

TRACK 1 · TRADecraft

Beyond the Breach: Understanding the Digital Black Market

How hackers target companies, what motivates them, and what happens to data after a breach

DURATION	FORMAT	SKILL	MAX	COURSE LEAD
2 days	Workshops + Case Studies + Live Demo	Beginner	12 - 14 students	Redacted

Data doesn't disappear after a breach. It circulates, gets traded, re-sold and weaponised — sometimes for years. This course gives participants a practical and grounded understanding of why organisations are increasingly targeted, how attackers obtain and monetise sensitive information, and what the long-term consequences look like.

Through real-world case studies, current threat intelligence, and live demonstrations, participants explore the full lifecycle of stolen data — from the moment of compromise through to underground marketplace trading, exploitation, and the downstream operational, financial, legal and reputational damage that follows.

The course concludes with practical, intelligence-led lessons that participants can apply directly to their own organisations: understanding exposure, interpreting underground activity as an early-warning signal, and building more resilient defences.

TARGET AUDIENCE

- Security officers,
- CISOs,
- Privacy officers,
- CEOs,
- CFOs,
- General counsel,
- Crisis communications leads,
- Risk and compliance officers,
- Board members and senior executives with accountability for organisational resilience.

PRICING

Individual	€1,899 / seat (Ex-VAT)
Custom	Custom pricing on request

Tier 2 covers bespoke in-house delivery for companies and teams, adapted to your threat environment.

→ **Practical component:** Threat actor profiling exercises, group discussions, scenario analysis, and a live demonstration of how dark web databases and leak sites are used by both attackers and investigators.

→ **Custom Target Audience:** Critical infrastructure operators (energy, water, transport, healthcare), Financial institutions and fintech, Logistics and supply chain companies, Data centres and Cloud service providers, Legal and professional services firms, Public sector and Government agencies and Any organisation subject to NIS2 obligations.

LEARNING OBJECTIVES

- Understand today's cyber threat landscape and threat actor motivations
- Explain why organisational data has become a high-value commodity
- Identify categories of threat actors and their objectives
- Understand how cybercriminals obtain sensitive organisational data
- Trace the journey of stolen data from compromise to exploitation
- Recognise the long-term impact of data breaches on organisations
- Identify your own exposure through dark web monitoring techniques
- Apply practical lessons to strengthen cyber resilience

SCHEDULE

Day 1

MORNING SESSION

- Course introduction and objectives
- The current cyber threat landscape: who is attacking, and why
- Why organisations are targeted: sector, size, data type and opportunity
- Why data is the new gold: what makes organisational data valuable and to whom

— *Lunch break* —

AFTERNOON SESSION

- How threat actors obtain data: phishing, supply chains, insider threats and zero days
- What happens when your data is exposed: from breach to dark web listing
- Operational, financial, legal and reputational consequences
- Lessons learned and best practices from real incidents

Day 2

MORNING SESSION

- Threat actor profiling: motivation, intent, capability and behaviour
- Financially motivated vs state-sponsored vs hacktivist actors
- How exposed data enables credential attacks, fraud and extortion
- Case studies: tracing real attacks from exposure to exploitation

— *Lunch break* —

AFTERNOON SESSION

- Live demo: dark web databases and leak sites (attacker and investigator view)
- What organisations can learn from underground activity
- Intelligence-led defence: translating dark web monitoring into practical, actionable risk reduction

WHAT YOU TAKE HOME

- Field Dossier — printed handbook of every lesson, framework and case study
- Cheat Sheets — threat actor profiling cards and breach response reference
- Granted Access — real world practitioners from Birdwatcher Group and its network
- Tradecraft Toolkit — dark web monitoring and OSINT tools with setup notes
- After Care — up to 6 months of direct email access to your course lead

Register for this course now!

Email us at: trainings@birdwatchergroup.com OR fill in the form on our website: www.birdwatchergroup.com/intelligence-nest