COMPANY OVERVIEW & SERVICES

SEC-INT



Prepare for the world ahead.

Protect your people.
Strengthen your decisions.

Intelligence that brings the picture into focus.
Threat awareness training that turns understanding into action.

INDEPENDENT. AMERICAN-BRITISH. PRACTICAL.

sec-int.co

01 / SEC-INT

Clarity before commitment. Preparation before pressure.

An independent security training and intelligence company helping people recognise risk, protect information and make better-informed decisions.

The details connect. The picture becomes clearer.

A convincing applicant. An unusual supplier request. A change in overseas markets. A conversation that asks a little too much. SEC-INT helps you examine what these signals mean for your organisation and choose a proportionate next step.

THREAT AWARENESS

Prepare your people

Live online and in-person briefings, workshops and exercises that build practical verification, information-handling and reporting habits.

MOSAIC / MIRROR

Understand your position

Focused research for a business decision; an outside view of your exposure; continuing review through MIRROR WATCH.

THE DAILY MOSAIC

Keep the world in view

Selected global developments, business consequences and practical questions, with personalised options for your priorities.

COMPANY OVERVIEW & SERVICES / CONTENTS

03-04 Purpose & background
05-06 Mosaic, MIRROR & WATCH
07-08 The Daily Mosaic
09-16 Training pathways
17 Media & press
18 Start a conversation

WHY WE OFFER THESE SERVICES

Because the consequences are personal.

Behind every organisation are people who have invested years of work, trust and hope in its future.

A business is more than its balance sheet. It is the salary a household depends on, the reputation a founder has spent decades building, the confidence a customer places in a promise and the team that expects to return to work tomorrow.

When the world changes, those commitments do not disappear. A conflict can unsettle a supply chain. A convincing deception can exploit a trusted relationship. A disruption that once felt distant can suddenly affect the people at your door.

We offer these services because people deserve the chance to prepare. They deserve clear information, honest acknowledgement of uncertainty and practical skills they can use when a decision becomes difficult.

Our purpose is to give organisations time to ask better questions, protect what they have built and support the people who depend on them. Intelligence helps make change understandable. Training helps people meet it with confidence.

Recognise the threat. Protect what matters.

Preparedness starts with a clearer picture and people who know what to do next.

02 / ABOUT SEC-INT

Experience behind clearer judgement.

Independent American-British perspective. International backgrounds. Practical application.

Grounded in hands-on intelligence work.

The SEC-INT team includes former intelligence professionals from international agencies. That experience informs the questions we ask, the way we assess information and the scenarios we use to help people learn. SEC-INT operates independently as a private company; previous agency service forms part of our professional background.

Specialist understanding, made usable.

An organisation’s value often lies in its expertise, information, relationships and access. The same everyday interactions that help it grow can create exposure. We translate counterintelligence principles into clear guidance about targeting, deception, information sharing and protective judgement.

OUR APPROACH

Clear thinking

Separate evidence from assessment. Explain the reasoning. Make uncertainty visible so decisions can reflect what is actually known.

OUR APPLICATION

Relevant learning

Connect specialist concepts to recruitment, professional conversations, digital footprints, travel and leadership responsibilities.

OUR STANDARD

Proportionate action

Encourage verification, context and appropriate reporting. Support fair treatment, employee welfare and existing organisational procedures.

03 / MOSAIC & MIRROR

Know more before your next move.

Mosaic Reports connect public information about an organisation, opportunity or market to the decision you need to make.

A focused question. A researched answer.

Before an important meeting, a prospective partnership, market expansion or strategic commitment, you need more than a collection of search results. A Mosaic Report brings relevant findings together, explains their implications and shows where further checking is needed.

What the report can examine

Research may cover leadership, organisational activity, competition, market position and relevant risks. The scope starts with your question, keeping the work tied to the decision rather than producing information for its own sake.

What you receive

A written report tailored to the agreed brief: relevant sourced findings; an assessment of implications, risks and opportunities; and clear uncertainties and follow-up questions. Evidence and assessment are distinguished so you can see what supports the conclusions.

When to use Mosaic

Use it to prepare for a significant meeting, understand a potential business relationship, assess a market or challenge assumptions before committing time and resources. Its value is a stronger basis for discussion and further scrutiny.

Illustrative decision question

“Before we commit to this relationship, what should we understand about the organisation, its market and the questions still unanswered?”

