XDR+SOC ECONOMIC IMPACT REPORT

BUSINESS CASE SUMMARY

PREPARED FOR [redacted]

MAY 2021

LIBERATING YOU FROM THE CONSTRAINTS OF CONVENTIONAL CYBERSECURITY

WWW.ARMOR.COM

Table of Contents

Executive Summary

The Armor XDR+SOC platform provides organisations with a comprehensive Managed Detection and Response (MDR) solution that streamlines and optimises security operations, leveraging native cloud services that further reduce the total cost of ownership of the cybersecurity stack. This business case summary is the result of a study conducted to examine the potential return on investment (ROI) customers may realise when deploying the Armor XDR+SOC solution and the various product tiers.

The key comparison drawn in this study examines two primary scenarios:

- Developing and deploying an in-house SOC capability
- Outsourcing the XDR+SOC capabilities to Armor Defense

Cybersecurity is a specialised field that requires both technical knowledge and experience in order to extract the maximum value from one's security investments. This makes the barrier of entry relatively high and as a result, has driven a continued increase in the cost-per-hire due to the shortage of qualified professionals. Inexperienced hires also require training and often present a long ramp-up period before they can begin contributing effectively to the organisation's security operations. Additionally, the turnover rate in Security Operation Centres (SOCs) is disproportionately higher than other technical fields due to the challenging nature of the job, whilst those who adapt well to these challenges typically demand a salary curve much steeper than that of their peers.

Armor addresses these issues by providing our clients a fully outsourced Managed Detection and Response (MDR) solution, that allows our customers to fully leverage our robust engineering and incident response expertise, without the need for them to build, train, and manage their own SOC.

Key Findings

Quantified Benefits

Initial Investment and Operational Costs

The initial investment to build a Security Operating Centre (SOC) and the resulting costs are quite significant for an organisation. Based on our analysis of the Armor XDR+SOC solution on a CapEx plus three-year OpEx basis, an organisation would need to spend average of 7.7 times more to support an effective SOC internally. As an MDR provider Armor Defense takes advantage of an economy of scale, which subsequently yields benefits from reduced operational costs.

Tools and Licensing Costs

Armor provides threat intelligence and other capabilities via several commercial licenses, the cost of which is shared across our entire customer base. For in-house SOCs the organisation would bear the full burden of these costs which would otherwise be shared. These costs are significant and represent a delta of 27% over three years.

Stable and Predictable Pricing Schedule

The Armor XDR+SOC solution utilises a cloud consumption cost model and scales with utilisation. And because an organisation is then only paying for what they consume organisations can save as much as 16% by avoiding these non-functional costs such as recruiting and hiring, attrition, training, and year over year cost of living adjustments.

7.7x

Lower 3-year TCO

27%

Savings in tools and licensing

16%

Savings in non-variable costs

Unquantified Benefits

Get Cybersecurity Skills Immediately

The major benefit of hiring external cybersecurity experts is that those specialists are immediately available with all their expertise in securing similar environments and their access to cyber-threat monitoring and research databases.

Ease of Implementation and Scalability

Adoption of an in-house SOC is both costly and difficult to implement as modern security operations must deal with overly complex IT infrastructures and sophisticated cyber threats. Scalability is another problem with in-house SOCs, as the organisation should invest heavily and continuously in expanding and updating the hardware and software tools required to support an acceptable level of cybersecurity.

Uninterrupted and Guaranteed Service

Cyber threats and bad actors do not sleep, and automated malicious tools are scanning for network vulnerabilities day and night. Maintaining 24/7 cybersecurity operations requires additional team members whilst immediate threat response is mandatory to quarantine a threat and prevent it from spreading across your networks. Armor grants you peace of mind by running a 27/7/365 SOC and by adhering to a service level agreement (SLA) that defines the scope and delivery of the service.

Framework and Methodology

The financial model used in this economic study compares the costs associated with outsourcing the XDR and SOC capabilities to Armor Defense with developing and deploying an in-house SOC capability.

Financial Model Framework

Armor Defense calculated the type of resources and the efforts required to Design, Build and Operate a Managed SIEM and SOC solution and compared it with the resources and efforts that Customer would require for an in-house SOC capability. We then made data- and experience-modelled estimates of the additional efforts that would be required by an organisation that is newly designing, building, and operating a SOC. Whereas Armor Defense is already operating a SOC, we modelled the initialisation costs to include recruiting and hiring, training, and developing the process and solutions.

Salary and Cost of Living Adjustments

When drawing comparisons between the different model features, in-house employee salary was modelled to include cost of living adjustments and other standard expenses associated with workforce management. The lower end of the standard deviation of salary range for a security consultant was used as a baseline and relative standard expenses included in the model.

