# Report Suite

## Unique Selling Proposition (USP) Summary

*A SECCEN Platform document | 25 June 2026*

## 1. Introduction

The SECCEN platform delivers a comprehensive suite of automated security intelligence reports, each designed to provide actionable insights for security professionals, corporate clients, and event organisers. Every report leverages real-time open-source intelligence (OSINT), live government data feeds, and advanced AI analytical frameworks to produce outputs that would traditionally require hours of manual research by experienced security analysts.

This document summarises every report available on the platform, detailing its purpose, what it analyses, and the value it delivers to end users.

## 2. Dashboard

**Subject of assessment:** The live security operating picture presented to every user on sign-in
Purpose: To give users immediate situational awareness of the current threat environment and the latest security-relevant news.

The Dashboard is the platform's real-time intelligence hub. It surfaces the current UK National Threat Level alongside AI-curated security news insights, refreshed every 30 minutes from authoritative UK sources including BBC News, Sky News, UK Government channels, BBC Health, and the UK Health Security Agency (UKHSA).

### What It Provides

- The current UK National Threat Level (MI5) with plain-English definitions, and a pop-up alert whenever the threat level changes.
- Security News Insights across five critical domains — Terrorism, Security, Intelligence, and Crime — plus Other Security-Impacting Areas such as health emergencies, natural disasters, and infrastructure failures.
- AI-synthesised narrative summaries for each domain, updated every 30 minutes.

### What It Delivers to Users

- Instant situational awareness without manually scanning multiple news sources.
- Continuous calibration of the wider platform to the prevailing threat level.
- A downloadable news snapshot for briefings and records.

## 3. Intelligence Report

**Subject of assessment:** A defined UK location or Area of Operation (AO)
Purpose: To deliver a comprehensive security assessment of any UK location, combining live crime data, environmental analysis, and OSINT.

The Intelligence Report is the platform's flagship product, utilising a multi-layer analytical framework to produce detailed threat and risk assessments for specific Areas of Operation, employing methodologies comparable to government intelligence agencies and private security consultancies.

### What It Analyses

- Geographic crime attribution using live Police UK API data within a defined radius of the AO.
- Violent crime composition, visitor demographic modelling, and built-environment defensibility.
- Proportional terrorism calibration aligned to the current UK National Threat Level.

### What It Delivers to Users

- A professional multi-section report with HIGH / MEDIUM / LOW risk ratings across all security domains.
- AO identification via OSINT (e.g. stadium, corporate office, retail) and actionable security considerations.
- Exportable professional document formatted to security consultancy standards.

## 4. Public Figure Report

**Subject of assessment:** A named individual with a public footprint — public figure, celebrity, artist, or VIP

Purpose: To assess the security risk profile of individuals with a public presence through comprehensive OSINT analysis.

The Public Figure Report provides security teams and personal protection officers with a thorough risk assessment of anyone with a public footprint who may be attending events, visiting locations, or requiring close protection, analysing public profile, controversy history, fan-base dynamics, and historical incidents.

### What It Analyses

- Public profile and media presence — scale of fame, social media following, and visibility.
- Controversy and incident history — past incidents, threats received, and harassment cases.
- Fan-base and crowd dynamics, threat-actor assessment, and travel/logistics risk.

### What It Delivers to Users

- A comprehensive risk profile with categorised threat ratings across multiple security domains.
- Specific considerations for close-protection planning and event security.
- Exportable professional report for briefing security teams and venue management.

## 5. Sports Team Risk Report

**Subject of assessment:** A specific sporting fixture and the teams/fan bases involved, categorised by sport

Purpose: To provide a detailed security risk assessment for sporting events, focusing on fan behaviour, rivalry dynamics, and event security.

Designed for security professionals managing sporting venues and events, the report is categorised by sport and analyses historical fan behaviour, rivalry intensity, policing requirements, and the crowd-management challenges unique to sporting fixtures.

### What It Analyses

- Fan behaviour profile, rivalry assessment, and supporter travel/logistics.
- Social media activity and historical incident data including arrests and banning orders.

### What It Delivers to Users

- Match-specific risk assessment with tailored threat ratings.
- Crowd-management considerations including segregation and stewarding levels.
- Exportable professional report for police liaison officers, stewards, and venue security.

## 6. Travel Report

**Subject of assessment:** A global travel destination being visited

Purpose: To deliver a comprehensive travel security briefing for visiting another country, combining FCDO advisories, OSINT, and local threat intelligence.