03 / MOSAIC & MIRROR CONTINUED

See your organisation from the outside.

MIRROR examines exposure. MIRROR WATCH keeps agreed changes in view as your organisation evolves.

MIRROR / Understand what others can connect.

Websites, recruitment adverts, professional profiles, announcements and publications can reveal more together than they do separately. MIRROR uses lawful public sources and information you are authorised to provide to assess what an outsider could learn, infer or value.

Exposure translated into protective priorities.

Depending on scope, outputs can include an external-view dossier, a map of connected disclosures, an assessment of professional-contact pathways and prioritised recommendations. The assessment explains plausible approaches while distinguishing established facts from inference. Public visibility alone does not establish compromise.

MIRROR WATCH / Keep the picture current.

Recruitment, contracts, partnerships and public announcements change an organisation’s footprint. Through an ongoing contract, SEC-INT reviews agreed sources, assesses significant changes and provides updated findings and leadership briefings.

A defined intelligence relationship.

Before work begins, we agree the scope, review frequency, significant-change criteria, deliverables and contract terms. This gives leaders a clear basis for revisiting protective priorities as their business changes.

Three different starting points

Mosaic: a decision to understand. MIRROR: exposure to assess. MIRROR WATCH: agreed exposure to keep under review.

04 / THE DAILY MOSAIC

Global events. Business consequences.

Selected news and analysis that explains what has happened, why it matters and what deserves attention next.

Important developments can disappear beneath competing headlines, political spin and outrage. The Daily Mosaic selects consequential stories across conflict, geopolitics, cyber threats, fraud, supply chains, infrastructure and climate-related disruption. It connects the wider picture to practical decisions for business and communities.

3 STORIES / 5 DAYS A WEEK

Free Edition

A focused global briefing, free to subscribe, delivered to your email inbox. Significant developments, context, potential implications and what to watch.

5 STORIES / 5 DAYS A WEEK

Personalised

A custom briefing shaped around your company, sector and agreed priorities, sent privately by email. The analysis considers developments in your business context.

5 STORIES / 7 DAYS A WEEK

Personalised Plus

Tailored coverage every day, including weekends, plus separate emergency email alerts for urgent developments relevant to agreed priorities.

For personalised services, coverage priorities, recipients and delivery arrangements are agreed in advance. Personalised Plus also requires agreed alert triggers and coverage arrangements. Email alerts support awareness alongside established emergency procedures.

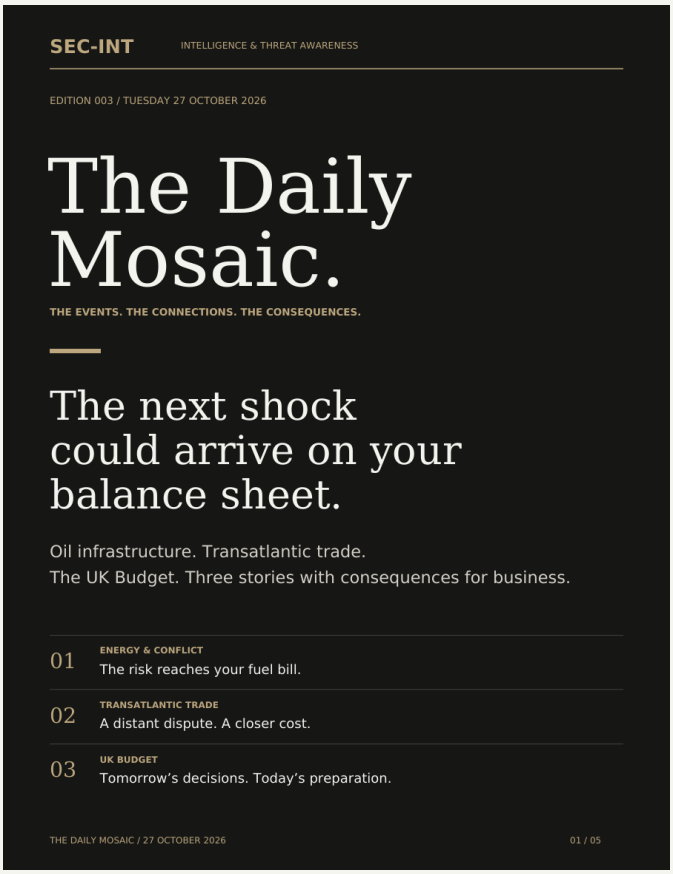
Read & subscribe free

Discuss tailored coverage

05 / THE DAILY MOSAIC IN PRACTICE

The events. The connections. The consequences.

