SEARCHLIGHT. CYBER

A GUIDING LIGHT IN THE DARK

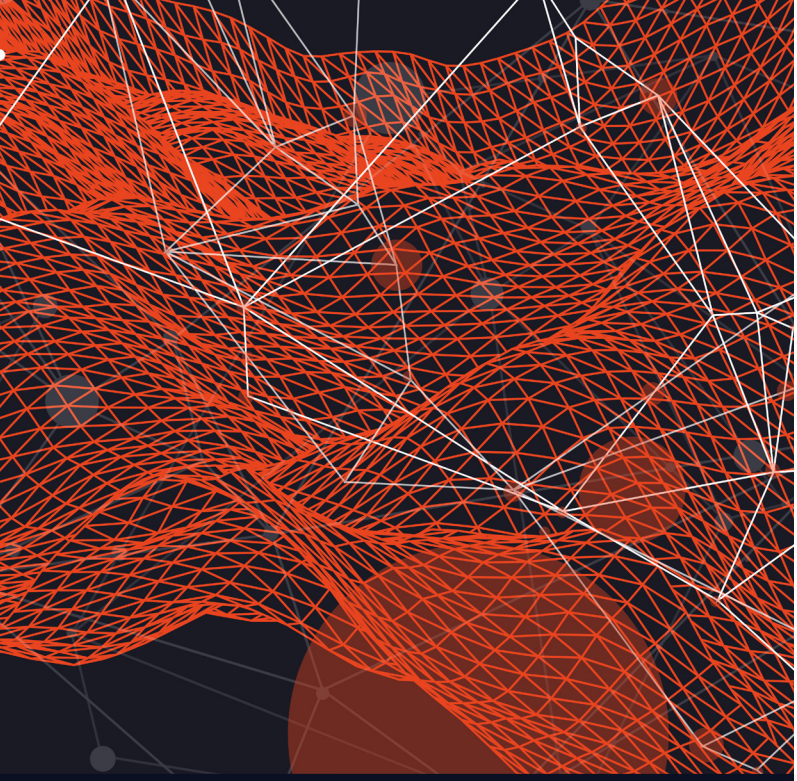
# HOW MSSPs ARE USING DARK WEB THREAT INTELLIGENCE

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service *Supplier*



# SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web threat intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service *Supplier*

# CONTENTS

# INTRODUCTION

Managed Security Service Providers (MSSPs)'s position in the market puts them at the forefront of emerging trends. They are required to be early adopters, identifying the latest tools and technologies to protect their customers. It is no surprise then, that MSSPs were among the first to recognize the opportunity of dark web intelligence as a source to identify threats emerging from the cybercriminal underworld.

We know this from working closely with MSSPs in this space but - to date - there has been no research to quantify exactly how many MSSPs are using dark web intelligence, what they are using it for, and how it benefits their customers.

We worked with Censuswide to rectify this, surveying 501 MSSPs: 251 in the US, and 250 in the UK. We also called on some of the industry's leading MSSPs to provide their insights, first hand experience, and expert analysis of the results.

The primary finding of this report is that there is high demand for dark web intelligence among MSSPs' customers. While some MSSPs are already helping by providing insight into the dark web, there remains a gap between demand and delivery, which MSSPs need to fill in order to address the understandable anxiety their customers have around dark web threats.

The report also provides detail on how MSSPs are integrating dark web intelligence into their services. It shows that many MSSPs have managed to unlock new revenue streams with dark web intelligence but there are clearly more opportunities to be seized.

For example, MSSPs are often using data from the dark web to inform their one-off engagements - such as pentests, security audits, and incident response. However, fewer have integrated dark web intelligence into their Security Operations Centre (SOC), where it could help in the ongoing defense of their customers.

I'd like to thank everyone who gave up their time and contributed to this report. We hope it will be insightful for the MSSPs that have already integrated dark web intelligence into their services and are keen to learn more from the experiences of their peers.

However, I especially hope it will be useful to those who have not yet taken up the mantle of being the "guiding light" to the dark web for their customers. This research demonstrates the opportunities that dark web intelligence brings to MSSPs but, with customer demand for dark web intelligence so high, MSSPs need to act fast to make sure that they are ahead of the pack.

**BEN JONES**
CEO and Co-Founder
Searchlight Cyber

# METHODOLOGY

The following findings are from a survey conducted by the research company Censuswide between November 17 - 29, 2022. In total, 501 respondents in managerial or leadership positions at Managed Security Service Providers (MSSPs) were interviewed: 251 in the US, 250 in the UK.

# TOP LINE FINDINGS

## DEMAND FOR DARK WEB INTELLIGENCE IS INCREASING

Two-thirds of MSSPs said that their customers have asked for threat intelligence from the dark web.

