
TRIDENT
SEARCH
CYBER TALENT
SOLUTIONS
IN OPERATIONAL TECHNOLOGY

OPERATIONAL TECHNOLOGY

In the rapidly evolving cyber landscape, the convergence of IT (Information Technology) and OT (Operational Technology) has become increasingly clear. While IT focuses on data storage, networks and software, OT is concerned with the hardware and software that monitors and controls physical devices, processes and events. As most industries embrace modern digital transformation, OT devices have been increasingly exposed to cyber threats, and the space is rapidly becoming an epicentre for investment to protect critical assets.

Even though OT is a fairly new area within cyber security, there's no doubting the industry's commitment to safeguarding it. Yet this urgency is met with a significant challenge – a scarcity of skilled professionals, creating a unique set of challenges for those desperately trying to push back against the attackers.

Operational Technology

Operational Technology refers to the hardware and software used to monitor and control physical processes in industries such as manufacturing, energy, utilities, and transportation. Unlike traditional IT systems, OT systems deal with real-time processes and the management of physical equipment like sensors, actuators and controllers. This integration of IT and OT has introduced a myriad of benefits, but it also exposes critical infrastructure to cyber threats.

The cyber security challenge

In the past, OT devices have been safe within their “air-gap” of isolation. Yet with the interconnectedness of the modern world, and the increased sophistication of threat actor methods, the risk level has significantly increased and we’re seeing a rise in cybercriminal activity on physical assets.

In fact, given the use of OT in industry, manufacturing and healthcare, amongst other industries, OT cyberattacks actually tend to have more severe consequences than those in IT. They can lead to catastrophic outcomes like shutdowns, outages, leaks and even explosions. Data from 2021 shows us that 35% of publicly reported OT cyberattacks had physical consequences, resulting in estimated damages of $140 million per incident.

There are a number of issues involved in protecting OT assets from cyberattacks, including:

Legacy systems: Many OT environments still rely on decades-old legacy systems that were not designed with security in mind. Updating these systems can be complex and expensive, leaving them vulnerable to modern threats.

Interconnectedness: The increased connectivity of OT systems to the Internet of Things (IoT) and corporate networks creates more entry points for cyber attackers. A breach in one part of the network can potentially affect the entire operational process, and in the manufacturing context in particular this can lead to broken production lines and huge financial losses.

Lack of standardisation: Unlike IT, OT lacks standardised protocols, and that’s because there are so many different areas of this space covering every aspect of our modern lives. The methods of protecting an MRI machine are totally different to those for an ATM, and entirely separate again from a robot or a weather station. The diversity in systems and processes makes it challenging to implement uniform security measures as each technology must be viewed in isolation. It also means that you tend to have highly specialised engineers looking after particular technologies.

Overcoming the talent crisis

We certainly have an understanding of the cyber security challenges facing Operational Technology, but the real crux of the issue is the people challenges in the sector. With such a range of technical expertise required, we're seeing a real shortage of skilled professionals with good levels of cyber awareness coming through, and this is giving rise to some pretty significant security challenges.

Skills Shortage: OT had previously been a completely separate entity to IT and IoT, staffed by skilled engineers with knowledge of the physical hardware and specialised software. Yet businesses now need professionals with both technical expertise in industrial processes and cyber security know-how, in effect combining the OT and IT spheres. As this is such a new area in the industry, the required talent is still in short supply.

Unclear divisions of work: As OT and IT teams become more blended, it becomes difficult to effectively centralise, manage and govern cyber operations. Determining which parts of the process are owned by IT and OT teams can be challenging; clear roles and responsibilities need to be assigned to ensure the business can respond quickly to cyber incidents.

Training needs: The fast-paced evolution of cyber threats creates a need for continuous learning and skill development. Employers face the financial challenge of keeping their workforce up-to-date with the latest security practices and technologies.

Investment constraints: With such a shortage of trained professionals, organisations are struggling to find skilled talent to address their cyber security needs without significant investment in talent solutions and HR.

It sounds like the situation is pretty bleak, but that's absolutely not the case. The talent shortage poses an exciting opportunity for professionals to upskill or move into the OT space to meet this pressing need. We need to address the situation urgently as the volume of cyber threats in OT will only increase, so employers cannot necessarily wait for the right people to move up though the industry in the normal way. Instead, we need to be thinking outside the box.

Investment in training and education: You can mitigate the talent shortage by investing in training programmes to increase cyber-awareness within your existing OT teams and drive a security-first mindset.

Using a Talent-to-Value Protection approach: Focus on hiring for skills that directly impact risk reduction and can create security value for the business. This may mean looking outside of traditional talent pools or job titles and focussing on relevant skills instead.

Understand business priorities: With the level of demand for cyber-aware OT professionals, employers and HR teams need to prioritise meeting the most urgent business needs, and hiring strategies must be flexible enough to adapt in real-time to emerging threats or critical requirements.

Cross-Skilling initiatives: Encouraging existing IT or IoT professionals to acquire OT skills and vice versa can help create a workforce with the cross-disciplinary expertise needed for effective OT cyber security.

"To overcome the talent crisis in OT cyber security we've got to look beyond traditional approaches. I tell the businesses I work with to explore unconventional talent pools and foster cross-disciplinary collaborations to cultivate the skills of their employees. In my view, it's the only way to rapidly develop a skilled workforce capable of safeguarding our critical infrastructure."

