How to Deter, Detect, Delay and Deny intruders

At Heras we advise companies and organizations in how to protect and secure their most valuable assets. Our proven approach takes a thorough look at each and every aspect of the situation. We ensure that we listen and understand our clients needs, to ensure that all potential risks are taken into consideration and that appropriate steps are taken to mitigate these risks. In this article, we explain how we implement and achieve the most

Heras actively operate in six European countries. Each country has slightly different laws and regulations in relation to perimeter security. In the Netherlands there are many guidelines but in the UK and Germany there are many requirements and regulations that products and installations must abide by. Over the last 25 years we have worked within these guidelines and regulations and we have gained a substantial amount of experience and knowledge. From this we have perfected our way of working and developed our own proven approach, based on best practices, and created the Heras Security Model. We now apply this in all countries and sectors we operate in, From business sites to airports and high-security locations. This document outlines and explains how we do this.

Which threat do you want to mitigate?

Protecting your most valuable assets is about keeping out unauthorized people. Every company faces numerous different types of threats. Some organizations are a potential target for organized crime, other companies may face petty thieves, activists, espionage or just curious walkers or animals. Appropriate security is required in all situations, but all require different measures dependent on the threat & risk level. Sometimes a warning sign or a white line on the road is sufficient, in most cases it needs much more than this.

That is why we a proven procedure to take into consideration the different threats, to understand which scenarios apply at the individual sites. What valuable assets do you have on your property? Which threat do you want to prevent? What is the purpose of the proposed security measure ? Is it to prevent crime ? or just to keep out casual passers-by. Is it to prevent visitors from entering dangerous areas?. These and many other questions must be answered to allow an effective system to be designed and implemented.

By understanding your specific situation, we can then discuss which scenarios are most relevant. By taking a critical look at your situation, we will propose an action plan for the most suitable security solution within your budget, time and requirements.

Demarcate, deter, detect, delay

This action plan is based on a number of proven methods. Firstly, we start from the 3Ds - deter, detect and delay (as used by the UK government security body, CPNI). This model prescribes that the security of a site must meet five conditions.

1. Clarify your perimeter boundary, indicating what is yours.
2. Deterrence – what level is needed.
3. Detection of an intrusion/attack attempt.
4. Delay of potential intruders.
5. Controlling access control of people and vehicles.

The first part of a perimeter security solution is to demarcate what's yours, and to decide how access to the site is undertaken. You will want to discourage potential unauthorized people from attempting to enter the premises. If the potential intruder is not dissuaded by the physical barrier , the intruder must be detected as early as possible to enable an appropriate response.
By detecting the attempted intrusion at the perimeter this ensures that you can respond in a timely manner. In addition to this, it is also very important that the intruder is delayed as much as possible. An analysis of potential attack points also needs to be highlighted and mitigated accordingly.

Over, through, under

Traditionally, there have been three basic scenarios in which intruders can gain access to your site. An intruder can climb over, dig under, or break through. In the latter case, someone can, for example, cut open the fence or ram a gate with a vehicle. All three ways must be taken into account when securing the site.

How much response time do you need?

You must ensure that the response time of the security team is taken into consideration when designing a perimeter security solution. To be able to do this we utilize the methodology from the UK security standards then we map out a time path analysis - INCI / DETAR (Incident / Detection „ alarm ,response). With this certified method of the DHM Security Institute, we determine how much response time you need to respond to an alarm or notification. In the example below, we assume that there is an intruder that wants to commit theft.

INCI / DETAR consists of two horizontal timelines.
The top timeline (INCI) shows in minutes how much time an intruder needs to gain access, acquire his target goods, and retreat to safety, basically from the moment an intruder enters the site until he leaves the site again.

The bottom line (DETAR) shows how long it takes for the police or security staff to respond and arrive on the scene. From the moment of detection to alarm and response. The idea is to ensure that your security setup is designed so that the bottom timeline is shorter than the top timeline i.e that the intruder is caught before leaving the site with their ill gotten gains.

For example, does your security response team take more than ten minutes to get to site? This may be too long if there is only an alarm on the building inside the perimeter, as they could get in and out in 5 minutes before the security team even arrives on site. In this case an extra level of security is required at the fence line in the form of a fence mounted detection system. This would then alert the security team in a more timely manner to get to site on time to catch the intruder. This time path analysis allows you to accurately determine how much time you need to allow for, thus ensuring that your security solution is effective.