## THIS DEMAND IS BEING DRIVEN BY WANTING TO KNOW MORE ABOUT THEIR ADVERSARIES

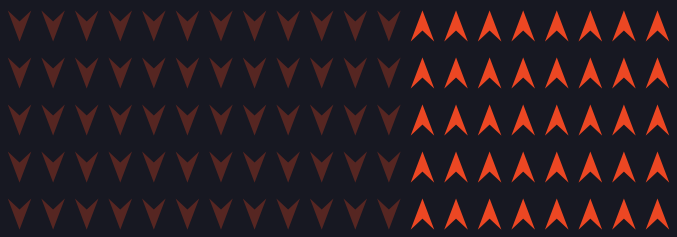
67 percent of MSSPs say that their clients want more information about threat groups.

## MORE THAN HALF OF MSSPS HAVE STARTED TO MEET THIS DEMAND

56 percent say they are undertaking dark web monitoring.

## THE MAIN BARRIER TO ADOPTION IS A PERCEPTION THAT IT IS COMPLICATED

35 percent of the MSSPs not using dark web intelligence said that it was because it is too complicated.



## BUT THOSE THAT ARE USING DARK WEB INTELLIGENCE ARE UNLOCKING NEW COMMERCIAL OPPORTUNITIES

40 percent listed the ability to create new products and services as a benefit of dark web intelligence.

# THE DEMAND FOR DARK WEB INTELLIGENCE

## ABOUT THE DARK WEB

The dark web is a part of the internet that is purposefully obfuscated, requiring a user to download specialist software such as The Onion Router (Tor) to access. While there are some ethical uses for the dark web - such as its use by whistleblowers - the vast majority of activity is explicitly illegal, with criminals taking advantage of the ability to browse and host websites anonymously.

Among other criminal activities, such as the sale of drugs, arms, and forgeries, the dark web is the home to cybercriminal activity. This includes (but is not limited to): marketplaces for buying and selling malware, exploits, and stolen corporate data; forums where cybercriminals discuss their tactics and share techniques; and ransomware leak sites where cybercriminals threaten to publish stolen data unless their demands are met.

Naturally, this makes the dark web a topic of interest for MSSPs' customers, who are trying to find ways to protect themselves from cybercriminals. Indeed, our survey found that MSSPs are increasingly being asked questions about the dark web:

ALMOST TWO-THIRDS (65 PERCENT) OF MSSPS SAID THAT THEIR CUSTOMERS HAVE ASKED FOR THREAT INTELLIGENCE FROM THE DARK WEB.

**This is consistent in both the US (64 percent) and the UK (66 percent)**

OF THOSE, 74 PERCENT SAID THAT THEIR CUSTOMERS' INTEREST HAS BEEN INCREASING.

**Interest in dark web intelligence is increasing quicker in the US than in the UK (80 percent vs 69 percent)**

## DEMAND DRIVERS

We asked MSSPs what they think is driving their customers' demands for dark web intelligence.

According to them **(Figure 1)**, the top requirement is to find vulnerabilities affecting their organization (39 percent), closely followed by wanting to find out if they are currently being targeted on the dark web (38 percent), and wanting to gather intelligence on threat groups such as ransomware gangs (38 percent).

Interestingly, MSSPs ranked these reasons above wanting to find leaked data from their organization (35 percent), and the desire to identify historic data breaches (29 percent), which suggests their customers see dark web intelligence as a preventative, rather than reactive, measure.

This fits with our own experience of how enterprises are using dark web intelligence - to "shift left" in the Cyber Kill Chain - and identify attacks before the cybercriminal hits the network, so that they can stop rather than just mitigate incidents.

