KELA REPORT

The State Of CYBER CRIME Threat Intelligence 2022

Key Findings

Here are seven of the key insights we learned from the security team members we surveyed:

- The most needed capability that defenders lack is additional training and proficiency in cybercrime investigations. Additionally, respondents want to be able to quickly access cybercrime sources in a secure and non-attributional manner and to receive an immediate notification of a suspected breach related to any organizational assets via proactive monitoring of the cybercrime underground.

- The majority of respondents (69%) are concerned that their organization's data will be released or sold on cybercrime forums, as well as other threats from the cybercrime underground.

- Additionally, many respondents don't have a way to detect if their data has been released or sold on cybercrime forums, either — only 38% say they're "very likely" to detect it. The fact that over half say they wouldn't be surprised to learn their data had been released to the cybercrime underground shows that they know their organization isn't as secure as it should be.

- Despite the majority being concerned about threats from the cybercrime underground, nearly half (48%) say they don't have a documented cybercrime threat intelligence policy in place. Those that do are outsourcing to a focused service provider, or are using a purpose-built cybercrime investigative software tool.

- Based on these findings, it unfortunately makes sense that less than half of respondents (41%) believe their current security program is very effective, and 31% say their approach is not very effective at all.

- The biggest challenge they face in successfully conducting cybercrime threat intelligence is not having system or browser isolation. They're also challenged by a lack of training or experience in cybercrime investigations and by not having visibility into private forums and private messaging groups.

- Overall, half of respondents (49%) are not satisfied with the visibility they have of the cybercrime underground. Yet even those who said they were satisfied with their visibility were still unable to prevent an attack.

Introduction

David Carmiel
CEO, Kela

Threats from the cybercrime underground emerge each day. Yet many organizations today don't see cybercrime threat intelligence as applicable to them — unaware that their private data may have already been released on the dark web and other underground sources, sold to malicious actors already planning their attack. Or, if organizations are aware of their need to monitor the cybercrime underground for potential threats, they're at a loss of talent and resources to do so effectively.

At KELA, our extensive intelligence expertise has shown us just how complex the cybercrime ecosystem really is. The threats are much more comprehensive. What organizations know and refer to as the dark web is changing within the hour. It has become an organized cybercrime ecosystem. In order to gain more insights into how organizations are approaching their cybercrime threat intelligence, we surveyed 400 security team members who are responsible for gathering cyber threat intelligence. Are they proactively scanning the cybercrime underground? What tools are they using to do so? What gaps do they see in their dark web and cybercrime threat intelligence approach? What we found is that organizations may be less prepared for cybercrime threats than they should or would like to be.

We hope these findings help you in assessing your own cybercrime threat intelligence approaches in 2022.

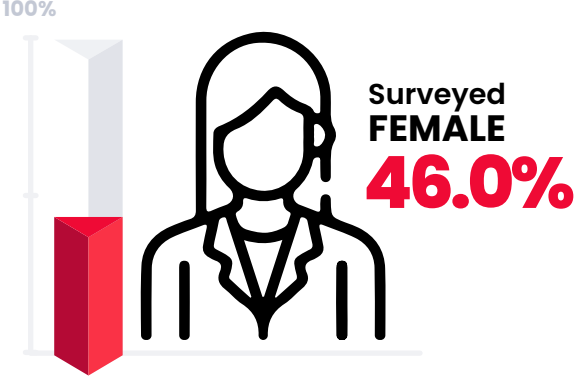
Who We Surveyed

Methodology and Participant Demographics

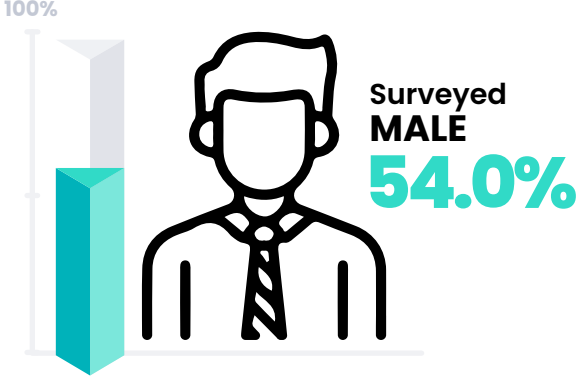
Starting on April 10, 2022, we surveyed 426 security professionals directly responsible for managing cyber vulnerabilities in their day-to-day work. The survey was conducted online via Pollfish using organic sampling. To provide greater context around the findings presented in this report, we offer more details about who we surveyed and the methodology used.
Learn more about the Pollfish methodology here.

Country Of Residence
100.0%
United States

Employment Status
100.0%
Employed for wages



Surveyed
FEMALE
46.0%



Surveyed
MALE
54.0%

Age Parameters

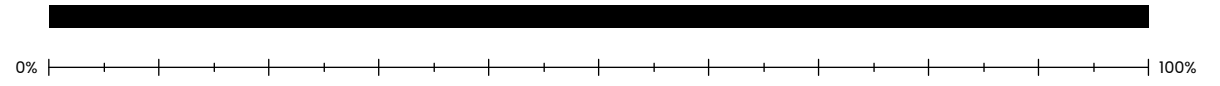
17.7%	28.2%	26.0%	11.7%	16.2%
18 - 24 YEARS OLD	25 - 34 YEARS OLD	35 - 44 YEARS OLD	45 - 54 YEARS OLD	> 54 YEARS OLD

Survey Results

What best describes the team you are on at work?

Security Team	100.0%

Which of the following most accurately describes your job duties?

