JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Protective Security and Hostile Threat Mitigation Training Course

22 March – 2 April 2027
Vienna

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Protective Security and Hostile Threat Mitigation Training Course

Ref: 520_19266 **Date:** 22 March – 2 April 2027 **Location:** Vienna **Fees:** 10600 GBP

Protective Security and Hostile Threat Mitigation is an advanced 2-week training course for security managers, protective security teams and defence and security professionals who must harden critical sites against deliberate attack, ending with a Protective Security Defence Plan. Hostile actors now study crowded places, energy assets and headquarters openly before they strike, so detection and layered defence decide outcomes. Jupiter Prime Training delivers this course to practitioners responsible for sites that attract hostile interest.

Why Protective Security and Hostile Threat Mitigation Matters Now

Three pressures shape protective security today: attackers who use low-cost methods such as vehicles, bladed weapons and improvised devices against crowded or symbolic sites, hostile reconnaissance carried out in plain sight and online, and owners, insurers and the public who expect visible yet proportionate defence. A site defended well detects planning activity early, delays an attack and limits casualties, while one defended badly offers easy targets and a slow response. The course draws on the Enterprise Security Risk Management ESRM guideline for owning these risks and on ISO 22341 protective security guidance for shaping the built environment.

Who Gains Most from Protective Security and Hostile Threat Mitigation

- Security managers accountable for defending sites that attract hostile interest
- Protective security team leaders who run screening, patrol and response on site
- Risk and threat assessment specialists who brief owners on attack scenarios
- Facility and venue operators who must keep public spaces open yet defended
- Defence and security liaison officers who coordinate with responding agencies

An operator of several crowded venues or critical plants that sends its security manager, protective team leader and threat specialist together gains most, because they can test one defence concept against shared attack scenarios and response times.

Protective Security and Hostile Threat Mitigation Capabilities

Participants learn to think like an adversary, read the warning signs of attack planning and organise defences that delay, detect and disrupt.

- Assess attack methodologies against a site's people, assets and crowded spaces — owners choosing defensive priorities
- Apply hostile reconnaissance detection and counter-surveillance routines — teams disrupting attack planning early
- Design perimeter, screening and response measures that buy time against an attacker — site leaders allocating resources
- Calculate blast and vehicle threat exposure to guide standoff and glazing decisions — engineers and facility managers
- Specify protective measures that rise and fall with threat levels — operators balancing openness and protection
- Test the defence concept through red team and live exercises — security managers and responding agencies

Key Protective Security and Hostile Threat Mitigation Terms

- Hostile reconnaissance — information gathering by an attacker to plan an attack, through site visits, photography or online research.
- Attack methodology — the combination of weapon, tactic and target an adversary is likely to choose against a given site.
- Counter-surveillance — deliberate observation of a site's surroundings to detect people conducting hostile reconnaissance.
- Stand-off distance — the space separating a protected structure from where an explosive device or vehicle can be placed.
- Threat level response — a pre-agreed set of protective measures activated as the assessed threat to a site rises or falls.
- Red teaming — testing defences by having a team act as a realistic adversary to expose weaknesses before an attacker does.

Protective Security and Hostile Threat Mitigation Day by Day

Day 1: The Hostile Threat Environment

- Attack Methodology Profiles — Comparing Vehicle, Bladed, Firearm and Device Threats
- Crowded Places and Symbolic Targets — Judging Site Attractiveness
- Attack Planning Cycle — Locating Points Where Plots Can Be Disrupted
- Insider Enablement of Attacks — Recognising Internal Assistance
- Threat Picture Briefings — Informing Owners Without Alarm

Day 2: Protective Security Strategy

- ESRM Risk Ownership for Hostile Threats — Agreeing Who Accepts Residual Risk
- Defence-in-Depth Concept — Layering Detection, Delay and Response
- Protective Security Objectives — Translating Threats Into Defensive Goals
- Proportionality and Openness — Balancing Protection With Public Access
- Protective Security Governance — Assigning Roles Across Owners and Operators

Day 3: Hostile Reconnaissance Detection

- Hostile Reconnaissance Indicators — Spotting Unusual Interest in a Site
- Counter-Surveillance Routes and Positions — Watching the Watchers
- Online Footprint Reduction — Limiting Useful Information About the Site
- Engagement and Questioning of Suspicious Persons — Disrupting Planning Safely
- Deterrence Messaging — Showing Hostile Actors They Will Be Seen

