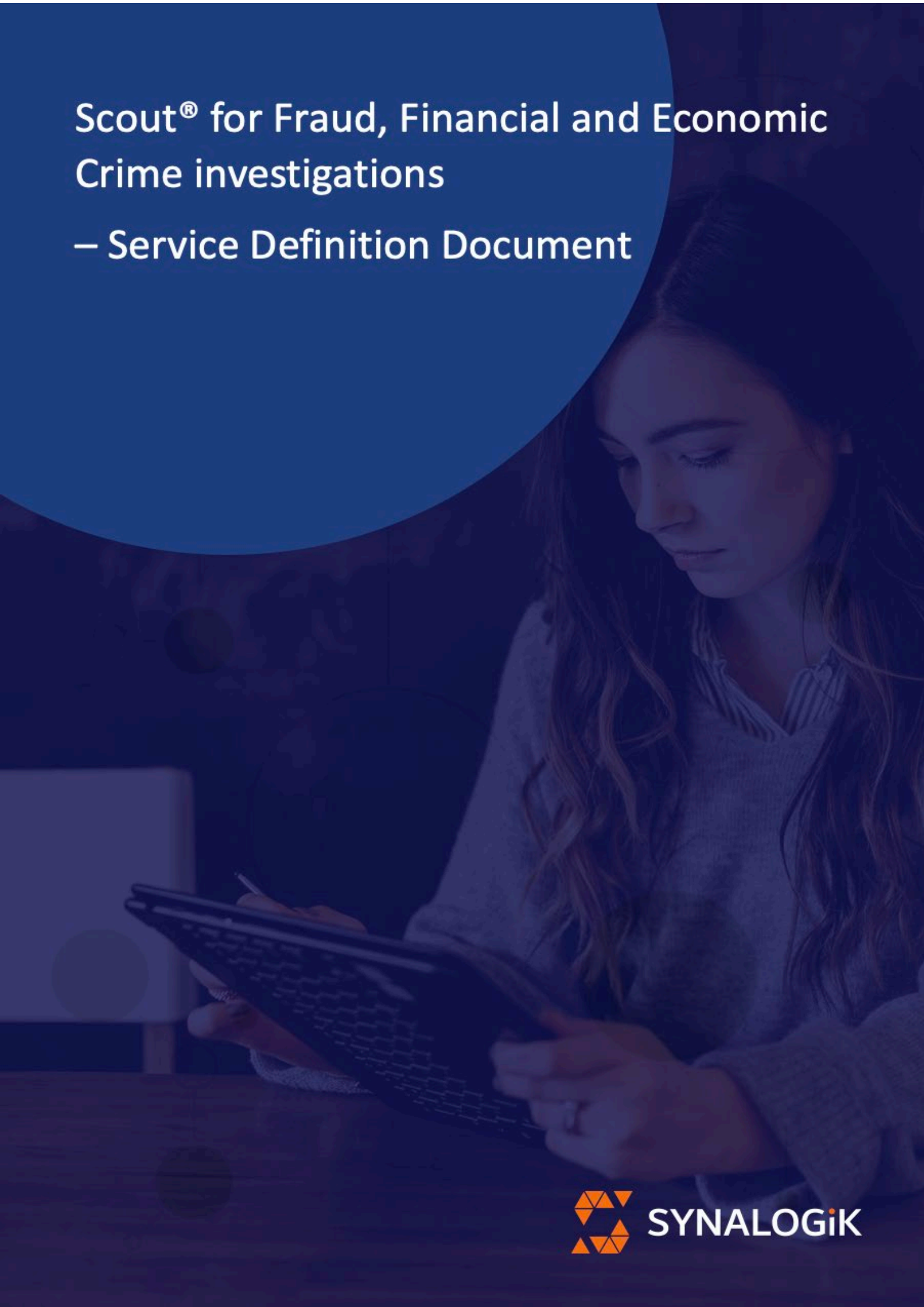
Scout® for Fraud, Financial and Economic Crime investigations

– Service Definition Document



SYNALOGiK

Solution Overview – Scout® Fraud, Financial and Economic Crime investigations

Meet Scout® by Synalogik, a one-of-a-kind, auditable and evidential data aggregation platform for discovering hidden risks and providing enhanced investigations across third-party, internal, and open-source data sets. Scout® automates enquiries into people, companies, vehicles, addresses, email addresses, IP addresses, phone numbers and any combination of the above.

