

# White Paper



## SiD Integrated Intelligence Solution

---

### Abstract

The challenge facing intelligence agencies is to notice and react to warnings and indications prior to the occurrence of events – for example, to discover a potential threat or terrorist’s plot in time to intervene. In pursuit of this goal, these organizations gather huge amounts of content from public and classified sources.

“Intelligence collection, however, is only the first step in combating terrorism. A piece of information is like a piece of a puzzle. Oftentimes, only when a piece of information is combined with many other pieces of information does the big picture emerge. Moreover, possessing information without more does not stop terrorism; rather, information must lead to action.” **Larry D. Thompson** Deputy Attorney General, Justice Department, 2001-03. Statement to the National Commission on Terrorist Attacks Upon The United States – December 8, 2003.

For an intelligence process to deliver the outputs necessary to define appropriate defences for the identified risks – the intelligence gathering mechanism must provide a level of integration and automation appropriate to handle the volume of raw information processed.

---



### For further information

Email: [info@superstructuregroup.com](mailto:info@superstructuregroup.com)  
Website: [www.superstructuregroup.com](http://www.superstructuregroup.com)

### UK Office

Superstructure Group Limited  
Ash House, Fairfield Avenue  
Staines, Middlesex TW18 4AB  
United Kingdom  
Ph +44 870 803 2579  
Fax +44 1784 224 245

### NZ Office

Superstructure Group (AP) Limited  
Level 1, 19 Tory Street  
P O Box 19127, Courtenay Place  
Wellington, New Zealand  
Ph +64 4 385 0001  
Fax +64 4 381 3934

---

Copyright © 2011 Superstructure Group Limited

All rights reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Superstructure Group Limited, the copyright holder.

This document is the property of Superstructure Group Limited and may not be disclosed to any third party or copied without consent.

---

Table of Contents

Abstract .....1

Preface..... 1

    Intelligence Value.....1

    Information versus Intelligence.....1

    Presentation Clarity.....1

Executive Summary ..... 2

    Intelligence Process .....2

    Solving Cases - Investigations.....2

    The Solution.....2

Key Challenges ..... 4

    Information Volume.....4

    Data Capture .....4

    Actionable Intelligence .....4

    Presentation.....4

    Security and Data Sharing.....4

Reducing Risk – Addressing the Challenges ..... 5

    Rapid Flexible Data Capture .....5

    Secure Enterprise-wide Intelligence Repository .....5

    Case and Collection Management.....5

    Secure Intelligence Sharing.....5

    Visual and Geographic Presentation .....6

Background..... 7

    Intelligence is.....7

Case Study – Immigration Intelligence ..... 8

Key Concepts..... 9

    Indicators.....9

    Indicator Triggers .....9

    Events .....9

    Incidents .....9

How does the Integrated Intelligence Solution support this Case Study? ..... 10

    Strategic Intelligence Collection.....10

    Intelligence Reporting .....10

    Strategic Intelligence Model .....10

How does the Integrated Intelligence Solution support the Strategic Model? ..... 11

    Strategic Model Level 1 .....11

    Inter-Agency Intelligence Solution .....11

How does the Integrated Intelligence Solution support the Risk and Defence Model? ..... 12

How does the Integrated Intelligence Solution support Risk and Defence Profiles? ..... 13

## Preface

---

### **Intelligence Value**

Intelligence Value is measured by the predictive probability inherent in the intelligence outputs. The more focused the intelligence product, the more specific the risks identified and the more predictable the model produced. These factors will determine the ultimate effectiveness in application of that intelligence - effectiveness specifically of the counter measures to mitigate the risks identified.

The higher the intelligence value – the higher the probability that real risk events are prevented by the defences or counter-measures derived from the intelligence.

---

### **Information versus Intelligence**

Information Is Not Intelligence. Information is the source of intelligence. In extracting intelligence from information it is necessary to go through a process of analysis and production.

Information is the content of textual documents gathered from public and classified sources. Agencies typically receive large amounts of information. The challenge is to understand the relevance of this information in the context of a current or potential future event.

The requirement for relevance underpins the importance of knowing what the content is about.

Intelligence is identifying the signals and meaning in the stocks and flows of content that are relevant to us. This is not just single statements that stand out for their uniqueness or relevance to our pursuits, but also patterns over entire collections.