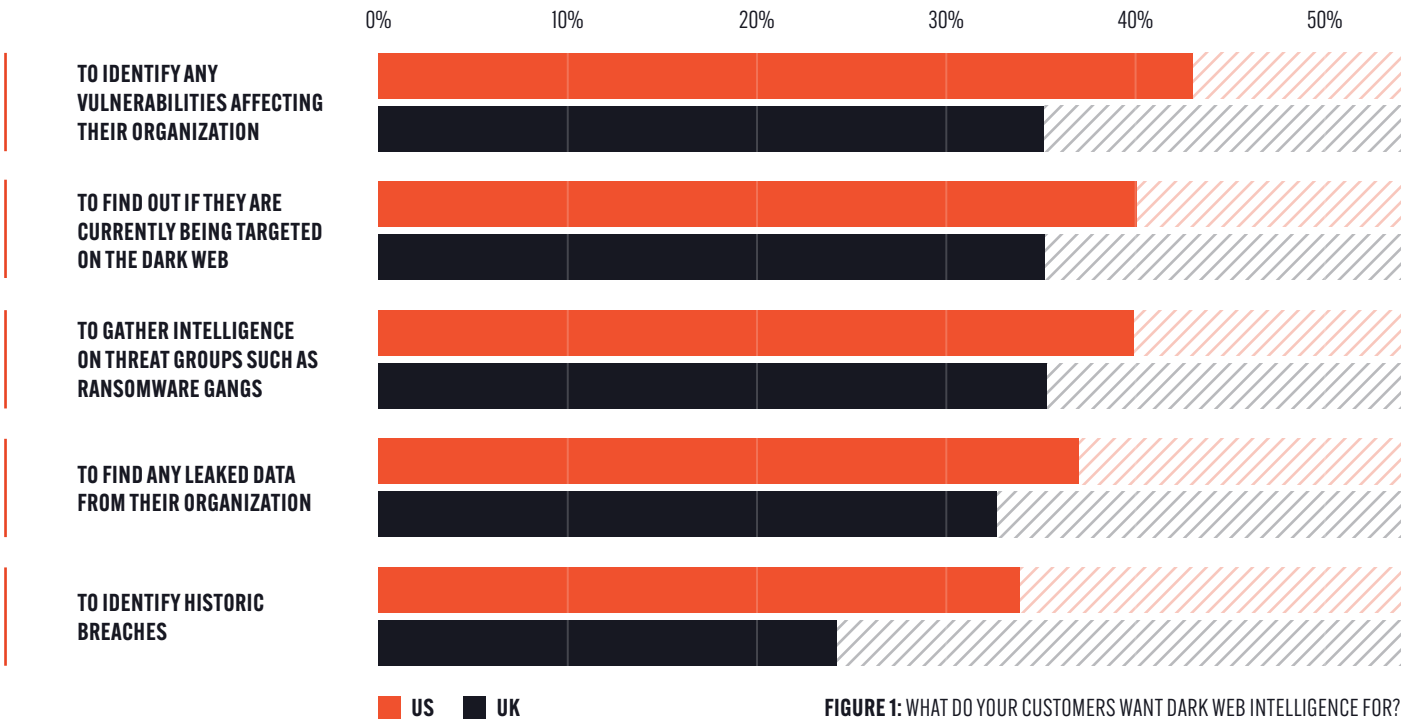



**FIGURE 1:** WHAT DO YOUR CUSTOMERS WANT DARK WEB INTELLIGENCE FOR?

These findings also demonstrate that the demand for dark web intelligence is very closely linked to customers' desire to find out more about threat groups. Indeed, our MSSP survey respondents were very consistent that their customers are increasingly interested in finding out more than their adversaries, with more than two-thirds (67 percent) saying that customers want more information about threat groups, such as who they are and how they operate.

This is something that our partner MSSPs have witnessed first hand:

## INSIGHTS FROM THE FIELD

**MATT HULL** // GLOBAL HEAD OF THREAT INTELLIGENCE, NCC GROUP

> As threat actors increasingly publicize and claim responsibility for ransomware attacks, leak breach data, and target executives on hidden sites and forums, there is an increased requirement from organizations to understand how they may be exposed and what they can do to mitigate risk. Effective and safe research across the dark web requires a degree of skill that is not often present within your average organization and as such, they are turning to us for help in understanding the threats emanating from the dark web.

# ADOPTION OF DARK WEB INTELLIGENCE

So how are MSSPs meeting this demand?

## MORE THAN HALF (56 PERCENT) OF MSSPs SAY THEY ARE UNDERTAKING DARK WEB MONITORING ON BEHALF OF THEIR CUSTOMERS.

This is consistent in both US and UK (55 percent and 57 percent respectively), demonstrating that - on both sides of the Atlantic - MSSPs have started to address the customer requirement for guidance on the dark web. While this is a fantastic start, there is still a notable gap (9 percentage points) between supply and demand and, as we'll see later in this report, MSSPs have often not integrated dark web intelligence across all of their services.

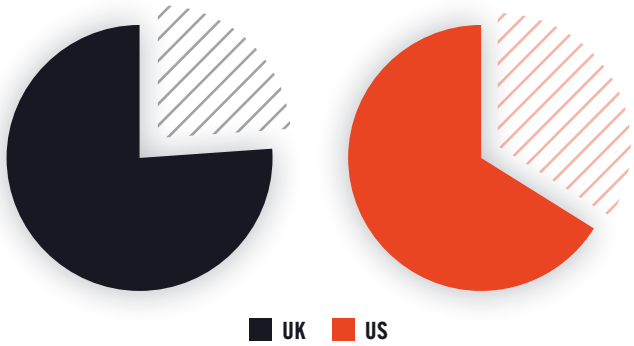
# BROADER THREAT INTELLIGENCE

This adoption level is particularly interesting compared against the baseline of how many MSSPs are using cyber threat intelligence in general.

