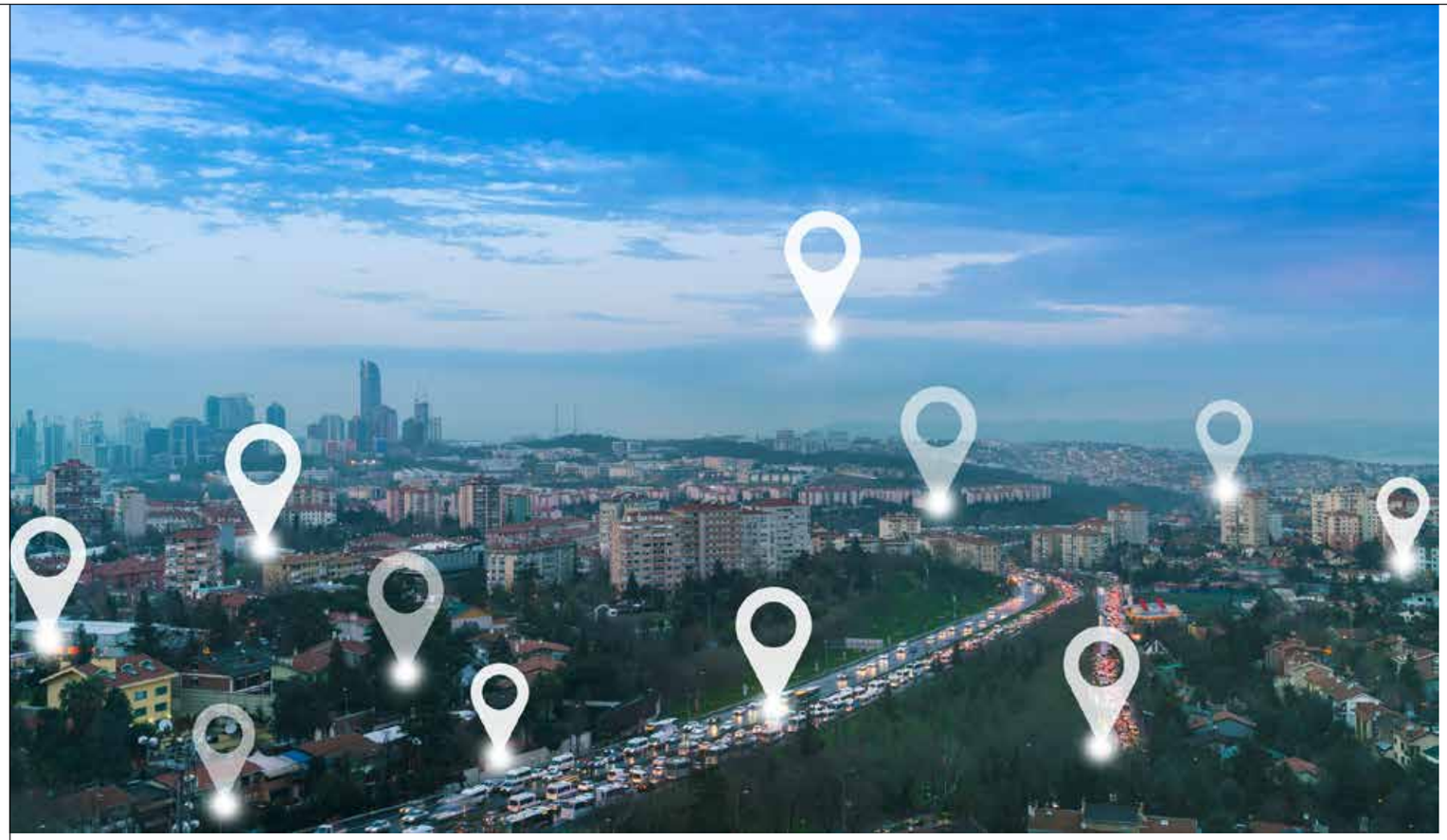

Picture credit: iStock

ONE PLATFORM TO RULE THEM ALL

Botan Osman *outlines how closed security systems have failed to deliver on their promises of integration, speed and adaptability*

For years, resilience and security leaders have been promised integration – one platform to manage people, risks, and response. Yet when a crisis hits, those legacy systems fall short: data sits in siloes, people are not located, comms fail and hours are lost searching for clarity. Similarly, closed systems proliferate in the resilience and security industry. Up until now, organisations have been given a single purchase option: a bundle of software, threat intel and assistance services locked into a single ecosystem. The result? Fragmented data, limited choice and slow response when it matters most.

