MANAGED SECURITY BUYER'S GUIDE

Insight

Introduction

Everyone, from CEOs and board members to individuals in their personal lives, recognises the importance of cyber security. It is rare to go a day without encountering a news story regarding a major brand experiencing a security breach or addressing a phishing email incident. The internet is vital to so much of our business and personal lives, and the global nature of the internet also exposes us to a global set of risks.

If the "cost of cybercrime" was a country, it would have the third largest economy globally, behind only the United States and China at $9tn in 2024[1].

We are living in a time of fraught geopolitics and hybrid wars. Conflict is no longer constrained to the battlefield – nation states and state aligned actors are regularly using disruption to our digital world to further their aims in the real world. Organised crime groups have gone high-tech and have realised there are vast fortunes to be made through ransomware attacks, with unfortunately little chance of being brought to justice.

In approximately 45% of cases this year, attackers exfiltrated data within a day of compromise[2].

The regulatory environment has never been stricter – with the European Union introducing legislation such as NIS 2 and DORA which compel organisations to improve their cybersecurity.

With organisations operating in this complex environment, sandwiched between a worsening threat landscape and tough regulatory requirements, we hope this guide helps break down some of the jargon and provides a pragmatic guide to how to navigate your organisation though these turbulent times.

For non-extortion-related incidents in 2022 and 2023, the median time to data exfiltration has consistently remained under one day, meaning defenders must react to a ransom attack in less than 24 hours[3].

The risks of doing nothing

Failing to invest in robust cybersecurity can lead to severe consequences:

- **Financial Loss:** Data breaches and ransomware attacks can result in fines, legal costs, and lost revenue.
- **Reputation Damage:** A security incident can erode trust with customers and stakeholders.
- **Operational Downtime:** Cyberattacks often disrupt business processes, leading to delays and lost productivity.
- **Regulatory Penalties:** Non-compliance with frameworks like NIS2 or GDPR can result in significant fines.

While it's clear that underinvestment in security has obvious risks – over-investment in security or investing in the wrong areas is also bad for business. Too much security can frustrate employees and customers, not to mention the opportunity cost of using that budget to grow your business.

Security is always a balancing act - with the aim of achieving "just enough" security without causing other impacts on your business.

Understanding the basics

There are a bewildering range of acronyms used by the industry – vendor marketing heavily adds to confusion. It's worth knowing and understanding a few of the most common so you can be sure you are speaking the same language with vendors and partners.

Technology:

- **Endpoint Detection and Response (EDR):** Focuses on identifying and responding to threats on individual endpoints (laptops, servers, mobile devices) by providing detailed forensic data and remediation tools.
- **Network Detection and Response (NDR):** is a cybersecurity approach that uses advanced analytics, machine learning, and behavioural detection to monitor network traffic in real-time, identify anomalies or threats, and provide actionable insights to mitigate risks and improve response times.
- **Extended Detection and Response (XDR):** Goes beyond endpoints, integrating data from multiple sources (network, email, cloud) for broader threat detection and context.
- **Security Information and Event Management (SIEM):** Collects and analyses logs from across the organisation to identify suspicious activity. Great for compliance and centralising data.
- **Ingestion:** A car is useless without the right type of fuel, and the SIEM is the same. It needs to be fed with logs from your existing IT assets – and the amount of logs you ingest will have an impact on the cost of the solution. Usually measured in gigabytes per day, or events per second. (EPS).
- **Security Orchestration, Automation, and Response (SOAR):** refers to a set of tools and processes that enable security teams to streamline and automate threat detection, investigation, and response workflows. By integrating disparate security systems and automating repetitive tasks, SOAR enhances efficiency, reduces response times, and allows analysts to focus on higher-value activities.

People and Process:

- **Managed Detection and Response (MDR):** Outsourced security services that combine technology (often SIEM or XDR) with a team of experts who handle detection, investigation, and response.
- **Security Operations Centre (SOC):** A centralised team or facility responsible for monitoring and responding to security incidents, either in-house or managed by a provider.