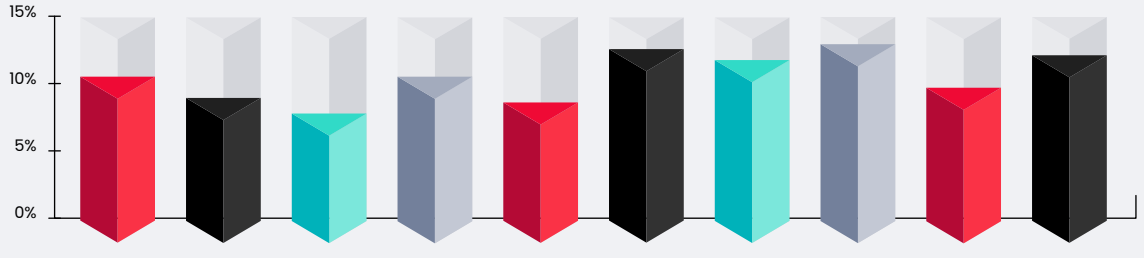


I am directly responsible for gathering cyber threat intelligence in my day to day work	100.0%

How often do you gather threat intelligence from the dark web?

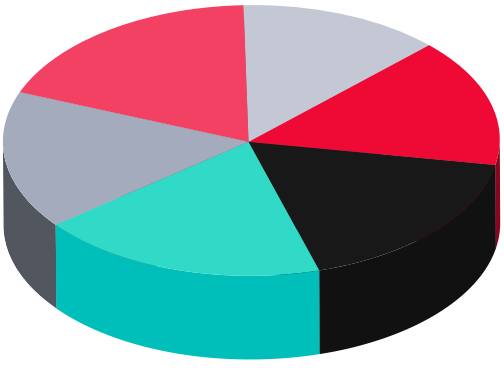
Daily	100.0%

What industry does your organization primarily operate in?



Financial services, insurance, real estate	10.2%
Higher education, K-12 education	8.5%
Non-profit	6.5%
Healthcare, biotech, pharma, medical	10.2%
Marketing, advertising, media	8.2%
IT, technology, software	12.5%
Manufacturing, warehouse, logistics	10.7%
State, local, federal government	12.2%
Military / defense	9.2%
Other	11.5%

What is your annual budget for information security?



Less than $250K	15.7%
$250k - $1M	17.1%
$1M - $5M	18.2%
$5M - $20M	17.5%
Over $20M	18.2%
I am not sure	13.3%

Section Summary

Now, with context around who our respondents were—members of security teams who are directly responsible for gathering cyber threat intelligence daily, and who work for a variety of different sectors—let's take a closer look at what we uncovered.

Table of Contents

Part #1

Cybercrime Threat Awareness

There's a lot of information swirling around the cybercrime underground—which may include your organization's data that you might not have realized was stolen and released. Security teams monitor their current environment for vulnerabilities, as well as the clear web for malicious threats, but are they including dark web and other cybercrime sources monitoring in their intelligence strategy? Or is a lack of visibility into the these sources creating a dangerous blind spot?

69% are concerned about threats from the dark web

69.0% of our respondents say they have some level of concern over threats from the dark web: 36.2% are very concerned about threats, and 32.8% are somewhat concerned. However, 31% say they're not very concerned about threats.

How concerned are you about threats that emerge from the dark web?

Over half say they would not be surprised to find their organization's private data on the dark web

48.5% of our respondents said they would be surprised to find their organization's private data on the dark web, which likely means they have the tools and methods in place to protect their organization from breach — and would be surprised to find it happened. However, 51.5% said they would not be surprised to find their data on the dark web, meaning that they know their organization isn't as protected as it should be.

Would you be surprised to find your organization's private data on the dark web?

30% say they're not very likely to be able to detect their data on the dark web

If their organization's private data was released on the dark web, how likely would they be to detect it using their current tools and resources? Only 38.0% believe that they're very likely to detect it. An additional 32.2% believe that they're somewhat likely to detect it, and 29.8% believe they're not very likely to detect it at all.

If your organization's private data was released on the dark web, how likely would your team detect it?

They're concerned about customer data and intellectual property or trade secrets being released on the dark web

Our respondents are generally concerned about all different types of data being released on the dark web. However, the largest segment (18.7%) is concerned about customer data being released, with the second largest segment (17.7%) worried that intellectual property or trade secrets will end up on the dark web.

Respondents are also concerned about personally identifiable information (PII) (15.7%) and controlled unclassified information (CUI) (15.7%) making it onto the dark web. Finally, they're concerned about financial data (15.2%) being leaked.

16.7% of respondents were concerned about other information being released not mentioned here.

What type of data are you most concerned with being exfiltrated and released on the dark web?

Personally identifiable information (PII)	15.7%
Customer data	18.7%
Intellectual property / trade secrets	17.7%
Controlled unclassified information (CUI)	15.7%
Financial data	15.2%
None of the above	16.7%

Section Summary

Attacks against organizations have only increased in recent years, and it's not enough for security teams to remain on the defensive. But a proactive approach to security not only means assessing threats and gathering intelligence from the clear web, it means having a proactive approach to assessing threats on the dark web and other complicated internet sources as well.

In surveying security team members, we found that when it comes to cybercrime threat intelligence, there's awareness and urgency, but not from everyone. Only 69.0% say they're concerned about threats from the dark web.
Nearly a third are not very concerned—they're not only ignoring the potential threat from dark web activity, but downplaying the necessity to dedicate tools and capabilities to detection.

The fact that 52.0% say they wouldn't be surprised to find their organization's private data on the dark web means they're aware of the potential danger the activity taking place on the dark web provides, yet may also feel unable to stop their data from being exfiltrated. Even if their data were to be released on the dark web, 30.0% say it's not very likely they'll detect it anyhow, with an additional 32.0% believing they'd only be somewhat likely to detect it.

In our next section, we'll uncover some of the reasons why they may not be as actively monitoring the dark web or as proficient in their efforts as they should be.