Having gathered the relevant results, Scout® applies risk assessments to the merged sources and allows the user to view the results within auditable reports, node view charts, on a map and combined within a spreadsheet. At the conclusion of your investigation users can export their findings such that they can be used for evidential or intelligence purposes; dependent on the data sources interrogated.

Scout® harnesses the power of automated data aggregation, robot process automation, and a sophisticated graph database providing investigation, cleansing, and analysis. It reduces manual investigation times per enquiry to around 60 seconds for any individual case; saving up to 85% of your teams' time.

Our ability to concurrently query, cleanse, and flag data from sensitive internal data sources, paid for third-party data sets and all kinds of Open-Source intelligence set us apart from the competition.

Scout® comes as a cloud-based software platform. All Synalogik platforms can be deployed upon a variety of cloud-based providers or on premise, however our standard platform is hosted upon AWS. The system has been deployed with a variety of police forces, Government Departments and Law Enforcement Agencies in a way that meets with their Data Protection, Information Security and all other requirements. The platforms are data agnostic, territory agnostic and cloud agnostic; giving our clients complete flexibility to deploy this complimentary technology in a manner which best works for them.

The Synalogik professional services team compliment the offering by providing an SC or DV cleared individual to evaluate client needs from a functionality and data source perspective. These "Discovery Phases" often enlighten our clients with regards to the variety of automated aggregation options which are available directly off the shelf, including access to a variety of sensitive policing and Government only data sources.

Key Benefits & Features

· Live data interrogation across all your data sources – Search your data sources and OSint together in near real-time, eliminating reliance on bulk data provision, which is outdated from the day it arrives.

· Discover hidden links in merged data sets –Scout® WorkBench allows users to carry out complex further investigations by visualising links between entities and providing the ability to select and investigate any one of them further at the click of a button.

· The ability to search against sensitive data sources concurrently, including pre-configured access, where hosting and legal requirements are satisfied, to PNC, Ident1, Nomis, HM Passport Office, HMPPS and many more.

· The "Data Clasher" functionality allows users to upload large or small additional repositories of data as a spreadsheet into the platform and thereafter to discover hidden connections between those uploaded sources and your ongoing enquiries. Data Clasher also enables users to compare large internal data sets using fuzzy logic or exact search terms to find linked cases of concern.

· Supercharged operational efficiency – Commercial, consented, open-source and the option for internal data create the 'Single Intelligence Environment' that maximises efficiencies through automation, reducing investigation time, cost, training time, and delivering standardised reports in less than a minute.

· Avoid bottlenecks and backlogs of investigations by relieving investigators of standard enquiries – Create templated searches with fixed risk assessments which can be used on bulk or individually; relieving pressure upon scarce resource and giving your wider team the time to focus on decision making, not researching.

· Proactive, victim focused enquiries – where members of the public rely upon timely decision making, but manual checks logging in and out of different data repositories are creating a backlog, let Scout® change the research time to seconds; ensuring greater victim focus and a higher quality of decision making.

· Greater accuracy – automated aggregation and auditing resolves the human errors that can sometimes occur when manually searching different data sources; drawing links and cross-referencing data across your internal, third-party and open-source datasets.

· Improved decision making – Standardised, in-depth and clear reports, free of human error, mean you are free to focus on decision making, rather than logging in and out of multiple data sources then typing up reports.

· Quicker training – Scout® aggregates all your data sources, meaning you only need to know how to use Scout®, not a multitude of different systems. When alternate sources of data are required, your previous reports, risk assessments and templated workflows remain, but Synalogik can provide you with pre-integrated additional sources as soon as appropriate data sharing arrangements are in place.

· Reduced reputational risk – Where Police forces and Government Departments are making decisions which could impact their reputation, they need to know that every stone is being lifted before decisions are made - even in golden hour or time sensitive scenarios. Our highly configurable, compliant profiling minimises your exposure to people and businesses of concern.