Threat intelligence is the broader category that dark web intelligence fits into, and includes all of the information organizations could gather on threats in cyberspace, such as attack techniques, the tactics of cybercriminals, the technologies they are using, etc.

Adoption of wider threat intelligence by MSSPs is higher but perhaps not as high as you would expect. On average, 71 percent of MSSPs are using threat intelligence and - interestingly - it is more common in the UK than in the US.

## MSSPs IN THE UK ARE MORE LIKELY TO USE THREAT INTELLIGENCE THAN THEIR US COUNTERPARTS




## **76** AND **66** PERCENT RESPECTIVELY

Therefore, dark web intelligence actually isn't that far behind.

In both the US and the UK, the most common use for threat intelligence was to inform pentests and security audits, followed by informing incident response, and delivering threat intelligence directly to customers **(Figure 2)**.

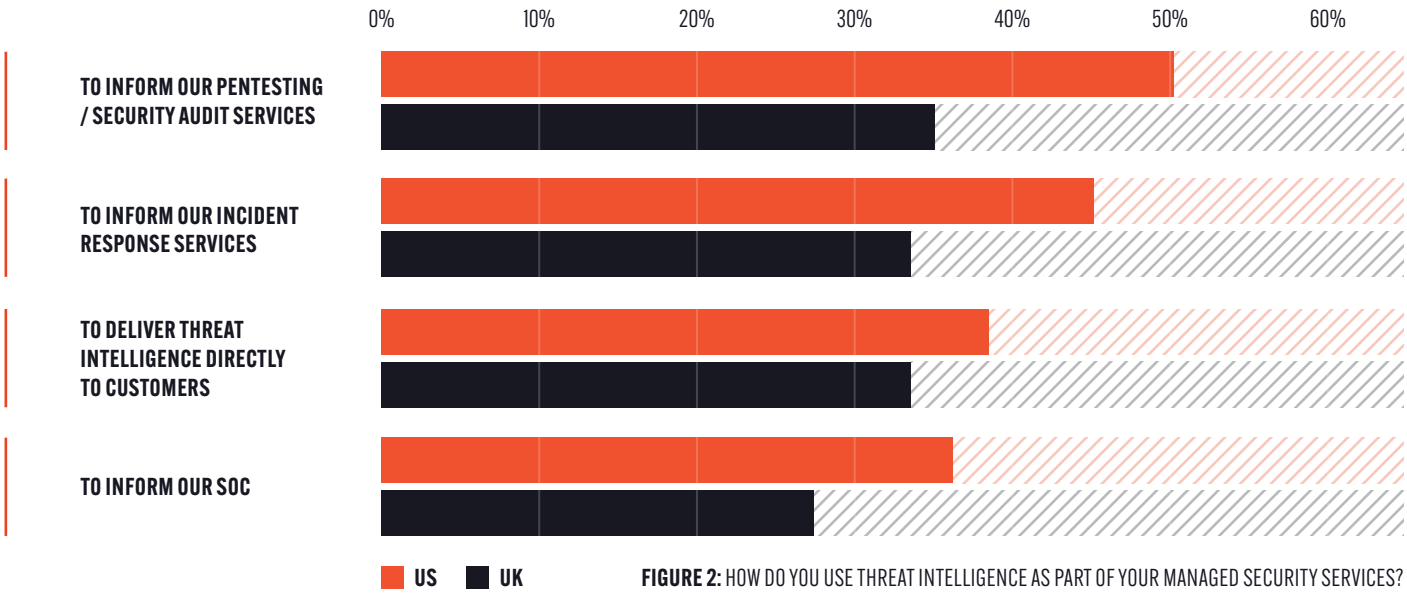



**FIGURE 2:** HOW DO YOU USE THREAT INTELLIGENCE AS PART OF YOUR MANAGED SECURITY SERVICES?

Of those that don't use threat intelligence, the most common reason is that they believe it doesn't deliver enough value (34 percent), followed by a belief that it isn't relevant to their services (31 percent), or that it is too expensive (25 percent).

However, visibility into the dark web, the area of the internet where cybercriminals congregate to plan their attacks, is providing some MSSPs with an advantage.