Part #2

Current State of Monitoring the Cybercrime Underground

It's crucial that organizations include dark web and cybercrime threat intelligence intelligence as part of their overall security strategy, in order to find if any data has been released so they can take action to protect against any resulting attacks. Being familiar with the dark web can also help security teams better understand threat trends as well. But do organizations have the right tools and capabilities in order to conduct dark web monitoring and threat intelligence investigations?

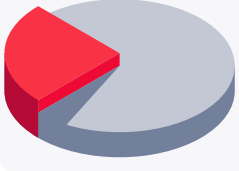
48% have no documented dark web threat intelligence policy in place

52.0% of respondents say they have a documented dark web threat intelligence policy in place to guide their actions and responses. However, 48.0% do not.

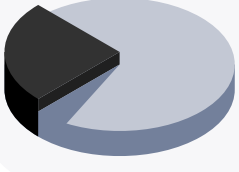
Do you have a documented dark web threat intelligence policy in place?

They monitor by either outsourcing to a service provider or using purpose-built software

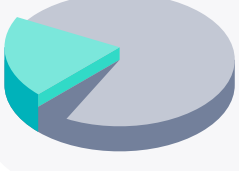
For those who do have a documented dark web threat intelligence policy in place, here are the top ways that they monitor for threat intelligence:



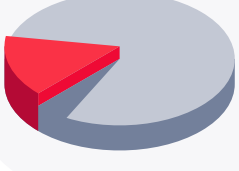
23.5% - Outsourced to a service provider focused on the dark web: The largest segment of respondents outsource their dark web threat intelligence to a service provider, and rely on their expertise to uncover threats and identify trends.



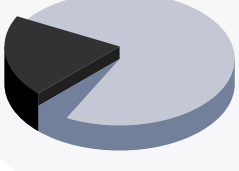
23.0% - Purpose-built dark web investigative software tool : Nearly the same amount of respondents are using their own internal purpose-built dark web software to monitor for leaked data and to gather intelligence.



18.2% - Existing threat intelligence tool that monitors the dark web for keywords, but does not allow direct access: Respondents are also using existing tools that are able to monitor the dark web for keywords related to their organization, but the tool does not give them direct access to the dark web.

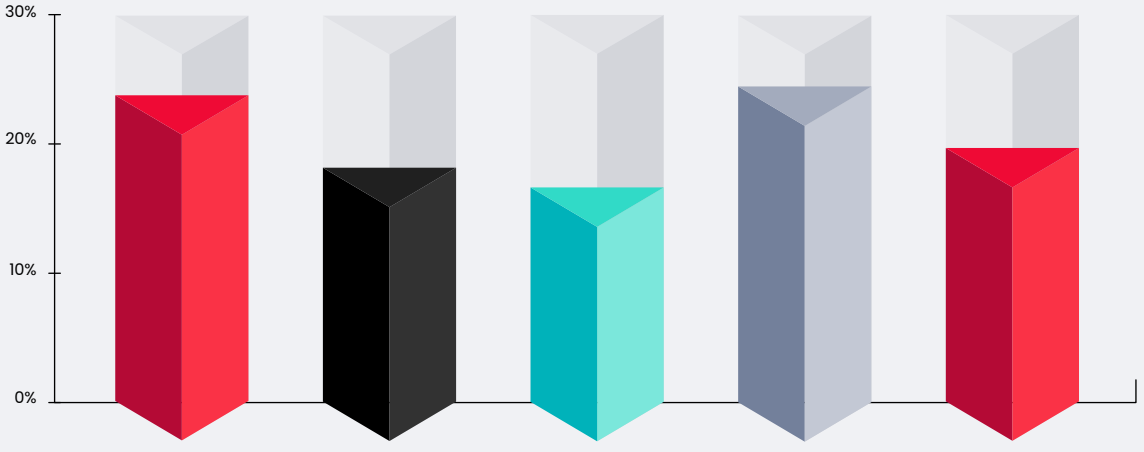


16.8% - Direct access to the dark web via a tool such as TOR: Others use a browser like TOR or other proxy that allows them to directly access the dark web to do their own investigations, but that may not necessarily do any automated monitoring or detection.



18.2% - Other: Finally, the remainder use an approach not listed here.

If yes, what best describes how you monitor the dark web for threat intelligence?



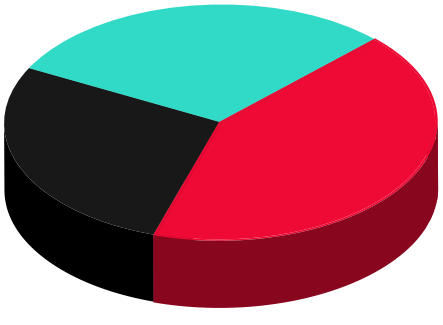
Purpose-built dark web investigative software tool	23.0%
Existing threat intelligence tool that monitors the dark web for keywords, but does not allow direct access	18.2%
Direct access to the dark web via a tool such as TOR	16.8%
Outsourced to a service provider focused on the dark web	23.5%
Other	18.2%

Only 41% believe their current security program is very effective at monitoring the dark web

Is their current security program effective at dark web monitoring for threat intelligence? 40.7% believe their program is very effective, with an additional 28.5% saying it's somewhat effective. However, 30.8% say their approach is not very effective.

For those who replied that their approach is very effective, the largest segment of respondents is using a purpose-built dark web investigative software tool, and 58.9% have a documented dark web policy in place.

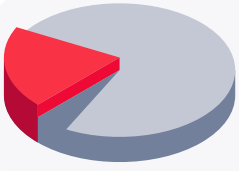
Overall, how effective would you say your current security program is at dark web monitoring for threat intelligence?



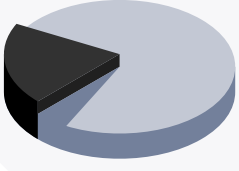
Very effective	40.7%
Somewhat effective	28.5%
Not very effective	30.8%

Specific training for analysts on conducting dark web threat intelligence investigations is what makes their program "very effective"

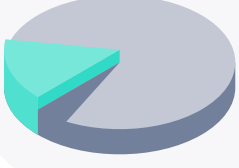
Of those in the previous question who replied that their program is very effective, they had the following reasons for why they believe it to be so effective.



