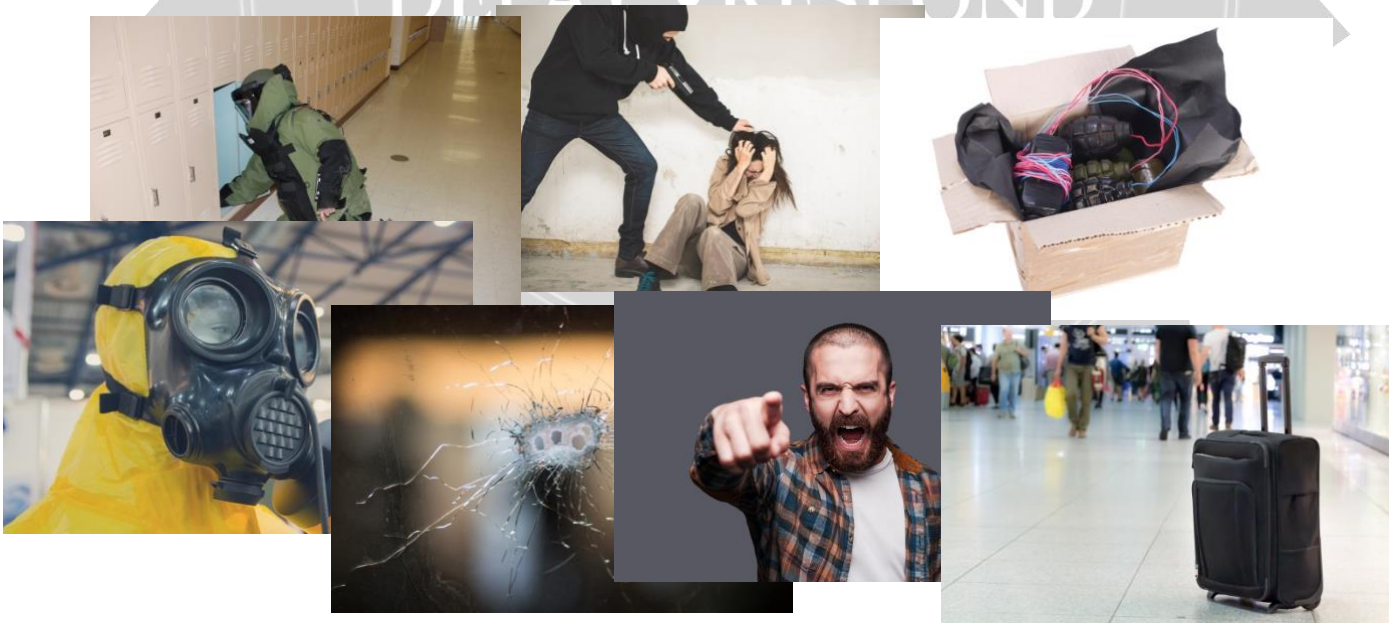
Threat Assessment

Making your world a safer place

In the constantly evolving world that we live and work in, the threat of those wishing to take hostile action against us is on the rise. Aggressive people, drug induced violence, active shooters, hostage taking, improvised explosive devices, hostile vehicle movements, biological and chemical attacks are commonplace around the world.

Operational safety and security are of paramount concern particularly if you operate in high-density crowded spaces or from critical high-profile infrastructure. Assessing the threat, and target hardening provides confidence and saves lives.



A threat assessment identifies and examines criticality, vulnerability and threats across the threat spectrum. Recommending proportional response, mitigation and recovery.

The following is a brief explanation, more specific information will only be provided in person or during process.

The methodology deployed strikes a balance between identified risk assessed proportional to the current national threat level.

Broadly speaking, the assessment is conducted in two parts:

a. Information gathering from key staff, systems, policies, and procedures.
b. Physical assessment of infrastructure and environs by day and by night.

In identifying, addressing and recommending countermeasures, a five-pronged approach is used:

c. DETER – Obvious physical and electronic target hardening measures.
d. DETECT – Visual detection and alert measures, alarm systems, CCTV.
e. DELAY – Physical countermeasures, bollards, trained staff, security.
f. RESPOND – Appropriate, timely coordinated response by staff and law enforcement.
g. RESILIENCE- Recovery and restoration, returning to normal business as soon as possible.

This is applied across the following categories:

a. Security Governance
b. Physical Security
c. Access Control
d. Perimeter Security
e. Hostile Vehicle Mitigation
f. CCTV
g. Improvised Explosive Device
h. Detecting Suspicious Behaviour
i. Information Security
j. Personnel Security
k. Emergency Logistic
l. Business Continuity

A threat assessment typically takes between one to two days to complete. It requires a time commitment from a senior staff member commensurate to business perimeters.

On completion, a report is furnished and debrief conducted to explain findings and recommended mitigations.

It is strongly recommended that assessments are followed by staff confidence training for two reasons. Firstly, exposing staff to this process can be unsettling, conducting training puts some context around response and generally eases minds.

Secondly, vigilance remains a key tool in combatting threats of any level, the more people we have aware of what to look for and how to respond, the safer we all are.

In order to be more durable, it places equal focus on relevant Health and legislation, with elements of the report folding back into your health and safety documentation to assist compliance.

Section 646 offers a range of services inclusive of threat assessments, target hardening, scenario training, document creation, penetration testing and onsite threat management

---

SEE SOMETHING SAY SOMETHING
VIGILANCE REMAINS OUR GREATEST DEFENCE – APATHY OUR GREATEST ENEMY