So how do these all fit together?

A managed security service consists of people, process and technology. The technology is crucial to be able to collect all the data needed to provide insights to the people managing the service. An absolute minimum requirement is an EDR tool which provides data about what is going on at the endpoint level. Many vendors are moving beyond EDR to XDR – which includes more than just the endpoint data, to provide a wider view across the organisation.

XDR tools are great for detecting incidents "in the moment", but they typically have a more short-term view on the world. Many organisations choose to augment XDR with a SIEM solution, which holds raw log data for an extended period – typically a minimum of 90 days but can be many years. If your organisation needs to align with compliance requirements, a SIEM might be necessary.

The people and process elements usually come from the managed service provider. If you have already invested in the technology, you will need a partner who is skilled in that technology, and has built up experience, rules and detections based on that vendor so they can provide value immediately. If you have not yet invested in the technology – many partners will be happy to suggest one.

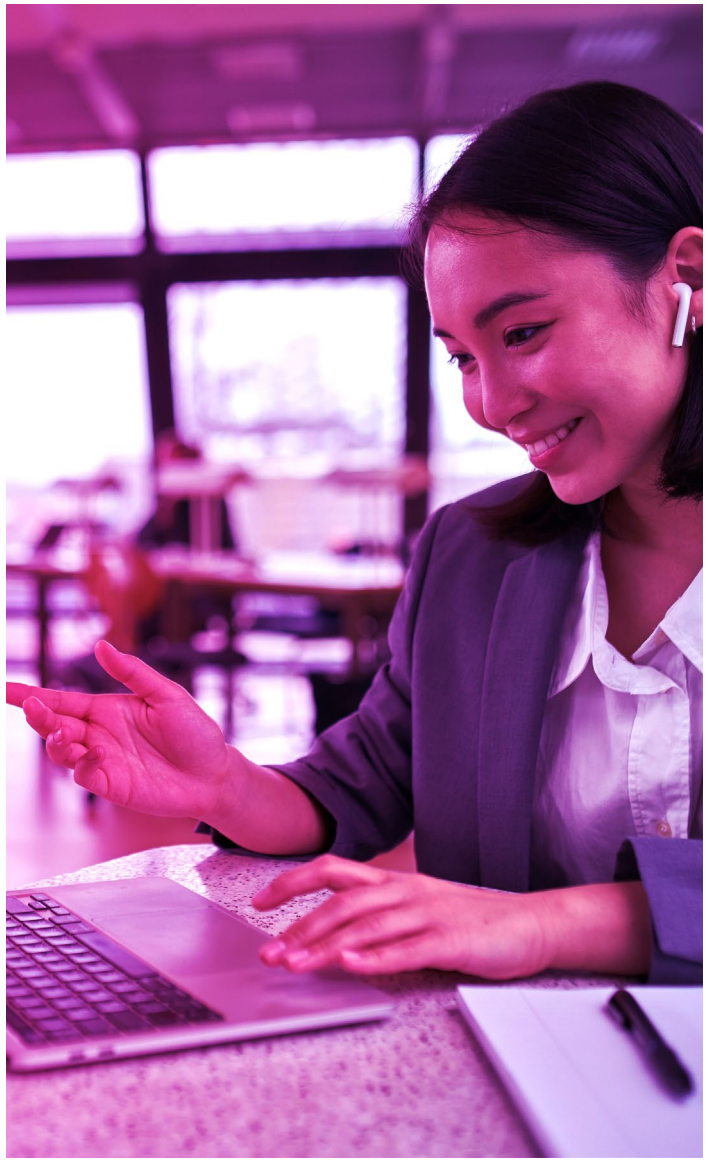
If you have decided to use a partner for Managed Security, ensure you are buying an outcome. If the technology is a proven market leader, it's more important to select a partner on the service they are offering and how well they can meet your security needs. Focus on how you will work together to improve security and let the partner worry about the technology.

SIEM vs XDR: What's the Difference?