A dated example from Edition 003, published 27 October 2026. The sample below shows how the briefing connects news to business decisions.



ACTUAL EDITION / PDF COVER

Energy & conflict

A reported claim concerning Saudi oil infrastructure prompts questions about fuel, freight and fixed-price commitments. The edition notes that the strike and operational effects were unconfirmed.

Transatlantic trade

An aircraft-financing dispute raises questions about contracts and who would absorb changing import costs. The edition distinguishes a warning from an announced tariff.

UK Budget

A Budget preview prompts employers to prepare payroll, staffing and investment assumptions, while separating expectations from final measures.

Each briefing combines sourced reporting with SEC-INT analysis, explaining the potential business implications and the developments to watch next.

Dated showcase from SEC-INT's own edition. Reporting and assessments reflect its publication cut-off and may develop. Visit sec-int.co/daily-report for the published briefing and its sources.

06 / SEC-INT TRAINING

Awareness becomes valuable when people can use it.

Live online and in-person briefings, workshops and scenario exercises built around real responsibilities.

Recognise. Verify. Protect. Report.

Training gives people a shared way to recognise suspicious approaches, check identity and authority, protect sensitive information and raise concerns through the right channels. Examples can reflect your industry, working relationships and existing procedures.

NOTICE & QUESTION

Recognise the approach

Understand unusual requests, manipulative contact, impersonation and attempts to build inappropriate trust or access.

CHECK & PROTECT

Verify before acting

Practise independent identity checks, sensible information boundaries and proportionate responses to urgent or AI-enabled requests.

RECORD & REPORT

Respond within your role

Document relevant facts, preserve useful information and coordinate with the people responsible for the response.

Audiences include leadership, HR, security, IT, operations, procurement, travelling staff, sworn officers and civilian personnel. Sectors include professional services, technology, government, utilities, education, agriculture, insurance and non-profits.

Eligible programmes may provide a numbered SEC-INT Certificate of Completion, with requirements agreed in advance. This records private training; it does not confer government qualifications, security clearance, professional licensing or academic accreditation.

07 / ORGANISATIONS TRAINING

Protect the decisions your people make.

Practical sessions for staff and managers who handle requests, conversations, information and trusted access.

35 MIN / STAFF & MANAGERS

That Wasn’t the CEO

Recognise impersonation cues, challenge urgency and verify authority before money, information or access changes hands.

40 MIN / STAFF & MANAGERS

Under the Influence

Recognise pressure and manipulative contact, practise professional boundaries and know when to raise a concern.

60 MIN / STAFF & COMMUNICATIONS

The Digital Shadow

Understand what public digital traces reveal about roles, relationships and routines, and reduce avoidable exposure.

60 MIN / TRAVELLING & REMOTE STAFF

Beyond the Office

Protect conversations, devices and professional information during travel, conferences, events and remote work.

35 MIN / STAFF & PEOPLE MANAGERS

The Insider Pathway: Workforce Edition

Recognise unusual access and information handling through observable facts, with a supportive reporting approach.

60 MIN / PROCUREMENT & VENDOR OWNERS

The Trusted Door

Review supplier and contractor access, protect information boundaries and recognise requests needing verification.

Individual sessions or a tailored programme. Listed catalogue timings, delivery and adaptations are agreed before booking.

07 / ORGANISATIONS TRAINING CONTINUED

Build a coordinated response when the pressure rises.

Focused learning for leadership, operational teams and the people who turn a concern into an organisational response.

60 MIN / MANAGERS & RESPONSE LEADS

When Suspicion Begins

Turn an initial concern into factual documentation, preserve relevant information and use agreed reporting routes.

60 MIN / STAFF & DECISION-MAKERS

False Signal

Evaluate sources, verify claims and communicate uncertainty when rumour or misinformation affects decisions.

90 MIN / EXECUTIVES, SECURITY & RISK

The AI-Enabled Human Target

Examine AI-generated impersonation, synthetic identities and executive targeting; strengthen high-value verification.

75 MIN / PROCUREMENT, OPERATIONS & RISK

Supply Chain Shock

Map critical inputs, supplier alternatives and knock-on effects to support practical responses to interruptions.

