# SureView Situational Awareness

A SINGLE VIEW TO IDENTIFY THREATS AND TAKE ACTION

SureViews Situational Awareness provides a single view of an organization's security operation—helping teams identify, triage, and respond to potential threats to key assets and personnel. By leveraging SureView's vast integration library, Situational Awareness provides a holistic view of all your threat data, working seamlessly alongside your traditional physical security assets. It utilizes a familiar map-driven interface so that teams can immediately grasp and evaluate the impact of potential threats and if required, raise events to responding teams so that they can take real-time action. It's the latest module to be delivered via SureView Operations' SaaS suite.
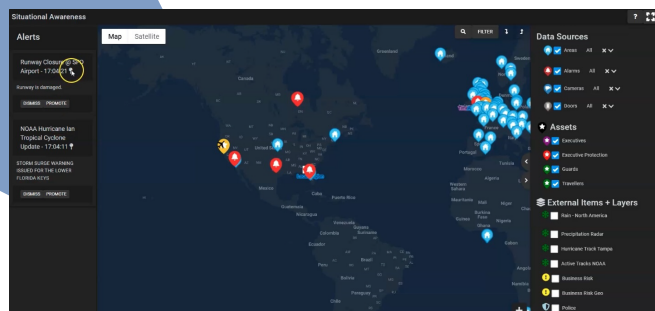
THE CHALLENGE

As more external threats impact an organization, teams are leveraging a series of tools that scour the web to identify potential risks. Different tools focus on different types of data—some focus on social media feeds, others public safety data. The data these systems create can be raw, or curated by a security analyst. Naturally, the amount of data being delivered by these systems can be overwhelming, making it difficult for teams to identify real risks impacting their organization.

THE SOLUTION

SureView Situational Awareness is designed to provide security operations teams with an immediate view of their entire operation so that they can see all incoming threat data alongside their security assets. Whether the team is monitoring one business risk service or multiple, SureView Situation Awareness eliminates the siloed nature of threat information

and provides a simple interface for analysts to triage incoming risks. They can quickly access different map layers to provide additional context, view live cameras near the event, reach out to nearby security officers for help—and they can do this in seconds without having to jump back and forth between multiple different systems. If a threat requires action it can immediately be promoted to SureView Response, where operators can coordinate the real-time response. If the event does not require an immediate response but does require follow-up, it can instead be promoted to SureView Cases where a workflow can be triggered for further investigation.

HOW DOES IT WORK?

The map-driven interface of SureView Situational Awareness displays 3 major types of information:

1 Incoming threat information. Alerts from various sources are collated into this feed and are displayed both on the map and in a threat queue.

2 Security Assets. All security assets in SureView are displayed on the map; this includes physical security assets such as live camera feeds, doors, alarm points, intercoms, and other assets such as officers, guards, vehicles, etc.

3 Map data. This can include floor plans of your buildings, nearby police precincts, hospitals, and weather overlays—the list is almost endless.

As threat data is received from multiple business risk services, these are added to the Alert queue. Analysts can review these alerts in the context of the map and determine if the data can be dismissed (i.e. poses no threat and no actions are required) or promoted. When an Alert is determined to pose a threat to the organization the analyst simply promotes it—immediately sending it to SureView Response where it's transformed into an alarm event. This alarm event will include the details about the originating Alert as well as any additional context from the analyst on why it's being promoted. The operator will be prompted to follow their Action Plan (SOP) walking them through the appropriate steps they need to properly respond to this type of event.

Behind the scenes, all of this information is being stored, including what alerts are being received, which ones are being promoted, and why. Using SureView Insights Plus, managers can visualize and evaluate this data, to better understand their risks, improve their response, and minimize the impact of future threats to their employees, customers, and assets.