# BENEFITS AND BARRIERS

## THE BENEFITS FOR MSSPs

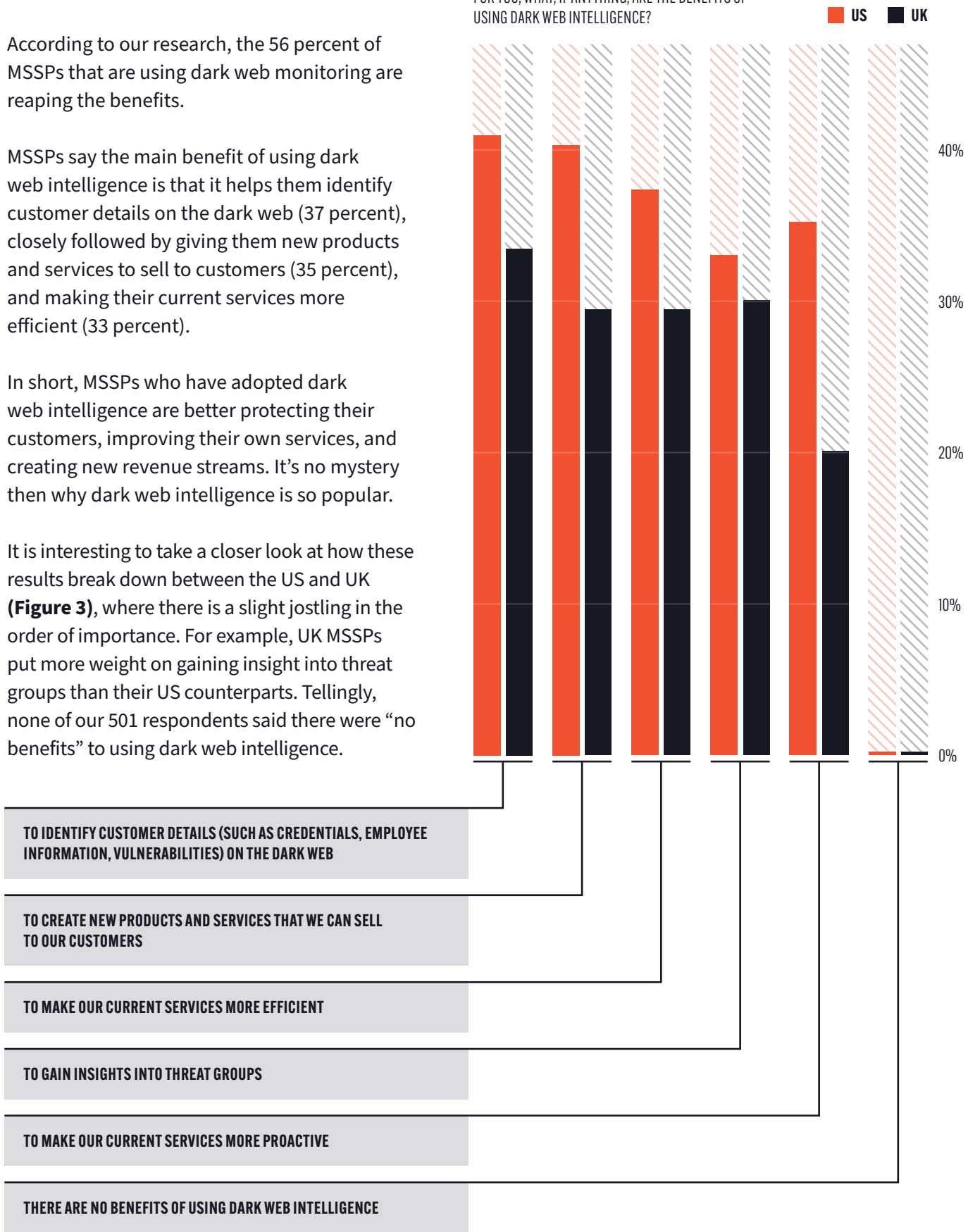
According to our research, the 56 percent of MSSPs that are using dark web monitoring are reaping the benefits.

MSSPs say the main benefit of using dark web intelligence is that it helps them identify customer details on the dark web (37 percent), closely followed by giving them new products and services to sell to customers (35 percent), and making their current services more efficient (33 percent).

In short, MSSPs who have adopted dark web intelligence are better protecting their customers, improving their own services, and creating new revenue streams. It's no mystery then why dark web intelligence is so popular.

It is interesting to take a closer look at how these results break down between the US and UK **(Figure 3)**, where there is a slight jostling in the order of importance. For example, UK MSSPs put more weight on gaining insight into threat groups than their US counterparts. Tellingly, none of our 501 respondents said there were "no benefits" to using dark web intelligence.

**FIGURE 3:**
FOR YOU, WHAT, IF ANYTHING, ARE THE BENEFITS OF USING DARK WEB INTELLIGENCE?



## INSIGHTS FROM THE FIELD

**ANDY BATES** // PRACTICE DIRECTOR - SECURITY, NODE4

> Planning and preparation are key to any project or business. Yet in cyber we have been conditioned to expect an attack out of the blue and respond. Over the years we have all moved from fire fighting to fire prevention, from looking after our hearts rather than dealing with heart attacks. In cyber we can now move ahead of the criminals for the first time by listening to the dark web. To be able to do this without funding criminals or becoming like them is an important moral standpoint in this necessary shift in modern day cyber combat.