90 MIN / LEADERS & SUPERVISORS

Leading Under Pressure

Work through competing priorities and incomplete information; make assumptions visible and coordinate decisions.

2-3 HOURS / CROSS-FUNCTIONAL TEAMS

The Tabletop Test

Test response arrangements through a facilitated scenario, identify capability gaps and capture improvement priorities.

Report findings can help focus training priorities. Module selection and scenarios are agreed with your team and aligned with existing policies.

08 / HUMAN RESOURCES

Recruit confidently. Protect trust at work.

Three focused courses for recruitment, employee welfare and HR’s role in insider risk.

Is This Candidate Real? / 45 minutes

For recruiters, HR teams and hiring managers. Examine AI hiring fraud, synthetic applicants, proxy and deepfake interviews, and identity inconsistencies. Strengthen consistent verification from application through secure onboarding, and route concerns before access is granted.

Under the Influence: HR edition / 45 minutes

For HR, people managers and employee-relations teams. Recognise coercive influence, isolation, loyalty demands and manipulative mentoring. Use observable conduct to support responsible escalation while keeping employee welfare in view.

Before the Breach / 60 minutes

For HR leaders, employee relations and people managers. Clarify HR’s contribution to insider-risk response, including pressure, coercion, unusual access, data hoarding and departures. Connect observations to privacy, factual documentation and coordinated action.

The complete pathway contains 150 minutes of listed course content. Breaks, discussion, scheduling and adaptations are agreed separately. Each course can also be selected as a standalone session.

Fair decisions. Consistent checks. Clear reporting.

Case-led workshops connect HR observations with security responsibilities, employee support and your agreed escalation arrangements.

09 / LAW ENFORCEMENT

Protect people, information and public trust.

The Advanced Counterintelligence Threat Course: ten modules applied to agency personnel, information and trusted relationships.

01 **The Modern Espionage Threat**
Why personnel, sensitive information and trusted access may attract intelligence interest.

02 **SEC-INT MIRROR**
Assess public exposure from an external perspective and prioritise protective questions.

03 **The Human Target**
Recognise elicitation and relationship-based approaches, with safe boundaries and reporting.

04 **The Insider Pathway**
Assess access, pressure and observable conduct with fairness, welfare and escalation.

05 **The Digital Shadow**
Understand how digital traces expose personnel, routines and agency relationships.

06 **The Trusted Door**
Examine vendor and contractor exposure, information sharing and trusted access.

07 **The Psychology of Espionage**
Understand influence and pressure through behaviour, context and professional judgement.

08 **Espionage at Machine Speed**
Recognise AI-enabled profiling and impersonation; practise verification habits.

09 **Beyond the Office**
Protect information during travel, events, remote work and informal contact.

10 **When Suspicion Begins**
Record facts, preserve relevant information and coordinate an authorised response.

The Counterintelligence Defence Series supports the programme in ebook and paperback. Timing, sequencing, module depth and coursebook supply are agreed with the agency.

09 / LAW ENFORCEMENT CONTINUED

A shared standard. A disciplined response.

Focused agency briefings and workshops for sworn personnel, civilian staff, supervisors and command teams.

90 MINUTES

Northern Ireland Intelligence Briefing

Public-source lessons on information discipline, officer exposure, intelligence sharing, ethical escalation and community trust.

90 MIN / ADAPTABLE BY ARRANGEMENT

Counterintelligence Awareness

An introduction to suspicious approaches, sensitive information and agency reporting; 60- or 120-minute formats by agreement.

2 HOURS

Supervisor Workshop

Practise measured assessment, factual documentation and appropriate escalation when a colleague raises a concern.

2-3 HOURS

Suspicious-Approach Tabletop

Test recognition and reporting arrangements using a simulated approach, without active or sensitive case material.

60 MIN EACH / SEPARATE SESSIONS

Digital Exposure / Drone Awareness

Digital Exposure: reduce online disclosure. Drone Awareness: safe observation, useful documentation and correct local reporting.

90 MIN / 60 MIN / SEPARATE SESSIONS

Information Handling / Vendor Exposure

Strengthen sensitive-information handling, or examine vendor and contractor information sharing and access.

Agency policies, authorised roles and reporting routes frame delivery. Learning emphasises observable behaviour, evidence, fairness and professional judgement.

10 / COMMUNITY TRAINING

Prepared households.
More confident communities.

