Tegus Transcript

Dataminr - Vice President of Intelligence at Flashpoint

Interview conducted on August 30, 2022

Senior Director, Collections & Monitoring at Flashpoint

VP, Intelligence at Flashpoint, a competitor to SpyCloud. The expert is responsible for overseeing the monitoring and collections efforts, which include any data that is collected, stored, and processed to the clients. The expert also oversees the technical collections that include credentials and technical threat data. The expert noted that before SpyCloud was a company, the expert had created a very similar system/product at a previous company. The expert holds multiple patents in the industry that cover processing large quantities of malware, the processing of compromised credential data, etc. The expert is very well versed in credential breaches, stuffing, human threat intel gathering, and breach data. The expert is considered influential in this industry due to his creation of a similar SpyCloud product. The expert noted that they compete directly with SpyCloud one of their main Sub-offerings.

Tegus Client

Hello, thanks for taking the time. I'm looking to learn more about the OSINT market, around open source intel, what kind of information is available, how do customers or enterprises use this kind of open source intel, does it really provide a value, and then who are the different kinds of vendors. So I'm trying to understand a little bit more about this market. So maybe if you can start with a little bit of your background, your current role and your exposure to the space.

Vice President of Intelligence at Flashpoint

Absolutely. Yes, so my background is a little bit of a blend of threat intelligence, where I've spent the majority of my career, I would say. And then I've also got a background in malware analysis and incident response, and I did that for a large financial institute. So my current role is the Vice President of Intelligence at Flashpoint Intelligence.

And what I do in that role is I kind of oversee a lot of Flashpoint's intelligence operations, our collections efforts, so identifying new sources of information, many of which are open source, so open source intelligence. Identifying communities or sources that we want to go and collect data from to be able to provide that data back to our customers in a way that helps them search through it or be alerted to it or support any of their use cases for leveraging that type of information and that type of data.

So I do have quite a bit of exposure to open source intelligence in my current role in my background. Also at a previous company, worked a lot with open source intelligence. And I know one of the companies that was of interest on the list in the project description was ZeroFox.

ZeroFox had acquired a company called Cyveillance, which really does a lot of open source intelligence. They acquired Cyveillance from a company called LookingGlass, which was one of my former employers. So I'm pretty familiar with them through that. And so happy to dig into that when we talk a little bit more about some of the organizations.

Tegus Client

So when you talk about open source intelligence, is that more from a cyber perspective? Or I think there are two, three different segments of open source intel, right?

Vice President of Intelligence at Flashpoint

Yes. So at Flashpoint and overall throughout my career, there's definitely a couple of different perspectives

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

when looking at open source intelligence. The heaviest of my focuses has certainly been on the cyber side of things. But here at Flashpoint and at other organizations, of course, the physical security aspect of open source intelligence is absolutely massive.

It's a really critical component to how consumers of open source intelligence get value out of it for a number of different teams within commercial enterprises and then, of course, on the public sector side as well.

Tegus Client

Can you talk a little bit more about the non-cyber part of the OS intel you're referring to?

Vice President of Intelligence at Flashpoint

Yes, of course, yes. So physical security use cases can range from anything like a live breaking event. Say, for example, there's like an active shooting situation, where organizations may need to, for example, understand their situational awareness or maybe even a video proximity to a location to have an understanding of whether or not there could be an impact to their business operations.

Any impact to one of their physical maybe brick-and-mortar storefront or office locations or of course, their employees. So any impact to employees could be ranging from collateral damage-type impact to the more specific executive protection space where somebody say, for example, on Twitter may not like the political stance of an executive of a certain company may be and is deciding to take specific threats towards a specific person. Maybe an executive at an organization. And it may be deemed a credible threat that was posted on social media. And the executive protection teams really, really appreciate that type of insight.

Tegus Client

So the focus of the call, we are more interested in the noncyber use cases. Cyber is more like a tertiary thing. Which products are you aware of in this open source for noncyber use cases?

Vice President of Intelligence at Flashpoint

Yes. Good question, yes. So the ZeroFox definitely plays in that space because they had brought on those capabilities of Cyveillance, Dataminr open source. And actually, Flashpoint, my own current employer, we just announced earlier this month the acquisition of an open source intelligence company called Echosec, which plays heavily in the open source intelligence space, primarily for physical security noncyber-type use cases.

Tegus Client

Got it. So let's focus on the last part you mentioned. Can you talk about what Echosec does and how it does?