# THE BARRIERS TO ADOPTION

With demand for dark web intelligence so high, and with so many benefits from adoption, why aren't all MSSPs using it? The answer changes depending on whether you are asking MSSPs from the US or the UK **(Figure 4)**.

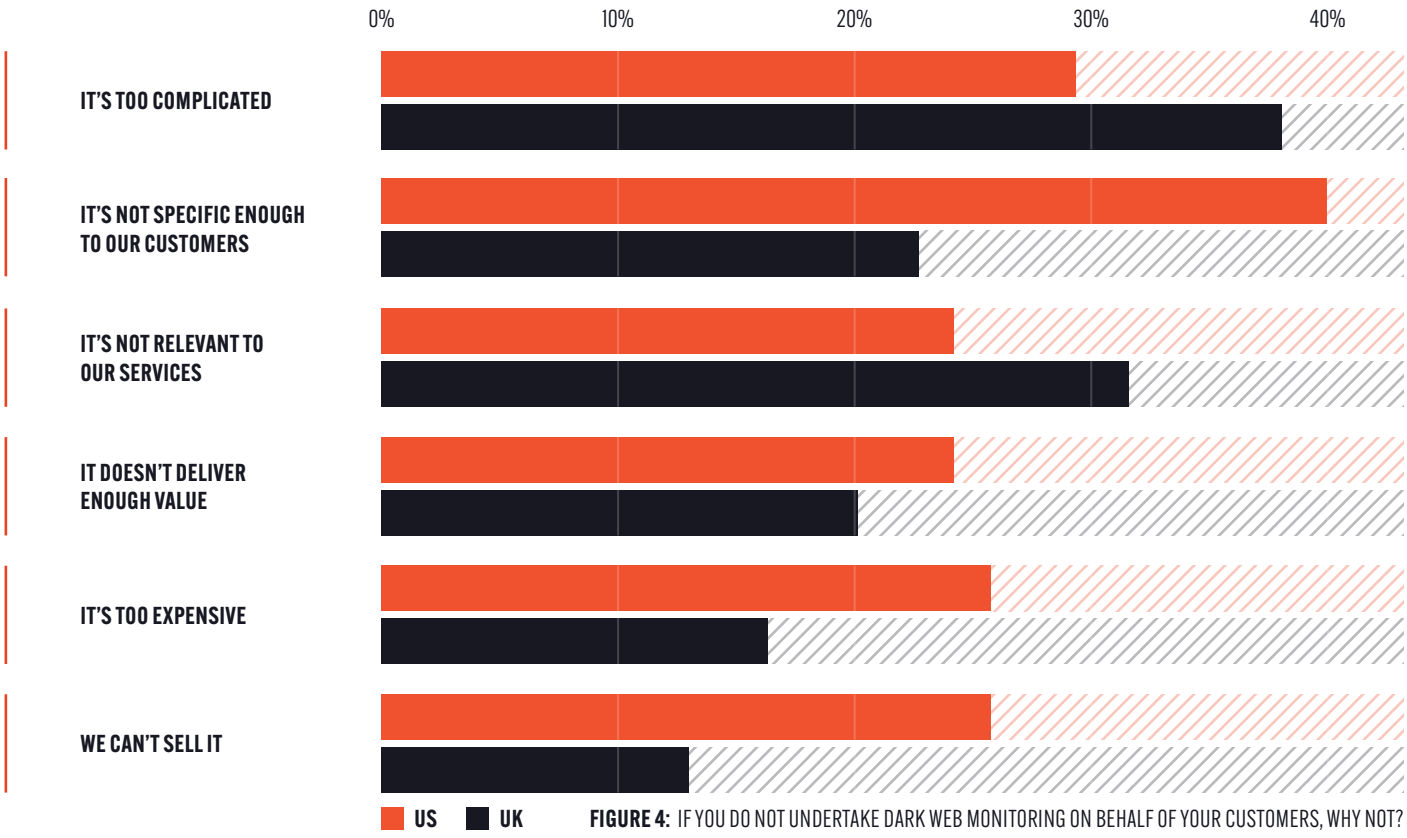



**FIGURE 4:** IF YOU DO NOT UNDERTAKE DARK WEB MONITORING ON BEHALF OF YOUR CUSTOMERS, WHY NOT?

In the US, the main barrier to adoption is the perception that dark web intelligence is not specific enough to customers. Complexity is the next most popular answer in the US and is, by far and away, considered to be the biggest barrier to adoption in the UK.

## BEN JONES, CEO OF SEARCHLIGHT CYBER, GAVE HIS TAKE ON THE RESPONSES:

"At first glance the rebuttal of dark web intelligence not being "specific enough" to customers might appear strange, given that it is clearly something MSSPs' customers are asking for. However, this finding probably refers to the quality of data gathered from the dark web, and its relationship to their customers.

