



När separata säkerhetssystem skapar blinda fläckar

En kamera kan spela in, en dörr kan logga en passage och ett larm kan skicka en signal. Ändå kan verksamheten sakna svaret på den viktigaste frågan: vem ser helheten och agerar när flera händelser hör ihop?

PUBLICERAD	12 september 2026
FÖRFATTARE	Siren Techs ingenjörsteam
LÄSTID	6 min läsning

Riskscenario: tre system, ingen gemensam incidentbild

Tänk er en verksamhet där kameror hanteras i ett gränssnitt, dörrbehörigheter i ett annat och larm via en separat mottagarlista. En dörr öppnas efter stängning, en rörelsesensor reagerar och en kamera har material från samma tid. Varje system har registrerat sin del, men ingen vy visar direkt hur händelserna hänger samman.

Det här är ett riskscenario, inte ett påstående om en namngiven Siren Tech-kund. Poängen är att teknik kan fungera var för sig samtidigt som ansvar, tidslinje och nästa åtgärd förblir otydliga.

Den blinda fläcken finns ofta mellan systemen

Problemet behöver inte vara en trasig kamera eller sensor. Det kan uppstå i överlämningen mellan en signal och den person som ska bedöma den. Om enhetsstatus, behörigheter och incidentunderlag finns på olika platser tar det längre tid att kontrollera vad som faktiskt har hänt.

En gemensam teknisk vy löser inte ansvar automatiskt. Verksamheten behöver fortfarande bestämma vem som tar emot olika händelser, vem som får agera och hur avvikelser dokumenteras och följs upp.

Fyra kontroller att gå igenom

En platsanalys bör börja med arbetsflödet och därefter kontrollera vilken teknik som behövs.

- Vilka entréer, rum och andra zoner behöver ge en händelse?
- Vilken person eller roll ska ta emot och bedöma varje typ av signal?



- Kan behöriga användare se enhetsstatus och relevant incidentunderlag utan att leta i flera system?
- Hur dokumenteras beslut, åtgärder och kvarstående risker efter händelsen?

Så kan Siren System bidra

Siren System kan samla kompatibla larmknappar, kameror, sensorer, hubbar, routrar, passerkort, lås, UPS och sirener i ett gemensamt ekosystem. I Siren Portal kan behöriga administratörer bland annat se enhetsstatus, senaste kontakt och anslutning samt arbeta med incidentrapporter och behörigheter.

Vilka produkter och funktioner som ska ingå avgörs efter verksamhetens lokaler, roller och arbetssätt. Befintlig teknik behöver kontrolleras innan Siren Tech kan bekräfta vad som kan återanvändas eller anslutas.

Vad en samlad lösning inte garanterar

Ett sammanhållet system förhindrar inte varje intrång, driftstörning eller felaktigt beslut. Kameratäckning, nätverk, ström, behörigheter, mottagarflöden och rutiner behöver planeras och underhållas som delar av samma säkerhetsarbete.

Siren Tech levererar teknik, installation och tekniskt stöd enligt vald lösning. Bemannad bevakning och fysisk larmuttryckning är separata funktioner och ingår inte automatiskt.

Börja med en konkret genomgång

Lista först de system som används i dag och välj en verklig händelsetyp att följa från signal till beslut. Om ansvar, information eller nästa steg blir oklart har ni hittat en punkt som behöver hanteras i lösningsdesignen.

Under en kostnadsfri säkerhetskonsultation går Siren Tech igenom lokaler, riskzoner, befintlig teknik, uppkoppling, ström, roller och larmflöden. Därefter diskuteras produktval, systemstruktur, installation och offert utan köpkrav.

Källor och vidare läsning

[Boka kostnadsfri säkerhetskonsultation](#)

[Se hur Siren System hänger ihop](#)

[Arbetsmiljöverket: arbeta systematiskt med risker](#)



When separate security systems create blind spots

A camera can record, a door can log a passage and an alarm can send a signal. Yet the organisation may still lack the answer to the most important question: who sees the whole picture and takes action when several events are connected?

PUBLISHED	12 September 2026
AUTHOR	Siren Tech's engineering team
READING TIME	6 min read

Risk scenario: three systems, no shared incident picture

Imagine an organisation where cameras are managed in one interface, door permissions in another and alarms through a separate recipient list. A door opens after closing time, a motion sensor reacts and a camera has footage from the same time. Each system has recorded its part, but no view immediately shows how the events are connected.

This is a risk scenario, not a claim about a named Siren Tech customer. The point is that technology can work separately while responsibility, timeline and the next action remain unclear.

The blind spot often exists between systems

The problem does not have to be a broken camera or sensor. It can arise in the handover between a signal and the person expected to assess it. If device status, permissions and incident information are kept in different places, it takes longer to verify what has actually happened.

A shared technical view does not assign responsibility automatically. The organisation still needs to decide who receives each type of event, who may act and how anomalies are documented and followed up.

Four controls to review

A site assessment should begin with the workflow and then determine which technology is needed.

- Which entrances, rooms and other zones need to generate an event?
- Which person or role should receive and assess each type of signal?



- Can authorised users see device status and relevant incident information without searching several systems?
- How are decisions, actions and remaining risks documented after the event?

How Siren System can contribute

Siren System can bring compatible alarm buttons, cameras, sensors, hubs, routers, access cards, locks, UPS units and sirens into a shared ecosystem. In Siren Portal, authorised administrators can view device status, latest contact and connection, among other details, and work with incident reports and permissions.

The products and functions included are determined by the organisation's premises, roles and ways of working. Existing technology must be checked before Siren Tech can confirm what can be reused or connected.

What an integrated solution does not guarantee

An integrated system does not prevent every intrusion, outage or incorrect decision. Camera coverage, network, power, permissions, recipient flows and procedures need to be planned and maintained as parts of the same security programme.

Siren Tech provides technology, installation and technical support according to the selected solution. Staffed guarding and physical alarm response are separate functions and are not automatically included.

Start with a concrete review

First list the systems used today and choose one real event type to follow from signal to decision. If responsibility, information or the next step becomes unclear, you have found a point that needs to be addressed in the solution design.

During a free security consultation, Siren Tech reviews premises, risk zones, existing technology, connectivity, power, roles and alarm flows. Product selection, system structure, installation and a proposal are then discussed without a purchase commitment.

Sources and further reading

[Book a free security consultation](#)

[See how Siren System fits together](#)

[Swedish Work Environment Authority: systematic risk prevention](#)