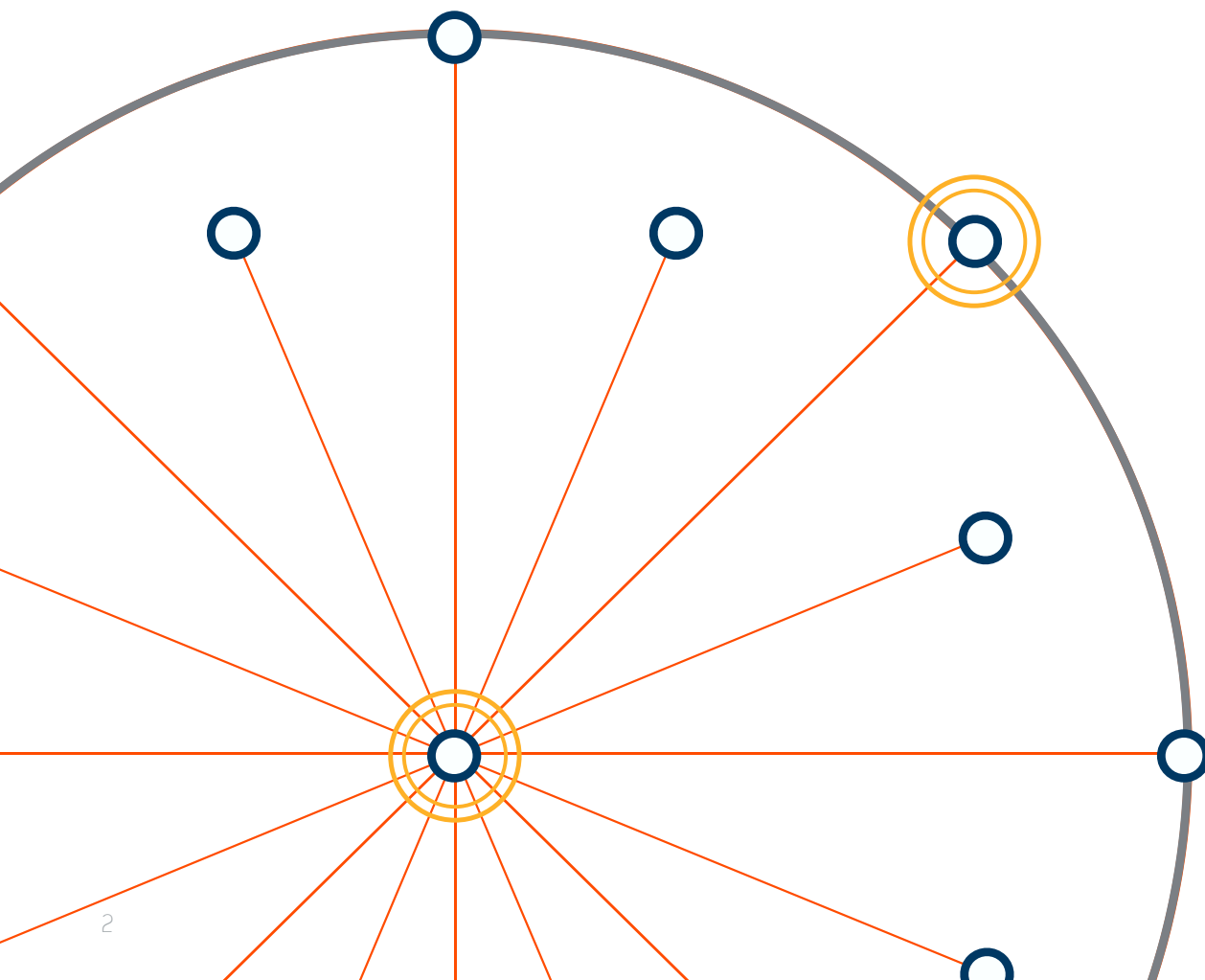# IntelligenceReveal™
Subject Management

BAE SYSTEMS

IntelligenceReveal Subject Management is a new product that enables analysts to more efficiently and effectively manage the key information assigned to individual Subjects of Interest and the monitoring of cyber threats and investigations.