Analysis of Benefits

Streamlined Security Operations without Significant Overhead

In addition to the costs and difficulty associated with hiring qualified security professionals to manage and investigate security incidents, there are considerable engineering costs associated with getting a SOC off the ground. Security solutions require constant tuning in order to ensure that the SOC receives high fidelity alerts, reducing false positives and pointless investigation as much as possible. With modern security solutions, automation and orchestration can streamline incident management and response, but they are not always easy to implement without a significant time investment in development and testing.

CATEGORY / TASK	ROLE	% OF WORKER CAPACITY
SIEM – Rule Development	SOC Analyst/Engineer	100-200% (based on number of distinct log sources)
SIEM – Rule Tuning	SOC Analyst/Engineer	100-250% (based on number of distinct log sources)
Threat Hunting	SOC Analyst	50-100%
Updates & Maintenance	SOC Analyst/Engineer	25-50%
SOAR Playbook Customisation	SOC Analyst/Engineer	75-150% (based on number of integrations)
Dashboards & Reporting	SOC Analyst/Engineer	50-100%

Between 4 and 9 dedicated staff required
(not including additional personnel for 24/7 coverage)

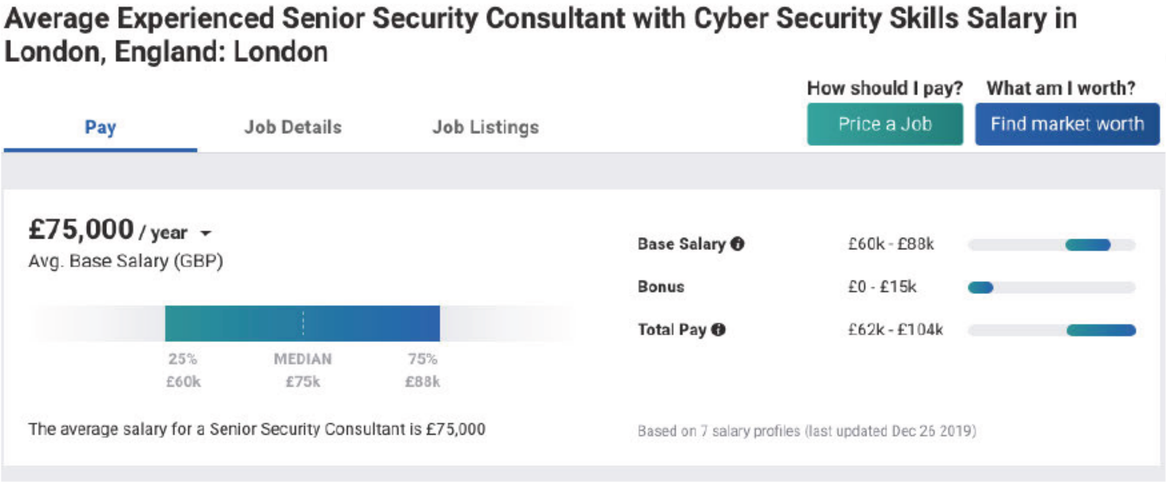
These requirements are subsequently compounded by the requirement that certain responsibilities, such as incident response, be ready and available 24/7. Whilst this can be achieved using various schedules, the most common is an 8x3 follow-the-sun model which we'll use to calculate total capacity requirements. Baseline coverage for incident response can typically be accommodated by junior-level analysts and responders with an escalation channel to senior personnel.

Threat Intelligence is a crucial component in Security Operations as they provide you with context and Indicators-of-Compromise (IOC) to enhance your detection capabilities. Instead of licensing commercial feeds, our customers can leverage our aggregated Threat Intelligence feed as part of our XDR+SOC offering and save on licensing costs.

Armor's continuous investment of time and effort in the development these critical pieces can be leveraged by organisations to significantly reduce the lead time required to design and implement these vital components of a SOC.

Access to Skilled Cybersecurity Professionals Immediately

Hiring and training is costly in cybersecurity. Based on data collected from PayScale.com, the fully loaded cost of hiring a senior-level security analyst in the United Kingdom is about £160,000 GBP, whilst a junior-level security analyst would cost £32,385 GBP per annum. In our collective experience, keeping a 24x7 security operations centre staffed, requires at least six analysts, with at least two of whom being senior-level analysts to train and manage day-to-day operations.