· Data agnostic – Scout® is data agnostic and pre-integrated with the majority of data aggregators; eliminating the learning curve and IT resource required to change suppliers and giving you the flexibility to choose a provider that best suits your needs.

· Conduct Open-source enquiries in a variety of languages at the click of a button - Scout® can be configured to retrieve precise OSint results relating to people, companies, cars, addresses, email addresses and phone numbers in most major languages whilst also focusing the search query upon that particular country.

· Configurable, secure, access using multi factor authentication, Single Sign On and IP address whitelisting.

Service Description

Scout® is designed for rapid gathering of information from third party data sources, open-source and your own internal data sources (including Police sensitive sources where hosting and usage requirements are met). Synalogik has incorporated these data sets into API's that are "called" in real time to give you up to the minute results. The search can be conducted on a person, a telephone number, email address, address, commercial entity, or vehicle. The results can be cleansed and reviewed using risk assessments, then viewed as text, node charts, on street view or upon a map. Scout® can perform your search in a fraction of the time taken to manually log in and out of multiple different data sources.

Scout® is made up of many innovative feature-rich tools, each of which contribute to maximising operational efficiency within your team.

Data Aggregation

Complex investigations require data from multiple different sources, which, when collated manually, are incredibly time-consuming to complete.

While some automation solutions exist, they often only include their own proprietary datasets, which are insufficient to conclude an investigation satisfactorily and inevitably result in the user having to log back into other data sources internally or on open sources before completing an enquiry.

Our automation platform, Scout®, resolves this with a data agnostic approach to aggregation, integrating all your chosen datasets into a single intelligence environment; allowing you to search once and automatically pull data from all these datasets in an auditable and compliant manner.

The Scout® and DataHunter platforms are pre-configured to interrogate data from all major data aggregators and Open Sources. The list of sources grows weekly, but key integrations include data from:

1. Equifax
2. TransUnion
3. Experian
4. GB Group
5. CreditSafe
6. LexisNexis
7. CIFAS
8. DVLA
9. DVSA
10. Companies House
11. Google API
12. Bing API
13. Sayari (global commercial data)
14. Land Registry

Policing data sources integrated into the DataHunter platform:

1. Police National Computer ("PNC")
2. Police National Database ("PND") [live from Q4 2022]
3. NOMIS (HM Prison and Probation Service intelligence database)
4. HM Passport Office
5. Ident 1 (Fingerprint data)

Open-Source Intelligence

Open-source intelligence is the fastest growing, yet most underused, source of information for fraud, asset recovery and financial investigations.
The Scout® open-source intelligence tool enables you to create templated, highly configurable searches around keywords, proximity, timeframe and document type from the world wide web.

· The Scout® platform complies with Data Protection Laws and is configured to protect your teams from reviewing privacy or firewall protected sites,

· Select from or customise our tried and tested OSint templates for your organisation; benefiting from the experience within our Synalogik team and our wide customer base of fraud investigators in both the public and private sectors,

· The Scout® OSint builder is sufficiently advanced to allow you to only retrieve results linked to your inputs, by putting filters around the location of the entity being investigated, the timeframe when the information was added to the web and even the type of document.

· If your team are "Googling" enquiries as part of their investigations, reviewing potentially millions of results, many of which are prioritised by your browsing preferences not actual relevance, then their time is being wasted. The Scout® OSint Builder reduces false positives and targets only relevant results, saving your team up to 85% of their time compared with manual investigations.

· Significantly reduce the number of results by adding keywords of relevance and templating those searches for ongoing use.

· Retain an auditable log, within a standardised report, for all the open-source search results your team produce.

· Start your search query from the country of origin in question to prioritise the results

· Exclude or include results from specific webpages of interest to avoid false positives.

· Combine the Scout® Risk Assessment tool with the OSint Builder to identify cases of concern from bulk uploads - giving you the ability to search large quantities of people, companies, phone numbers and more, all at the same time - highlighting those that appear upon certain webpages.

· Easily create, save and add the searches into Scout® workflows that can be applied to individual, batch or inbound automated API queries.

· Retrieve OSint results from live webpages, cached webpages or via direct link to the Wayback Archive – giving you the chance to review results which have otherwise been removed from the web.