Vice President of Intelligence at Flashpoint

Yes. So Echosec is a company as I just mentioned, that Flashpoint had just acquired, where they focus on open source intelligence gathering and collection of information from a variety of different open sources. And again, just to sort of frame the conversation, when I'm saying open sources, I mean are things that are available through search engines.

Or that my parents could go and find online compared to, of course, like the deep and dark web stuff that Flashpoint also has a focus in on. But so Echosec, they focused primarily on open sources. Social media being a big component of that. And I think that, that's a common theme throughout the open source intelligence companies that focus in this space.

Just because we see the majority of exigent threats, imminent threats emanating from the likes of social media sites like a Twitter or other specific sites where users are actively posting and expressing frustration or anger or threats of violence. So Echosec, they do a really unique job of pulling in a lot of those open-

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

source datasets and overlaying those data sets on a map, basically. So they blend the geo intelligence to the geographic intelligence with the open source intelligence.

So Cyveillance and, therefore, ZeroFox and Dataminr, of course, have some of these capabilities, too, where if I'm a customer of one of those types of platforms or consumer of that type of information, I can draw a geo-fence on a map maybe around areas of interest, like I said, for example, maybe brick-and-mortar stores or office locations.

Tegus Client

I understand. So how does Echosec do that social media monitoring? Like you said Twitter or Facebook, how does that happen?

Vice President of Intelligence at Flashpoint

Yes. Good question. So as any of these other types of companies would do that, it would be through scraping the content on those social media platforms. Twitter, specifically, you basically need to have a corporate agreement actual contract in place with Twitter to be able to consume their information from the API at an enterprise level. You need to be able to have an established relationship, go through strict compliance checks and everything like that.

To ensure that the use cases for those data sets comply with Twitter's terms of service in how those data sets could be leveraged by the consumers of, say, an Echosec or a Dataminr or a ZeroFox platform. So when we talk about open source, Twitter is front and center, just because of the volume of information and the real-time nature of information being posted there.

Tegus Client

So quick question on Twitter, I mean I read about the Twitter firehose access versus Twitter API access. Like what are we talking about here? Like are you talking about a firehose access? Or there is a different API access that you can get? What is the product that you're talking about use?

Vice President of Intelligence at Flashpoint

From my perspective, and I don't know all of the nuances of Twitter's vocabulary from a contract perspective. The fire hose and what is available in, say, an enterprise agreement, contract paid for API for Twitter are effectively the same. And I think the difference is the volume of information and tweets that come back to you and the use cases that you're allowed to leverage.

So Echosec, and same with Dataminr and ZeroFox. They have key corporate enterprise relationships in place with Twitter to be able to consume large amounts of volume of tweets and associated metadata via an API at scale through that contracted agreement.

Tegus Client

Understood. What about, say, Facebook or other social media, how does content from those upsides get into the product?

Vice President of Intelligence at Flashpoint

Yes. So Facebook is definitely a different kind of animal there because they could forbid any type of scraping and data storage at any sort of scale just because they've really, of course, wound up in the headlines in Congress for a number of different reasons of storing users' information and what level of detail they store.

So Facebook, while I shouldn't say is a blind spot for a lot of these types of platforms, it's really one where, if there is any type of Facebook content in any of these platforms, it's really very, very surface level. It's not giving you the ability to search across Facebook's entire data corpus or be able to pull information from

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

private Facebook groups or anything of that nature.

So any content from any of these types of platforms that are related to Facebook is really going to be incredibly specific, more targeted, rather than that firehose-type approach with Twitter, as we were talking about, where you can make API queries across the entirety of Twitter's tweet database and be able to pull back information in real time. You can't do that with Facebook.

Tegus Client

Understood. So in addition to Twitter, Facebook, which other sources does Echosec get the data from?

Vice President of Intelligence at Flashpoint

Tons. There's a lot of different foreign social media, places that they're collecting from. VK is another big one, the Russian version of Facebook. Weibo, which is a social media site over in China. I'm not sure if Dataminr or ZeroFox/Cyveillance offer that type of coverage. When looking at Echosec, we thought that, that was a pretty unique capability, and we were excited to be able to offer that to our customers.

Tegus Client

Understood. And let me ask you this, with this OS intelligence data collection, how does the privacy and GDPR come in. When you talk about collecting data from VK or Weibo or Twitter or Facebook or any of these things, how does that align with the privacy regulations?