The world is becoming a more hostile environment. Critical event prediction is becoming more difficult, and the change will remain constant; six months ago the world looked different and in the next six months it'll look different again.

External and internal threats are proliferating across organisations. CSOs are asking how to handle an increasing number of threats while they also have a growing organisation with more assets and demands. Fortunately, the number one characteristic of security and resilience teams in general is agility and a willingness to adapt. The way these teams succeed is fundamentally dependent on the people and tools they have.

The problem with change is that you need to stay nimble to react swiftly. To that end, CSOs have acquired various service and product bundles to keep on top of software security, tracking, medical assistance and intelligence. The components are not necessarily the best choice, they're just part of the bundle. Unfortunately, that really kills your organisation's ability not only to adapt, but also to be confident you're offering the absolute best solution.

How has this happened? Companies have been created in order to serve one problem – alerting to potential threats, for example – but in an effort to try and deliver a comprehensive service more and more elements have been bolted on, with varying degrees of success. An organisation that is agnostic regarding threat intelligence allows you to choose what works best for your company.

What CSOs are entitled to is a platform that can be open to all intelligence data sources, threat and risk providers. Assistance provider independence means the freedom to buy what works for your organisation – not making do with what you have been sold.

An open architecture enterprise resilience platform is what has long been required, that offers the option to bring your valuable data in, ideally from an integrated data hub, integrate with preferred providers and respond by adding in different threat and risk providers as circumstances change over time. In this way the assistance provider of choice can operate seamlessly with the technology.

After all, the aim is real-time people-visibility. This requires a tapestry of data sources, creating layers that work together. The structural threads are places that people have travelled from or to; the real time view of their access to those places through access control systems is woven alongside that, along with the travel data that moves them between these places and countries. Layered with that is the GPS data from their mobile devices. Relying on all five together produces a powerful matrix of resilience to get the most accurate view possible.

So how would that look in practice? Having the freedom to include what matters to your specific organisation could mean including weather alerts, configurable pre-travel advisories, country risk reports and custom risk levels. This gives you not the provider's view of the world, but yours.

Your technology needs to operate seamlessly with all assistance providers and their threat intelligence. Ideally, the industry would sign up to an open standard for technology and service interoperability so that moving from one assistance provider to another from a technology perspective would be a smooth transition while you keep the technology. In addition, freedom to include everything you need for real-time people visibility means a step beyond the itinerary. The problem with the itinerary is that it's just my flight or my trip. There are so many other data sources that determine how you can protect your people in any environment. This is holistic people safety rather than travel risk management; one screen and the knowledge you are protecting your people. This isn't just a nice-to-have, it's a necessity in a volatile world. When an incident hits, you should be able to categorise the event based on the location of your people and who's most at risk, not be hunting across five screens and seven log-ins.

When an incident hits, you should be able to categorise the event based on the location of your people and who's most at risk

Impact calculations and intelligent workflows allow you to filter the noise of constant alerts coming in across various threat providers and real time people visibility reduces the 'Cry Wolf' syndrome as it gives you a far more accurate view of who is impacted as well as reducing the number of alerts.

As CEOs demand how AI could be introduced into their organisations, bringing AI into resilience software adds sensitivity to the platform and performs the vital task of collecting together disparate data streams from different parts of the organisation in various formats to present a clear picture.