4 Important Security Measures/considerations

Before designing a security system there are many operational and company processes that must be discussed and accounted for to ensure that everything works seamlessly together, because it only takes a small oversight to ruin or compromise the security of the system. These measures/considerations broadly fall into four categories.

1.Organizational - Measures that a company must actively manage.
Access control procedures with defined access rights to utilize both physical (Key management) and electronic (cards/tags etc.) means. Procedures for staff and visitors, contractors, emergency services and security staff with regards to access rights and operational functionality (e.g. unlocking and locking the premises each day) .
The front door can be one of the weakest points, especially when it is wedged open by staff to let some fresh air into the premises ! . Without support and clear rules/procedures , all other security measures could be seriously compromised.

2. Physical - What physical constraints or features can help or hinder security ? Fencing, gates, anti-running mats, barbed wire and other mechanical and physical measures can deter or slow down incoming intruders. But we must also consider how physical barriers can effect emergency protocols on how to safely evacuate a building.

3. Electronic - The purpose of electronic measures is to detect potential intruders and classify them as to whether they are a real threat or not, as quickly as possible. For example by utilizing camera systems, access control, PIDs detection systems and many other sensor technologies. By integrating these systems, and combining them together utilizing a Software management system (SMS), this gives a very reliable and efficient security system and the appropriate action can then be taken to alert the relevant parties of an intrusion attempt.

4. ICT - Computers, network / infrastructure, servers, firewalls and virus scanners. All software and hardware that supports the management of the perimeter security system. Consider, for example, a security management system that responds to a sensor that detects an event then immediately provides an ARC (alarm receiving center) with the pertinent alarm images to enable classification & clarification of the alarm event to then follow up with a pre-determined response action.

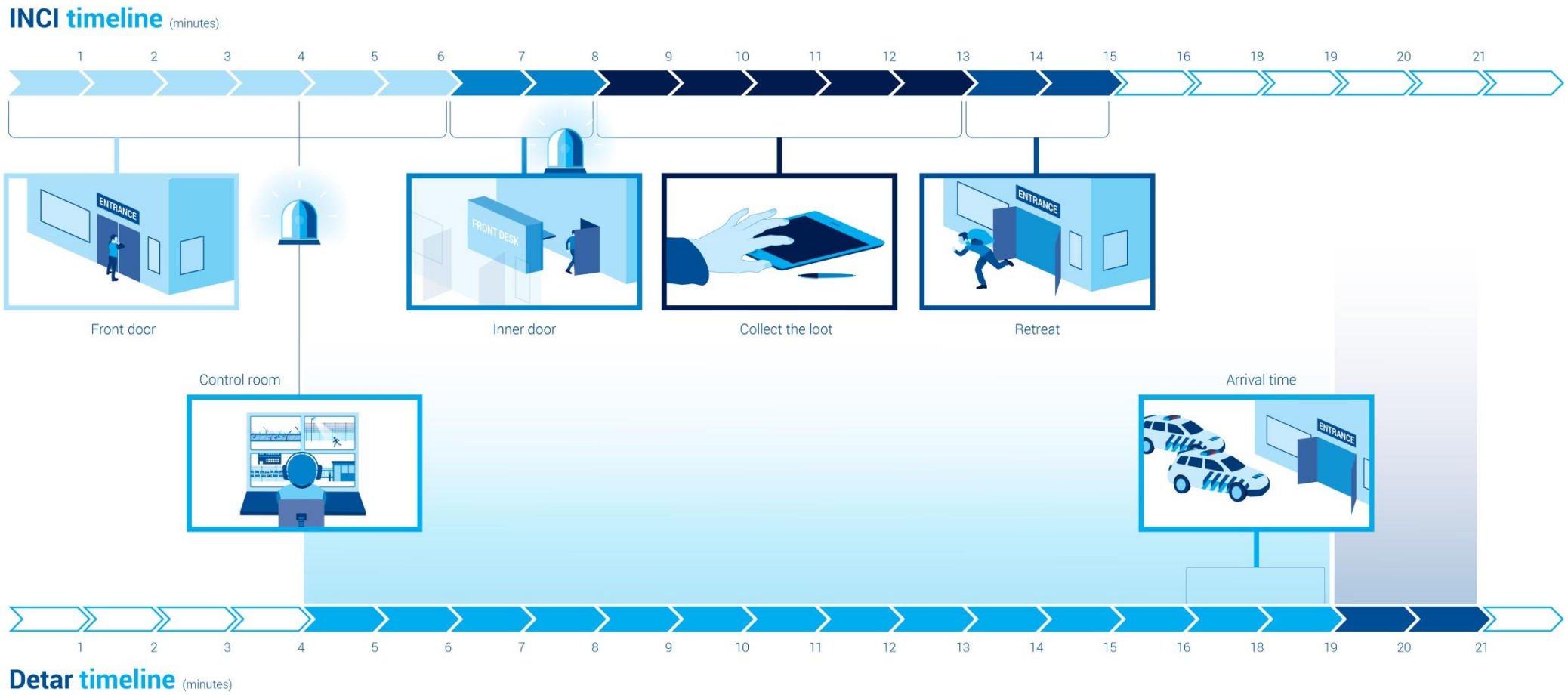
Choosing the correct alarm detection devices