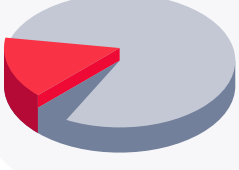
19.6% - The largest segment of respondents attribute their effectiveness to **specific training for analysts on conducting dark web threat intelligence investigations** — in other words, knowledgeable and skilled team members are the key to their success.



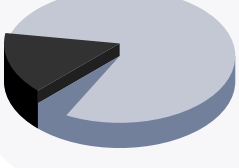
17.7% - The second largest segment say their program is effective because they use an **internet connection separate from the corporate network in order to conduct their investigations.**



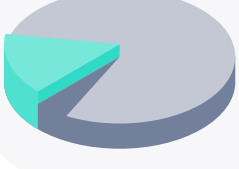
16.5% - Similarly to using separate internet access, say their program is very effective because they use **dedicated investigative workstations or virtual machines that are recomposed after dark web threat intelligence investigations.**



16.5% - The same amount attribute their success to **written policies and procedures for auditability, chain of custody, evidence gathering, purchasing dark web data, and other initiatives.**



15.3% - Their effectiveness is because of the **method or tool they use to connect to the dark web.**



14.1% - Finally, the smallest segment says they're very effective because of the **involvement of legal counsel to create specific "rules of engagement" for analysts conducting threat intelligence dark web investigations.**

What's of note here is that there's only a 5.5% split between the largest segment and the smallest segment, and that those who say their security program is "very effective" are finding it effective because of all different factors — from personnel, to the methods used to connect to the dark web, to their policies and procedures. The method may be effective for them, but not for others, and we don't necessarily find one specific factor that will create an effective program for everyone.

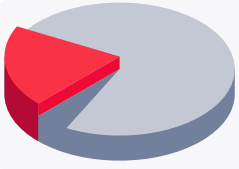
One reason for this pattern of variation could be a lack of training and awareness, resulting in the security team not fully understanding how to run an effective cybercrime threat intelligence program. Another reason could be playing catch-up to the major changes over the past two years in the cybercrime underground, and still trying to figure out the best approach to combat the increase in crimes and threats coming from the cybercrime underground.

What would you say is the #1 thing that makes your program/strategy so effective?

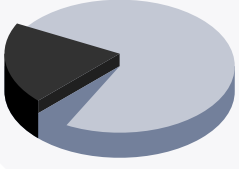
Separate Internet connection from corporate network to conduct investigations with	17.7%
Dedicated investigative workstations or virtual machines that are recomposed after dark web threat intelligence investigations	16.5%
Specific training for analysts on conducting dark web threat intelligence investigations	19.6%
Involvement of legal counsel to create specific "rules of engagement" for analysts conducting threat intelligence dark web investigations	14.1%
Written policies and procedures for auditability, chain of custody, evidence gathering, purchasing dark web data, etc.	16.5%
Method / tool used to connect to the dark web	15.3%

Top Most-Wanted Tools Missing from Dark Web Monitoring Programs

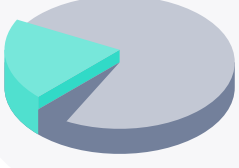
When asked what they thought was missing from their dark web monitoring program, our respondents said the following:



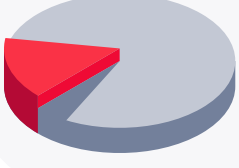
18.5% - Method or tool used to connect to the dark web: As we saw above with some respondents using a method for monitoring without access, the number one tool they see missing from their program is a way to access the dark web — which is the first step if you want to monitor it for intelligence.



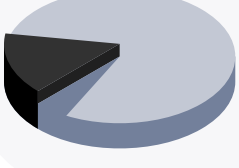
18.2% - Internet connection separate from corporate network through which to conduct investigations: Similarly, respondents say they have a way to access the dark web, but it's currently through their own company network. Or, they're waiting for separate VPN access to be created before setting up dark web access altogether.



18.0% - Dedicated investigative workstations or virtual machines that are recomposed after dark web threat intelligence investigations: They're also missing dedicated workstations or virtual machines through which to conduct threat intelligence investigations, and are either using their own machines or waiting to start until they get dedicated workstations.



17.2% - Specific training for analysts on conducting dark web threat intelligence investigations: Considering the largest segment above attributed their success to trained analysts, this segment sees the training, knowledge, and skills missing from their current approach.



14.7% - Written policies and procedures for auditability, chain of custody, evidence gathering, purchasing dark web data, etc.: Lower down the list is the need for a set of policies and procedures directing how their team should go about dark web threat intelligence.

13.2% - Involvement of legal counsel to create specific "rules of engagement" for analysts conducting threat intelligence dark web investigations: Finally, the smallest segment see the involvement of legal counsel missing from their current approach.

In looking at the top three selections, what our respondents are missing the most from their current dark web monitoring program is access: a way to access the dark web, secure internet through which to do it, and dedicated machines that can perform the work.

What do you think is missing from your dark web monitoring program?

Separate Internet connection from corporate network to conduct investigations with	18.2%
Dedicated investigative workstations or virtual machines that are recomposed after dark web threat intelligence investigations	18.0%
Specific training for analysts on conducting dark web threat intelligence investigations	17.2%
Involvement of legal counsel to create specific “rules of engagement” for analysts conducting threat intelligence dark web investigations	13.2%
Written policies and procedures for auditability, chain of custody, evidence gathering, purchasing dark web data, etc.	14.7%
Method / tool used to connect to the dark web	18.5%

Section Summary

As we found in the previous section, there are a number of respondents who are concerned about threats from the dark web, yet who believe they'll be likely to detect their organization's data if it was released there. However, there are a number of respondents who remain unconcerned and unprepared.

