GROUNDAWARE®

EVOLVING TO EVENT-BASED LAYERED SECURITY

An OWL Whitepaper

OBSERVATION WITHOUT LIMITS LLC
1000 Explorer Boulevard
Huntsville, Alabama 35806 U.S.A.
888-297-9559
www.owlknows.com

OWL

OBSERVATION
WITHOUT
LIMITS

INTRODUCTION

The landscape of critical infrastructure security is evolving and becoming more complex at a rapid pace. Security concerns that were once viewed largely as threats to customer service and efficiency now impact regulatory compliance, indemnity, operations, maintenance, and many other areas.

Unfortunately, industry approaches to security have failed to keep pace with evolving threats, as many companies continue to rely primarily or solely on physical barriers and video surveillance. Despite advances in optical technology and analytics, video surveillance continues to require significant infrastructure and maintenance investment, while asking error-prone security personnel to monitor more and more video systems manually. Further compounding the problem is the reality of how low lighting, weather, and other environmental phenomena impact the efficacy of video monitoring alone.

Yet the impediments to security innovations are real. Transitioning to new systems is traditionally expensive, requiring significant capital investment and retraining of personnel. And new systems often integrate poorly with legacy systems that remain in place.

The way forward involves an evolution in the way the security solutions are envisioned, integrated, and used. Specifically, industry leaders should transition to event-based (not continuous monitoring-based) security using technologies well integrated to provide multiple layers of surveillance with each layer filling in gaps not fully addressed by other layers.

EXECUTIVE SUMMARY

Critical infrastructure security needs are growing in complexity and scale beyond ability of traditional approaches to efficiently and effectively address.

Concepts of operations and technologies exist today to evolve to a new model of surveillance and security operations.

Traditional surveillance methods requiring manual continuous monitoring of sensors should evolve to models that use technology for event-based response to security threats.

Effective and efficient physical security architectures leverage multiple layers of capabilities to provide wide-area and focused situational awareness while minimizing false alarms and automating detection, tracking, alarming, deterrence, and response.

Evolving to event-based, layered solutions can reduce operating and maintenance costs for reasonable capital investment.

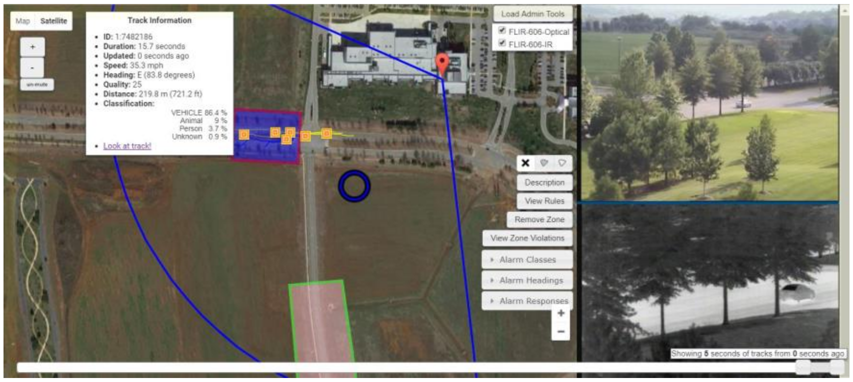
EVENT-BASED VS. CONTINUOUS MONITORING

Traditional surveillance monitoring by security personnel originally required an individual to watch one or many screens at all times, manually noting any change or suspicious activity. As video surveillance assets were added, multiple personnel were used to watch more video feeds simultaneously. As yet more video surveillance assets have been added, analytics have been employed with limited success to enable monitoring of more areas with a finite number of personnel. But as the need for increased infrastructure security

Security operators today typically continuously monitor multiple feeds of information. An event-based model eliminates manual operations in favor of managing events in real time.

grows, so does the difficulty in resolving competing realities. This leads to a strategic question for security stakeholders: What is the “next” evolution in critical infrastructure security that will enable increased surveillance, while decreasing manpower requirements and workload?