The correct choice and installation of a detection device is critical to the usability and accuracy of the security system. Not only physical and electronic factors need to be considered but also environmental factors also. If the correct detection system is not specified or installed correctly then there will be a higher chance of false or unwanted alarms. Unwanted and false alarms are very different. An unwanted alarm is one that is due to a fault of the system or an alarm that cannot be verified. A false alarm is an alarm event which can be verified, such as those relating to animals or bad weather conditions.
With our expertise and knowledge of many different detector types we can design and install a system to keep both unwanted and false alarms to an absolute minimum. Correct configuration of these detectors is needed to achieve the aim of reducing these false alarms to a maximum of 1 per zone per month.

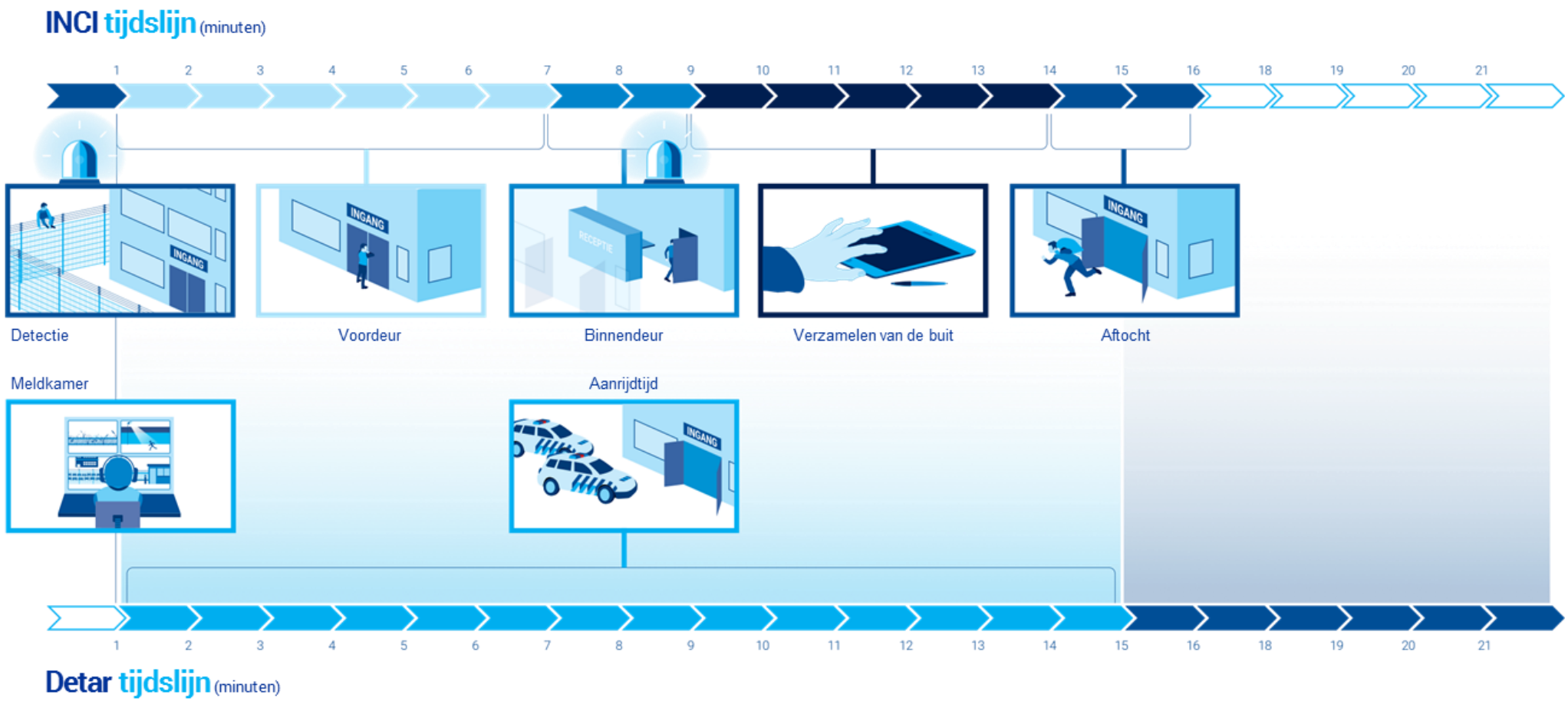
Integration

All of the points mentioned so far in this document all contribute to the effective security of your site. The individual components work even more effectively when they are integrated together. This ensures that all the information is collated in a very efficient and timely manner. For example, a fence detection system working in conjunction with a camera system can react very quickly to an intrusion attempt, the camera images from the alarm can then be used to verify if it is a real alarm or not. So based upon our many years of experience we implement our Heras Security model and advise which solutions are most appropriate to allow you to Deter, Detect and Delay any potential intruders at your site, to be able to react and respond in a timely fashion to allow the security response team to apprehend the intruders.

INCI DETAR | Only inside security



INCI DETAR | perimeter protection



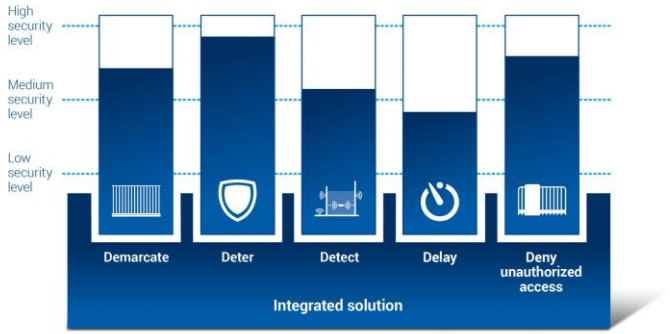
How our experts build your perimeter

Before implementing a new security solution for your site (or modifying an existing one), our security experts advise you on the best way to combat the potential risks. Our advice also includes checking all local environmental and geographic restrictions to ensure you have an effective solution. We are experts in identifying and supplying the right solution at the right time to secure your site, your people, your data.

