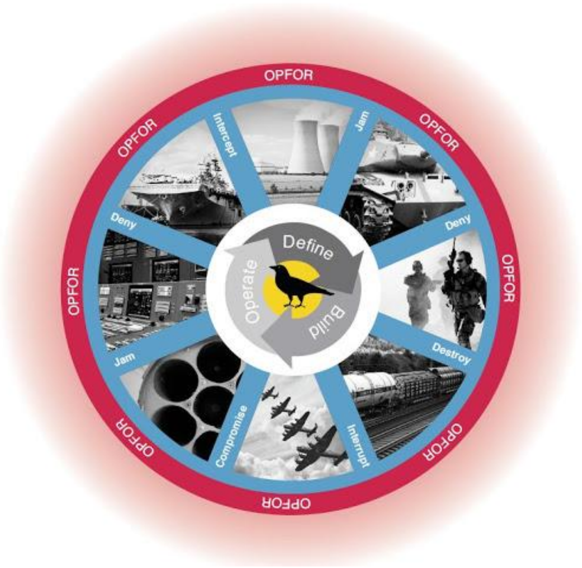
The KTC Approach:
A White Paper

Undertaking the task of securing a site, an asset or some specific information can seem like an overwhelming and complex task. KTC's knowledge of Physical Security and IT Security Services can help you understand who the attackers are likely to be, when and where they may attempt entry, and what exactly you should be doing to protect your site/asset/information.



Threat Assessment

KTC employs a detailed, multilayered Threat Assessment to determine just what the situation is. We begin with site surveys leading to an overall vulnerability analysis. This may include studying maps and land surveys, photographic reconnaissance as well as visual analysis. The goal is both to obtain a general idea of the complexity of the threat matrix and as well the scope of the project. If we are securing a large nuclear plant the scope of the threat will be much larger than security for a small location with less importance to the critical infrastructure CIP of a nation.

Determine the Threat

We must determine where attacks most likely will be coming from. If the expected attacks are local and limited to a few specific people, our plan of development will be different than a potential large-scale attack by foreign forces. Threats in our world are no longer limited to individuals or small groups of persons moving toward us, now it can be an attack from an organization with individuals hacking systems from all over the globe – people we cannot see.

Study, Prove, Survey
After our initial assessment of the location and type(s) of possible attackers, we begin an in-depth survey of the site. Going beyond our initial survey, we get very detailed data giving us a threat matrix with each element of the matrix expanded into a "Likely Attack Plan" and "Likely Impact." 7 Critical Considerations We study the site not only for all possible locations of entry but also possible exits for attackers.

We also study the vulnerabilities in daily operations. For example, with a large electricity generator you must be cognizant of the physical and IT threats to the generator. For another example, you must be aware of the less intangible threats to the computer system that runs ALL the programs, plus the security and the other functions in the plant.

Prioritize Vulnerabilities
The final part of the initial assessment is to prioritize the vulnerabilities. The prioritization may comprise assessments of cost and benefits, time available to implement, relationship to other nearby or remote facilities, local responder access and many other factors. No one wants to spend thousands of dollars on a security camera system if the attack will likely be coming from a hacker. Cyber Pearl Harbor Blog

Design Planning and Procurement

After we have assessed the threat to a site or asset we begin the design, planning, and procurement stage of the project. In this stage we begin to layout exactly what security measures we will recommend/install to protect against the threat. SCADA and assembly; Electronic Warfare

Define Threat, Identify Defeat Methods
In this stage we define the threat to the site, but we also go beyond that by developing the methods to defeat the attacks. To defeat an Internet attack we can take firewall-like precautions that will shut that attack out. Whereas, protecting a power generation facility against a physical attack may require an overt and covert camera system to monitor fences, locks or other advanced technologies as the first line of actual defense.

