Nouvelles menaces, nouvelles architectures de protection : repenser la sécurité NRBC des infrastructures critiques et des grands événements

Un paysage de menaces en constante évolution exige une vigilance accrue

Les grands événements et les infrastructures critiques évoluent dans un environnement de menaces toujours plus diversifié, accessible et imprévisible. Les organisations de sécurité doivent désormais prendre en compte un éventail plus large de substances, de modes de dispersion et de cibles potentielles que par le passé.

La menace ne se limite plus aux agents chimiques de guerre traditionnels ni aux capacités sophistiquées des États. Les produits chimiques industriels toxiques, les agents d'origine pharmaceutique, les toxines biologiques, les substances corrosives et les dispositifs binaires improvisés peuvent être produits ou assemblés à partir de matériaux relativement accessibles. Parallèlement, les substances modifiées et les agents biologiques émergents peuvent mettre en difficulté les systèmes de détection et d'identification reposant exclusivement sur des bibliothèques moléculaires prédéfinies.

La vulnérabilité s'étend bien au-delà des murs du site protégé. Protéger les grands événements et les infrastructures critiques, c'est protéger les personnes, les foules importantes et les personnalités, mais aussi les sites sensibles dans lesquels elles se rassemblent, travaillent ou se déplacent. La protection doit donc dépasser le périmètre du site principal et s'étendre à l'ensemble de l'écosystème qui soutient les événements, les réunions officielles et les activités quotidiennes : pôles de transport, parkings, files d'attente, postes de contrôle de sécurité et points d'entrée, hôtels, fan zones et autres espaces publics à forte densité ou lieux stratégiques. Une attention particulière doit être portée aux zones environnantes dans lesquelles les foules se rassemblent, circulent ou patientent.

Cette évolution impose de repenser les solutions de sécurité et de protection. Les architectures de protection efficaces associent de plus en plus des moyens de détection fixes et mobiles, plusieurs technologies de détection complémentaires ainsi

que la transmission des données en temps réel, aussi bien sur le site que vers les centres de commandement et de contrôle de niveau supérieur. La connectivité devient essentielle pour corréler les alarmes, partager une vision opérationnelle commune et permettre des décisions plus rapides et mieux coordonnées à tous les niveaux.

Les drones : un risque émergent et une nouvelle capacité de protection

Le développement rapide des drones, y compris des modèles disponibles dans le commerce, transforme à la fois la menace et les moyens d'y répondre.

En tant que vecteur potentiel de menace, un drone peut contourner les points de contrôle conventionnels ou survoler des zones sensibles. Il peut être utilisé à des fins d'observation, de perturbation, ou encore pour transporter et disperser des matières dangereuses.

Cependant, cette même technologie ouvre également de nouvelles possibilités en matière de protection. Un drone équipé d'un détecteur peut être envoyé en direction d'un rejet suspect sans exposer immédiatement le personnel. Il peut contribuer à la reconnaissance du périmètre, explorer une zone inaccessible, suivre un panache suspect ou recueillir des mesures au-dessus et autour d'un site protégé.

La valeur d'un drone ne repose pas uniquement sur la plateforme elle-même. Les données de son détecteur doivent être associées à sa position et transmises en temps réel à la structure de commandement. L'approche système de Proengin permet ce type d'intégration en connectant les détecteurs aux drones et aux véhicules terrestres sans pilote, en transmettant les informations de détection et de positionnement, puis en affichant les données obtenues au moyen d'une cartographie en deux ou trois dimensions. L'objectif est d'étendre les capacités de détection au-delà du périmètre fixe tout en réduisant l'exposition des opérateurs.

D'une protection distribuée à une réponse coordonnée

À mesure que le périmètre de protection s'élargit, la sécurité ne peut plus reposer sur des points de détection isolés. Elle nécessite une architecture connectée et organisée en plusieurs couches, combinant une surveillance fixe continue avec des moyens mobiles capables d'examiner les alarmes, de combler temporairement les lacunes de couverture et de suivre une menace en mouvement.

À l'intérieur des bâtiments, la réponse doit également s'adapter à l'origine du rejet. Une menace extérieure peut nécessiter la fermeture des prises d'air et la mise en

surpression des zones protégées, tandis qu'un rejet intérieur peut imposer l'isolement de certaines zones de ventilation et la modification des itinéraires d'évacuation.

Les systèmes de détection, les dispositifs de gestion des bâtiments, les équipes de sécurité et les services d'intervention d'urgence doivent donc contribuer à une même vision opérationnelle. Les équipes locales doivent disposer de l'autonomie nécessaire pour agir immédiatement, tandis que les centres de commandement de niveau supérieur ont besoin d'informations consolidées afin de coordonner les ressources sur plusieurs sites. L'objectif n'est pas simplement de déployer davantage de capteurs, mais de créer un réseau cohérent capable de détecter, de caractériser et de gérer une menace dans de multiples environnements opérationnels.

De la détection à la décision : l'innovation Proengin

Le principal défi consiste à transformer des données issues de capteurs hétérogènes en informations exploitables, disponibles au moment opportun. Proengin Shield connecte des détecteurs fixes et mobiles, des capteurs tiers, des échantillonneurs, des caméras, des véhicules, des drones et des véhicules terrestres sans pilote au sein d'une architecture ouverte et modulaire.

La gestion de la menace est structurée autour de trois niveaux : le niveau local, destiné à permettre une action immédiate au plus près du capteur ; le niveau central, chargé de la coordination à l'échelle du site et de la qualification des alarmes ; et le niveau global, consacré à la supervision consolidée de plusieurs sites et à l'appui des centres de commandement de niveau supérieur.

En reliant les informations provenant de plusieurs capteurs, plateformes et sites, cette approche réduit le délai entre la détection et la prise de décision. Elle permet ainsi aux opérateurs de comprendre plus rapidement la situation et de coordonner la réponse appropriée.

Tout commence par la détection. La protection commence lorsque l'information devient compréhensible, fiable et exploitable.