While both SIEM and XDR are foundational technologies in cybersecurity, they serve different purposes:

FEATURE	SIEM	XDR
Primary Function	Aggregates and analyses logs for compliance and threat detection.	Unified threat detection across multiple vectors with automated responses.
Deployment Model	Typically requires in-house configuration and maintenance.	Delivered as a fully managed service or software platform.
Scope	Broad and flexible, supporting custom integrations.	Narrower scope but deeper integration between supported tools.
Use Case	Best for compliance-focused organisations with existing expertise.	Ideal for organisations seeking simplified, integrated detection and response.

Both have their strengths. Many organisations pair the compliance capabilities of a SIEM with XDR's advanced threat detection to cover all bases.



The Business Case for Managed Security

A couple of decades ago, many organisations did not consider security at all. As the first cyber threats occurred, organisations started to invest in anti-virus, firewalls and other basic security controls to keep them safe. The "security person" would manage these controls and things were simple. More threats meant more investment in new controls, however. The "security guy" become a security team, each member with a different set of skills. Securing data, applications, infrastructure, the cloud, and AI systems all require a different skill set, and all these different skill sets need to be managed cohesively to ensure end to end security coverage.

The cost and complexity of managing security internally is a barrier to entry for many. The alternative is to partner with a Managed Security Service Provider.

ASPECT	In-House SOC	MSSP Partner
Cost	High upfront costs for infrastructure, tools, and hiring.	Lower upfront costs and ongoing service costs due to paying for fractional FTE.
Expertise	Requires hiring and retaining highly skilled professionals.	Access to a broad range of expertise without the need for recruitment.
Scalability	Scaling requires additional investment in resources, staff, and infrastructure.	Easily scalable with existing infrastructure of the MSSP.
24/7 Coverage	Expensive and complex to achieve with in-house staff. Needs at least 12 individuals to cover around the clock.	Typically included as part of the service.

ASPECT	In-House SOC	MSSP Partner
Control	Full control over SOC operations, customisations and prioritisation.	Limited control, with some reliance on the MSSP's processes and prioritisation.
Implementation Time	Longer due to setup, hiring, and configuration.	Faster setup as MSSPs often have pre-built solutions and processes.
Technology Updates	Organisation is responsible for staying current with tools and technologies.	MSSPs provide access to the latest tools and technologies as part of the service.
Compliance & Governance	Full responsibility for meeting regulatory and compliance requirements.	MSSPs typically provide services aligned with compliance requirements but may not cover organisation-specific nuances.
Threat Intelligence	Requires building or subscribing to threat intelligence feeds independently.	Access to aggregated threat intelligence from multiple clients.
Customisation	Highly customisable to organisation-specific needs and workflows.	Standardised offerings may not fully align with unique requirements.
Knowledge of Business Context	Strong understanding of organisational structure, priorities, and context.	Limited understanding of the organisation's specific environment.
Internal Collaboration	Easier to align SOC operations with internal IT and security teams.	Requires more coordination between the organisation and the MSSP.

What are the costs involved in setting up an in-house team?

Setting up an in-house Security Operations Centre (SOC) requires careful financial planning, as there are multiple cost factors to consider:

1. Staffing Costs

- SOC Analysts: Assume an absolute minimum of two analysts per shift to maintain 24/7 coverage, accounting for sickness, holidays, and burnout prevention.
- Security Engineers: At least two dedicated engineers to build, manage, and update the SOC tooling and infrastructure.
- Specialised Roles: Consider adding incident responders, threat hunters, and a SOC manager to ensure the team operates effectively.
- Training and Certification: Ongoing training to keep the team up to date with evolving threats, tools, and compliance requirements.

2. SIEM (Security Information and Event Management) Costs

- Licensing and Subscription Fees: Costs are often based on the volume of log data ingested.
- Infrastructure: Hosting the SIEM on-premises or in the cloud may incur additional costs for servers, storage, and bandwidth.
- Open-Source Alternatives: While free platforms exist, they may require substantial investment in skilled personnel or external consultancy for setup, maintenance, and tuning.