In looking further into their various approaches to cybercrime threat intelligence, we found that 48.0% have no documented dark web threat intelligence policy in place — which puts them at a lack for ways to monitor and detect threats on the cybercrime underground. Of the 52.0% who do, they're either outsourcing their dark web threat intelligence to a service provider, or using a purpose-built dark web investigative software tool. Despite the approach they're taking, however, only 41.0% believe their current security program is "very effective" at monitoring the dark web.

What makes a dark web threat intelligence program "very effective"? Respondents attribute their success to having specific training for analysts on conducting cybercrime threat intelligence investigations. They also say it's key to use an internet connection separate from the corporate network — and what they say is missing most from their approach are methods or tools used to connect to the dark web and other cybercrime sources. However, considering the increase in new threats coming from the dark web and the rapidly evolving cybercrime underground, what they find "very effective" today might not keep up with tomorrow's security needs.

What's become clear in this section is that for security teams wanting to create an effective cybercrime threat intelligence program, two things are needed: trained analysts who know how to conduct cybercrime investigations, and a secure network and dedicated machines through which to do so. It's hard to conduct dark web threat intelligence if you have the right people but no access; it's also hard to conduct threat intelligence if you have safe access to the dark web, but don't know what you're looking for.

In our next section, we'll look at a few more of the challenges security teams face each day with dark web access and detection.

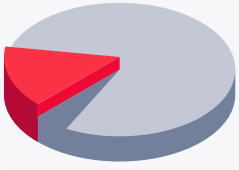
Part #3

Challenges to Dark Web Threat Intelligence

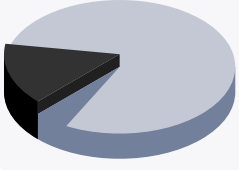
The cybercrime underground is intended to be invisible, secret and a constantly changing environment. Because of its ever-shifting nature, dark web threat intelligence can be a challenge to even the best of security teams. This is why visibility into the dark web in order to monitor for exfiltrated data and gather intelligence in order to prevent an attack is so important. Here are some of the pain points our respondents are looking for solutions to address.

Top Challenges to Monitoring the Dark Web

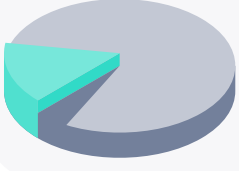
Monitoring the dark web for threat intelligence is necessary, but not always easy. Respondents say that when it comes to monitoring, their top challenges are:



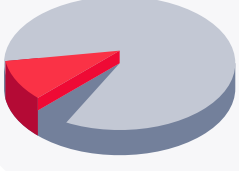
15.7% - No system or browser isolation, placing their current system at risk of compromise: Their number one challenge stems from the concerns we saw above regarding separate VPN access and dedicated workstations.



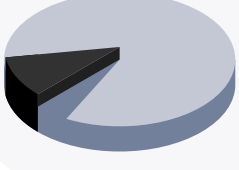
14.2% - Lack of training or experience in dark web investigations: After network requirements, respondents felt there was a lack of trained analysts doing dark web investigations, or those on their team with the necessary experience.



13.5% - Lack of support from the organization (e.g., management, legal, etc.): They're also finding a lack of leadership support and buy-in, from policies and procedures, to budgetary allotment for new machines, to legal counsel's guidance.



12.5% - Difficulty finding relevant information on the dark web: Another challenge is being able to find relevant information and intelligence on the dark web — perhaps linking back to the need for trained analysts to know where to look.



11.7% - Difficulty in accessing various dark web sources: Finally, they're also challenged by accessing sources on the dark web, which could also stem from the lack of training as well, but could also stem from the lack of straightforward access.

Other challenges include no ability to manage attribution (11.2%), no separate network to conduct dark web investigations (10.5%), and not enough internal resources to conduct dark web investigations with regularity or with which to become proficient (10.5%).

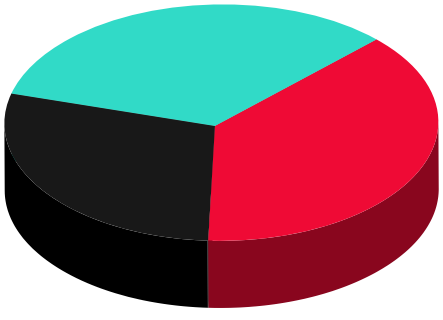
What are your top challenges when it comes to monitoring the dark web for threat intelligence?

No ability to manage attribution	11.2%
No system or browser isolation, placing a system at risk of compromise	15.7%
No separate network to conduct dark web investigations	10.5%
Lack of training or experience in dark web investigations	14.2%
Lack of support from the organization (e.g., management, legal, etc.)	13.5%
Not enough internal resources to conduct dark web investigations with regularity or become proficient	10.5%
Difficulty in accessing various dark web sources	11.7%
Difficulty finding relevant information on the dark web	12.5%

37% said strategic intelligence is the most challenging to collect from the dark web

In continuing to look at the challenges they face, respondents were somewhat evenly split between what type of intelligence they find difficult to collect from the dark web. For 36.8%, strategic intelligence is the hardest to collect. 32.2% found operational intelligence hardest to collect. 31.0% said tactical intelligence is the hardest to collect.

Which type of intelligence do you find most challenging to collect from the dark web?