Day 4: Perimeter Defence and Screening

- Perimeter Barrier Performance — Matching Fences and Gates to Attack Methods
- Search and Screening Regimes — Selecting People, Bag and Vehicle Checks
- Screening Point Layout — Avoiding Queues That Create New Targets
- Intrusion Response Times — Comparing Delay With Guard Arrival
- Temporary Event Perimeters — Securing Venues for Large Gatherings

Day 5: Vehicle Threat Mitigation

- Vehicle-as-a-Weapon Scenarios — Identifying Approach Routes and Speeds
- Vehicle Security Barrier Selection — Choosing Rated Bollards and Blockers
- Traffic Calming and Approach Design — Reducing Impact Speeds
- Vehicle Checkpoint Operations — Controlling Authorised Access
- Vehicle Dynamics Assessments — Testing Barrier Placement Against Run-Up Distances

Day 6: Blast Effects and Building Protection

- Blast Effects on People and Structures — Understanding Injury Mechanisms
- Stand-Off Distance Calculations — Setting Safe Separation
- Glazing Protection and Fragment Risk — Choosing Laminated and Film Solutions
- Protected Spaces and Safe Areas — Sheltering Occupants During Attack
- Mail and Delivery Screening Rooms — Containing Suspect Items

Day 7: Marauding Attack and Armed Intruder Response

- Escape, Shelter and Alert Guidance — Preparing Staff and Visitors
- Lockdown Procedures — Securing Buildings Quickly
- Invacuation Versus Evacuation Decisions — Choosing the Safer Option
- Guard Force Response Tactics — Containing Threats Until Responders Arrive
- Casualty Care Before Emergency Services — Reducing Fatalities

Day 8: Threat Level Response and Integration

- Threat Level Response Matrices — Raising Measures in Steps
- Liaison With Responding Agencies — Agreeing Rendezvous and Roles
- Communications During an Attack — Alerting Occupants and Neighbours
- Business Recovery After Hostile Incidents — Reopening Safely
- Protective Measures for Executives and Visitors — Reducing Personal Exposure

Day 9: Testing the Defence

- Red Team Exercises — Probing Defences as an Adversary Would
- Tabletop Attack Scenarios — Rehearsing Decisions Under Pressure
- Live Lockdown and Screening Drills — Measuring Response Times
- Exercise Evaluation Criteria — Judging Readiness Objectively
- Lessons Identified Registers — Turning Findings Into Improvements

Day 10: Practising the Protective Security Defence Plan

- Applying Attack Methodology Analysis — Selecting Scenarios for a Chosen Site
- Applying Reconnaissance Detection — Setting Counter-Surveillance Routines
- Applying Perimeter, Vehicle and Blast Measures — Defining Layered Defences
- Applying Threat Level Responses — Linking Measures to Alert States
- Protective Security Defence Plan — Presenting Defences, Response and Exercises

Applying Protective Security and Hostile Threat Mitigation After the Course

- Lead a hostile reconnaissance walk-through of your site with the protective team, recording vantage points and online information an attacker could use.
- Run a tabletop exercise on a vehicle or armed intruder scenario and report response time gaps and agreed improvements to the security manager.

Protective Security and Hostile Threat Mitigation Questions FAQ

What is protective security and hostile threat mitigation and why does it matter now?

Protective security and hostile threat mitigation is the defence of sites and people against deliberate attack through detection, delay and response. It matters now because attackers use simple methods against crowded and symbolic places after studying them openly.

Which roles gain most from protective security and hostile threat mitigation training?

Security managers, protective security team leaders and threat assessment specialists gain most from protective security and hostile threat mitigation training, with venue operators and agency liaison officers.

How does protective security and hostile threat mitigation differ from a security planning course?

Protective security and hostile threat mitigation focuses on defending an operating site against attack: reconnaissance detection, screening, attack response and exercises. A security planning course focuses on designing protection into new facilities and their budgets.

What do you bring back from protective security and hostile threat mitigation training?

You bring back a Protective Security Defence Plan for a real site. It sets attack scenarios, layered defences, threat level responses and an exercise schedule.

Protective Security and Hostile Threat Mitigation: The Way Forward

The Protective Security Defence Plan first informs which defences a site strengthens before its next high-profile event or threat change. Security managers, protective teams and responding agencies use it to align screening, lockdown and liaison. After the first exercise, revisit the attack scenarios against observed response times, whether at an energy terminal or a sports venue, so the defence stays credible.