The importance of good management

Where do the physical and cyber threats to your nation, government, business or society come from? Who are behind the threats? And how do you keep track of those who may pose a threat (Subjects of Interest (SoI) or threat actors)? What are the relationships between SoIs or threat actors? Are any of the SoIs or threat actors actually different manifestations of the same, single person or group of individuals?

These are all valid questions. For those tasked with enacting defence against threats to our societies, the challenge lies not only in finding the answers to these questions, but also, in an effective and scalable way, in managing the vast amounts of information which analysts can find and then attribute to specific SoIs, threat actors or threat investigations being conducted by agencies. In addition, it is important to ensure that whatever information is recorded during an investigation or is linked to a SoI or threat actor, can be securely shared, retrieved and analysed at the point and time of need by those with the authority to access it. Furthermore, it would be ideal if information indexed against one investigation stream or SoI/threat actor identity (hence forth collectively referred to by the single term 'SoI'), could be easily linked to and analysed in relation to others.
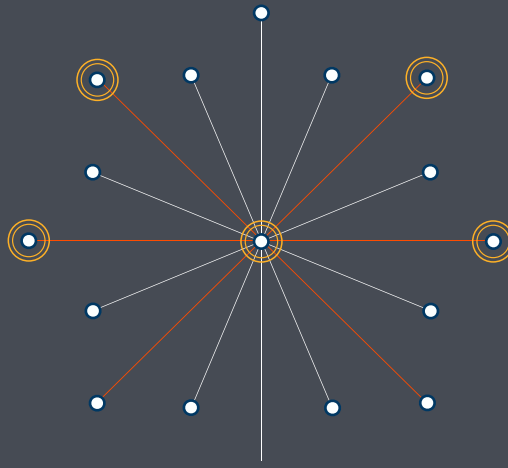
IntelligenceReveal Subject Management

IntelligenceReveal Subject Management is a new specialist product that facilitates the management and storing of information associated with SoIs and investigations (e.g. a new telephone number, address, email address, IP address, MAC address, people, places, online IDs) and ensures that it is easily manageable and accessible to those who need it. Where required, it enables data to be securely shared with others. In addition, role-based security ensures that analysts can only view information on SoIs and investigations that they are authorised to see.

Enhancing the management of data

IntelligenceReveal Subject Management enables analysts to maximise the intelligence insight which can be derived from existing SoI data by managing it and sharing it more cleverly and efficiently. It enables analysts to create groups of SoIs and entities which may be involved in a particular threat (an investigation) and to organise and manage the data within those groups. The solution provides a common virtual and highly visual workspace wherein analysts can conduct investigations and maintain data pertinent to an investigation or SoI identity. And as analysts carry out operations, the solution enables them to easily index or update data during analysis and attribute it to either an SoI or an investigation.The product aids analysts in the enrichment of other data, making it easier to spot and store other information points.

IntelligenceReveal (IR) Subject Management is a stand-alone product which can be deployed individually. However, when deployed alongside other IntelligenceReveal products or solutions, further operational efficiencies can be realised: as analysts working with related IntelligenceReveal solutions or products identify key information relating to SoIs or investigations, analysts can manually tag data found during their investigations and assign it to a 'shopping basket' linking data to specific SoIs or investigations. Periodically, or at the end of each session, the analyst can then manage the content of a shopping basket and upload its contents to the Subject Management solution, with the information going to the relevant SoIs and investigation files.
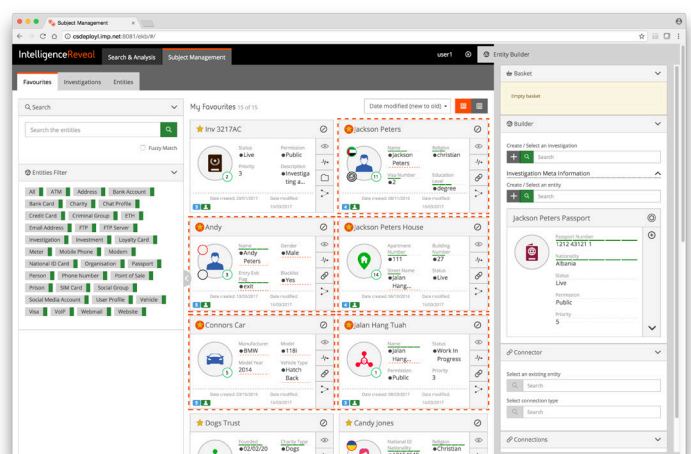
Managing investigations

IR Subject Management enables analysts to manage all known information relating to that investigation which could be associated with a physical or a cyber threat: this includes grouping individual SoIs/threat actors into supersets which are associated with specific investigations.