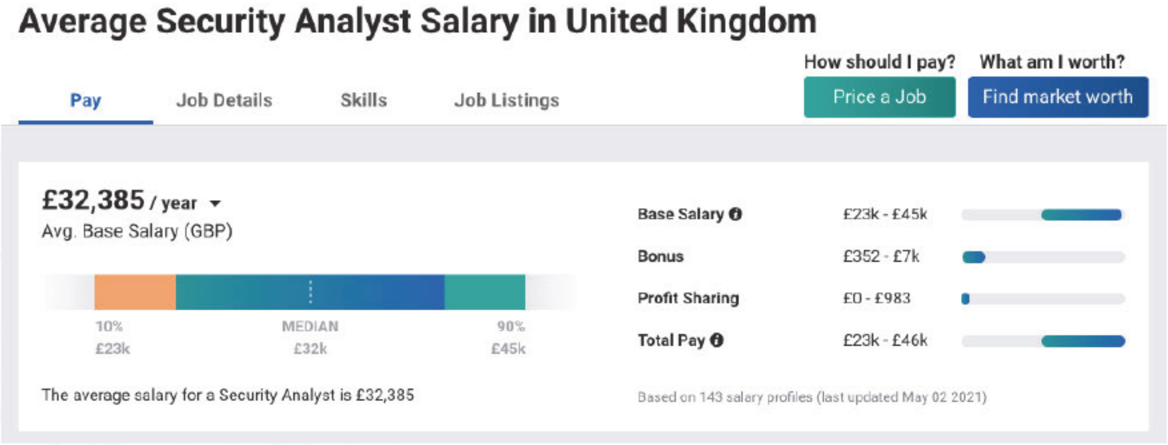
Average Experienced Senior Security Consultant with Cyber Security Skills Salary in London, England: London

£75,000 / year
Avg. Base Salary (GBP)

Base Salary	£60k - £88k	
Bonus	£0 - £15k	
Total Pay	£62k - £104k	

The average salary for a Senior Security Consultant is £75,000

Based on 7 salary profiles (last updated Dec 26 2019)



Average Security Analyst Salary in United Kingdom

£32,385 / year
Avg. Base Salary (GBP)

Base Salary	£23k - £45k	
Bonus	£352 - £7k	
Profit Sharing	£0 - £983	
Total Pay	£23k - £46k	

The average salary for a Security Analyst is £32,385

Based on 143 salary profiles (last updated May 02 2021)

Continuous training is also key in order to ensure that your SOC team adapts to the ever-changing threat landscape. Relevant training courses for a security analyst would cost on average $2,000 USD, with renowned training providers like SANS charging upwards of $7,000 USD. Combined with the high turnover of security analysts, companies often struggle to make their investments pay off.

With Armor's XDR+SOC solution, our customers gain access to our security analysts and consultants to run their security operations. Our analysts have the certifications and experience needed to ensure that customers can hit the ground running and maximise their return on investment.

Fast & Scalable Implementation

Armor’s engineering team utilises the latest cloud technology to manage and scale infrastructure through modern DevOps practises. Deployments leverage infrastructure-as-code, using Terraform declarative configuration to deploy requisite infrastructure quickly and consistently to onboard our customers rapidly.

DEPLOYMENT ITEM	ARMOR XDR+SOC	IN-HOUSE DEPLOYMENT
	PERSON HOURS	
Initial Deployment Time	4.00	16.00
Initial Dashboard & Reporting Setup	4.00	16.00
Machine Learning Rule Tuning	20.00	420.00
Onboarding Management Overhead	16.00	76.50
Total Onboarding Time	**44.00**	**528.50**

Armor leverages infrastructure-as-code techniques that ensures that our deployments always follow a strict set of configurations and aims to remove the human element from the process. This greatly accelerates deployments and reduces the risk of human error.

Traditional deployment strategies that require manual configuration can lead to issues, which further delays deployment due to the additional time required to troubleshoot these matters. Additionally, the overhead of ensuring that everything is properly validated and documented (either for change management or other purposes) further increases the amount of time required for a successful deployment.