Plain-language learning for adults, parents, carers and community groups. No specialist background required.

Beyond the Fake / AI fraud & impersonation

Recognise cloned voices, altered media, fake profiles and requests built around urgency or secrecy. Practise independent contact checks before sending money or sharing personal information.
Practical takeaway: a repeatable pause-and-verify routine.

When Streets Change / Civil unrest & disruption

Plan for interrupted journeys, changing crowd conditions and public disorder. Check official alerts and transport updates, avoid confrontation and prepare household contact arrangements.
Practical takeaway: a personal disruption plan focused on distance, communication and safer choices.

Ready at Home / Emergency & disaster planning

Prepare for severe weather, power cuts, sheltering or evacuation. Consider contacts, supplies, documents, communications, children, medication needs, accessibility and pets.
Practical takeaway: a household checklist to complete, share and review.

Your Digital Shadow / Privacy & account protection

Review public profiles, sharing permissions and location details. Strengthen passwords, two-step verification and account recovery while recognising suspicious messages.
Practical takeaway: a prioritised privacy and account-security review.

10 / COMMUNITY TRAINING CONTINUED

Useful skills. Everyday decisions.

Realistic examples, guided discussion and practical planning, delivered live online or in person.

Everyday Awareness / Personal safety

Notice changes in behaviour and surroundings, set boundaries, create distance and identify safer places. Verify unfamiliar callers or visitors and seek appropriate help.
Practical takeaway: a simple framework for recognising a concern and choosing a safer next step.

Before You Go / Travel awareness

Use official destination advice, check arrangements and protect documents, devices and personal information. Consider backup transport, accommodation and communication.
Practical takeaway: a pre-travel checklist and clearer backup plan.

Under Pressure / Manipulation & online relationships

Understand how apparent friendship, romance, authority or opportunity can lead to secrecy, urgency or requests for money. Practise independent checks and seeking support without blame.
Practical takeaway: a clearer way to assess a request and discuss concerns with someone trusted.

Check the Story / Misinformation & crisis rumours

Check original sources, dates, locations and context. Compare alarming claims with relevant official updates and decide what is appropriate to share.
Practical takeaway: a source-checking routine for calmer, better-informed decisions.

Session length, format and group arrangements are confirmed on enquiry. Emergency planning follows relevant local authority guidance; personal safety focuses on awareness, avoiding confrontation and seeking help.

11 / MEDIA & PRESS

Clear insight.
Beyond the headline.

Interviews. Written comment. Podcasts and broadcast. Background briefings.

Explain the event. Explore the consequences.

SEC-INT helps journalists make the human side of security understandable: how people, trust and everyday information create exposure, and what organisations can do about it. Our wider Daily Mosaic work connects current affairs to business and community preparedness.

A broader conversation about risk.

Commentary topics include suspicious recruitment and false identities; the connections hidden in public information; elicitation, conversation and influence; and the everyday risks involving colleagues, contractors, professional networks and travel. The focus is on behaviour, context and practical implications.

Measured explanation, grounded in experience.

Hands-on intelligence experience informs our perspective. We distinguish what is known, what is assessed and what remains uncertain, with care over evidence, confidentiality and the limits of any assessment. Counterintelligence is explained through the practical task of protecting information and trusted access.

Requesting an interview or comment.

Include your name and publication or programme, story angle, questions, deadline and time zone, format and interview length. Availability depends on the subject, deadline and confidentiality requirements. Attribution and background-briefing terms should be agreed in advance.

Press enquiries

12 / CONTACT SEC-INT

Prepare before the pressure arrives.

Start with the decision you need to understand, the people you need to prepare or the exposure you want to examine.

Tell us what matters.

A useful first enquiry includes your organisation and role; the service you are considering; your main concerns; and the audience, deadline or delivery preferences that matter. A short general outline is enough to begin.

Define a practical next step.

We will clarify your priorities and discuss a relevant training option, report scope or briefing service. For training, that means the right audience and scenarios. For intelligence, it means a defined question, relevant sources and agreed deliverables.

Choose your starting point.

An upcoming hiring round. An important business relationship. A team handling sensitive information. A need to understand changing global conditions. You do not need to have a complete brief before starting the conversation.

Start a conversation

sec-int.co/contact

Keep initial enquiries general.

Agree suitable channels before sharing sensitive material.

SCAN TO CONTACT