Vice President of Intelligence at Flashpoint

That's a really good question, and honestly something that I'm probably not in the best position to answer. But at a super high level, what Flashpoint and I think what these other organizations are collecting are going to be described as something that is categorized as publicly available information, so things that are published publicly.

And then at least we, at Flashpoint, we are GDPR compliant, and if we received any sort of request for removal of information, we would abide by that. But I'm probably, to be honest, not the best person to speak to the specifics of GDPR as it relates to open source collection.

Tegus Client

Got it. So just to understand that comment a little bit better, when you say that somebody's GDPR compliant, if they collect information that is publicly available, like if I put my e-mail address, my name, my date of birth, SSN on any public-facing website, then anybody could scrape that information and that would not be GDPR violation? Is that correct?

Vice President of Intelligence at Flashpoint

I'm certainly not a lawyer. And I wouldn't want to misspeak there.

Tegus Client

Got it. Because you said that if it is publicly available information, then I thought you mentioned that, that might have a lack of regulation. But then the second part is, you could still be GDPR-compliant, or if somebody says, remove my information, if you're able to do that, then you could be compliant.

Vice President of Intelligence at Flashpoint

Again, I'm certainly not a lawyer and not the best person to speak to that. But I know that, that is one of the

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

provisions of us and one of the requirements of us being GDPR compliant is that if requested, we remove information of anybody who asks.

Tegus Client

Understood. Let's switch gears for a second. I want to talk about the market opportunity or market need for this kind of OS intelligence. Can you talk about, from your perspective, who needs this? Does like everybody who need it already have it? Is it an emerging area? How do you think about the market opportunity for this open source intelligence?

Vice President of Intelligence at Flashpoint

Yes, great question. And I think Flashpoint's acquisition of Echosec is probably indicative of the larger market opportunity in general, where from my personal perspective is, I think this is going to continue to only expand and grow as we see the types of capabilities that these types of companies Echosec, Dataminr, ZeroFox.

As these capabilities expand and add more the nature of human interaction continues to shift online and more and more folks are active on social media and different types of platforms that may or may not be as regulated as others, the need to be able to have an understanding of what threats are out there that could impact your business is really, really important.

And I think that the traditional physical security-type team who may have not necessarily considered the digital aspects of physical security have, over the past year, and I'd say longer than that, too. But they are really waking up to that fact that a lot of the physical security threats that our country and that our businesses or that individuals face nowadays, there are a lot of precursors that show up online.

And being able to monitor for any indication, any early warning signs is really, really important. And not suggesting by looking at our data sets that we could have prevented a certain shooting or a certain terrorist event or anything like that, but the precursors are there.

There are manifestos that are posted in these types of communities, and had the right person been looking, searching for the right thing at the right time, there are instances where real-world violence would be able to be stopped. So a lot of these companies are really cognizant to this fact now and really get excited at the types of capabilities that folks like Echosec or Dataminr or ZeroFox bring to market.

And their physical security budgets are quite large, and there's really a need that these organizations are seeing to be able to incorporate the digital focus into what would have traditionally been like force protection when you're talking about executive protection or how you actually tap the security of your buildings or anything.

Tegus Client

So here, when you talk about the market opportunity, you are talking about the private enterprises, their desire to enhance the physical security with these kinds of products, correct?

Vice President of Intelligence at Flashpoint

Yes.

Tegus Client

So that is different from a law enforcement agency, the police department using these to prevent a mass shooting?

Vice President of Intelligence at Flashpoint

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

Yes. And that's absolutely a law enforcement-type use case in there as well from a lot of what I just discussed. But the commercial application of that as well, I'm not sure which grocery store chain there was just a shooting in yesterday or the other day, but companies need to be aware of these types of threats as well.

The Buffalo shooting from earlier in the summer, the shooter had posted a specific manifesto and explicit instructions of exactly the detailed time line of what he was going to do and where he is going to do it. And he executed it down to the minute and I'm sure that grocery store chain would have loved to see that information before it happened because it was online, which is mind-blowing, unfortunately.

Tegus Client

Understood. And do these companies like Echosec, today, do they focus more on the commercial, like the grocery chains and companies? Or do they focus more on the law enforcement side?