Workflow Templates

Spending time manually logging in and out of different data sets before being able to make decisions is inefficient. With Scout® you can create bespoke workflows to cover every investigation need, ranging from basic to complex crime investigations.

· Chose the data inputs you want to research – name, address, email address, telephone number, commercial entity, vehicle registration or IP address

Select how Scout® compares inputs to potential results using “fuzzy”, “exact”, “contains” or “begins with” as search filters.

· Filter potential results by name spelling, age or proximity to help remove false positives.

· View and select from a list of all data sources which you want Scout® to interrogate.

· Save these configurations as templated workflows to your Scout® home screen for your team to use time and time again.

· Initiate your workflow via API, individually or in bulk.

Automated reports

Creating reports that require information from multiple, disparate data sources made up of different formats is incredibly time-consuming, often leading to reports that differ in terms of quality and depth.

Scout® automatically collates, cleanses, risk assesses and reports all the disparate data sources your team manually research, then creates a standardised report on its findings from all of them.

· Get compliant and accurate reports, automatically, in under 60 seconds.

· Download reports as PDFs or as a spreadsheet with attribution for every result set out in the report.

· Easily conduct follow up searches on related results within the same Scout® WorkBench.

· Comply with Data Minimisation principles by using Scout® to cleanse potential results by name spelling, date of birth or proximity.

Risk Assessment

Decisions about multiple individuals, companies, phone numbers or email addresses are complex and subject to human error when numerous datasets are involved. Manually reviewing risk from multiple data sources is extremely time consuming and the consequences of getting it wrong can serious.

The Scout® risk assessment tool allows you to create sophisticated rules that automatically look for specific risks, and then score them to get an overall assessment of their level, helping your team to make the right decision, save you money and reduce investigation times.

· Build any number of negative or positive risk rules and weight the results to build out a holistic risk view.

· Highlight risk as a score or Red, Amber, Green rating ("RAG").

· View risk assessments in your Workbench or embedded within reports.

· Get an auditable, transparent and detailed assessment on people, companies, vehicles, addresses, email addresses and phone numbers.

· Consult with our expert team to get bespoke risk evaluation support and guidance.

Synalogik Knowledge base

Scout® has the optional and highly configurable capability to automatically identify disparate links between seemingly disassociated enquiries, when requested. Each time a search is initiated, Scout® cross references the findings against the existing "knowledge base" of that user and highlights where searched entities are linked. These "flags" are seen within the report providing the most recent user with the contact details for the previous user who created the linked report - subject to access management rules.

For example, Scout® can take the output of a phone download and review where potentially hundreds of dialled phone numbers appear on the web, within intelligence databases or your internal data. Attribution of email addresses, phone numbers, people and more are now done within minutes and presented within the Scout® report, which can be appended to a witness statement or investigation file as used or unused material (subject to the selected data sources).

When selected, the "Synalogik Knowledge Base" searches across your database to automatically find if anyone has looked at these search inputs before; providing you with unrivalled insight into the holistic risk this new line of enquiry presents.

· Understand where your latest enquiry ties in within your organisation or team

· Scalable and customisable access management for your users, both in terms of functionality and data source access.

Commercial Monitoring Functionality

When investigating an entity, Scout® can monitor all potential changes to a business with predetermined regularity or constantly.

· Get immediate warnings if there has been a change of concern to a company in your investigation.

· Pre-format Scout® to flag those cases and risk score them where appropriate.

· Target precise changes, even down to a particular form lodged at Companies House, so that you're only informed of those that matter to your enquiry.

· Changes to company ownership, company details, registered addresses, annual filings or borrowing can each be selected and monitored separately with corresponding risk scores.

Advanced Investigations

Scout® risk assessments and search workflows can be used to research specific types of risk and get immediate, automated reports highlighting those factors of concern.

However, investigators and analysts employed by Law Enforcement Agencies and Police forces are likely to need to conduct follow up searches to discover hidden links, uncover organised crime groups and build in-depth profiles.

Scout® WorkBench allows users to carry out complex further investigations by visualising links between entities and thereafter providing the ability to select, investigate and risk assess any one of them at the click of a button.

