Descifrando la *pila de seguridad*

Ella Ortenberg, HiveWatch

La seguridad física conlleva muchos conocimientos que se dan por sentados. Se utilizan acrónimos como VMS, ACS, PSIM y CV como si todo el mundo supiera lo que significan. No existe un glosario oficial y entender cómo funcionan estos sistemas en conjunto (spoiler: a menudo no lo hacen) lleva tiempo.

Si eres nuevo en el mundo de la seguridad, vienes de otro campo o estás harto de asentir con la cabeza en las reuniones mientras luego buscas frenéticamente en Google, aquí tienes una explicación detallada

Los fundamentos: los sistemas de gestión de vídeo (VMS)

Empecemos por el elemento más visible de la infraestructura de seguridad. Un sistema de gestión de vídeo (VMS por sus siglas en inglés) reúne las señales de vídeo de varias cámaras en un único lugar desde donde se puede supervisar, grabar y buscar las grabaciones. Piensa en él como el centro de control de tus cámaras.

La mayoría de las organizaciones ya cuentan con un VMS desde el primer momento. A menudo es la primera gran inversión en tecnología de seguridad que realiza una empresa, y se convierte en el punto de referencia para todo lo demás.

Lo que nadie te cuenta sobre las plataformas VMS es que generan una cantidad abrumadora de datos. Una sola cámara puede producir terabytes de material de vídeo con el paso del tiempo. Multiplica eso por docenas o cientos de cámaras, y tendrás un problema de almacenamiento y búsqueda mayor de lo que la mayoría de la gente cree.

Sistemas de control de acceso (ACS): quién puede entrar

Los sistemas de control de acceso (Access Control Systems por sus siglas en inglés) gestionan quién puede acceder a qué espacios y cuándo. Se encargan de los lectores de tarjetas, las cerraduras, los torniquetes y la lógica que determina si las credenciales de una persona son válidas.

Las plataformas ACS conectan el hardware físico (los lectores y las cerraduras) a una base de datos de usuarios y permisos. Cuando alguien pasa su tarjeta, el sistema comprueba sus credenciales con respecto a las normas de acceso y concede o deniega la entrada, creando un registro del intento en cualquier caso.

Lo que complica los ACS es que las normas de acceso se vuelven complejas rápidamente. No se trata solo de gestionar “¿puede esta persona abrir esta puerta?”. Se gestiona el acceso basado en el tiempo, las credenciales temporales para visitantes o contratistas, la integración con los sistemas de RR. HH. para la concesión y retirada automáticas de permisos, y los requisitos de cumplimiento en materia de registros de auditoría.

Visión artificial (CV): enseñar a las cámaras a comprender

La visión artificial (CV por sus siglas en inglés) es una forma de inteligencia artificial que analiza las imágenes de las cámaras para detectar objetos, comportamientos o situaciones concretas. En lugar de que una persona esté pendiente de los monitores e intente detectar algo inusual, los algoritmos de visión artificial pueden identificar elementos como armas, bolsos abandonados, personas que acceden a zonas restringidas o vehículos sin los permisos adecuados.

La visión por computadora realiza el análisis utilizando la infraestructura de cámaras ya existente. La tecnología ha mejorado considerablemente en los últimos años, pero aún no es mágica. La visión por computadora es tan buena como los datos con los que se ha entrenado, y funciona mejor cuando busca elementos específicos y bien definidos, en lugar de conceptos vagos como “comportamiento sospechoso”.

La realidad práctica del CV es que reduce el problema de “buscar una aguja en un pajar”. En lugar de revisar horas de grabaciones en busca de un incidente concreto, el CV puede señalar los momentos que se ajustan a tus criterios. No lo detectará todo y, en ocasiones, señalará cosas que no son amenazas, pero hace que la vigilancia a gran escala sea viable de formas que no eran posibles cuando se necesitaban ojos humanos en cada cámara.