Vice President of Intelligence at Flashpoint

That's a good question. I can't speak to Echosec, specifically, just because it's so new for us. But overall, I would say that the use cases for physical security are there for both law enforcement and commercial. So I would expect that there is a pretty good distribution between the public sector use cases for this type of use case and the commercial side of things.

Tegus Client

Got it. I'm trying to get a sense of the market opportunity here. So from what you have seen or known, do you see the commercial opportunity to be a larger market or the law enforcement to be a larger market? And any sense of market size there?

Vice President of Intelligence at Flashpoint

Yes, I'm not typically exposed to like sales pipelines or anything like that to be able to give a breakdown of like what percentage would be public sector versus private sector opportunities and what dollar volumes there would be in place.

But just from an understanding of the size of many of these contracts and the direction, it feels like the market is heading in terms of interest from both public sector and the commercial aspect of it, I would say that this is a huge market. I wish I could tell you like there's X billion market opportunity in this space in the next quarter or something like that. But unfortunately, I just don't have that type of information.

Tegus Client

Understood. And maybe another way to look at this is to say, compared with the cybertech intel market, right, so that is a more quantified thing, do you see this? How do you compare that with the cybertech intel market? 10%, 20% or maybe orders of magnitude bigger? Is there a way to think about it that way?

Vice President of Intelligence at Flashpoint

Yes, that's a really good question and an interesting way framing it. And I think it's a difficult question to answer because I think the companies like Dataminr and ZeroFox, well, Dataminr is probably a little bit more well ingrained into that physical security use case. But ZeroFox and Echosec, I think, had traditionally been more cyber-oriented and are now kind of making their foray into that physical security use case.

And really now are getting the introductions into those physical security teams, where the typical buying center for these types of offerings is going to be more on the cyber side rather than the physical side. So I think the market share from some of these companies is probably going to be smaller than the cyber side of things.

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

But again, that's just probably because of where those companies started and the use cases that they initially had been providing. And with that being said, though, that probably gives a little bit of insight into the opportunity that is there for the physical security use cases.

And I think it's really just a matter of a lot of these organizations and these companies being introduced to the right teams within the physical security departments, now that those physical security teams are seeing more of a need to incorporate the online threat into their into their portfolio.

Tegus Client

Got it. And in terms of the market adoption, like how many people use like a Dataminr or a Echosec? Like how well understood are the capabilities of these products? How many customers kind of use these products?

Vice President of Intelligence at Flashpoint

Yes. I know Dataminr, they're a significantly larger company than Echosec is. So I'm not sure what like the user count is for either, of course. But I know, at least Echosec, they pride themselves, and I'm sure Dataminr is similar, but they pride themselves on their platform and their product being very intuitive and easy to use and figure out.

So that you log in and you see a map and you realize that you can draw a circle or a shape on the map and start seeing content related to keywords that you put in, in that geographic location. So from a usability perspective, yes, I think that these types of platforms and offerings help support the ease of many users using it.

Tegus Client

And I understand Dataminr may be much larger, like maybe in terms of Echosec. Is it like dozens of customers, hundreds of customers? How should I think about the adoption of these kinds of products?

Vice President of Intelligence at Flashpoint

Echosec is certainly smaller, I would say. And I honestly don't know the total number of customers, again, just because the acquisition is so new, and I wasn't part of like the due diligence process or anything like that. But if I had to estimate, I would say Echosec has probably got less than 100 customers. But the opportunity to cross-sell into Flashpoint's much larger customer base is already really exciting on a number of levels.

Tegus Client

Got it. I think that makes sense. And you talked about the physical security teams purchasing these kinds of products. Have you seen what kind of budgets people are willing to spend on these products? Do they see this as a priority? How much do they spend on these kinds of products?

Vice President of Intelligence at Flashpoint

Yes. And I can tell you from experience as a consumer of this type of information and from previous employment, the budget of these types of buyers for these types of solutions can be anywhere from the hundreds of thousands to millions.

These types of offerings are worth their weight in gold if you can demonstrate that you can actually stop a real-world threat or something that would have significant impact to your brand or your organization. And companies are willing to pay for that.

Tegus Client

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

Interesting. So that is like a similar budget, like a cyber purchase, right? If people are paying $100,000 plus for the solutions, that is pretty much in line with some of the larger cyber budgets.

Vice President of Intelligence at Flashpoint

Yes, for sure. I would not say that physical security budgets are smaller than cyber budgets.

