BLUE TEAM MANAGED SERVICE

Human-driven cyber security protection, detection, and response designed for your business; providing round-the-clock defence that is tuned to combat the threats you face.

Solving the managed detection and response effectiveness problem

We routinely come across organisations with ineffective cyber security protection, detection, and response despite having invested significantly in third-party products and services.

The cyber security products and services marketplace can be challenging to navigate for buyers who are unsure on specifically what they need, and why they need it. This leads many organisations to gather a jigsaw of capabilities over time, with an array of acronymised products and services broadly tagged as SOC, SIEM, EPP, EDR, MDR, ASM, ZTA...

Without the expertise to assemble the jigsaw, combining these off-the-shelf solutions inevitably leads to a generic, decentralised, and disconnected cyber defence capability. Characterised by reactive, alert-driven detection using generic use cases and rulesets, this approach results in unreliable, low-fidelity monitoring which is not tailored or relevant to the organisation's operating model, threat profile, or digital landscape.

We designed our 'Blue Team' service to overcome these challenges and enable effective cyber security operations.

We don't believe in a generic, one-size-fits-all service model

JUMPSEC's Blue Team service is a **consultancy-led, human-driven** approach to managed cyber threat protection, detection, and response, equipping skilled analysts and investigators with the right tooling and methodologies to enable effective security operations. Our approach has evolved organically from long-term client partnerships in which we have designed tailored security solutions to meet their individual technical and operational requirements.

JUMPSEC's service philosophy means that:

- **We bring together detection, triage, investigation, and response –** many providers will help you to spot malicious activity but leave you powerless to do something about it. We seamlessly shift to investigation, containment, and response when we find something that looks suspicious.
- **We don't wait for attackers to trigger alerts –** we proactively hunt for valid threats both inside and outside the network, leveraging relevant threat intelligence to identify malicious campaigns targeting our clients' businesses, technologies, and employees.
- **We provide a single source of security operations –** we facilitate continuous human-to-human communication with our dedicated account team, providing a level of service tailored to whatever form your IT and security teams take.
- **We don't charge extra to ensure the service remains up to date –** our solution grows with your business over time without expensive upgrade and contract change clauses, and you receive continuous development and new features for the core service within the contract price.
- **We use a consultative approach to tailor the solution to client needs –** we invest in understanding the threat profile and attack surface of our clients. This enables defensive controls to be mapped to the most prevalent threats and adversarial techniques that they face.
- **We don't push a generic, out-of-the-box product with tiered pricing –** often, only the premium tier works as intended and delivers real security protection. We don't offer service levels that won't work for your business or fulfil your security needs.

Our human-driven approach defines all aspects of service delivery

All aspects of JUMPSEC's Blue Team service – across detection, response, and service delivery – place our people at the heart of what we do. Our human-driven approach provides a fully tailored and proactive solution for clients, exceeding the generic protection provided by automated, product-centric services. **The core components of our solution include:**

- **Pre-authorised remote response** by JUMPSEC's expert investigators using our proprietary intercept agent, enabling rapid containment and eradication of threats anytime, anywhere.
- **Consultancy-informed security controls** to tailor detection to your business context, designed to defend against the ways that real-world attackers will target your business.
- **Proactive manual investigations** driven by JUMPSEC hunters to uncover esoteric, difficult-to-detect threats and drive the creation of new and improved alerts.
- **Autonomous alert triage** by JUMPSEC analysts, reducing overheads by ensuring that we only engage client teams once a threat is confirmed.
- **Hands-on-keyboard interception and containment** designed to combat advanced attackers, stopping them before they can cause real harm.
- **Deep-dive technical analysis** enabling up to full reverse engineering of novel malware types by our in-house engineers.
- **Touchpoint human support** with direct access to a dedicated account team for ad-hoc queries and regular scheduled meetings.
- **Continuous service development** by JUMPSEC's engineers, regularly deploying new features and capabilities at no additional cost.
- **Tailored dashboards and reporting** informed by continuous dialogue, with real-time access to bespoke monitoring dashboards tracking the data points you care about.

The advantages of partnering with JUMPSEC

Incremental security improvement over time

Many providers rely on a generic catalogue of detection rules which are not effectively updated or tuned as digital infrastructure changes, and threats evolve in the wild. For subscribers of these services the level of security never truly improves; at best it stays the same, and at worst it depreciates as the attackers effectively invest more than the defenders.

JUMPSEC's model is designed to continuously increase the security baseline by developing broader and deeper coverage aligned with the threats faced, with defensive controls tuned to the methods and objectives that real-world attackers will have when targeting the organisation. We want your security investment to work for you and to be paid back with interest in future years.

Flexible commercial and delivery model

Managed security services and products often leverage tiered models which promise a level of protection from a recognised brand. In our experience, entry-level 'Bronze' service packages rarely perform as intended, providing generic and automated solutions which are not informed by client context.

JUMPSEC engages up front to determine the level of service and coverage that is appropriate for your business and capture any novel requirements which require engineering time. All functional improvements and updates are rolled out to clients as they are completed, at no additional cost. We don't believe in locking essential security features behind costly upgrades.

Reduced internal security overheads

Buyers of security products and services often find themselves dedicating resources in IT or security teams to monitoring security dashboards and reviewing alerts to identify false positives. This can detract from other essential operations and delay the triage and investigation of potential security breaches.

JUMPSEC frees your staff to perform their duties and reduce overheads by taking on more of the responsibility for security operations. Further efficiencies can be gained from JUMPSEC's experts driving existing security tooling to maximise the return on previous investments or demising those tools which fail to add real security value.

Don't take our word for it

"Whether we're developing our security strategies, assuring our development lifecycle processes or continually improving our SOC activities, having industry leader JUMPSEC by our side as our security partner gives us the confidence to move forward in an increasingly challenging environment."
- Greggs

"JUMPSEC consistently provides high quality and reliable support, demonstrating expert knowledge in their field and composure in challenging situations, which gives us full confidence that they are the right security partner for the job!"
- Groupe Atlantic

"They don't just give you something out of a box; they're quite willing to work with you to provide you with a solution that meets your needs."
- Hertfordshire County Council

To learn more about how JUMPSEC can support your business, get in touch at:

hello@jumpsec.com 0333 939 8080 www.jumpsec.com