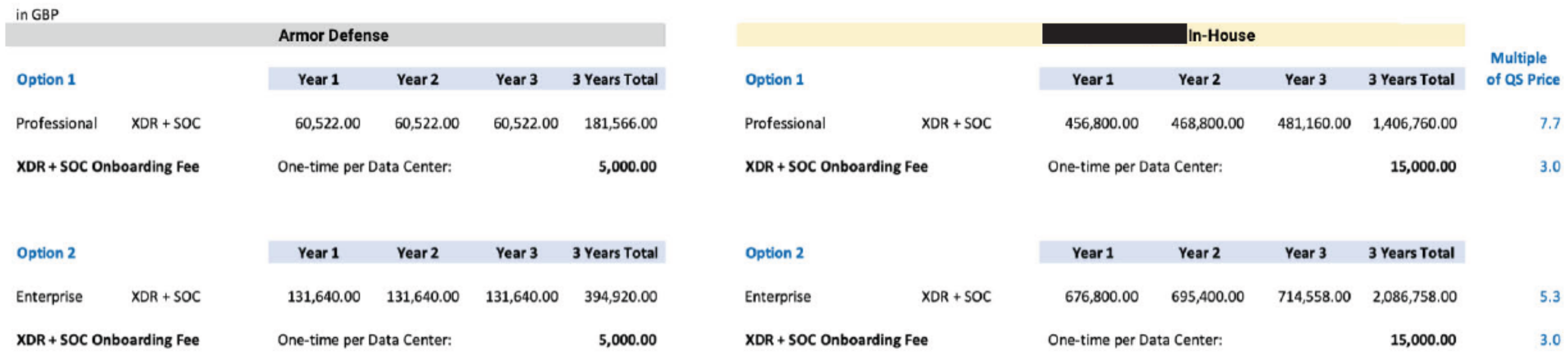
Our deployment methods can provision our SIEM solution in less than 30 minutes, including our rule library and dashboards. This reduces the lead time and allows your organisation to start realising the desired security outcomes faster. We also provide customers access to our knowledge to better understand these methods as well as to integrate them into their own DevOps workflows.

Analysis of Costs

An external SOC is much cheaper because most equipment, solutions and experts are shared. For 24/7 monitoring and analysis via an in-house SOC, a budget of approximately £450,000 GBP is required each year (assuming the professional package). Whereas outsourcing it to Armor Defense would require approximately £60,000 GBP.

The initial investment to build a Security Operating Centre (SOC) and the resulting costs are quite burdening for the organisation. Based on our analysis, organisations would need to spend average of 7.7 times more compared to the Armor XDR+SOC Professional solution and 5.3 times more compared to the Enterprise solution in order to achieve equivalent cybersecurity outcomes (see financial summary below).

Financial Summary



in GBP

Armor Defense

Option 1		**Year 1**	**Year 2**	**Year 3**	**3 Years Total**
Professional	XDR + SOC	60,522.00	60,522.00	60,522.00	181,566.00
XDR + SOC Onboarding Fee	One-time per Data Center:				**5,000.00**

Option 2		**Year 1**	**Year 2**	**Year 3**	**3 Years Total**
Enterprise	XDR + SOC	131,640.00	131,640.00	131,640.00	394,920.00
XDR + SOC Onboarding Fee	One-time per Data Center:				**5,000.00**

[redacted] **In-House**

Option 1		**Year 1**	**Year 2**	**Year 3**	**3 Years Total**	**Multiple of QS Price**
Professional	XDR + SOC	456,800.00	468,800.00	481,160.00	1,406,760.00	7.7
XDR + SOC Onboarding Fee	One-time per Data Center:				**15,000.00**	3.0

Option 2		**Year 1**	**Year 2**	**Year 3**	**3 Years Total**	
Enterprise	XDR + SOC	676,800.00	695,400.00	714,558.00	2,086,758.00	5.3
XDR + SOC Onboarding Fee	One-time per Data Center:				**15,000.00**	3.0

Key Commercial Terms

1. Above amounts are in GBP.
2. Armor is proposing the above price based on a 36-month term.
3. The above Armor Defense charges relates to Armor Defense Managed Services only. This does not include the costs associated with Microsoft Azure.
4. All prices quoted by Armor is exclusive of all applicable taxes and duties.

XDR+SOC Solution Overview

Armor combines cloud-native detection and response capabilities with our 24/7 team of cybersecurity experts and our comprehensive AI-enabled threat hunting and alerting library to deliver critical security outcomes.

Detect Malicious Behaviour

Collect logs and telemetry across your enterprise and cloud environments and leverage Armor's robust threat-hunting and alerting library to detect threats.

Prioritise Applicable Threats

Using open source, commercial, and proprietary threat intelligence, the Armor platform enriches incoming data to enable smarter, faster determinations of threat levels.

Respond to Threats

When threats are detected, alerts and incidents are created – you can rely on Armor's team of security experts around-the-clock to respond to threats.

Identify and Remediate Weaknesses

Armor can perform advanced forensic investigations during and after an incident to identify the path an attacker took and how to remediate weaknesses the attacker exploited.

Save Time with Automation

Armor's platform was built to take advantage of advanced AI and machine learning, as well as cloud-native automation engines to make all aspects of the security lifecycle simpler.

Network and system protections only tell part of the story. Modern cybersecurity threats involve compromising more than just a single endpoint – lateral movement, cloud service exploits, and advanced persistent threats are the new norm. **Extended Detection and Response (XDR)** connects the logs and telemetry data from all of these sources and correlates them, giving you a complete picture from which you can identify threats. Armor's expert **Security Operations Centre (SOC)** adds a layer of cybersecurity expertise to respond to threats quickly and thoroughly, and to inform and guide remediation efforts.