Sistemas de gestión de visitantes (VMS... Sí, es el mismo acrónimo)

Los sistemas de gestión de visitantes registran quién entra en las instalaciones, cuándo llega y a qué zonas tiene autorización para acceder. Estas plataformas han evolucionado con respecto a las antiguas hojas de registro en papel y ahora gestionan el registro previo, la impresión de acreditaciones, las notificaciones a los anfitriones y la integración con el control de accesos.

La gestión moderna de visitantes no se limita a saber quién se encuentra en el edificio. Se trata también del cumplimiento normativo (quién ha accedido a zonas sensibles), la respuesta ante emergencias (a quién hay que localizar durante una evacuación) y la eficiencia operativa (reducir las demoras en recepción sin descuidar la seguridad).

Los sistemas de detección de intrusiones (IDS): la red de sensores

Los sistemas de detección de intrusiones (IDS por sus siglas en inglés) utilizan sensores como detectores de movimiento, sensores de rotura de cristales y contactos de puerta para alertar cuando alguien entra en un espacio al que no debería acceder. Estos son los sistemas que activan las alarmas cuando se produce una intrusión en el perímetro fuera del horario laboral.

Las plataformas IDS suelen ser la tecnología más antigua de un conjunto de sistemas de seguridad, ya que llevan más tiempo en el mercado que los modernos sistemas de vídeo o de control de acceso. Son fiables, pero tienen sus limitaciones. Te indican que ha ocurrido algo,
pero no necesariamente qué ha ocurrido ni quién ha estado involucrado.

El reto de la integración con los IDS consiste en conseguir que las alertas de estos sensores activen acciones en otros sistemas, como que un detector de movimiento muestre automáticamente las imágenes de la cámara más cercana o desbloquee una puerta de salida en caso de emergencia.

Gestión de la información sobre seguridad física (PSIM): la capa de agregación

Aquí es donde la cosa se pone interesante. Las plataformas PSIM (Physical Security Information Management) intentan resolver el problema fundamental de todo lo que he descrito hasta ahora: todos estos sistemas funcionan de forma aislada.

Una plataforma PSIM conecta la información procedente de múltiples sensores y sistemas, correlaciona los eventos y ofrece una visión unificada de lo que está sucediendo. En lugar de tener que supervisar cinco paneles de control diferentes, los equipos de seguridad disponen de una única interfaz que muestra de forma conjunta las alertas procedentes del VMS, el ACS, el IDS y otras fuentes.

La teoría es estupenda. La puesta en práctica suele ser complicada. Las implementaciones de PSIM requieren una configuración considerable y un mantenimiento continuo, y su eficacia depende en gran medida de las integraciones que puedan establecer con los sistemas existentes. Sin embargo, cuando se hace bien, el PSIM transforma el funcionamiento de las operaciones de seguridad al reducir la carga cognitiva de los operadores y ayudarles a comprender el contexto completo de un incidente.

Detección de armas: enfoques de hardware y software

La detección de armas puede llevarse a cabo mediante escáneres de hardware específicos o mediante el análisis de visión artificial de las imágenes de las cámaras. El enfoque de hardware utiliza dispositivos similares a los detectores de metales de los aeropuertos, pero diseñados para ser más rápidos y menos intrusivos. El enfoque de visión artificial analiza el vídeo para identificar armas de forma visual.

La tecnología en este ámbito varía enormemente en cuanto a capacidad y precisión. La detección por hardware suele ser más fiable, pero requiere que las personas pasen por puntos de control específicos. La detección mediante visión artificial puede cubrir un área mayor, pero presenta mayores índices de falsos positivos y funciona mejor en condiciones de iluminación controladas.

Se trata de un ámbito en el que las afirmaciones de los proveedores suelen superar el rendimiento real, por lo que es fundamental realizar pruebas en su entorno específico
antes de tomar decisiones.

Comunicación masiva (Mass Comms): difundir el mensaje

Los sistemas de comunicación masiva (Mass Comms) facilitan el envío rápido de alertas de emergencia a grupos grandes de personas. En el transcurso de un incidente, estas herramientas resultan esenciales para notificar a los ocupantes, sincronizar las acciones de los equipos de respuesta y establecer canales de comunicación con las autoridades policiales.