3. Threat Intelligence Costs

- Subscriptions: Paid access to threat intelligence feeds for data enrichment and contextualising alerts.
- Integration: Additional costs to integrate threat intelligence platforms into your existing ecosystem.

4. Endpoint Detection and Response (EDR/XDR) Costs

- Tooling Licences: Licences for detecting and responding to threats on endpoints, networks, and other assets.
- Scaling Costs: Costs scale based on the number of devices or assets being monitored.

5. Infrastructure Costs

- Hardware and Software: Servers, storage devices, and software for log collection, analysis, and storage.
- Redundancy and Disaster Recovery: Backup systems and disaster recovery plans for SOC operations.
- Physical Space: Secure office space or a dedicated operations room with appropriate environmental controls.

6. Monitoring and Detection Tools

- Tools for monitoring network traffic, behaviour analytics, and intrusion detection systems (IDS/IPS).
- Regular updates and tuning to ensure effectiveness against evolving threats.

7. Incident Response Costs

- Playbook Development: Time and resources to develop detailed incident response processes and workflows.
- Forensic Tools: Specialised tools for deep-dive investigations into breaches or suspicious activity.

8. Compliance and Regulatory Costs

- Ensuring adherence to industry standards (e.g., ISO27001, NIS2, PCI DSS) may require additional investments in tools, auditing, and expertise.
- Periodic assessments and audits to verify compliance.

9. Vulnerability Management Costs

- Tools for vulnerability scanning and management across your IT landscape.
- Staff time or consultancy for patch management and remediation efforts.

10. Licensing for Security Platforms

- Additional licensing costs for DLP (Data Loss Prevention), cloud security tools, or firewalls integrated with } SOC operations.

11. Testing and Optimisation Costs

- Penetration Testing: Regular testing of SOC processes and defences to identify gaps.
- Red Team/Blue Team Exercises: Training exercises to improve SOC readiness and refine incident response capabilities.

12. Integration with Existing IT Systems

- Costs to integrate SOC tools with IT management systems, such as Active Directory, ticketing systems and ITSM platforms.