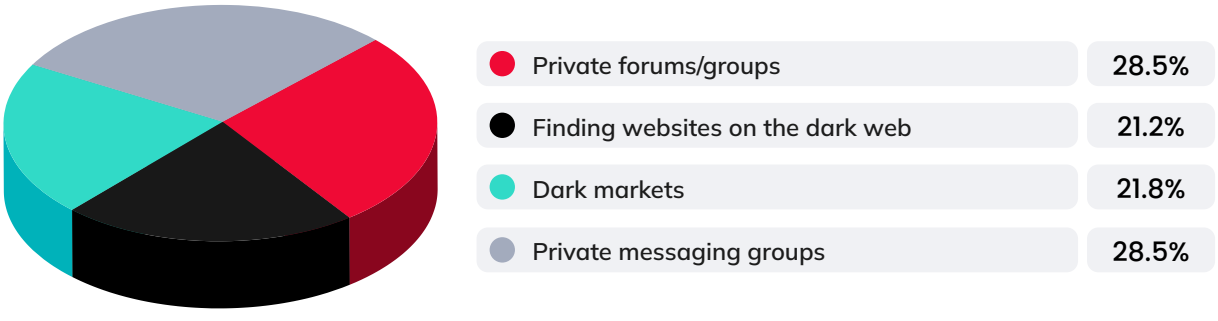


Strategic Intelligence	36.8%
Tactical Intelligence	31.0%
Operational Intelligence	32.2%

They have the least visibility into private forums and groups, and private messaging groups

When it comes to visibility into the cybercrime underground,, respondents have the least visibility into private forums and groups (28.5%) and into private messaging groups (28.5%). Others have the least visibility into dark markets (21.8%), and others have the least visibility into finding websites on the dark web (21.2%).

What areas of the dark web do you have the least visibility on?



49% are not satisfied with the visibility they have of the dark web

When it comes to their visibility into the dark web, only about half (51.2%) are satisfied with the visibility they currently have. 48.8% are not.

Are you satisfied with the amount of visibility you currently have into the dark web?

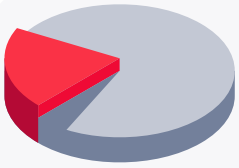
Despite being satisfied with their visibility, 39% were still unable to prevent an attack

Of those who, in the last questions, replied that they were satisfied with their visibility, only 61.0% were able to prevent a possible attack on their organization based on that visibility. 39.0% were not able to do so.

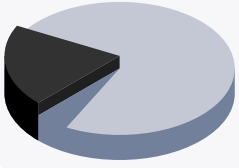
Were you able to prevent a possible attack on your organization based on that visibility?

Top Benefit of a Dark Web Monitoring Strategy

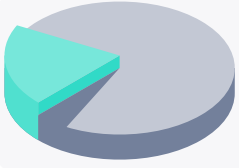
Finally, what types of benefits do our respondents see their dark web monitoring strategy providing to their organization?



18.7% - The largest segment of respondents **see their monitoring program as being able to reduce their risk and enhance their security resilience.**



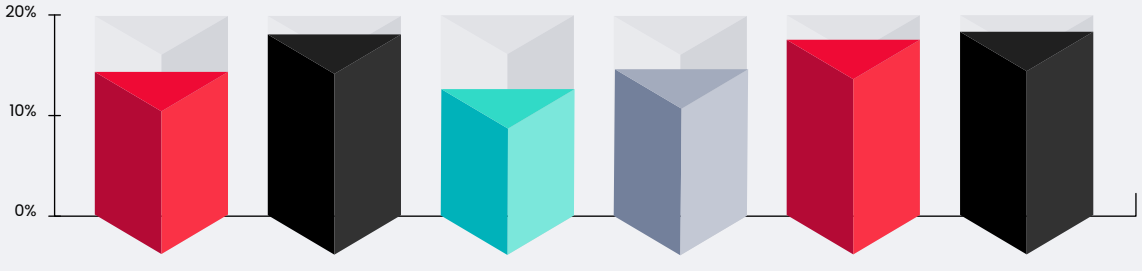
18.5% - Another similarly-sized segment say **their dark web monitoring helps them better understand and prevent threats to their executives or their organization, like solicitations to compromise a network or harm an individual.**



18.0% - Finally, the smallest segment of the top three benefits say **they benefit from learning about new vulnerabilities that are actively being targeted.**

Additional benefits include gathering intelligence about potential breaches of an organization (15.7%), finding adversaries offering access to an organization's networks (Access as a Service) and being able to perform takedowns (15.5%), and monitoring online forums and chatter about new zero day exploits (13.5%).

What benefits does your dark web monitoring strategy provide your organization?



Gathering intelligence about potential breaches of an organization	15.7%
Understanding threats to executives and/or organizations (e.g., solicitations to compromise a network or harm an individual) and being able to prevent them	18.5%
Monitoring online forums and chatter about new zero day exploits	13.5%
Finding adversaries offering access to an organization's networks (Access as a Service) and being able to perform takedowns	15.5%
Learning about new vulnerabilities that are actively being targeted	18.0%
Reduce risk and enhance security resilience	18.7%

Section Summary

In the previous section, we learned that security teams need two things for successful cybercrime threat intelligence: analysts who know how to conduct investigations, and access through which to do so. So it should be no surprise that in this section, the top challenges respondents face are similar. The biggest challenge is that they don't have a system or browser dedicated to accessing the dark web and other hidden sources, and they lack training or experience in cybercrime intelligence investigations. Because an isolated network, dedicated machines, and training take investment, their third challenge is a lack of support and buy-in from their organization to invest in dark web detection and investigation.

Other challenges include what type of data they want to find, with strategic intelligence being most challenging to collect from the dark web. They're also challenged with their visibility into private forums and groups, and private messaging groups. Overall, 49.0% are not satisfied with the visibility they have of the cybercrime underground — and of the 51.0% who were satisfied with their visibility, 39.0% were still unable to prevent an attack anyhow.

Considering these deficiencies — training, technology, buy-in, and visibility — what are the top priorities for security teams going forward?

