vidsys

Leveraging Converged Security for Crisis Management + Response

Incidents that cause widespread impacts to public safety and security, such as natural disasters, pandemic outbreaks or threats of terrorism, are not always at the forefront of discussion when it comes to developing an enterprise security strategy. It can be particularly challenging for organizations to prepare for and manage these risks, as they tend to occur with little forewarning and can create situations that escalate both quickly and unpredictably.

Amid a large-scale public incident or crisis, having the information needed to take swift, decisive action is crucial to protecting people and other critical assets from harm. Organizations that can quickly access high quality, real-time data from multiple sources across their security network have a significant advantage in navigating a crisis and recovering from it. Converged Security & Information Management or "CSIM" platforms, help organizations use technology to support and enhance traditional crisis management methods, both during and after an emergency. This can help mitigate the impact of an incident and support an efficient response, allowing the organization to quickly return to a state of normalcy.

Using Technology to Facilitate Situation Management

CSIM software solutions help support the precise decision-making required to navigate a public security crisis. By pulling together data from disparate physical and logical systems into a single, unified operating platform, CSIM helps security personnel get a better grasp on complex situations.

Comprehensive CISM platforms, like Vidsys Enterprise, include a wide variety of configuration and integration options that allow stakeholders to create automated situation alerts, standardize event response workflows and connect to hundreds of different security systems and devices.

Using technology to centralize security operations provides the ability for organizations to remotely manage developing situations in real-time, regardless of their security team's geographic proximity to the transpiring event.

Converged Security Solutions in a Crisis

There are a number of ways an organization can use CSIM to support operational security in an emergency situation:

1. Providing Situational Awareness and Visualization Capabilities

CSIM solutions provide a real-time view of macro-level data, allowing operators to monitor multiple, critical information sources such as news media feeds, outbreaks of violence or illness and severe weather alerts across an area of interest.

When coupled with information from connected physical security inputs, such as cameras and other sensors, operators gain a complete picture of the evolving security environment.

2. Intelligently Managing and Automating Workflows

Dynamic action response plans, based on each organizations own unique Standard Operating Procedures, can be configured to automatically trigger actions such as distributing mass communications (via email, SMS, VoIP, etc.), locking down a facility or dispatching response personnel per the policies and procedures of the organization.

3. Enabling Remote Operations and Mobile Situation Awareness

Thin-client CSIM platforms, like Vidsys Enterprise, run on modern web browsers. This provides rapid access to the platform from remote and/or temporary locations as well as for designated organizational stakeholders who may only need access during the crisis.

4. Supporting Organizational Resilience and Business Continuity

Many CSIM platforms offer support for high availability and disaster recovery measures that help organizations maintain critical functions after an emergency or disruption.

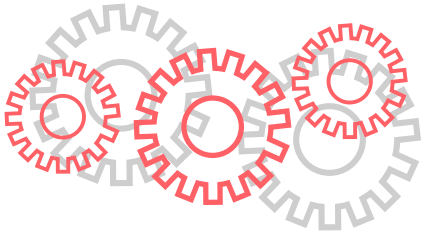
5. Facilitating Situation Management across Multiple and Disparate Sites

CSIM platforms that offer global dashboard views with access to events managed by both local and regionally deployed assets give even the largest and most widely dispersed organizations total visibility across their entire enterprise.

Amid a security crisis organizations should be prepared to:

+ Monitor security vulnerabilities, including both internal and external threats
+ Visualize and correlate data from across the enterprise
+ Maintain global situational awareness of people and business assets
+ Automate security alerts and communicate incident response plans
+ Generate timely and accurate reports for real time and future analysis

Accelerating Decision-Making with AI



Organizations that rely on a large or complex network of security devices and systems to maintain operational security may find themselves overwhelmed with the amount of data flowing into their security operations center, especially during an emergency.

Integrating CSIM with an AI (artificial intelligence) powered analytics tool helps security operators perform tasks more effectively.

By intelligently monitoring security device data feeds, automatically identifying relationships and streamlining workflows as required, AI relieves security personnel of tedious and error-prone monitoring tasks, empowering them to focus on the complex aspects of incident management that require human consideration. In a crisis, this means operators can rely on AI to make quick, effective and data-driven decisions, while still providing a high level of security, even when resources are limited.

Visit our website to learn more about how Intelligent GSOC can help revolutionize your security operations by bringing the power of AI and Big Data analytics to Converged Security.

Organizations should consider the following factors *before* an incident occurs:

+ **Which triggers initiate, escalate and deescalate a situation?**
+ **Who within your organization needs to be informed of a crisis? When and by what means?**
+ **What steps should be followed in response to an incident?**
+ **Which response activities can be automated? Which require human attention?**

Planning and Recovery Considerations

Thinking ahead is critical when preparing for the risk of an unexpected crisis. Preparation should be supported by an effective risk identification process to determine which events may occur and deciding how best to manage them.

During Vidsys' deployment process, this step is called the Concept of Operations, or "ConOps" plan, and is used to guide associated secondary activities that take place during an incident and play into an organization's operational needs.

Whenever possible, it is important to perform table-top scenarios and other training activities during normal operations to enhance preparedness before a situation occurs. After a crisis has deescalated and the organization returns to normal operations, it is critical to revisit the ConOps plan and make adjustments as necessary to continuously improve and streamline processes.

Ready to Take the Next Step?

To learn more about Vidsys or request a demo of our converged security software platform, visit our website:

www.vidsys.com

vidsys

Situation Management Simplified.

Washington DC | Boston | Europe | Middle East