Extracting intelligence from content is the process of Information Extraction and includes:

- Entity Extraction – identifying what objects in the world a statement is talking about, and
  - Fact Extraction – identifying what the statement is saying about them.
- 

### **Presentation Clarity**

Having gathered information, the analysis process needs models of presentation that can expose patterns with succinct clarity. Analysis tools must have ability to manage the volumes of raw information and to provide indicators to possible risks from that volume. Delivery of output must be in forms that can clearly illustrate the risks in nature, method and timing.

---

## Executive Summary

---

### **Intelligence Process**

Achieving an effective Intelligence strategy is a significant challenge that is both complex and costly. The collection, processing, analysis and dissemination of intelligence necessitate effective utilization of information associated with the interception and interpretation of messages, tracking the flow of money, and the movement of people. As threats to our society and public fears escalate, the demand for detection and prevention is increasing exponentially.

---

### **Solving Cases - Investigations**

Today Investigators gather significant amounts of evidence when investigating crime. Information is gathered using interviews (statements and transcripts), receiving phone calls, collecting clues, spot checks, DNA tests, traffic movement, transaction flows and so on. All this information then has to be stored and indexed in a way that makes it possible to identify trends, similarities, abnormalities, inaccuracies, or any other kind of clue that would help in solving the case. Often and certainly in large complex cases, the resources required to effectively manage and sift through all this data is well beyond the resources available. The bottlenecks encountered when processing pieces of information can be attributed to the sequential nature of capture and value assessment.

---

### **The Solution**

Any organization tackling these challenges will have expertise in intelligence and investigative processes. Those individuals are the gold of the organization. This resource must be optimized by applying and integrated set of tools. These tools provide a support framework for the critical facets of this process – maximizing the power of the collective human intelligence available by minimizing the mundane and otherwise unmanageable tasks.

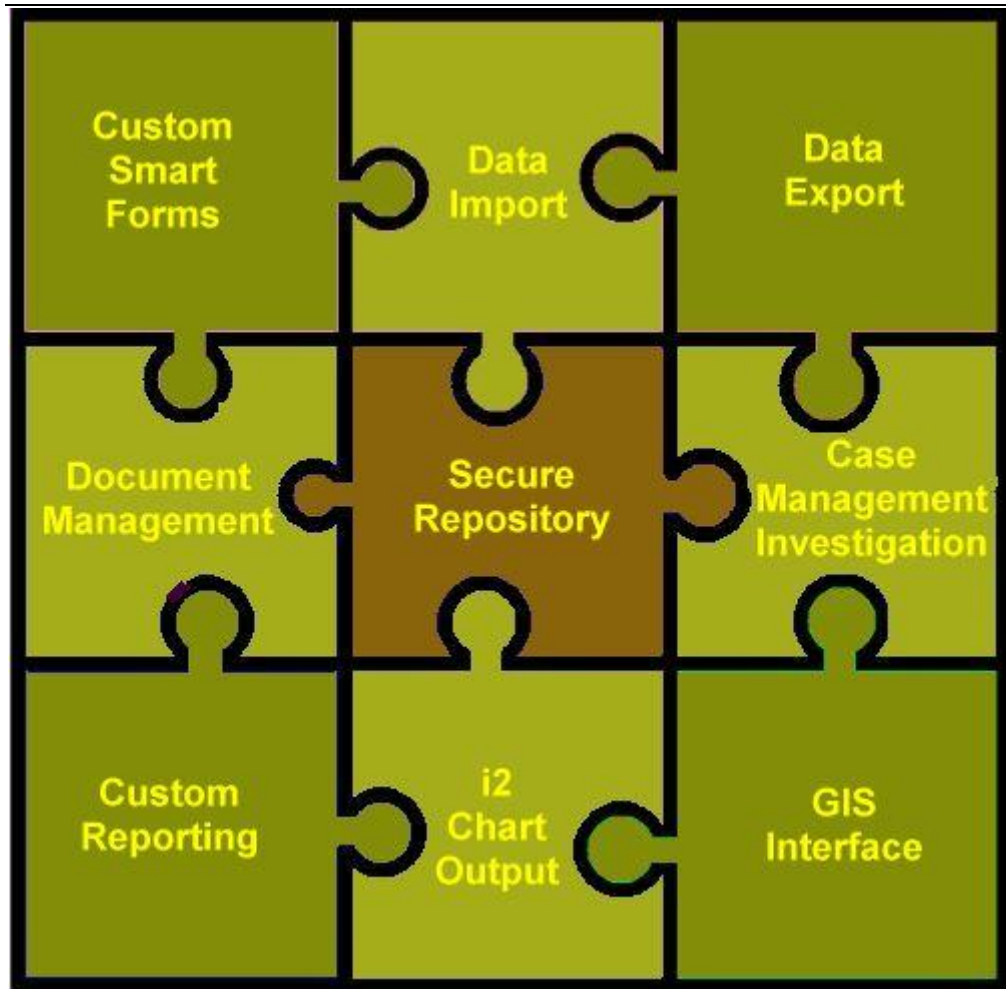
SiD Integrated Intelligence Solution provides the engine to drive the following processes:

- Powerful and rapid filtering of unstructured text – content recognition
- Automated entity and association extraction
- Fuzzy identity searching to ensure search scope is maximized
- Flexible electronic and manual data capture from business forms or data sources; including remote mobile capability; Cleansing of telecom call record data
- A secure enterprise intelligence repository with need-to-know access control
- Flexible and secure internal and external data sharing
- Management for the case investigation or collection processes
- Visual presentation of event and entity-association data
- Geographic presentation of data

Providing an enterprise wide, integrated intelligence solution, the intelligence value is maximized for any organization – irrespective of size or infrastructure.

---

Figure 1. Integrated Intelligence Solution



## Key Challenges

---

### **Information Volume**

An organization with security protection, defence or enforcement mandates will face challenges in resource to gather and analyse the volume of information necessary to produce high value intelligence outputs. Having obtained that information – the challenge is then to refine and focus the intelligence with a direction that will most rapidly determine any risks. The challenges here are data management, data analysis and data presentation.

---

### **Data Capture**

Capture of information will be from diverse locations and sources with levels of communication varying from enterprise networks, the internet, or even unconnected field and mobile devices.

---

### **Actionable Intelligence**

From raw information – the intelligence analysis process requires extraction of “actionable intelligence”, specific entities of interest and the association between those entities. Information can be sourced from electronic unstructured documents, from databases or from manual input. Those sources may change over time and traditional electronic interfaces are costly to implement.

---

### **Presentation**

Having gathered high volumes of entity-association structured intelligence, pattern determination and filtering to make sense of that information is paramount. Here issues of presentation clarity and extensibility of the analysis process are critical. Visual presentation tools provide mechanisms to provide instinctive clarity to high volume information. Geographic representation provides

---

### **Security and Data Sharing**

The security over the intelligence must be provided at certified protection levels. The security model must be comprehensive and flexible – strictly implementing classification standards. Sharing of information must be managed under strict security protocols – starting with Memorandums of Understanding between the organizations concerned. Typically the sharing of information is fraught with costly variations in technology and diverse data representations.

---

## Reducing Risk – Addressing the Challenges

---

### **Rapid Flexible Data Capture**

Using SiD template form definition capability web data entry forms can be delivered anywhere. The custom design allows business specific reporting models to be supported. Entity and association data is determined directly from the form structure and can be then transferred directly to the intelligence repository.

Remote PDA and tablet type devices are supported for disconnected field data capture – which can be synchronised with the host at the nearest network point.

Electronic forms of data capture – allow direct mapping of external data sources to load entities and associations of interest. Where the data is call record data from telecom sources, that data can be pre-processed using TAPS (Telephone Processing and Analysis System from Visual Analysis Limited). Allowing cleansing and standardisation of that data. This eliminates a massive burden placed on analysts responsible for the collection of call record data in typically inconsistent and untidy formats.

---

### **Secure Enterprise- wide Intelligence Repository**

Organisations in the intelligence arena will demand military strength security to protect their intelligence data. Security is core to the SiD intelligence repository and access is controlled strictly according to classification and “need to know” basis. A fully configurable security model allows the organisation to manage this model to meet the most stringent of security needs.

Communication of the information contained in the intelligence repository is critical for prompt response. All communication traffic is protected with the appropriate level of secure protection.

---

### **Case and Collection Management**

Organisations managing investigations require a task control mechanism to monitor status of multiple lines of investigation. SiD provides a comprehensive case management capability with tracking and status reporting – linked directly back to supporting documentation. All lines of enquiry can be visually tracked – to facilitate tight operational control.

---

### **Secure Intelligence Sharing**

Under certain legally agreed criteria and memorandums of understanding, agencies need to share intelligence data. Internally data from internal data sources needs to be made available for intelligence purposes.