The product offers the following key features:

Create

Create an investigation as the primary means for managing a co-collection of SoIs relating to a specific threat.

View

View all of the information related to an investigation, including related SoIs and key attributes, such as the name of the investigation, status, access level, priority, investigation type, points of contact, summary, objectives, etc.

Add

Add additional information to an investigation as it evolves, e.g. if the status and priority changes or if the analysts connected to the investigation change.

IntelligenceReveal Subject Management enables analysts to maximise the intelligence insight which can be derived from existing SoI or threat actor data.

Managing SoI cards

IR Subject Management enables analysts to create and manage interactive cards for tracking SoIs, cyber threats or threat actors, where that identity may represent a person, organisation, location or asset related to an investigation. The solution allows users to manage the content of SoI or threat actor cards in the following way:

- Manage and store SoI information including biographical data (e.g. name, DOB, hair colour), key devices, online identifiers and locations.

- View all of the information related to a SoI including recorded attributes, assets and connections.

- Search for SoIs within IR Subject Management in order to easily locate information that the organisation has on a specific person or identifier.

- Receive notifications when an SoI or investigation record has been updated.

- Add SoIs and investigations to designated 'favourites', enabling rapid navigation to the most commonly-used records, and ensuring that users are notified when these records are changed.

- Each data element within a SoI file can have a security policy associated with it. When SoI files are viewed by other analysts they can only see information which they are allowed to see or which meets their security clearance level.

Click to view favourite list

Screenshot of **interactive user capability** for SoI or threat actor cards

Understanding the data

Priority, confidence and provenance

As well as recording data as attributes associated with SoIs and investigations, IR Subject Management records and provides analysts with a wealth of information about the data itself, which aids and assists them in the decision making processes of investigations, for example:

Priority

Analysts can assign a metadata tag to an entity in the database which helps analysts to record and understand the priority they may wish to assign to related contacts, i.e. this could represent the seriousness of a threat, or reflect the hierarchy of organisations or individual entities with respect to each other: e.g. the leader of an organisation/highest threat SoI under investigation may be tagged with a priority of 1, whereas the lowest ranking members of that organisation/lowest threat SoIs in an investigation may be tagged with a priority of 5.
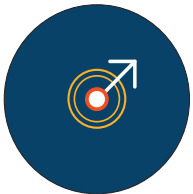
Confidence

IR Subject Management helps record the level of confidence analysts have in each data element, and displays this information in a simple configurable format. It helps the analyst quickly and easily identify which information is trusted, and which may need further investigation.

Provenance

IR Subject Management helps keep a record of the source of information and the justification for adding it to the database. It also stores the date of the provenance and has useful tools to enable the analyst to easily see the provenance of an entity and all of its attributes.

With over forty years experience in defending nations and their critical assets, BAE Systems understands the threat to governments, businesses and law enforcement agencies in the cyber intelligence age.

About IR Subject Management

The IR Subject Management product was designed and developed for intelligence and cyber analysts from the experience and understanding gathered from years of working with and supporting agency analysts in pursuit of their missions.

We understand that information is changing all the time and that the threat landscape is dynamic. As such the product encompasses many features which analysts need to help them continuously update existing data, enabling them to optimise their mission processes and empowering them to make dynamic decisions based upon the best information available to them at any point in time.