· View the results in multiple formats: Workbench Report; Table View, Map View and Node View.

· Get a diagrammatic visualisation of the links between entities using Node View.

· The ability to search historic reports within your Scout® Archive and populate them into your latest WorkBench report on a temporary or permanent basis to visualise where links of interest occur.

How Scout Works

Technical Description

Scout® is an Open-Source Intelligence (OSInt) and data aggregation investigation platform which retrieves data from the web, third party APIs and sensitive 'internal' data sources usually only available on standalone systems. The platform will require firewall access configuration within organisational security policies.

Scout® is accessed using via all standard web browsers, including but not limited to Firefox, Chrome and Internet Explorer. Appropriate internet bandwidth must be available. Our cloud service and resources are provided in the eu-west-2 (London) region within data centres that are accredited to the PASF (Police Assured Secure Facility) standard.

We create a separate environment (or VPC, Virtual Private Cloud) for each customer, there are no shared resources and no opportunities for data to leak between customer systems.

Synalogik provide our customers with access to Scout® via a URL, meaning that no on-premise infrastructure is required within your organisation. If the highest levels of security are required for specific customers or projects, Scout® can be deployed on premise or within secure private clouds. Scout's rules and risk algorithms are customisable, meaning clients can refine and tag certain results or types of data to suit the investigation.

Scout® was designed and built by law enforcement officers and specialist criminal and regulatory barristers, ensuring that it automates the capturing of all evidence in a manner that is compliant with the Criminal Procedure and Investigations Act 1996 (CPIA) and all Data Protection Laws.

Every search is auditable, and every node of data brought into the platform is time and date stamped down to the second. Scout® also captures individual users' activity for internal audit ability from a legislative and professional standards perspective. Users access

Scout® via their existing hardware and IT infrastructure. Everything in the onboarding process has been designed to ensure that cost efficiencies are maximised for the client.

Scout® is accessed via a secure, pre-authorised, URL at fixed IP addresses; allowing users to login via a username and password - in addition to SSO and MFA, where requested. Once within the investigation console, users can search unlimited internal, third party or open-source data sets for information relating to: people; postal addresses; email addresses; commercial businesses; telephone numbers; and vehicles. Searches can be completed individually, on bulk via the spreadsheet uploader, or automated API.

Purposefully designed to increase the capacity and capability of teams, Scout® is a secure, real-time investigation platform that enables the user to automate the laborious, manual searching and re-searching of internal, third party or open-source data. Scout® reports can be retained within our auditable case management system (Scout® WorkBench) or the results can be exported into a pdf or spreadsheet. The data sources for all results are clearly attributed within the report. If sensitive data sources are used, these can separately be retained within a different report and form part of a sensitive unused schedule.

The abundance of data provides a real opportunity for users within strategic, operational and intelligence teams to make evidenced based decisions more swiftly. Whether you're looking to investigate more cases or make a more informed decisions, Scout® allows you to look under every stone in a fraction of the time.

Levels of Access

Access, Data Protection and System Security are paramount design features of the platform and its operational deployment. The system is capable of operating to Official Sensitive and is fully compliant with Data Protection, Criminal Procedure and Investigations Act 1996 (CPIA), Information Commissioners Office (ICO) and Information Security standards.

User and system access is provided at four levels:

Admin	Synalogik Administration & Helpdesk	Ability to reset passwords, unlock accounts, disable user access.
Super User	Investigator functionality with admin functionality.	Ability for investigators to also reset passwords & unlock accounts.
General User	Investigator / Analyst	Ability to use full functionality of Scout platform.
Audit	Professional Standards / Compliance	Ability to view user activity.

User Management

Scout® provides users with a platform to interrogate data sets rapidly and whilst it can be procured as a commercial-off-the-shelf capability, it has also been designed in a way that allows Synalogik to work with customers to identify and ingest additional data sets and complement existing in-house technologies to bring further efficiencies in the investigation process and to solve a wider range of user cases.

Individual users have the capability to: customise OSINT search 'wizards' for individual cases, create bespoke search templates into all our headline types of search and proactively monitor any changes to commercial entities in near real time.