13. Ongoing Maintenance and Updates

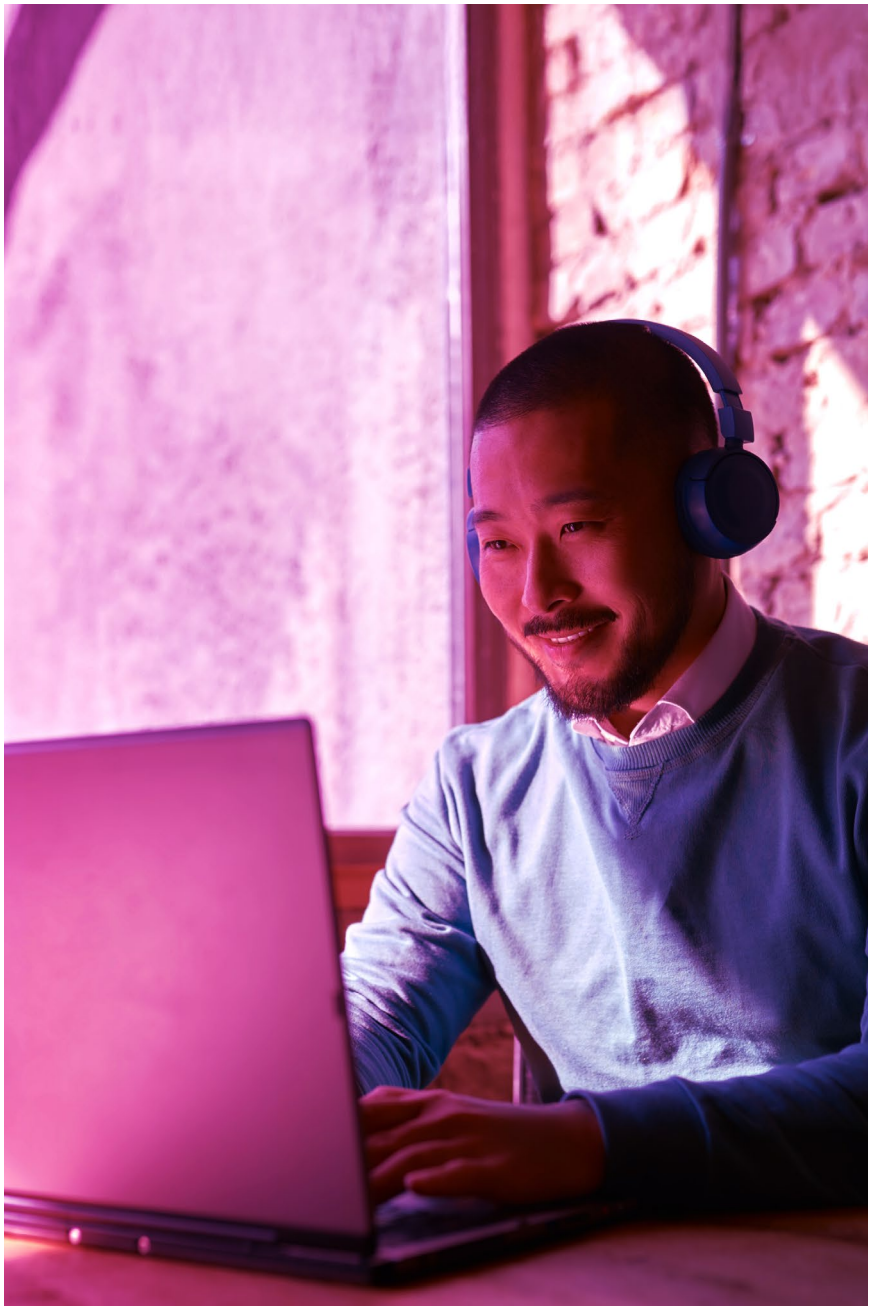
- Regular software updates, patches, and configuration adjustments.
- Replacement of outdated hardware or software over time.

14. Third-Party Consultancies and Partnerships

- Short-term costs for specialised consultants to assist with initial setup or complex tasks.
- Potential partnerships with vendors for support and co-management during early operational stages.

15. Hidden and Indirect Costs

- Time Investment: Significant time required to set up, tune, and optimise the SOC before it is fully operational.
- Opportunity Costs: Time and resources diverted from other IT and security projects.



What are the costs involved in partnering with an MSSP?

As the provider has already invested in all the above line items, you will pay a proportion of these costs – usually based in some way to your consumption. The benefit to you is that you won't be paying for an entire team who will be underutilised – but you will have access to an entire team when they are needed.

Typical managed security service providers will price up a service based on a combination of the below:

- **Number of users** – of course, the more users – the assumption is that there will be more incidents to manage.
- **Number of endpoints** – these days, users often have multiple endpoints, and servers are critical to monitor too.
- **Volume of log data** –Some small organisations generate a lot of data, where other large organisations may have quite simple infrastructure. By looking at the amount of log data you generate, MSSPs can assume the level of incident response that will be required.

While you most likely know the number of users and endpoints – unless you have a SIEM or SOC already, the volume of log data might not be known. A good partner will help you to estimate this based on the quantity and types of devices you have on your estate; this work is usually carried out free of charge as part of the presales engagement.

The provider may offer an upfront payment to cover the consulting work required to set up the service, followed by a monthly fee – or they may combine both into a single monthly fee. Ideally, they will be able to work with either, depending on your preference.

There may be costs associated with the licencing of the SIEM platform itself. This may be included in the monthly fee or paid separately to a SaaS provider like Microsoft or Cisco. The partner should clearly call out if any additional fees are payable to third parties and should estimate these for you to provide a total price.

SLAs & Reporting: The Foundation of Service

A Service Level Agreement (SLA) defines the expectations, responsibilities, and performance metrics between you and your managed security provider. A strong SLA ensures clarity, accountability, and alignment with your business needs –but not all SLAs are created equal.