Always remember that physical security measures are only part of an effective security solution for your site. They must be implemented to effectively support organizational processes for site security and operations. Our solutions ensure that on site security teams and support bodies (such as the police) can respond effectively and efficiently to any incidents.

Heras Security Model

Our model ensures that we seamlessly combine the most effective protection strategies and thus subsequently forms a reliable, practical security solution for every application.



By considering the different possible scenarios we can use our model to assign the relevant security level to each aspect of the perimeter security system and then propose the pertinent products to achieve that security level. This also means we can offer a tailor-made and integrated solution for every specific client need.
Based on these needs, we can agree a plan of action to implement the security proposal utilising the all of our experienced team members.

Conclusion

The security of each and every site is a often a challenge for every company as there are so many factors that need to be taken into consideration, but by utilizing our experienced team and the steps laid out in the Heras Security model we are very confident we can provide the best solution for our clients.

We first determine the threat and what valuables you want to protect. Then we describe the scenarios that are relevant to your company. Then we determine together how to prevent these scenarios with the time path analysis. Finally, we choose which measures you can take to achieve this.

By following these steps, we are able to provide our client for all over Europe with a complete security solution. We would be more than happy to help you any of your perimeter security challenges. Should you wish to know more about our approach and methodology we are contactable at : advice@heras.co.uk and we can then contact you to arrange a free consultation.