The technology chosen to effect intelligence data sharing is an XML schema – which allows mapping to key national and international standards (such as the US Department of Justice National Information Exchange Model (NIEM) initiative. Around this model is a security model that complies with, or incorporates, a wide a range of certified security standards for authentication and encryption of the shared data so that is protected from end to end.

---

### **Visual and Geographic Presentation**

---

Visualisation of intelligence data provides a clarity of view, which speeds up the analysis cycle and provides clarity in presentation outputs. The integrated solution provides the world leading i2® visual analysis capability with selective seamless outputs. Managing geo-coded data and providing GIS (geographic information system) output allows presentation of intelligence output in a graphic mapping format. For military use both in i2 and for mapping the NATO standard APP-6A mapping symbols are supported.

---

## Background

### Intelligence is...

A body of evidence, and the conclusions drawn from that, acquired and furnished in response to the known or perceived requirements of consumers. It is often derived from information that is concealed or not intended to be available for use by the acquirer.

Simply put, the "intelligence cycle" is the process used to make intelligence as focused, accurate and effective as possible. The processes by which information is acquired and converted into intelligence, and made available to customers are usually defined within five steps in the cycle:

#### Planning and Direction

– This is management of the entire effort, from identifying the need for data to delivering an intelligence product to a consumer. It is the beginning and the end of the cycle--the beginning because it involves drawing up specific

collection requirements and the end because finished intelligence, which supports policy decisions, generates new requirements.

**Collection** – This is the gathering of the raw information needed to produce finished intelligence. There are many sources of information including open sources such as foreign broadcasts, newspapers, periodicals, and books. Technical collection -- electronics and satellite photography -- plays an indispensable role in modern intelligence, such as monitoring arms control agreements and providing direct support to military forces.

**Processing & Exploitation** – This involves converting the vast amount of information collected to a form usable by analysts through decryption, language translations, and data reduction for the production of intelligence.

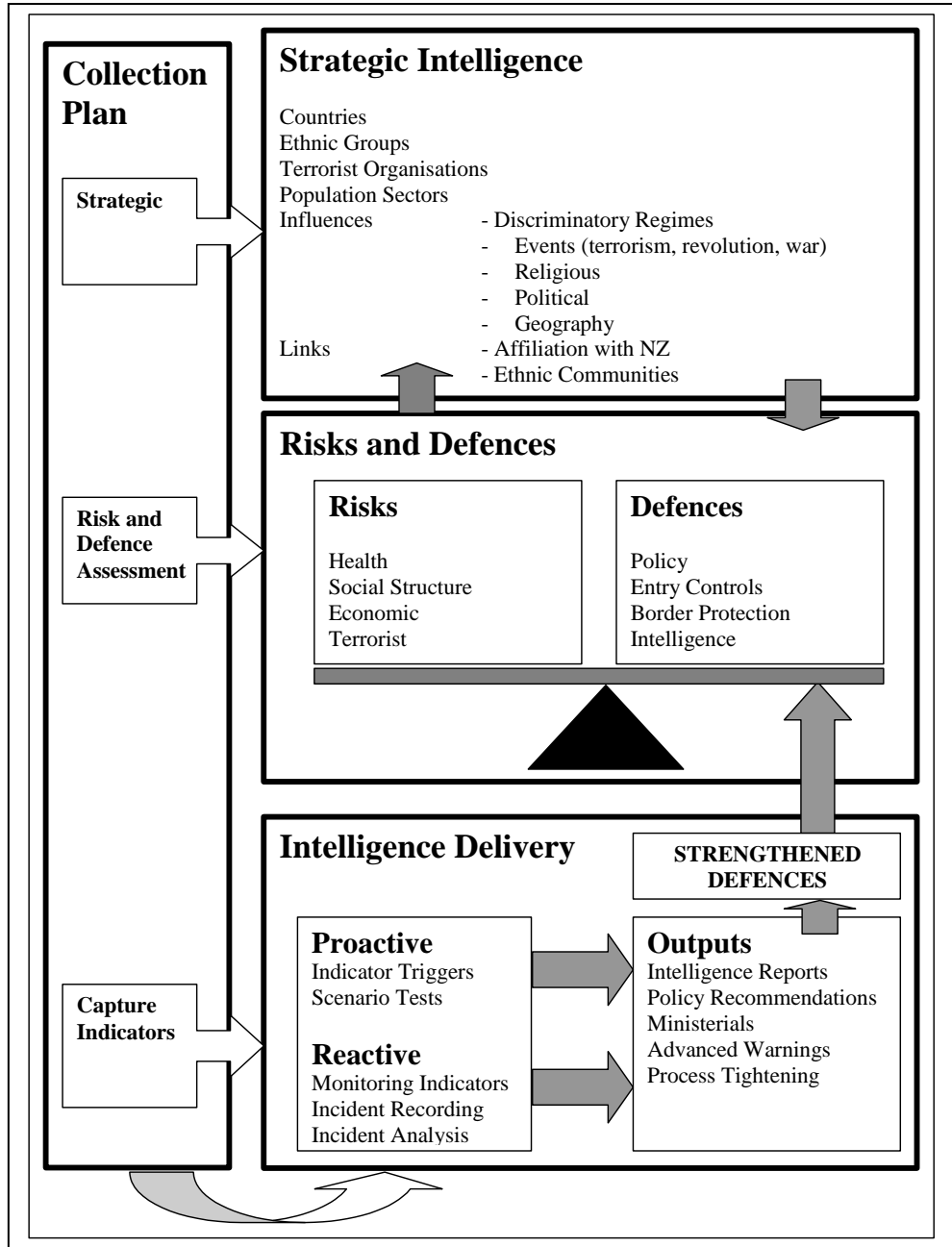
**Analysis and Production** – This is the conversion of basic information into finished intelligence. It includes integrating, evaluating, and analyzing all available data -- which is often fragmentary and even contradictory -- and preparing intelligence products. Analysts, who are subject-matter specialists, consider the information's reliability, validity, and relevance. They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information.