The solution is to transition to an event-based concept of operations using primarily technology, rather than human security operators, to detect, track, deter, and respond to physical threats. Consider the following examples of how an event-based security approach contrasts to traditional approaches currently in use:



Track Information

- ID: 1:7482186
- Duration: 15.7 seconds
- Updated: 0 seconds ago
- Speed: 35.3 mph
- Heading: E (83.8 degrees)
- Quality: 25
- Distance: 219.8 m (721.2 ft)
- Classification:

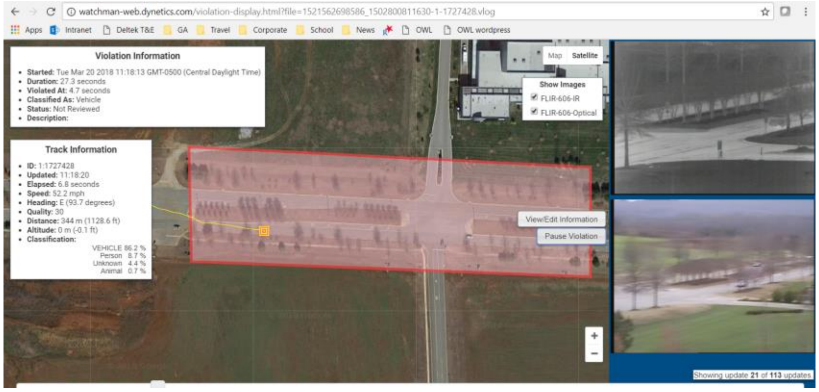
VEHICLE 86.4 %
Animal 9 %
Person 3.7 %
Unknown 0.9 %

- Look at track!

Showing 5 seconds of tracks from 0 seconds ago

Shown at left is screenshot of a ground surveillance radar system that captures wide-area and focused surveillance information for critical infrastructure. System provides real-time detection, tracking, alarming, deterrence, and response as security events transpire.

- Detection: Many traditional video-anchored systems -- even those with analytics --require operators to notice that threats have been identified. Next, operators must manually assess where threats come from, what they are, and if they are approaching or within restricted areas. An event-based approach would use technology to surveil much larger areas that include areas of interest (both the primary area and wider surrounding areas); archive activity history of objects detected near infrastructure; classify objects as humans, vehicles, or animals to minimize alarms; automatically alarm and notify operators if objects enter operator-defined security areas; and continue archiving the movement of objects throughout incursions.
- Tracking: Traditional systems require operators to manually track -- or rely on analytics to track -- objects once detected. However, issues arise when multiple objects enter the security area and proceed in different directions. When objects pass from one video surveillance asset to the area of another that may or may not be trained to see the object and may or may not be of the same type of video system. Tracking can quickly overwhelm



watchman-web.dynetics.com/violation-display.html?file=1521562698586_1502800811630-1-1727428.vlog

Violation Information

- Started: Tue Mar 20 2018 11:18:13 GMT-0500 (Central Daylight Time)
- Duration: 27.3 seconds
- Violated At: 4.7 seconds
- Classified As: Vehicle
- Status: Not Reviewed
- Description:

Track Information

- ID: 1:1727428
- Updated: 11:18:20
- Elapsed: 6.8 seconds
- Speed: 52.2 mph
- Heading: E (93.7 degrees)
- Quality: 30
- Distance: 344 m (1128.6 ft)
- Altitude: 0 m (-0.1 ft)
- Classification:

VEHICLE 86.2 %
Person 8.7 %
Unknown 4.4 %
Animal 0.7 %

Showing update 21 of 113 updates

Shown at left is screenshot of a live ground surveillance radar system showing real-time capture of information on security events as they happen. Also shown is the capture of video of the security event. On fully automated basis, information is captured for real-time deterrence and response, as well as for after-action review.

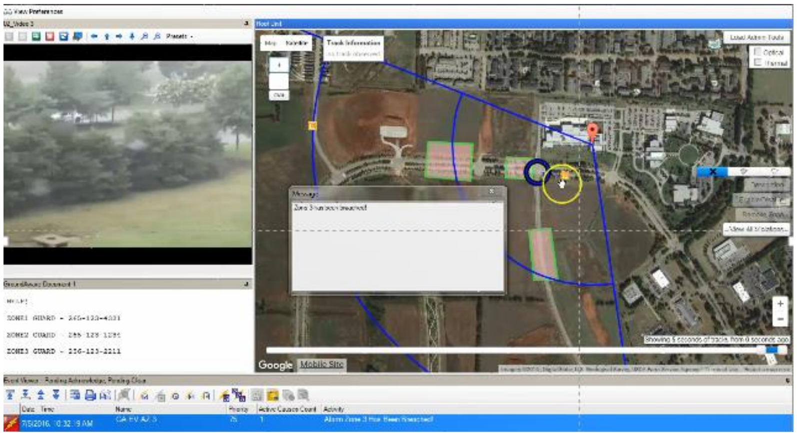
the ability of a manual operator to keep track of all objects simultaneously, which impacts their ability to deter and coordinate a response. An event-based approach would enable continual recorded tracking of all objects around the area independent of operator involvement. This frees the operator to break away as needed to perform deterrence or response coordination without dropping surveillance on objects of interest.

