful workflow automation, helping to aggregate and visualize alerts, thereby accelerating investigation speeds and response times[x].

The flexible, digital solutions which boast such information-management modalities work by capturing and consuming information from multiple sources, to provide a real-time common operating picture of the task or operation at hand.

Leveraging powerful, yet easy-to-set-up workflows, these solutions control and automate management processes and standard operating procedures, keeping the right stakeholders informed across multiple communications mediums. Analytics and reporting tools then ensure that decision-makers have the correct information in the best available format, when they need it.

The solution also tracks tasks to ensure that the right actions are taken and followed through, helping you to assign, manage, and track resources.

What's more, the system provides a case management framework, orchestrating information flows throughout the organization, providing consistency where multiple systems, sources, and processes are employed, and enabling the secure exchange of information and coordination of resources across multiple stakeholders.

Integration options to ensure the right information gets through at the right time

The genius of these solutions is that they offer a full range of integration options, making it easy to connect and synchronize data and plug in customer systems. The Noggin platform, for examples, integrates with ERPs and CRMs, as well as other service management, cyber security, and EHS systems.

When it comes to actionable data alerts for critical event and operational security management, relevant Noggin integrations include:

For security threats. Integrating with Noggin, Signal is an open-source intelligence tool for security teams who may deal with disruptive or unexpected events. Customers monitor multiple online data sources with a simple, easy-to-use interface, with Signal providing relevant, actionable information in real time. And so, with Signal, you can:

- Identify emerging threats faster
- Receive real time alerts
- Monitory developing situations

For event and risk detection. Integrating with Noggin, the Dataminr AI platform detects the most relevant, high-impact events and emerging risks in real time – so customers can respond with speed and confidence. The platform enables a diverse customer base to manage crises more effectively:

- Businesses can identify and respond to emerging risks across the enterprise, with the earliest indicators of business-critical information about risks to people, brands, and physical and virtual assets.
- Public sector entities can respond to real-time events faster, know where to deploy first responders, and provide aid to citizens on the ground within minutes.

For IT ops. Integrating with Noggin, PagerDuty provides a source of truth and coordination for real-time operations and major IT disruptions, useful in the following business cases:

- IT on-call management
- Operational analytics
- IT incident response
- IT team activation and coordination
- Automated IT incident resolution

Finally, the complexity of today's critical events means that single sources of information no longer are sufficient to establish and heighten situational awareness. Alerts from multiple data sources, however, aren't necessarily the solution.

As noted, alert fatigue is on the rise with personnel increasingly tuning out automatic notifications from noisy data sources. Response agencies, though, worry staffers are throwing out the baby with the bath water as actionable alerts are getting ignored, too.

What's the answer? Disruption management platforms, like Noggin, have the information management capacity to make data alerts actionable through powerful (yet configurable) workflows that can be tailored to your organization's business processes.

What's more, these platforms come equipped with integration options, making it easy to connect and synchronize rich data sources for security threats, event and risk detection, as well as IT ops, with the end-result that the right information gets in at the right time, making enterprise resilience simple.

Sources

i. *Endsley, M.R. (1988). Design and evaluation for situation awareness enhancement. In Proceedings of the Annual Meeting Human Factors Society, (Vol. 32 pp. 97–101). Los Angeles: SAGE Publications Sage CA.*

ii. *Government of Canada: GeoRSS. Available at https://www.nrcan.gc.ca/earth-sciences/geomatics/canadas-spatial-data-infrastructure/standards-policies/georss/8920.*

iii. *Bruno Merz et al, Review of Geophysics: Impact Forecasting to Support Emergency Management of Natural Hazards. Available at https://agupubs.onlinelibrary.wiley.com/doi/full/10.1029/2020RG000704.*

iv. *Aaron S Kesselheim et al, Health Affairs: Clinical Decision Support Systems Could Be Modified To Reduce 'Alert Fatigue' While Still Minimizing The Risk Of Litigation. Available at https://www.researchgate.net/profile/Kathrin-Cresswell/publication/51858562_Clinical_Decision_Support_Systems_Could_Be_Modified_To_Reduce_'Alert_Fatigue'_While_Still_Minimizing_The_Risk_Of_Litigation/links/0deec51b6ea2099aba000000/Clinical-Decision-Support-Systems-Could-Be-Modified-To-Reduce-Alert-Fatigue-While-Still-Minimizing-The-Risk-Of-Litigation.pdf.*

v. *Ibid.*

vi. *Ibid.*

vii. *Deloitte: Impact of COVID-19 on Cybersecurity. Available at https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.*

viii. *Edward Segal, Deloitte: Impact of COVID-19 on Cybersecurity. Available at https://www.forbes.com/sites/edwardsegal/2021/11/08/alert-fatigue-can-lead-to-missed-cyber-threats-and-staff-retentionrecruitment-issues-study/?sh=1f2f3c9135c9.*

ix. *Ibid.*

x. *Alexander S. Gillis, Tech Target: Alert Fatigue. Available at https://www.techtarget.com/whatis/definition/alert-fatigue.*

Like what you read? Follow Noggin on social media

@teamnoggin facebook.com/teamnoggin linkedin.com/company/noggin-it

noggin
for Security

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Security gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Security solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**