**Dissemination** – The last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers, the same policymakers whose needs initiated the intelligence requirements. The policymakers, the recipients of finished intelligence, then make decisions based on the information, and these decisions may lead to the levying of more requirements, thus triggering the Intelligence Cycle.



# Case Study – Immigration Intelligence

Figure 2. Immigration Intelligence Model



## Key Concepts

---

**Indicators** Indicators are key recordable metrics, which give an indication of some known trend towards risk or breach of defence – or change in threat status. For example a significant increase in interest in immigration to the target country or the number of residency applications per month.

---

**Indicator Triggers** Indicator Triggers are preset limits set against recorded indicator levels to attempt to proactively monitor changes in status. For example and increase of X number of immigration enquiries in diplomatic posts. Indicator Triggers will alert the intelligence team to re-assess the risk status in the area concerned – and correlate any event records influencing the change.

---

**Events** Events are time based “happenings” which may have an influence on the risk balance. Events may include terrorist events, political events (elections, coups, revolutions) or military events (invasions, wars) or more mundane changes in immigration policy. Events may also include technological advances (eg passport photo protection capability, biometric entry screening and so forth). Events should be monitored on a risk assessment basis – to avoid overload on the collection process. The “risk assessment basis” is readily determined from the Strategic Intelligence model – by the question “is there any link to the entities of influence described in that model?”.

---

**Incidents** Incidents are indicators in the risk versus defence model that defences may have weaknesses. Incidents are more specific than events – in that they will relate to a specific individual(s) or organisation. These may include border incidents – such as stowaways or people smuggling. The incident analysis process should examine and document in detail the particular defences that were breached. Often incidents will be reported via other agencies – such as Customs, Police or Identity Services. The intelligence collection plan for incidents should include data-sharing arrangements with such agencies.

---

## How does the Integrated Intelligence Solution support this Case Study?

---

### **Strategic Intelligence Collection**

Overseas diplomatic and consular posts will provide valuable strategic information in terms of local events or pressures. Information available to these posts will typically be high volumes of public domain (media, www, MS Word pdf, e-mail, text) material and intelligence reports from other agencies.

Recording this information into the SiD secure intelligence repository will enable combining the refined public domain background material with classified information from intelligence reports.

This mechanism provides immediate base structure to the intelligence – for classic event and association analysis.

---

### **Intelligence Reporting**

Using the SiD custom “smart form” capture capability - an internal intelligence-reporting template would be used to record any incidents with some degree of irregularity or suspicious activity. Use of the intelligence noting would be limited to content analysis triggered when any area of focus comes up on the radar for more detailed review. These general reports may include indicators or specific details of relevance.

Collation of entities for intelligence analysis will allow tools such as the i2 Analyst Notebook to be applied at this early stage. Such early structure delivery will allow a far more proactive response to the intelligence analysis and production phase.