Tegus Client

Understood. Then how are these different products are differentiated in this market? You talked about a couple of names. Where does the differentiation come from? How do customers choose between these products?

Vice President of Intelligence at Flashpoint

That's a really good question. I think a lot of it is really just about timeliness. Who has the best data collection capabilities, how fast can it be in the customer's hands and enable those other types of use cases. I think probably the obvious functionalities in a lot of these platforms that we've been talking about is the ability to very specifically alert on certain posts or data that matches a very specific set of criteria.

And the faster that these platforms can enable customers to make a decision from a broader variety of sources and, therefore, data and potential threats, the more valuable and the more differentiated those platforms can be. One of the other big pieces of differentiation there, I think, would be how the data can actually be leveraged in internal environment and workloads.

So for example, to be able to be integrated into other platforms that the customers may already have set up from their existing physical security setups or workflows or anything like that and to be able to incorporate these types of data sets and the alerting mechanisms and everything into their existing capabilities, I think, goes a long way as well.

Tegus Client

So how does ZeroFox compare with Echosec or Dataminr? Or any of these three vendors, like how would you compare?

Vice President of Intelligence at Flashpoint

In terms of differentiation?

Tegus Client

Yes, in terms of capabilities differentiation. Like how does Echosec compare with ZeroFox?

Vice President of Intelligence at Flashpoint

Yes, that's another good question. So while I'm not as familiar with Dataminr's capabilities, I know that they probably are the largest of the three and have probably the most brand awareness of Dataminr as an organization and the use cases that they support. So I think that certainly helps them.

I know they have deep relationships with Twitter and maybe have more flexibility in terms of the approved use cases and how the data can actually be used, and who is allowed to use the data through Dataminr. So I think that's definitely a big plus for them. And they have broad collection capabilities as well. Again, they're just a much larger company, so they have more resources and a bit further reach.

One of the things I would say is a big positive about ZeroFox, and I believe Dataminr has this as well. Actually, I'm almost positive Dataminr has this as well. But they also have 24/7 analyst support in terms of

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

like analysts actually reviewing content and flagging things that are escalation support. So to be able to call somebody in the middle of the night if something goes boom at the customer site.

To be able to let them know, again, in as near real time as possible that something went wrong. Echosec does not have that capability currently. And I think that where Echosec strives to bridge that type of gap is really in the breadth of their collections and the ability for them to process some unique media and unique sources, so unique social media.

So the ability to look at sources like TikTok or Snapchat and to be able to extract out information from those types of sources and be able to alert on them in real time. And of course, I think this is probably more common across the platforms like ZeroFox, Dataminr and Echosec.

But the ability to, on the fly, translate languages or content from a number of different languages. So to be able to pull in threats from other languages and other communities. So that's definitely some interesting thesis of functionality or benefits to each of those.

Tegus Client

When we talked about TikTok and Snapchat, the content more is in a video format there, right? So if it is text like Twitter, I understand that could be interpreted, how does it work for the video kind of content?

Vice President of Intelligence at Flashpoint

Yes. Great question. So a lot of it is based on like a text of the captions or overlaid text on top of the video, being able to extract that out with optical character recognition, being able to pull that type of text-based information out of videos.

Tegus Client

Understood. Let me take a pause there and see if my colleagues have any questions. I see one there. One quick question. You mentioned that the importance of these platforms will only increase with time. But there's also a trend of individual users trying to protect their data.

There's more noise around data privacy. A lot of these platforms are probably moving in that direction. So how do you see that trend kind of change, impacting the effectiveness of these solutions as more and more platforms become more private and maybe less information available online?

Vice President of Intelligence at Flashpoint

Yes, that's a fantastic question. It's something that we think about regularly, too. A lot of it is really a cat and mouse game. It's definitely a challenge. Let's see. We're always going to wind up starting to collect sources that may not necessarily be as privacy-centric to start, and they may head in that type of direction.

And we're not going to we're not going to see the industry go down a path where everyone is trying to break terms of service or break the law to be able to collect information. So it's definitely a big cat and mouse game. And there is a worry, not just from the physical security side, of course, but from the cyber side of things as well that as users and platforms become more in tune with whether it's operational security for their own actions.

Or whether that platforms becoming more privacy-centric, there's always going to be that shift, where certain platforms, we may get diminished value out of them over a longer period of time if their policies change and everything. But I think there's always going to be a balance, right? Because there's always going to be those users who are lazy and not taking into consideration, it's a pain to try to be private online.