"While "general trends" of what is happening in the dark web are useful in understanding the threat landscape, MSSPs know that they also need actionable intelligence to help their customers. What they are looking for is data that will warn them of an imminent threat against a specific organization, which provides clear actions they can take.

"MSSPs can derive this kind of insight from the dark web but they need to find the right dark web intelligence provider. This relates to the "complexity" point. The last thing MSSPs need is another tool generating alerts on generic dark web threats, or swamping them with dark web data that is unintelligible. They need to find a partner that can derive specific, actionable data for them and provide them with the context to make it simple for their customers."

### INSIGHTS FROM THE FIELD

**SOUMEN PAUL** // FOUNDER AND HEAD OF CONSULTING, ICYBER DEFENCE

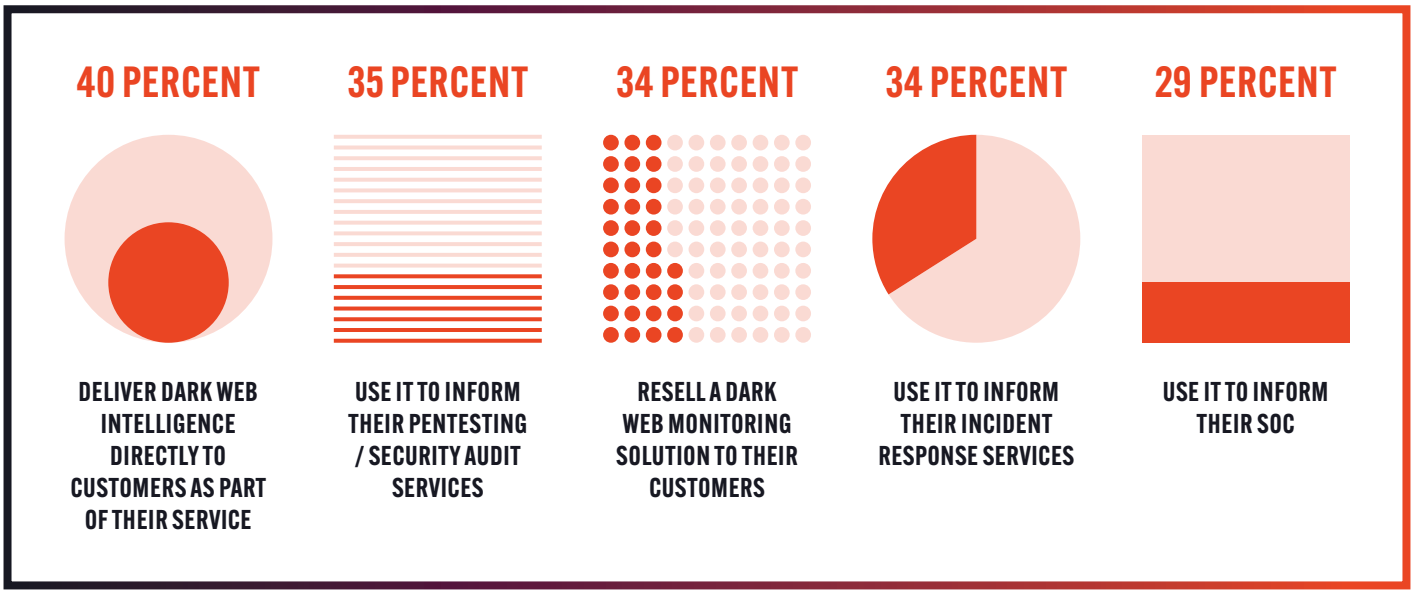
> Adding dark web threat intelligence to our offering has been immensely valuable, both to our service and our business. As called out in this report, customers are increasingly asking for insights about the dark web, and for support in monitoring it for threats that could impact their brand and people. By gathering intelligence from the dark web, we are helping them pick up threats before they reach their security perimeter.

# BUILDING DARK WEB MONITORING INTO THE BUSINESS MODEL

Another interesting group to call out from **Figure 4** are the MSSPs (26 percent in the US, 13 percent in the UK) who say that they aren't using dark web intelligence because of the belief that they can't sell it.

As we know, the MSSPs who have adopted dark web monitoring have not only successfully sold it, but they're actually creating new revenue streams. So how are they doing it?

We asked MSSPs how they use dark web monitoring as part of their services:




## BEN JONES, CEO OF SEARCHLIGHT CYBER COMMENTED:

"These results also demonstrate a missed opportunity for some of the MSSPs that are already using dark web intelligence. While its use in one-off engagements - such as pentests, security audits, and incident response - is popular, its use in MSSPs' Security Operations Center (SOC) is lagging behind.

