CYBERSECURITY INCIDENT RESPONSE EXPERT

Who we are

Approach Cyber is a pure-play cyber security and privacy company.

Approach Cyber has been providing cyber security services to international clients for over 20 years and employs around one hundred experts in the field.

At Approach, we believe that everyone deserves **digital peace-of-mind**. This is our vision, our aspiration for a society where each and every one is reassured, where there is **confidence** and **security** in the digital world. Therefore, our role is to bring **cyber serenity** to society.

Every day, we take **care** of our clients' cyber security while they focus on their business. We help them to prevent, withstand and recover from cyber security incidents and enable them to keep their full attention on their core activities.

We offer **360-degree solutions** to improve our customers' cyber resilience: anticipate, prevent, protect, detect, respond and recover. We are committed to delivering **top-notch services**: consulting and audit, training and awareness, security technology integration and software development. Approach is also a true Managed Security Service Provider (MSSP) thanks to our shared Security Operations Centre (SOC).

Our ambition

Having achieved sustainable growth in Belgium (Approach is regularly listed among the "Trends Gazelles" and is one of the key cybersecurity leader in Belgium), and recently opened of a new office in Switzerland, the company now aims to accelerate its development in Belgium and Europe.

From around 100 people currently, our goal is to make all our teams grow while keeping and strengthening our values and company culture in a balance between top-notch services and management, no-nonsense mindset, and a dose of humanity in our internal and external contacts.

Who we are looking for

We are currently actively looking for **key people** who will run and improve our **Digital Forensic & Incident Response Services** (**DFIR**) and co-create innovative solutions for our human-sized clients.

In the team, we **provide expert support and assistance through challenging situations.** We offer calm and **decisive action to mitigate crisis** effectively. Thanks to our guidance, our clients can navigate uncertainties with **confidence**, knowing they have a **dedicated partner** by their side every step of the way.

In this frame, we are recruiting a **Cybersecurity Incident Response Expert** who will play a key role in ensuring our team and services growth over the next few years.

Your Role

As a **Cybersecurity Incident Response Expert**, you'll integrate our **close-knit SOC Business Unit** where around **20 multi-disciplinary experts** (Red teamers, pentesters, technical experts, SOC analysts, …) work side by side every day.

You'll become your **colleague's reference** within the SOC/Blue team for what concerns our Incident Response strike force.

We expect you to take **various responsibilities** which could be represented as a mix between

- **Hands-on actions** in the frame of incident response operations:
  - Perform data acquisition on various system and network,
  - Collect and preserve artefacts and IoC,
  - Collaborate with threat intelligence,
  - Perfom forensics analysis,
  - Perform threat hunting campaign,
  - Apply containement and eradication measures in the context of our clients incidents.

- Comprehensive **management of cyber attacks** from both a **technical and human** perspective:
  - Take the leadership on critical cyber incidents occurring at client
  - Be our customers trusted point of contact in case of cyber attack
  - Define & implement threat containment and eradication strategies
  - Advise customers in the set up of IR plan

- Organize and Orchestrate efforts and resources through crisis resolution
- Provide clear and concise reporting (C-level and technical) and contribute to take the right decision
- Collaborate with external stakeholders like client's IT teams, authorities, …

- Internal responsibilities like **coaching** of colleagues and asset/**solution co-creation**:
  - Coach and follow our SOC/DFIR Analysts to ensure that processes/tools are followed, and technologies are mastered.
  - Design,implement and improve organisation, processes and technologies required to deliver best-in-class cyber security services to our customers,
    - Drive the evolution of our solutions, keeping abreast of new developments, emerging technologies and threats

Your profile

You have :

- Minimum **5 years of experience** managing complex cyber crisis, as a DFIR expert or Incident Response leader.
- People oriented with excellent communication skills and assertiveness
- Trustworthyness and strong stakeholder management (of all types and levels) skills, emergency and crisis management
- Strong Cybersecurity acumen, "risk-based" thinking
- English, French and/or Dutch is a must have.

Considered as a plus:

- Certifications in cyber security like GIAC Certified Incident Handler Certification (GCIH), GIAC GCFA or GCFE, or equivalent.
- A first use of incident response and threat analysis tools like Microsoft Sentinel, Time sketch, Velociraptor, OpenSearch, Microsoft Defender for Endpoint, FTK, Plaso, Log2Timeline, …
- Familiarity with threat analysis frameworks like MITRE ATT&CK

Mindset:

- Willingness to provide high quality deliverables and to go the extra mile
- Helicopter view and ability to take into account all the elements of a context
- Teamplayer
- Manage diverse workloads and prioritize accordingly
- Ambassador for the professional values that are at the heart of our philosophy:
    - TOP-NOTCH

      We strive for best-of-the-best while staying up to date with the latest technology.
    - HUMAN-CENTRIC

      We care about people in the digital world, listening before interacting respectfully in a responsible environment.
    - NO-NONSENSE

      We go for it, we work together, we are committed to deliver, to exceed expectations.

Our offer

- Join a dynamic and fast-growing company in a booming sector
- Participate in the development of the company as a co-creator of innovative solutions
- Drive ambitious incident response projects from the business situation up to the resolution, taking direct decisions while keeping a concrete view of the human-scale IT networks at our customers' sites, and direct contact with the C-level client sponsor
- Develop your career path and add top-level trainings and certifications to your CV
- Benefit from an attractive salary package, including a full range of benefits:
    - Company car and fuel card
    - Competitive group insurance including pension fund, death, and disability coverage,
    - Attractive complementary insurances for non-work-related accident and loss of salary in case of sickness, company fully supported contribution
    - 32 days holiday/year (on a fulltime equivalent basis)
    - Flexible home working policy
    - Other fringe benefits (meal vouchers, eco vouchers, …)
- Fun company events, exclusive team experiences

- Contribute to a safer, fairer world for data subjects and citizens, ensure the serenity of great businesses and essential public institutions
- Live your values daily in a dynamic, fun and multicultural working environment.

Interested?

Don’t wait and send us your CV and application to jobs@approach-cyber.com. Join us in our commitment to deliver cyber serenity and contribute to a safer digital world.