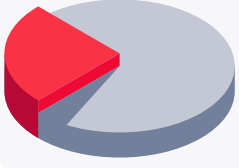
Part #4

Priorities for the Future

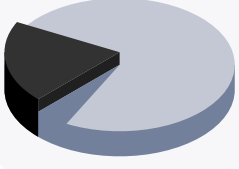
Protecting an organization's data and assets effectively and proactively is a much more involved process than it was just five years ago. Considering the rising threats to organizations in general, and the rise in use of the cybercrime underground through which to release stolen data specifically, we wanted to learn more about what our respondents' priorities are for the future of their approach to the dark web.

Top Most Helpful Capabilities for Dark Web Threat Intelligence

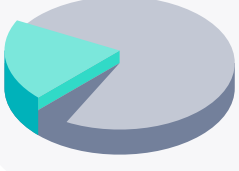
Considering that in the last section we found gaps in the efficacy of their current program, we wanted to know what features or capabilities would help our respondents the most to be able to use the dark web as a source of threat intelligence? While different respondents see different choices as beneficial, here's how they ranked overall:



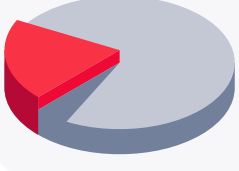
22.7% - Additional training and proficiency in dark web investigations: As we saw above, respondents' teams are lacking trained analysts proficient in dark web investigations — which is what they believe will help them be more effective in their security.



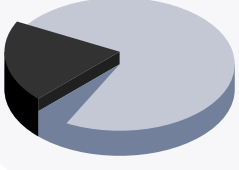
20.7% - Quickly access the dark web in a secure and non-attributional manner: Again, respondents are looking for ways to access the dark web securely that won't compromise their network or systems.



20.2% - Proactive monitoring of the dark web for organizational assets by a third-party and providing immediate notification of a suspected breach: They're also looking for a service provider who can proactively monitor the dark web for them and provide alerts and notifications when needed.

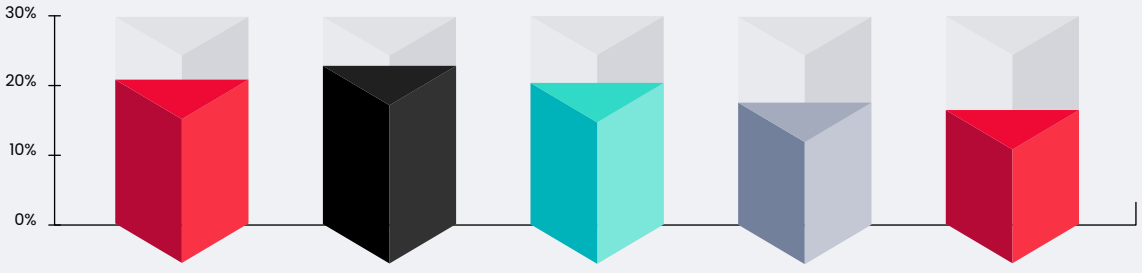


18.2% - Searching across dark web sources (forums, paste sites, leaked databases and data dumps, etc.): Respondents also want the ability to better search across the dark web, which relates to their challenges above of having difficulty finding relevant information on the dark web and accessing various dark web sources.



18.0% - Understanding of vulnerabilities actively being exploited, including zero day attacks: Finally, they want a way to better understand their vulnerabilities by knowing what information has been released on the dark web

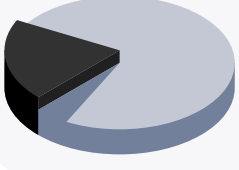
Which features/capabilities would help you the most with effectively use the dark web as a source of threat intelligence?



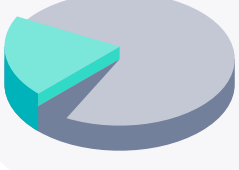
Quickly access the dark web in a secure and non-attributional manner	20.7%
Additional training and proficiency in dark web investigations	22.7%
Proactive monitoring the dark web of organizational assets by a third-party and providing immediate notification of a suspect breach	20.2%
Searching across dark web sites (forums, paste sites, leaked databases and data dumps, etc.)	18.2%
Understanding of vulnerabilities actively being exploited, including zero day attacks	18.0%

Top Priorities for Cybercrime Threat Intelligence

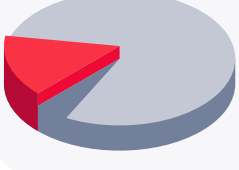
When it comes to the priorities of their dark web threat intelligence program, here's what our respondents are focusing on over the next year:



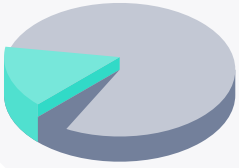
18.5% - The largest segmen is **focused on adding additional analysis capabilities to their dark web program, such as analyzing images for exif data and documents for metadata.**



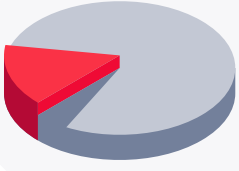
18.2% - Say they'll be **creating capabilities to regularly integrate dark web monitoring and research into their cyber threat intelligence workflow.**



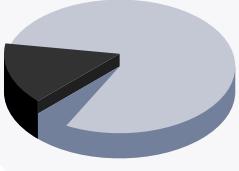
16.7% - Since one of the concerns above was connecting safely to the internet using dedicated machines, this segment will be focused on **obtaining a non-corporate network connection and separate systems to access the dark web directly.**



16.0% - Next, respondents want to **develop policies and procedures for dark web access in coordination with management and legal counsel.**

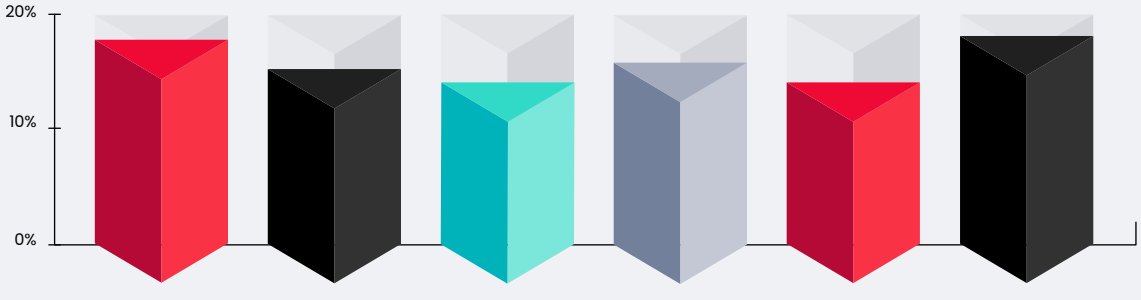


15.0% - Will be focused on **enriching their threat intelligence program with data from more dark web sources.**



15.0% - Finally, an additional percentage want to focus on **selecting a third-party vendor to provide access and visibility to relevant threats emerging in the dark web.**

What would you say is the #1 priority of your dark web threat intelligence program over the next 12 months?