- **Mean time to detect:** how much time elapses between an incident occurring and it being detected by the SOC? With modern SIEM platforms, detection should be near real-time – however detecting an incident depends on how well the platform is configured, which log sources are ingested and the quality of the rules. It's difficult to directly compare SLAs at this level.

- **Mean time to respond:** Once an incident is detected – how quickly does the SOC respond? While this measure is often the most important – it's not as simple as looking for the partner with the quickest time… (see callout "What a good SLA looks like")

- **Mean time to remediate:** How long does it take between responding and resolving the issue. There is a vast range of incident types and complexities – so again this number is difficult to compare like for like. Additionally, some remediation activities may require your internal IT team or a third party to resolve – MSSPs exclude these times from this SLA.

What a Good SLA Looks Like

A well-crafted SLA balances performance with practicality. Look for:

- **Risk-Based Prioritisation:** Higher urgency for critical incidents and lower priority for minor issues.
- **Transparent Metrics:** Clear definitions of response and resolution times with measurable results.
- **Realistic timelines:** On the surface, a 5-minute time to respond might look better than a 30-minute time to respond. But what is the content of a "response"? Do you really want to be called at 3am every night because a partner is prioritising their SLA over removing false positives? You pay the partner to triage and confirm true positives – not just forward every alert from the SIEM directly to you.

SLAs are the foundation of trust between you and your provider. A good SLA doesn't just promise speed—it ensures quality, accountability, and alignment with your business goals.

Reporting

You will generally encounter two types of reports. "Ad-hoc" reports which are generated when an incident is detected and notified to you. These are aimed at rapid communication of a problem – usually something which requires your intervention or timely notification.

The MSSP should not only engage when there is a problem, however. There should be a regular cadence of meetings, both with technical and business stakeholders covering topics such as:

- **Log source coverage:** The service is only as good as the logs it has access to. Does the provider use a framework like MITRE ATT&CK to advise you on additional log sources which might add value?
- **Performance against SLA:** An opportunity to look at how the service is performing against SLA – and put in place corrective plans if needed.
- **Review of previous incidents:** A look back at some of the more serious incidents – what went well, and could anything be improved?
- **A wider view:** the world doesn't stand still – your organisation will change over time, as will the threat landscape. There should be a regular opportunity for you to inform the provider of any business changes (e.g. mergers and acquisitions) which might impact the service, and for the provider to provide insights into new threats and solutions.

Capabilities to look for in a Managed Security partner

Automation & AI

Modern threats require fast detection and response. Providers should leverage automation and AI to:

- Identify anomalies in real-time, reducing reliance on manual analysis.
- Streamline incident response workflows, ensuring rapid containment.
- Can automate common actions like isolating a device or locking out a compromised account. This is especially important if you want the partner to be able to take action on your behalf out of hours.

Threat Intelligence

Actionable threat intelligence helps you stay ahead of evolving risks. Look for providers who:

- Maintain up-to-date threat feeds and integrate them into their services.
- Share insights about new attack trends relevant to your industry.
- Use intelligence to enhance detection and prioritise critical threats.

Threat Hunting

Proactive threat hunting ensures threats don't linger undetected. Assess whether the provider:

- Offers regular, manual threat-hunting activities.
- Utilises advanced tools to identify hidden risks.
- Provides detailed reports on findings and mitigation steps.

Remediation

Alerts are only part of the equation—effective remediation is critical. Ensure the provider:

- Offers clear guidance on containment strategies.
- Has consulting capability to help you action larger projects to improve security maturity.

Practical Considerations

Accreditation

Any partner will be able to show you slick marketing materials, but what external validation can they provide to support the efficacy of their service?

- Look for unbiased, external validation from sources like MSSP Alert: www.msspalert.com/top-250

- Check if they are accredited in their vendor of choice. You want to ensure they are experts in their toolset, and that their service has been vetted by the vendor. This also indicates they will be working closely with the vendor on improvements and will have a good relationship with their engineering team.