Sean Hendon, Director at Trident Search

The Trident Search Approach

Trident Search specialises in sourcing the very best GTM and software product professionals for cyber security vendors across EMEA, the USA and MENA. We have become a trusted partner to over 100 vendors, supporting them to build high-performing teams to achieve their ARR growth metrics and gain market share.

Through our experience working with OT and IoT vendors, we have developed a deep-rooted understanding of the challenges facing those working in the sector, and of the unique position Operational Technology occupies within the cyber landscape.

As the only specialist cyber security recruitment agency offering a full wrap-around service from product to sales and marketing, we can offer advice and guidance throughout the hiring process, drawing on our extensive global network to source the best talent for your open roles.

SPEED

We work to an average of just **27 days** from sourcing a candidate right through to placement.

REPUTATION

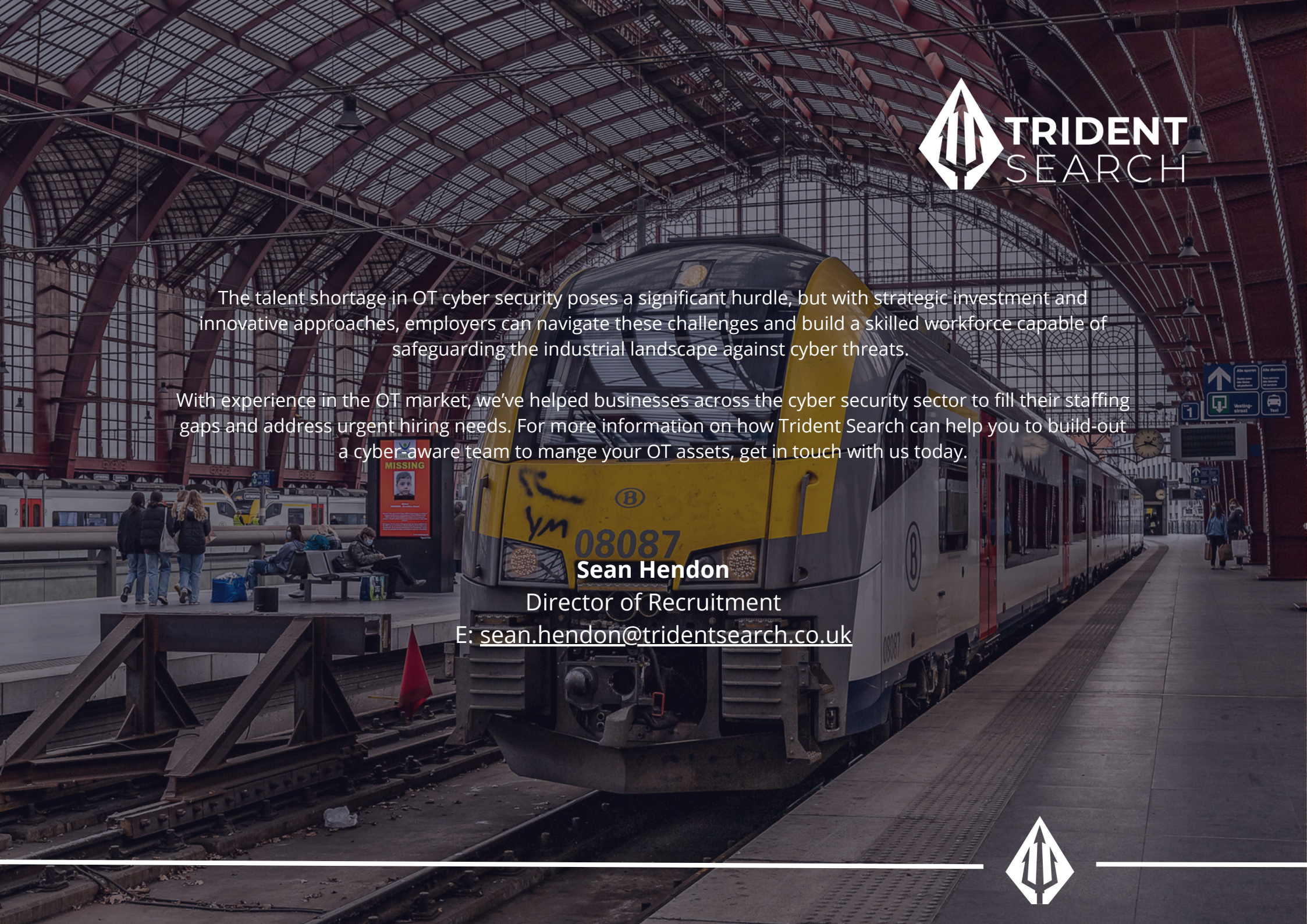
We're the highest rated cyber recruitment agency on Google, with over **150 five-star reviews**.

VETERAN OWNED

Our strong **military affiliation** connects us with clients and candidates across the industry.

REACH

Our Cyber Vendor team works extensively across **EMEA, the USA and MENA.**



The talent shortage in OT cyber security poses a significant hurdle, but with strategic investment and innovative approaches, employers can navigate these challenges and build a skilled workforce capable of safeguarding the industrial landscape against cyber threats.

With experience in the OT market, we've helped businesses across the cyber security sector to fill their staffing gaps and address urgent hiring needs. For more information on how Trident Search can help you to build-out a cyber-aware team to mange your OT assets, get in touch with us today.

Sean Hendon
Director of Recruitment
E: sean.hendon@tridentsearch.co.uk