User Reports

Custom activity report can be created detailing user activity and itemised searches on a monthly basis, if requested. This functionality is designed to aid organisations with compliance in respect of The Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Criminal Procedure and Investigations Act 1996, The Data Protection Act 2018 and The General Data Protection Regulation. Organisations trust Scout® to ensure their users are not only operating lawfully, ethically and within the parameters of their role, but so that they can prove they are should the need arise.

Management Reports

Management Information reports are available showing usage of Scout®, thus enabling managers to identify any non-usage and respond accordingly. The reports can also help to identify training and tradecraft gaps and weaknesses, which can then be addressed in learning and development sessions – all of which are delivered by Synalogik as part of our commitment to best-in-class investigations and customer support.

Reporting consists of a monthly emailed "MI" report setting out the required information - names of users, API calls, and search inputs. If a particular instantiation has been deployed to Official Sensitive or above, the Synalogik team cannot gain access to this information and as such MI reporting is not available, however, it can be retrieved by internal users directly from the system.

Security

The Company operates to ISO 27001. Scout® is regularly PEN tested by Crest accredited third parties as part of this certification requirement.

The Synalogik team are vetted to NPPV Level 3 and have a minimum of SC Clearance. Many of the Professional Services team have heightened levels of clearance. Details of which can be provided upon application.

Synalogik also have Cyber Essentials Plus certification.

Professional Accreditations

1. ISO 27 001
2. Cyber Essentials Plus

Data Location

All Scout® Data is held in AWS Servers solely within the UK.

All system backups are retained within the UK.

All data is encrypted at rest and in transit.

Backup/Restore and Disaster Recovery

Synalogik has complete internal plans, processes and systems in place regarding business continuity and resilience of a client's unique data store.

Any specific requirements for backup, restoration and disaster recovery, where appropriate, would be discussed and agreed with the customer prior to an order being placed.

GDPR compliant investigations

Scout and DataHunter platforms interrogate the databases which our clients are lawfully entitled to access. Platform users are trained upon the system and each time they access it they agree to its terms of use, forming part of the auditable log of activity.

The system minimises volumes of personal data processed, by cleansing potential results prior to processing them into reports - this is done by filtering potential results by name spelling, date of birth and proximity.

Each platform is created with specific data retention periods put in place and replicating the Clients Data Protection needs.

Individual users can delete individual reports or OSint results if they prove to be false positives.

The platforms retain an auditable log of every search, data set interrogated, user details and results ensuring you can evidence every step of your data processing for non-punitive, civil or criminal enquiries.

Onboarding

User onboarding and training is available as part of minimum licence package arrangements or separately as requested.

Support Services

Synalogik operate a standard business hours UK-based support service providing telephone and email support. Typically, this is second line support working with the customer's local technical team, although other options are available as required. Support is included as part of the Scout® licence.

Support Helpdesk

Contact details for the service desk will be provided during the onboarding process, and users are encouraged to user either email or telephone to log questions, queries or requests for support

When logging a call by email the following information should be provided as a minimum, and sent to: helpdesk@synalogik.com

- Contact Name
- Contact Number
- Contact email
- Priority
- Username experiencing the issue
- Nature of the problem experienced
- Telephone number

Fault Priority

The Fault Management SLA specifies that faults will be assigned a priority, upon which the response to complete the diagnosis of the fault is as detailed by the Key Performance Indicator (KPI) for that category of fault.

For reference, the SLA categorises the different fault priorities as follows:

Priority	Description
Priority 1 (P1)	Scout® is inaccessible or unusable with the potential of causing critical impact to the customer's business operations if service is not restored quickly. The customer is willing to commit substantial resources around the clock to resolve the situation. For any Incident to be assigned Priority 1, the Customer must guarantee the necessary access & resource required to help diagnose and resolve the incident.
Priority 2 (P2)	Scout® is severely degraded, impacting significant aspects of the Customer's business operations. The Customer is willing to commit full-time resources during business hours to resolve the situation.
Priority 3 (P3)	Scout® performance is degraded. Functionality is noticeably impaired, but most business operations continue.
Priority 4 (P4)	The Customer needs information concerning product capabilities, installation advice, or the creation/deletion of users.