The Travel Report combines official UK government travel advisories with real-time OSINT analysis to produce actionable travel security intelligence for visiting another country, going beyond standard FCDO guidance.

### What It Analyses

- FCDO advisory status, terrorism and crime environment, and political stability.
- Health, environmental, transport, cultural, and legal considerations.

### What It Delivers to Users

- A destination security briefing with an overall risk rating.
- Pre-departure, in-country, and emergency considerations.
- Exportable document suitable for corporate travel security and duty-of-care compliance.

## 7. Organisation Risk Assessment

**Subject of assessment:** A named company or organisation assessed as the unit of risk — not a physical location or event

Purpose: To assess an organisation itself as a risk: how that organisation, by virtue of who it is, what it does, and who it is associated with, attracts, generates, or is exposed to security threats.

The Organisation Risk Assessment shifts the analytical lens from a place to an entity, asking "how does this organisation report as a risk?" — evaluating it as a potential target, as a generator of risk to others, and as an entity whose corporate profile, sector, leadership, and public associations shape its overall threat exposure.

It draws on Companies House records, SIC code sector mapping, director and ownership structures, adverse media, and OSINT — suited to due diligence, supply-chain assurance, partner vetting, insurance underwriting, and pre-engagement risk screening.

### What It Analyses

- Corporate identity and standing — Companies House registration, filing history, and corporate structure.
- Sector and activity risk — SIC code mapping of inherent sector exposure.
- Leadership and ownership exposure — directors, persons of significant control, and threat associations.
- Target attractiveness — how the organisation may attract activism, protest, extremist attention, or hostile state interest.
- Risk generated to others — how associating with the organisation could transfer reputational or security risk.
- Adverse media and controversy footprint — litigation, regulatory action, and historical incidents.

### What It Delivers to Users

- A structured assessment of the organisation as a risk subject with HIGH / MEDIUM / LOW ratings per domain.
- A justified, sourced narrative explaining why the organisation reports at the assessed risk level.
- Due-diligence-ready output for vetting partners, suppliers, clients, and acquisition targets.
- Exportable professional document for compliance, procurement, and board-level briefings.

---

## 8. Crime Statistics & Environmental Threat Assessment

**Subject of assessment:** A given UK postcode or address and its surrounding crime environment

Purpose: To provide granular crime data analysis and an automated Environmental Threat Assessment for any UK postcode.

The Crime Statistics report combines live Police UK crime data for a given postcode with an AI-generated Environmental Threat Assessment (ETA), delivering both quantitative data analysis and a qualitative environmental assessment.

### What It Analyses

- 12-month live crime data within a 1-mile radius of the postcode, broken down by category.
- 5-year historical trends and comparative analysis against regional and national averages.
- Environmental factors including lighting, CCTV coverage, natural surveillance, and access/egress points.

### What It Delivers to Users

- Interactive crime data visualisation with charts, graphs, and trend indicators.
- An automated 12-section Environmental Threat Assessment (ETA) synthesised by AI.
- A consolidated downloadable report combining all statistics and the environmental assessment.

---

## 9. Corporate Tiered Accounts

**Subject of assessment:** Organisations requiring self-managed, branded access for their own users and staff

Purpose: To allow companies to operate a corporate tiered account administered by their own organisation administrator.

Beyond individual reporting, the platform supports corporate tiered accounts. An organisation can hold its own tier of access where a designated organisation administrator manages the account independently — controlling who within the organisation can access the platform and what they can do.

### What the Organisation Administrator Can Do

- Manage their own users and staff — create accounts, allocate seats, and remove access as needed.
- Restrict reporting levels — control which reports each user or role can access.

- Apply a single brand colour to re-theme the look and feel of the system for their users.
- Set the company name displayed across the platform for a tailored, branded experience.
- Administer the account independently under organisation-admin delegation.

### What It Delivers to Users

- A self-service corporate capability without reliance on central administration.
- Granular control over reporting access aligned to each team member’s role.
- A branded environment that reflects the organisation’s identity.

---

## 10. Summary

The SECCEN report suite transforms a time-intensive, manual process into an automated, AI-powered intelligence capability, delivering professional-grade security analysis in minutes rather than hours whilst maintaining the analytical rigour expected by security professionals.

### Key differentiators across all reports

- Real-time data integration reflecting the current security environment.
- Professional analytical standards using British English and established frameworks.
- Exportable professional documents suitable for client-facing use.
- Consistency and repeatability through AI-driven methodology.
- Scalability — delivered on demand to any authorised user.

---