- Check for relevant compliance frameworks which are relevant in your region or industry. Certificates like Cyber Essentials+ and ISO27001 indicate that the organisation takes their own security seriously and should be a minimum requirement for a security provider.

Onboarding Process

You should expect a good partner to lead you through the process of onboarding. The high-level steps involved are included in the table below. While the partner should be doing the heavy lifting, it's important to be aware of any dependencies on your staff so you can plan for it.

What	Your involvement
Scoping and discovery: To be able to provide an appropriate solution, the partner will need to ask lots of questions about your aspirations for the service and your current technology stack.	You should expect to involve several stakeholders to be able to provide an overview of the makeup and size of your estate. Knowing things like the number of endpoint devices and the make, model and quantity of firewalls, cloud services and other assets will help to ensure the design works for your needs.
Platform Build: If a SIEM tool needs to be deployed, or XDR needs to be rolled out across your estate, you will want to be involved in this to ensure disruption to users is minimised.	Your IT team may need to provide access to your cloud environment for the partner to deploy the SIEM. You should expect to work with the partner to create a joint plan for how and when endpoint agents will be deployed.
Customisation: Any good partner will have a default set of rules which work to detect incidents for most organisations. But if you have specific customisations you require, you will need to work with the partner to ensure these requirements are captured.	If you have existing rules in a legacy system which need to be rewritten, providing these can lead to a quicker onboarding than starting from scratch. If these are new requirements, then documenting these in natural language can help communicate your needs to the partner.
Early life support: Once the service moves into operations, there will be a period of further tuning to reduce false positives and tweak the system for your specific environment.	There will need to be close working between your IT team and the partner. While many incidents will be easy for the partner to triage as false or true positives, they will want to work with you on the "grey zone" to ensure knowledge base articles can be written and rules customised to ensure false positives are minimised in operation.
Live Operations: Once early life support is completed, the solution will move into steady state. The customisation work of the partner does not stop at this point, but it should slow down considerably as the focus switches to incident detection.	You will need to provide a contact map for who should be notified when a security incident occurs. This could be a single distribution list for smaller organisations but could have added complexity like different escalation paths in or out of business hours, or specific resolver groups for issues with certain technology. This could even include third parties where you have outsourced some operations.