- Deterrence: Traditional systems require manual intervention to attempt deterrence of threats remotely, which is often a priority when sites are unattended and response times by the nearest personnel are long (e.g., at remote electric utility transmission substations). Imagine being a security operator who must look up information on existing deterrence capabilities at a site (e.g., lights, sirens, etc.) and how to initiate them. All the while the intrusion is proceeding. An event-based system automates these functions and initiates deterrence capabilities on site when an alarm is induced, increasing the likelihood that the intrusion can be stopped or be delayed.

Shown above are lighting and audio systems used for critical site security. These systems can be triggered into action as security events transpire, with goal of ending or minimizing the impact of intrusions.

- Response: With traditional systems, security operators must manage response information manually. Again, imagine security operators responding to an alarm triggered at a remote site. Where is the threat physically? What law enforcement agency has jurisdiction? What is the phone number? Who within the company has authority for that site in that area? The list of information needed to address an alarm is significant and impossible to retain in memory for the many sites being surveilled simultaneously by an operator or team of operators. An event-based system retains all of the response information and procedures for each site and automatically displays them to security operators when an alarm is triggered for that site.

Succinctly, critical infrastructure security needs have become complex enough that automation must be used more extensively to increase security capability. Of course, it is also true that no single technology addresses all of today's security requirements. Technologies typically integrate poorly and at increased lifecycle cost to companies investing in them. Technology often works against operators, increasing training requirements and decreasing efficiency due to nuisance alarms. The solution is a layered security architecture composed of the right



Zone 3 has been breached!

Showing 5 seconds of track, from 0 seconds ago

7/5/2016 10:32:19 AM | Alarm Zone 3 Has Been Breached

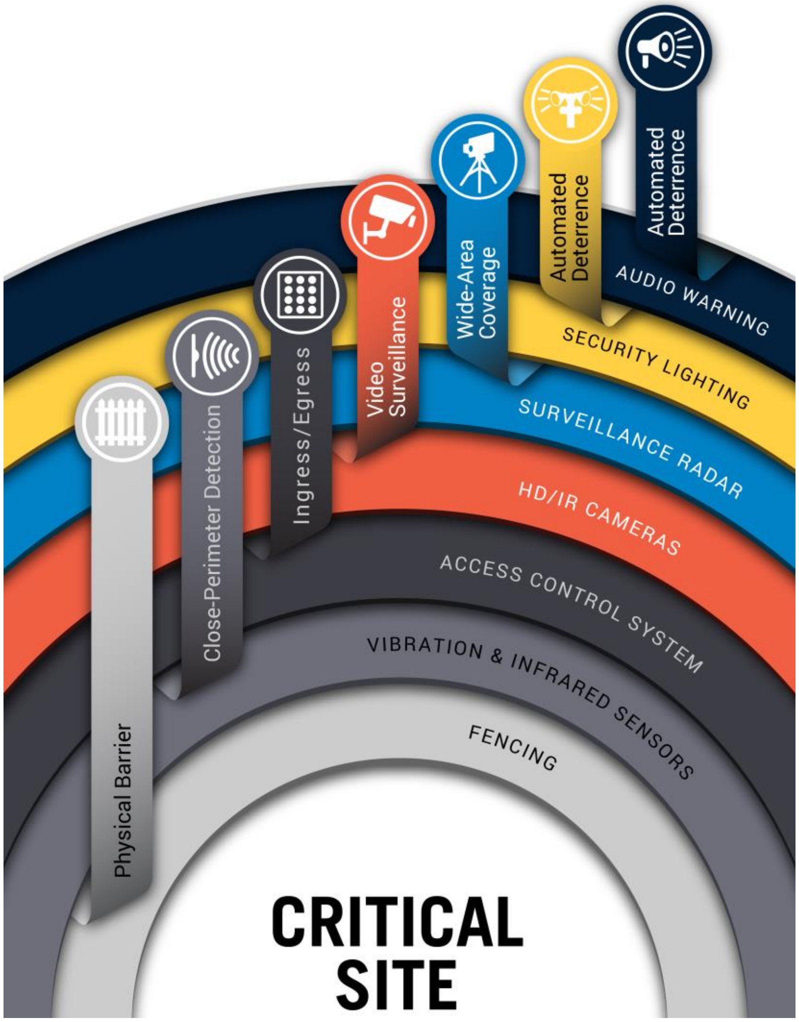
Shown at left is screenshot of a ground radar system detecting, tracking, cueing and slewing, and sending alarm to physical security information management system. In real time, operators have the information to track, assess, deter, and respond to security threats in a single location. No labor-intensive continuous monitoring is required.

technologies, which are integrated properly with legacy and new systems to maximize security awareness while minimizing nuisance alarms.