Estas plataformas se integran con los sistemas de seguridad, de modo que cualquier incidente detectado por su sistema IDS o CV pueda activar automáticamente las comunicaciones. El reto consiste en encontrar el equilibrio entre la rapidez (enviar las alertas de forma inmediata) y la precisión (evitar el pánico por falsas alarmas).

Los buenos sistemas de comunicación masiva gestionan múltiples canales, como mensajes de texto, correo electrónico, notificaciones de aplicaciones y altavoces. También realizan un seguimiento de quién ha recibido y confirmado los mensajes, lo cual es importante a la hora de rendir cuentas en situaciones de emergencia.

Inteligencia de fuentes abiertas (OSINT): más allá de su perímetro

Las plataformas OSINT (Open Source Intelligence) rastrean la web y las redes sociales para identificar posibles amenazas antes de que lleguen a su espacio físico. Estos sistemas supervisan las publicaciones con etiquetas de ubicación, las palabras clave relacionadas con amenazas y los patrones que puedan indicar incidentes planificados.

La OSINT ha cobrado mayor relevancia, ya que las amenazas potenciales se anuncian cada vez más en línea antes de pasar a la acción física. La tecnología puede proporcionar una alerta temprana, pero también plantea cuestiones de privacidad y requiere una política cuidadosa sobre cómo se recopila la información y cómo se actúa en consecuencia.

Gestión de casos e incidentes: seguimiento de la respuesta

Las plataformas de gestión de casos ayudan a los equipos de investigación a documentar incidentes, realizar un seguimiento de las pruebas y gestionar los flujos de trabajo de investigación. Las plataformas de gestión de incidentes ayudan a los equipos a registrar y responder a los eventos de seguridad en tiempo real.

Esta distinción es importante porque la gestión de casos se centra en la investigación tras un incidente (como el trabajo de un detective), mientras que la gestión de incidentes se centra en la respuesta operativa durante un evento (como el envío de personal y la coordinación). Muchas organizaciones necesitan ambas, pero empiezan por la gestión de incidentes porque esta aborda las necesidades operativas inmediatas.

¿POR QUÉ ES TAN IMPORTANTE TODO ESTO?

Comprender la estructura de seguridad no consiste solo en conocer definiciones. Se trata de reconocer que la infraestructura de seguridad física es, en esencia, un problema de integración de datos. Cada sistema genera información, pero el valor reside en conectar esos puntos de datos para convertirlos en inteligencia útil.

Cuando tu sistema de control de acceso muestra que alguien ha accedido con su tarjeta a una zona restringida, tu VMS debería mostrar automáticamente las imágenes de la cámara de esa ubicación. Cuando se activa un sensor de intrusión, tu PSIM debería correlacionarlo con los intentos de acceso recientes y las pruebas de vídeo. Cuando se detecta un arma, tu sistema de comunicación masiva debería alertar inmediatamente a las personas adecuadas.

Esa es la teoría. La realidad es que la mayoría de las infraestructuras de seguridad se sostienen con integraciones que fallan, procesos manuales que generan retrasos y operadores que gestionan una complejidad que no debería existir.

El sector avanza hacia plataformas más unificadas que reducen el número de sistemas independientes, y la IA está ayudando a salvar las brechas entre sistemas que no pueden integrarse directamente. Pero aún no hemos llegado a ese punto. La mayoría de los equipos de seguridad siguen gestionando un conjunto de soluciones puntuales que requieren un esfuerzo considerable para que funcionen conjuntamente.

Si estás dando tus primeros pasos en el mundo de la seguridad, aprender cómo funcionan estos sistemas y cómo deben integrarse te hará mucho más valioso. Si estás evaluando nuevas tecnologías, comprender toda la pila te ayudará a plantear mejores preguntas sobre cómo encajarán las soluciones en tu infraestructura actual.

Y si solo intentas seguir el hilo en las reuniones, ahora ya tienes el glosario que nadie te dio el primer día.