To learn more about IntelligenceReveal Subject Management, please contact your local sales consultant.
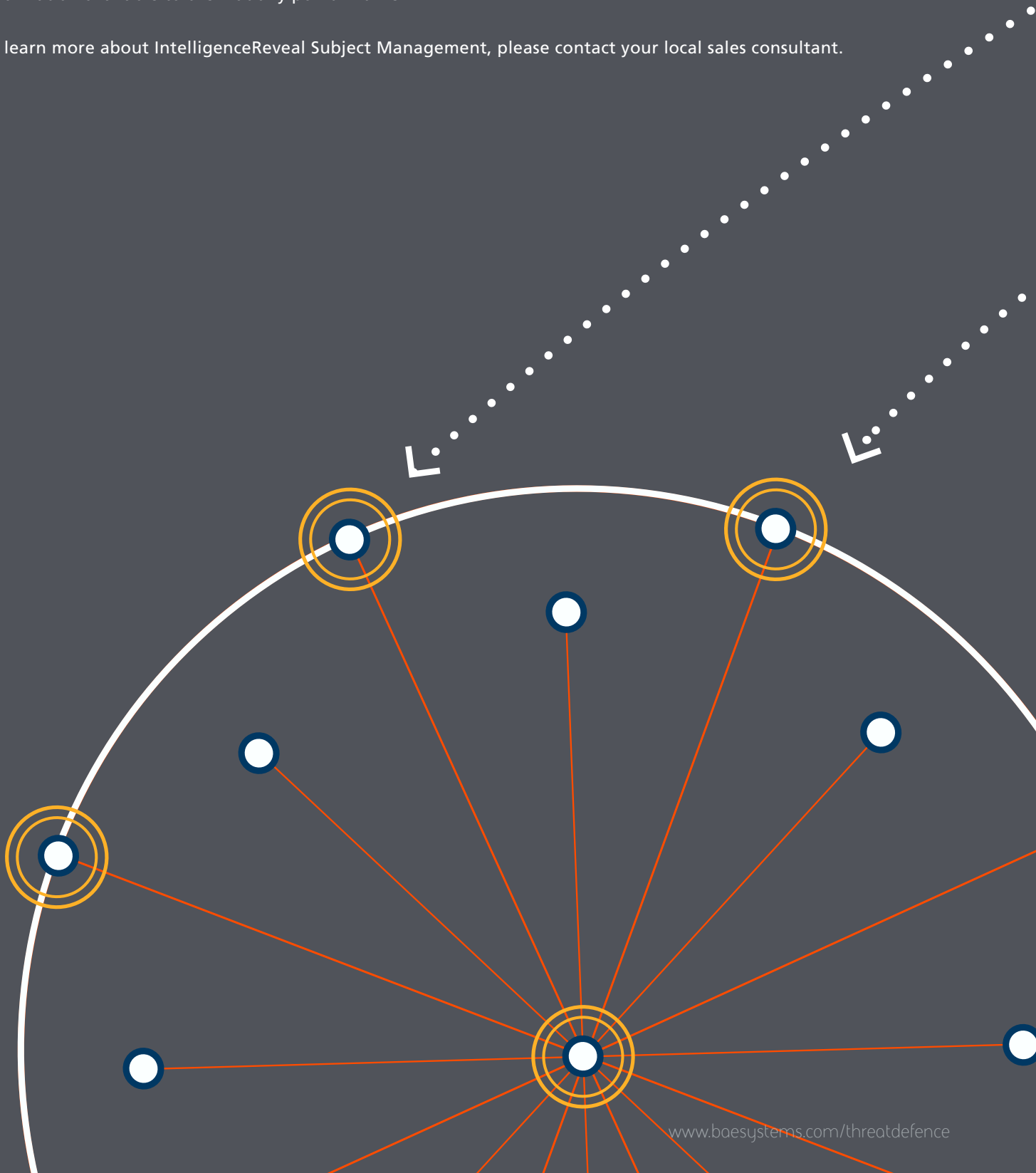
We are BAE Systems

We help nations, governments and businesses around the
At BAE Systems, we provide some of the world's most
advanced technology defence, aerospace and security
solutions.

We employ a skilled workforce of 82,500 people in
over 40 countries. Working with customers and local
partners, our products and services deliver military
capability, protect people and national security, and
keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #23-03, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/threatdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency
response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST

CESG Certified Service

CPNI
Centre for the Protection
of National Infrastructure

Cyber Incident Response