AN INTEGRATED, LAYERED SECURITY SYSTEM OF SYSTEMS

Every organization has different needs and, therefore, relies on security systems comprised of multiple subsystems (e.g., physical barriers, access control, surveillance, deterrence, alarming, lighting, etc.) to achieve its security objectives. A layered, well integrated security architecture is comprised of a set of systems – beginning with wide area surveillance and concluding with localized response. Each layer fills a gap poorly met by the others, while integrating as seamlessly as possible with other layers of security to reduce operator requirements and workload.

Such a layered-architecture system begins with a wide-area surveillance sensor, such as a ground surveillance radar, that can detect, track, classify, and drive deterrence and response to potential threats immediately outside and within the site. The use of such sensors provides a number of benefits:



Layered security involves the design and deployment of a *"*system of systems.*"* In essence, this means that owner/operators employ multiple capabilities, structures, and technologies to provide effective security for critical sites. Illustrated here are layers for physical barrier; ground-level sensors in immediate vicinity of the perimeter; ingress/egress management; video surveillance; ground surveillance radar; and security lighting and audio warning systems for deterrence.

- Establishing multiple alarm zones, each with tailored response procedures. For example, within 100 feet of a critical site's perimeter, security personnel may be notified of an alarm to provide optimal situational awareness with no further alarm, deterrence, or responsive actions initiated.
- Tracking continually all objects near and within sites of interest while they are present, with all related information archived for later use as needed by security.
- Collecting more information about potential threats and, thereby, reducing nuisance alarms. For example, only objects identified as of interest (e.g., humans and/or vehicles) travelling toward the site and getting within a certain distance of it are alerted to the operator, while animals or other pedestrian traffic near but not approaching the site are ignored.
- Integrating and controlling additional surveillance assets as needed. For example, understanding the location of all existing cameras and cueing and slewing the closest camera to the threat to track the threat while at the site.
- Time-coordinating all surveillance asset information at the site so that security operators see real-time and archived information from all sensor assets (e.g., radar time integrated with video playback).
- Coordinating and employing deterrence techniques at points of intrusion. For example, turning on lights around the exterior and interior of the site or sounding an alarm nearest to the intruder.

Perimeter physical barriers that are integrated as fully into the overall security picture of the site as possible are the next key element in a layered architecture. For instance, this would include, at a minimum, sensors that can inform the overall security system about the state of vehicle and pedestrian gates and whether they have been opened in an authorized manner or not. These sensors can be integrated with access control and the complete security system to disable interior alarming when an authorized entry has occurred, among other purposes. Further, fence vibration monitors, unattended ground sensors, and infrared beam sensors can be used to increase the situational awareness of the perimeter barrier in view of potential threats.

Interior to the site, pan-tilt-zoom and fixed high-definition cameras with both day and night video capability are fully integrated and controlled by the wide area surveillance asset until manual control is taken by the security operator. These systems should be fully integrated with the video management systems and all video information integrated with the other security sensors (e.g., time-integrated with radar and alarm data).

Deterrence technologies such as area lighting, strobe lights, targeted spot lights, audible warnings, and even-two way audible systems are coordinated by wide-area surveillance systems to delay or stop intrusions at point of egress into critical sites. Intruders witnessing active responses to intrusion attempt are more likely to stop and flee; or, at minimum, deterrent actions will likely delay intrusions while intruders attempt to determine what to do after they have been detected. This may result in unsuccessful intrusion attempts, or at the least provide security personnel longer to coordinate and execute a response.

In response to this vision, industry must drive vendors to develop and offer sensors and information management systems that integrate easily with existing legacy systems, minimize false alarms, utilize known or familiar platforms to minimize operator training, and provide real-time and actionable surveillance and response information to security personnel.

OWL

www.owlknows.com

888-297-9559