"This means many MSSPs are missing a trick in integrating dark web intelligence into their value proposition and hence recurring revenues, where they could be capitalizing month-on-month. To take advantage of this opportunity, MSSPs need solutions that facilitate continuous dark web monitoring for their customers. This would allow them to build new revenue streams into their SOC, while assuring their customers that they are always across emerging dark web threats that could impact them."

# CHOOSING THE RIGHT DARK WEB INTELLIGENCE PROVIDER

One factor that may be influential in determining whether MSSPs can successfully sell dark web intelligence is the partner vendor they use to source it. Indeed, for the very few MSSPs who reported that they are unhappy with their current dark web intelligence provider, the number one reason (37 percent) was that they have trouble fitting dark web data with their current business model.

MSSPs looking to take on dark web intelligence as part of their remit should therefore make sure their provider not only ticks the boxes in terms of data sources and cost, but also that they tailor their product to how MSSPs do business.

**DO THEY:**

- ☐ MINIMIZE UPFRONT COSTS SO THAT YOU ONLY PAY FOR AS MUCH AS YOU SELL?
- ☐ MAKE IT EASY FOR YOU TO MANAGE YOUR ENTIRE CUSTOMER BASE THROUGH ONE PORTAL?
- ☐ PROVIDE DIFFERENT MODELS FOR ONE-OFF ENGAGEMENTS (SUCH AS PENTESTS) AND ONGOING DARK WEB MONITORING (FOR MANAGED SERVICES)?

As this research demonstrates, there is already a huge opportunity for MSSPs that are able to integrate dark web intelligence into their services. As this topic grows in prominence, those that have started to build out their capabilities, data sources, and understanding will be able to capitalize as more customers look for guidance on the dark web, giving them an advantage in the competitive market of managed security services.

> MANY MSSPS ARE MISSING A TRICK IN INTEGRATING DARK WEB INTELLIGENCE INTO THEIR VALUE PROPOSITION AND HENCE RECURRING REVENUES, WHERE THEY COULD BE CAPITALIZING MONTH-ON-MONTH.

SEARCHLIGHT. CYBER

# DARK WEB INTELLIGENCE

## FOR MSSPs

## ENHANCE YOUR SECURITY WITH THE WORLD'S MOST COMPREHENSIVE DARK WEB DATASET

MSSPs use Searchlight Cyber to proactively find the assets, vulnerabilities and activity on the dark web that could impact their customers - to deliver intelligence, prevent attacks, and prove their ROI from day one.

## BUILT WITH MSSPs IN MIND

### SPECIFIC, ACTIONABLE INTELLIGENCE ON YOUR CUSTOMERS

Identify indicators of a possible cyberattack, such as leaked credentials, IP addresses, open ports, compromised devices, and dark web traffic.

### INTUITIVE INTERFACE BUILT FOR MANAGING MULTIPLE CUSTOMERS

Easily monitor your entire customer base through one multi-tenant environment, without having to toggle between profiles.

### INSTANT HEALTH REPORT

Start every customer engagement with a snapshot of where they are exposed on the dark web, delivered in minutes.

### UPSELL OTHER SERVICES

Use dark web intelligence as a basis for service wraps including consultancy and certifications.

### INFORM INCIDENT RESPONSE

Forensically examine the chain of events in the dark web that led to a cyberattack.

### MODELED THE WAY YOU DO BUSINESS

Strategic licenses for managed security services or 30 day tactical licenses for one-off customer engagements.

# PROTECT CUSTOMERS FROM DARK WEB THREATS WHILE OPTIMIZING YOUR MARGINS

## STRATEGIC LICENSES
FOR MANAGED SECURITY

### PRICING

- PAY MONTHLY
- PAY BY LICENSE
- PAY AS YOU SELL

### BENEFITS

**LEAN**

No requirement to buy licenses in bulk.

**PROTECT YOUR MARGINS**

Easily add a license once you've converted a customer, not before!

**VALUE ADDED OPPORTUNITY**

Provide customers with direct access to DarkIQ or manage their profile as a Value Added Reseller.

## TACTICAL LICENSES
FOR ONE-OFF ENGAGEMENTS

### PRICING

BUY TACTICAL CREDITS TO CREATE 30 DAY COMPANY PROFILES IN DARKIQ

### BENEFITS

**FLEXIBLE**

One-off 30 day engagement with no strings attached.

**INTUITIVE**

Quickly understand a company's dark web exposure with reports and insights that can be easily exported.

**UPSELL INTO MANAGED SECURITY**

Extend the use of DarkIQ for another 30 days with a tactical credit or easily convert customers onto strategic licenses.

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

SEARCHLIGHT CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.


**UK HEADQUARTERS**
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

**US HEADQUARTERS**
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States