THE DATA USED AS THE FOUNDATION OF THE SYSTEM MUST BE ROBUST AND ACCURATE

Human-first AI assists the operator, rather than replacing it, and uses your data aligned to your rules to minimise hallucination. As an example, an AI alert assistant can autogenerate and disseminate an emergency mass notification of an unfolding incident, in the relevant language of the recipient, via their preferred channel (email, WhatsApp, Teams, SMS *etc*). When you combine that with an open ecosystem – which is bringing in threat feeds from multiple providers, along with the rules engine that determines which of those threats you are going to respond to and who it impacts – CSOs can respond accurately, decisively and swiftly to any external threat.

By understanding exactly where the key data is held and exactly which data the AI is using to inform its decisions, security leaders can have confidence in its interpretive abilities. From there, tasks that previously required manual effort across multiple systems can now be handled via an intuitive UI and agentic support, freeing teams to focus on strategy and the decision-making that will keep their people safe.

Some groundwork is necessary to position your organisation to maximise the benefits of an open security system, however. Emergency situations tend to shine a spotlight on data accuracy. The information required to account for an organisation's employees is often siloed, out of date or in the wrong format. Security teams have long had to accept that pulling together people-data is a long and arduous task, with confusion often over whose task it is.

These shortcomings have real-time, real-life effects on those on the ground. Although many companies do have multiple tracking systems, they are often outdated and not integrated, making it impossible to generate a reliable country or regional headcount during a crisis. The core challenge for many organisations in the recent conflict in the Middle East, for example, was not a lack of data but its fragmentation across multiple systems – POB, travel, mobile, vehicle tracking and HR records, all of which were operating independently with inconsistent accuracy and governance. Manual travel recording was required during the conflict to supplement gaps in automated systems, including personal leave

tracking. The inability to rapidly consolidate data sources meant establishing a reliable real-time view of who was affected was slow and in some cases impossible. This directly impacted response speed, decision quality and duty of care.

Many companies, including large multi-nationals, still have their employees' data on travel trackers and Excel spreadsheets only. The data has not been integrated. In turn this means they do not have a single, accurate picture of where their people are located. Access Control, Safety Apps, mobile-based people locating and vehicle tracking and Intelligent Video Management System data is frequently

EMERGENCY SITUATIONS HAVE A TENDENCY TO SHINE A SPOTLIGHT ON DATA ACCURACY

managed locally and is not connected to central systems, limiting its usefulness during a crisis.

Where information sources are disparate, communications are manual, labour-intensive and slow. Information moving up and down the chain relies on human effort. There is no automation for daily summaries or consistent distribution across business units. Some companies reported during the Middle East crisis using spreadsheets on Sharepoint and a warden system, which has not changed for 24 years; indeed some personnel remembered using the same workarounds in the Iraq war of 2003 and the Arab Spring in 2006.

The data used as the foundation of the system must be robust and accurate. For any organisation keen to implement AI systems, anchoring it in strong data sets with robust and comprehensive guard rails is vital to avoid decision-making based on bogus assumptions.

A simple mapping exercise to establish the maturity of an organisation's security & resilience technology & data environment is a great starting point for any would-be implementer of an open security system with AI as the conduit. By understanding where it sits on the 'maturity ladder', an organisation can begin to introduce AI in a way that complements its operational systems. This type of assessment lays the foundation for future success.

By understanding exactly where the key data is held – and exactly which data the AI is using to inform its decisions – security leaders can have confidence in its interpretive abilities. From there, tasks that previously required manual effort across multiple systems can now be handled via an intuitive UI and agentic support, freeing teams to focus on strategy and decision-making.

The security industry deserves better than bundles. The world of resilience and security ensures people safety and operational continuity, the criticality is clear to all. Second best should not even be an option. As security as an issue moves steadily up the agenda, companies are demanding resilience software with the flexibility to adjust as their requirements change. AI integration is opening budgetary opportunities and security is finally being recognised as a tool for retention and a benefit rather than a cost. In tandem with open, provider-agnostic technology, organisations have a real chance to gain total control over how they build and scale resilience to keep everyone safe, everywhere ●

Botan Osman is CEO of Restrata.

Where information sources are disparate, communications are manual, labour-intensive and can be slow

Picture credit: AdobeStock