Creating a capability to regularly integrate dark web monitoring and research into our cyber threat intelligence workflow	18.2%
Developing policies and procedures for dark web access in coordination with management and legal counsel	16.0%
Selecting a third-party vendor to provide access and visibility to relevant threats emerging in the dark web	15.0%
Obtaining a non-corporate network connection and separate systems to access the dark web directly	16.7%
Enriching our threat intelligence program with data from more dark web sources	15.0%
Adding additional analysis capabilities to our dark web program, such as analyzing images for exif data and documents for metadata	18.5%

Section Summary

From the insights in previous sections, it may be a bit easy to anticipate what security teams will focus on for 2022. The top capability they want to evolve to help them become more effective at cybercrime threat intelligence is implementing additional training and proficiency in cybercrime intelligence investigations across their team. They also want the ability to quickly access the dark web in a secure and non-attributional manner, likely through the aforementioned isolated networks and dedicated machines.

Another focus for the future is leveraging a third-party service provider to do their dark web threat intelligence for them, including the abilities to proactively monitor the dark web for organizational assets, and to provide immediate notification of a suspected breach. Of those who selected this response, 23.2% are using purpose-built investigation software, so want to look outside of their company for dark web monitoring. However, another 23.2% say they're already outsourcing their dark web monitoring — meaning they may not be finding the results they want with their current service provider, and hope to find a new one that offers better detection and more immediate alerts.

Finally, their top priorities include building in more analysis capabilities to their current approach, and integrating dark web monitoring and research into their cyber threat intelligence workflow — in other words, making their program more sophisticated.

Part #5
Takeaways

Organizations can't simply monitor the clear web for threats and leaked data. As new threats emerge from the cybercrime underground, and as the sophistication of attacks increases, organizations need to include cybercrime threat intelligence into their everyday security activities. Being able to uncover that data from the cybercrime underground means being able to quickly pivot to focus on specific threats, minimize the risk exposure of sensitive data, accelerate incident response and more.

Yet while many security teams do have dark web threat intelligence processes in place with trained analysts and dedicated networks and machines to their investigations, many do not. Whether it be through lack of buy-in or lack of awareness, many security teams are blind to the danger the dark web poses to their organization.

Based on what we found, here are five actions security teams should adopt today in order to better position them against threats from the cybercrime underground.

- **Monitor cybercrime sources for organizational assets**

  Having a more proactive approach to security starts with monitoring the cybercrime underground for exfiltrated and released organizational assets. But as we saw above, organizations who say they're not effective at doing this lack the training and skills to perform cybercrime intelligence investigations, as well as the isolated network and dedicated workstations to perform investigations without compromising the rest of the organization. Monitoring begins by having safe access, and knowing what you're looking for.

- **Keep up with new trends and threats on the cybercrime underground**

  Cybercrime is not only increasing, but it's getting more sophisticated and tactical. No longer are we seeing one threat actor perform an attack from start to finish, either, as many actors working in specialized niches perform each step involved in an attack — making them more complex and harder to track. Security teams intent on taking a proactive approach to cybercrime need to keep up with current trends and threats. This could be through industry websites and publications, security blogs, and other sources that are actively monitoring evolving criminal approaches.

- **Measure reduced organizational risk**

  You may be monitoring for threats from the cybercrime underground, but are you taking action to protect against that risk, and are your efforts reducing your overall organizational attack surface? Security teams need robust ways to identify and remediate vulnerabilities, assess risk, have a way to continuously monitor threats, and be proactive in securing every corner of your environment — especially your cloud environment. If you find your organization's private data released on the dark web — and many above said they wouldn't be surprised if it was — You need to take action to prevent this from happening again.

- **Analyze adversaries' behavioral patterns, personal details, and areas of interests**

  Monitoring for threats, assessing risk, and keeping on top of trends in the ever-changing world of cybercrime are great proactive approaches to keeping your organization's assets safe. But security teams should go one step further to "know thy enemy" by understanding the mindset and approaches of the

adversaries attempting to attack them. Learning their behavioral patterns, methods of attack, areas of interest, and even personal details will help you better anticipate their next move — and take action to protect your organization before they get there.

- **Define best mitigation actions and act on valid, relevant threats**

  As we saw above, half of respondents have no documented cybercrime threat intelligence policy in place. Another action security teams can take to more proactively protect their environment in a consistent way is to have a strategy for response, which includes defining the best mitigation actions to received threats. Additionally, security teams should have a way of assessing, contextualizing, and validating the threats they receive — and then act on the credible ones. Having a process in place for mitigation can also help you measure your success, and iterate towards better results.

- **Prioritizing Cybercrime Threat Intelligence**

  Threats to organizations are only going to continue to grow, both in scale and in frequency. Threat actors are always looking for vulnerabilities they can exploit — and their job becomes much easier if an organization's data is released on the dark web and that organization isn't monitoring for it. In order to proactively protect data and assets from breach, theft, or exploit, security teams need to make cybercrime threat intelligence — including training and access — a priority for 2022.