Service Level Agreements

Severity	Contact method	Response Time	Resolution Time	Customer Updates (email or phone)
Priority 1	Phone	1 working hour	24 hrs	Every 2 working hours
Priority 2	Phone / Email	2 working hours	48 hrs	Every 4 working hours
Priority 3	Phone / Email	4 working hours	3 working days	Every 8 working hours
Priority 4	Phone / Email	48 hrs	5 working days	Daily

Availability and Planned Maintenance

For a service of this nature, it is important that the solution is kept up to date with the latest patches released by Operating System and Software / Hardware vendors. In most cases this work will be carried out without disruption to the user, however, disruption may be unavoidable from time to time.

For this type of maintenance Synalogik will notify the customer 5 days in advance of any planned maintenance windows unless deemed critical to the security of the platform. Work will be completed outside of normal business hours e.g., 18:00hrs to 06:00hrs to minimise any impact this may have.

Training

Synalogik provide standard new user training packages. Further training can be customised to suit client need, including: SuperUser Training, Risk Assessment Training and Search Templates Training.

User Guides

- Online self-help portal - with search functionality for the user
- Business Hours Helpdesk - to answer any queries about the product
- 1 x 90-minute basic user session giving introduction to the functions and capability within the Scout® platform
- 1 x 30-minute extension to the 90-minute basic user session for super-users to deal with managing users' permissions
- Videos in the self-help portal, covering all aspects of the platform's functionality
- Regular user clinics hosted online on various new areas of functionality

Synalogik can also provide training on any aspect of intelligence, investigation or internet-based enquiries, including bespoke courses designed to your needs.

Proof of Concepts and Trials

Synalogik usually offer new customers a complimentary 20-day trial of the core Scout® platform (for up to 5 Users) to demonstrate functionality and operational value. In advance of any trial, appropriate contracts for Data Protection purposes need to be agreed and signed.

Related Scout Products

Scout® Supporting Services

Scout® Training

Acceptable Use

The customer responsibilities include:

· Completing any whitelisting, firewall and security accreditations required for the use of the platform

· Data ownership / agreement with relevant third-party data providers, if required,

· Identify users and contact email addresses

· Ensuring user logins and passwords are kept secure are not shared

· Ensuring that users are appropriately available to be trained

· Ensuring appropriate Internet bandwidth is available

In addition to the Data Protection requirements of Scout®, when each user logs into Scout®, purchasing organisation shall adhere to the following acceptable use policy for the management of the licence software:

· Each Scout® licence is for a named individual and cannot be shared or used in a concurrent model

· Scout® licences can be revoked by the customer and re-issued to another user during the contract period

· You may not share, rent or lease Scout® access credentials to any other individual or entity, for any reason

· You may not sub-license Scout® access credentials to any other individual or entity, for any reason

· You may not issue our access credentials licences to any third party's that are not employed by your Organisation, without written authorisation from Synalogik Innovative Solutions Ltd.

Company Overview

Synalogik Innovative Solutions Ltd ("Synalogik") is a privately-owned company that was formed to deliver solutions, to both the public and private sectors, based around the process automation of data gathering, analysis, risk scoring and report writing for the intelligence and investigation communities or indeed any role or department that complete the laborious manual researching of databases.

Founded in 2018, Synalogik was conceived with a specific objective: to undertake intelligence and investigations differently, to empower investigators to exploit data to prevent and detect non-compliant behaviour and criminality. As the volume of data available to investigators has continued to expand, Synalogik has continued to evolve our product offering to combat current tactics; every Synalogik customer gets the most updated version of Scout® at no extras cost, throughout the contract term.

Synalogik's proprietary intelligence and investigation platform Scout® is based in AWS, highly secure and operationally proven to lead to significant efficiencies in time and investigation success.

Scout® is the market leader in providing an automated Open-Source Intelligence & Investigation platform for HMG, law enforcement agencies and other public sector authorities.

Synalogik Innovative Solutions Ltd

Unit A, The Courtyard

Tewkesbury Business Park,

Tewksbury

United Kingdom

Company Registration number 11601168s

For more information on the services we offer please consult our secure website at the following URL: WWW.SYNALOGIK.COM or email public.sector@synalogik.com