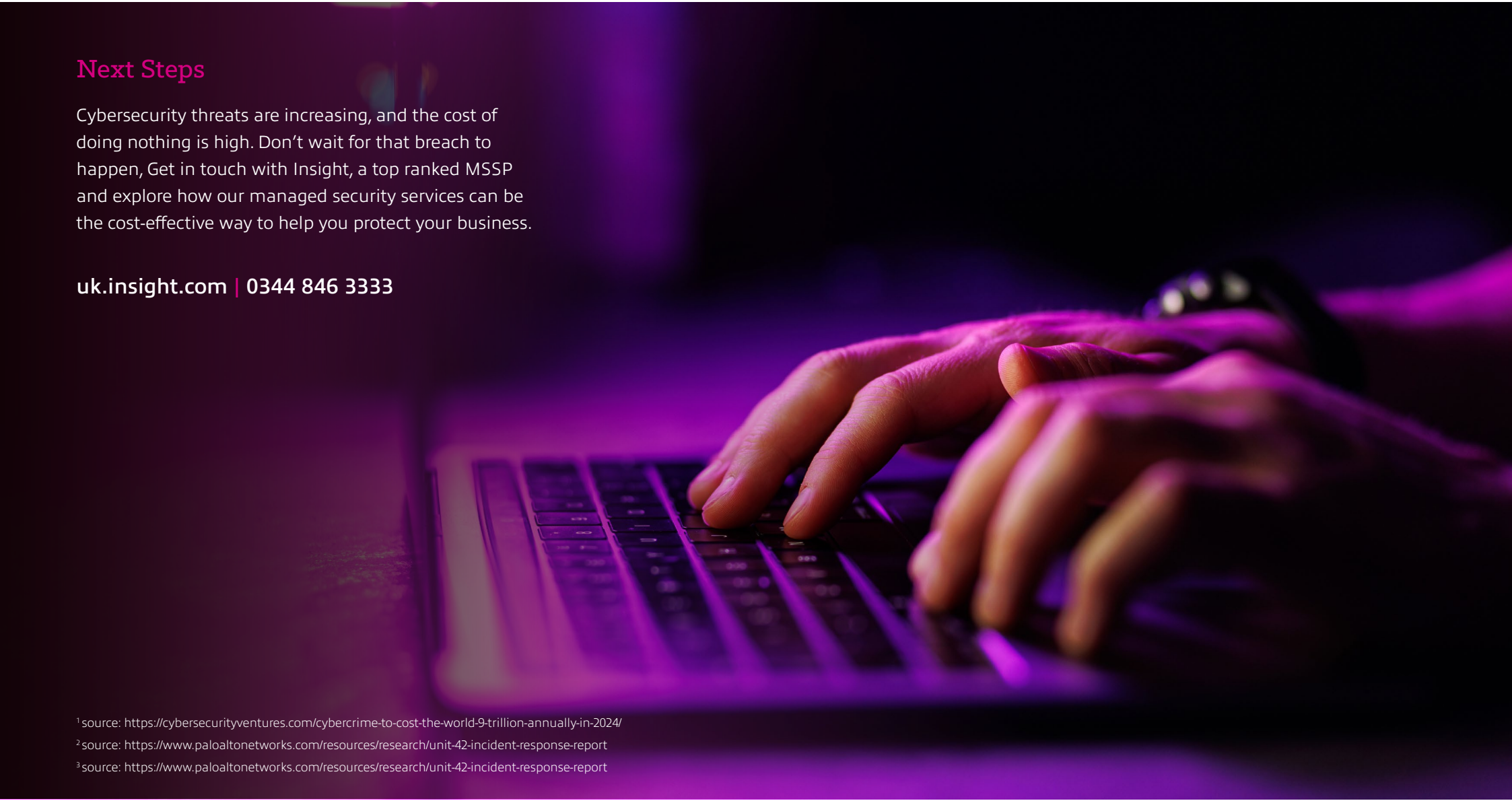
Value-Add Services

While your primary concern in looking for a Managed Security provider will be to help you to detect and remediate security incidents, there are often other services which naturally fit with a Managed Security provider, and it's worth considering if any of these might be useful to you – and could be bunded in at the same time. There are often benefits from having multiple services provided by the same partner – as they will have a wider visibility of your security and can often make more informed decisions.

Vulnerability Management is a natural companion to a SOC, proactively identifying, assessing, and prioritising security flaws across an organisation's digital environment. By integrating this service, organisations benefit from continuous monitoring for vulnerabilities and actionable remediation plans that align with the SOC's threat detection capabilities. This reduces the risk of exploitation by closing security gaps before attackers can exploit them.

Digital Risk Protection Services (DRPS) offer another strategic addition, extending the SOC's reach beyond the corporate network into the wider digital landscape. DRPS monitors for threats in external environments such as the dark web, social media, and external-facing systems. By identifying brand impersonation, credential leaks, or exposed sensitive data, organisations can gain early warnings of potential threats, allowing the SOC to respond swiftly and mitigate risks.

For organisations facing active threats or breaches, bundling **Digital Forensics and Incident Response (DFIR)** with Managed Security ensures rapid containment and detailed post-incident analysis. DFIR teams can leverage the SOC's telemetry and logs to investigate root causes, scope the extent of the breach, and recommend recovery steps. This holistic approach enables businesses to respond decisively while gaining insights to prevent recurrence. Bundling these services creates a seamless, end-to-end security solution, giving organisations confidence in both prevention and resilience.



Next Steps

Cybersecurity threats are increasing, and the cost of doing nothing is high. Don't wait for that breach to happen, Get in touch with Insight, a top ranked MSSP and explore how our managed security services can be the cost-effective way to help you protect your business.

uk.insight.com | 0344 846 3333

[1] source: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[3] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

MKT7295_UK