The Result of All These Steps is The Integrated Security Plan (Isp)

CONOPS
The concept of operations (CONOPS) for every situation will be different. CONOPS change to meet the SPECIFIC operational needs of a site. Every site is run in a different manner and to expect the defense of different locations to follow the same

steps in every situation would likely lead to failure and loss of the asset. CONOPS Physical Security

Procure Designated Equipment

We then gather, if authorized, the necessary equipment to ensure the best security for the site, according to the CONOPS and ISP. At KTC we have connections the world over which allow us incomparable variety and pricing structures to offer our clients. We can offer a range of prices and equipment (hardware, software) to fit the client's budget and schedule. We also can coordinate the civil works, if any are required. A BOX 4 U Blog; Perceptics: License Plate Readers

Receive, Test & Prepare Equipment

We typically receive the equipment at one of our facilities and "kit" it for delivery to the client's site; we can receive it at the client's facility if needed. At either location we facilitate the preparation of the equipment, the building and assembly if needed and the testing. We ensure all equipment is in perfect working order before final delivery and installation at the site.

Palletize & Ship

If we assemble and test the equipment off-site we carefully kit and ship the equipment to the site, maintaining its security en route.

Customs & Duties Closed Out

For the ease of our clients, we take care of the customs process for all foreign clients. We have relationships with multiple global governments and forwarding agencies to expedite the shipping and receiving of goods.

Installation, Integration, Test

In this phase KTC implements a plan of action for assuring successful installation and integration of the equipment coming to the site.

Prepare Site and Train Workers

To guarantee the site can be integrated quickly, KTC directly trains all personnel who will be involved in the act of unloading, setting up structures, installing wiring, cameras, sensors, computers and racks of electronic hardware, and so forth. This critical site preparation and training is managed by KTC. This is not the Operational and Maintenance training, which comes later.

Distribute Work Packages

Once the training has begun we can begin to distribute the specific work packages for each installation subgroup (including integration drawings and layouts) and the structural items (poles, buildings, barriers) that will hold the equipment. Next, the actual equipment is distributed to the work groups that will be installing the pieces of equipment.

Begin and Track Work

This stage is the first time that we see the full picture of all the facets of the surveying, planning and preparation begin to fit together, although this is still in the tracking stage.

Integration

Integration begins the full realization of the previous planning stages. After the equipment has been installed and connected up we provide an overview (introductory level) training for the client's staff leadership. This is the first step in what is sometimes termed a "train the trainer" program. KTC's team and the client's site team will work seamlessly during this period to help that site team begin the transition to a fully operational state. The first actual "live" operation occurs in the next step: testing. Integration Blog

Subsystem and System Test

In this phase the teams, working in unison, will test the system and its subsystems for possible problems (and there are always problems – the job is to catch them at this stage). The teams and the system will be run through simulations ranging from false alarms to full emergencies.

Training and Assistance

The training and additional assistance for a site's defense is one of the most important activities we deliver. Without proper training all the work to develop the physical security and IT security for a site may become meaningless!

There are specific types of training provided as part of the completion of the installation and commissioning of a site:

Counterinsurgency

One type of training focuses on attacks by insurgents – that is, persons who are not part of a practiced military force but nonetheless are bent on destroying the asset or its protectors. This counterinsurgency training includes preparing to defend against a more random, perhaps non-uniformed (perhaps even attackers who look identical to the guards and site operators) group of attackers.

Force Protection (FP)

Another type of training focuses on "force protection," which assumes an attack in force by uniformed/highly trained and skilled attackers (trained as a military or paramilitary unit). We train guards/employees in FP techniques, many of which our personnel have learned from US/NATO/Allied military and civilian governmental training and operations throughout their careers.

Security System Operations

We train the site staff fully in the operation of the facility. Because we work from conception to implementation we know the ins and outs of every system. We pass this information on to the staff of the site using classroom training, emulations and one-on-one training. When we have completed our training, which usually also involves the "train the trainer" personnel we met earlier, we hand over the training to the client.

On The Job Training

Simulations and emulations can take trainees only so far. Trainees understand best when training continues in their actual situation surrounded by their workday environment. It is essential that the staff that runs the equipment is comfortable running the security system under BOTH normal and extreme circumstances. For this reason we wholeheartedly recommend continued on the job training.