---

### **Strategic Intelligence Model**

The intelligence analysis and production phase will enable an iterative representation of a strategic intelligence model.

SiD support of such a model has been tested in principle at Massey University School of Defence and Strategic Studies in Jan 2004.

The Strategic Model of Immigration Intelligence would include global influences on a geographical, ethnic, terrorist organisation and political linking. The strategic model provides a graphic representation of the influences – which may or may not be risks. The intelligence collection plan would be geared towards a simplified model of the countries, groups and influences concerned.

---

## How does the Integrated Intelligence Solution support the Strategic Model?

---

### Strategic Model Level 1

SiD meta-data driven flexibility allows a model representation that is both dynamic and expandable. The strategic model would include profiles of the following structure:

- Country

  - Groups within Country

    - Ethnic

    - Political

    - Terrorist

  - Influences within Country

    - Political

    - Nationalism/Separatism issues

    - Discrimination/Land Ownership

    - Health

    - Terrorist

Events of significance, which may alter the dynamics or risk, level with any or all of the identified groups

- Coups

- Revolution

- Terrorist Attacks

- Massacres

- Wars

Geographic representation of the model via the GIS interface also adds significant value to the intelligence representation and clarity.

---

### Inter-Agency Intelligence Solution

Early delivery of an intelligence product above – will in turn make this intelligence available for other agencies to value-add to the content. At this stage the dissemination phase of the intelligence process can be supported by the SiD secure intelligence sharing capability.

A key intelligence collection capability is in the ability to inwardly and outwardly share intelligence with other agencies. Obviously such arrangements will be underpinned by appropriate inter-agency MOUs. At the operational level these will need to be protected with a security framework, which maintains the integrity of the MOU and ensures other generic considerations (such as privacy legislation) are protected. Ideally (especially for low security classifications) such exchange should be possible under existing inter-government exchange protocols.

Such exchange must be selectively manageable in terms of content. The transfer of information must be totally flexible in terms of mapping to the intelligence model used at either end of the transfer – both in terms of detailed profiles and associations.

Such intelligence sharing would be available at all levels of the intelligence collection model.

---

## How does the Integrated Intelligence Solution support the Risk and Defence Model?

### **Risk and Defence Model**

---

The Risk and Defence model proposed is strongly supported by Causal Faction Risk Research undertaken and rigorously developed by Professor James Reason.

Fundamentally the model identifies the balance between the identified risks and the defined defences. Incidents are viewed as an indication of a potential breach in defence. Major holes in defences are indicated by incidents that are able to breach multiple defences (for example identity fraud plus false language certificate plus forged documentation). By analysis and investigation of specific events against the total defence process (policy, rules, processes, training) a more holistic prevention regime can be recommended – in terms of actions to be taken in each area.

It is suggested that the risk and defence model be included in the intelligence system in some detail. Each Risk should be linked to defences that protect against that risk. URL links can be made to policy of legal defences, to make the assessment of risks tightly coupled with current protection.

Any incidents, which appear to have breached specific defences – should be linked to those defences. Obviously the clustering of incidents around a particular defence could indicate a higher risk category. Using the secure intelligence repository coupled with i2 Visual Analysis capability the analysis of such clustering would be strongly supported.

The capture of such intelligence is stored within the enterprise intelligence repository. The data partitioning capability allows separation of views of the intelligence outputs from the various intelligence models (strategic model or risk and defence model). Sharing of key entities and cross boundary identity resolution are provided by the SiD profile combination facility.

---

## How does the Integrated Intelligence Solution support Risk and Defence Profiles?

### **Risk and Defence Profiles**

The SiD “need-to-know” operational security partitioning allows a second level of intelligence model to represent the risk model identified from the risk and defence intelligence production.

The risk/defence model would include profiles of the following structure:

#### **Risk Profile**

- Nature of the risk
- Risk description
- Target area of risk (country, ethnic group, terrorist group)
- Risk assessment rating
- Links to supporting documents
- Links to Incidents
- Links to defences

#### **Defence Profile**

- Nature of the defence
- Defence category (e.g. Policy, entry controls, electronic identity checks etc).
- Defence description
- Links to supporting documents
- Links to Incidents
- Links to risks

#### **Incidents**

- Type of incident (standard lookup category)
- Date of incident
- Incident category
- Incident description
- Links to defences
- Links to risks
- Links to entities involved (persons, organisations, countries)

---