Security Alert & Counterterrorism Updates

Beyond the normal operations of the security system and the occasional drill, the team and the system must be kept up to speed on breaking information. Attackers and information are always changing. We regularly provide our current level of knowledge and threat assessments to our clients (as part of the continued warranty and calibration activities). We also have teams that periodically can move back into a site and train/retrain/give seminars to staff.

Inspection, Test/Probe, Upgrade

The proper maintenance and testing is essential to every facility; whether it is a manufacturing plant, a military facility or a high-risk nuclear facility, upkeep is of the highest importance. To assure that equipment and people are working well together and the security plan is working as designed, we check it:

Periodic Inspections & Drills

To maintain the proper running of any system, KTC provides routine inspections – a necessary part of the upkeep. We also recommend drills on all phases of operations (clients can contract with KTC to provide this or handle it on their own). Drills keep employees functioning at the highest levels.

Live Probes

Beyond drills and random inspections KTC has found it particularly helpful to run live probes. By running live probes (simulated or very real "attacks") we are able to witness how the site is operating.

Security Readiness Ratings

By witnessing drills and conducting probes, we can issue a "Readiness Rating," which is a "grade" or indication of the excellence (or lack of it) in staff's performance.

Overflights, Hidden Tests

By using overflights we can get an idea of how well the systems have been implemented. We can test covert sensors and we can see how the computer tools responded to an "attack." Hidden tests of the systems give us additional insight into how our clients are running their systems. We install covert sensors in the operating equipment (ONLY with the client's permission and full knowledge) and using these tools we are able to identify "holes" in performance.

Design of Remediation

From time to time systems may fall into disrepair and neglect. If improvements are needed in a defense system we can design and launch a remediation program.

Security Operations

KTC's focus on security the world over provides our customers a unique opportunity. As a privately owned company we have the uncommon ability to use technology and skills from branches of the military and governments worldwide to establish a superior security standard. With decades of experience in multiple fields KTC has a reputation of on time, under budget exemplary work. Here we lay out some of the fields in which KTC excels. Integration Security

Task Force

We can provide a task force to respond to our clients' needs. A task force can be made up of one or many members of KTC. Our task force personnel have been trained in a wide array of skills and can quickly move into a multitude of situations. A task force handles the entire security operation, as compared to:

Embedded Assistance

Much like a task force but using only one or two of our KTC staff we can provide embedded assistance. The difference here is that an embedded operator works seamlessly with an existing client's forces; the embedded element can be in the area for an extended period of time.

Personal Protection

KTC's protection and security plans can easily be scaled to provide PSD (personal security details). We have teams that are set-up and extensively trained to provide exclusive security for individuals and small groups.

Nuclear Operations

At the other end of the spectrum we have large-scale nuclear operations. Locations such as nuclear power plants require multiple fields of protection. With a nuclear plant we must protect system operations, covert and overt physical/visual security operations using cameras and sensors as well as data and technology (to prevent data mining and infiltration). Designing and implementing such programs typically requires many months. Defense Blog

Port Operations
Similar to other large-scale operations, a port requires multi-level security. Ports may not have the obvious destructive capabilities of a nuclear operation but they are critical to a country's infrastructure and if compromised can become a critical issue for a country's infrastructure and commercial viability. We have developed a range of port-specific measures that maintain security during the many phases of loading, unloading, warehousing, and intermodal shipping.

Anti-Piracy Operations
KTC offers anti-piracy abilities that focus on a client's ship/tanker or a shipment. Just as a PSD detail requires extensive memoranda of agreement covering a wide range of details (weapons, ROEs, levels of authority, command structure) an anti-piracy operation requires careful thought. Most such operations are brief.

Aviation Operations
KTC both uses aviation resources and on the other hand protects aviation resources.

By using manned or unmanned units we can easily monitor large areas of land . Our aviation operations also minimize human risk in high-danger situations. An example of these is the "overflights" noted above.

Protecting aviation assets is in part a physical security operation, an IT security operation, and a military-like force protection guard program.

SOW Chart

KTC offers a wide array of technology and real-world knowledge to our clients. We have unique capabilities and information that give us an edge in the defense and securities markets.