And I think there's a lot of platforms that recognize that as well and kind of default more towards the open nature of things and making it easier for their users to use things, it's a question that goes back to like driving adoption of your platform and if it makes it too tough to use for the users.

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

We've seen like examples of different communities pop up that are super privacy-centric, and threat actors or the online communities, they just don't adopt those types of communities sometimes because they can be a pain. And it inhibits that communal nature of some of these types of communities that are looking for that type of stuff. So it's definitely something that we keep front center on our radars very regularly.

Because, yes, things can change, terms of the service can change at any point. But with the way that new communities pop up very regularly, we're confident that these types of solutions and platforms are going to continue to bring value to customers just because there's always going to be different communities that threats are coming from that we're able to pull data from.

Tegus Client

I think that's a very pragmatic view. I want a replay what I understood, the world will never be in a place where everybody just made their profile private or all the data is under privacy. The world will never be in that place. There will always be this other communities, other websites where this information will be there. So you still need a solution to surface that data? Is that what are you saying?

Vice President of Intelligence at Flashpoint

Yes, I think that's really succinct way of summing that up.

Tegus Client

Got it. But to take that one more step further. Let's say, if Twitter removes the API access or I mean, I don't know how TikTok works today, about API or about scraping. If some of these major platforms like VK or Weibo, if some of those major platforms prevent these kind of third-party solutions to access content from them, then wouldn't these solutions become less valuable or maybe are not needed? They don't serve a purpose.

Vice President of Intelligence at Flashpoint

I wouldn't say not needed because there's always going to be those smaller types of communities, and it's really a balance, right? Because some of these larger communities like Facebook or Twitter, they may, at some point, pull that type of functionality and remove that ability for third-parties to use. But they spend so much money policing their own type of content, doing the content moderation and everything.

There are so many smaller places that pop up that don't do anything on the content moderation side. And I think there's always going to be that balance, right, for organizations, where Facebook and Twitter, they sell their user data and they make a ton of money on it. And they have to always balance that.

But there's always going to be those smaller communities that a lot of the threats are actually coming from and don't do content moderation. And they want to promote that openness and the ability to post whatever you want without being censored or anything like that. So it's definitely a balance, but I don't think that there is going to be any situation where there is no need for these products.

But yes, I mean, certainly, over time, if some of the giants like Twitter decide that they don't want to make money on selling this type of data anymore, then a lot of the value could go away. I don't see that happening anytime soon. But yes, it's always certainly a possibility. But then again, all of these platforms and products would be in the same boat.

Tegus Client

So you mentioned that some of the platforms may never go that route, but it seems that Facebook has already taken that approach, and that's why it's a very surface-level scraping that's being done right now.

And in terms of the individuals being lazy, I understand like there will always be a significant percentage of the population that's lazy enough. But those are not the people who we want, who probably will post some

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

threat, right? Unless and until someone is just radical in nature and wants to be out and about telling the world what they were trying to do. So that's one question that how do you see some of these cases being handled?

And second is around accessing leaked or breached data, right? Like there are always leaks in the databases. Facebook, Twitter has gone through multiple leaks and the data is available on dark web. And some of these platforms, at least when we have done the research, say that they can access the dark web. So what's the posture around accessing the leaked or breached data? Is that legal? Do you see any issues of accessing that data?

Vice President of Intelligence at Flashpoint

So I'll start with that second one. But just a clarifying question. Do you mean, is it okay for these types of platforms like an Echosec or a ZeroFox or a Dataminr to collect those breaches or those leaks and provide them to a customer?

Tegus Client

Yes. So the question is, I think there's like another question in that is, is it okay for them to access the data without having any legal ramifications? And second is, how do they know it's leaked or breached data? They're just scraping the net.

Vice President of Intelligence at Flashpoint

Yes. So if these platforms were consuming that type of like leaked or breached, it would likely be labeled as such. That this would say, a couple of years ago or a year or two ago, there was like 500 million records of Facebook users or something like that, that was leaked in the dark web.

And yes, if those were made searchable to different customers of those platforms, they would highly likely be labeled as leaked or breach data. And that's an interesting question, and it would be probably something more for those legal teams in terms of what is the vendor's stand on, is this leaked data. Even though it clearly had emanated from something like Facebook.

Is this something that by making it available to customers, would that be something that violates Facebook's terms of service, even though the vendor, like Echosec, ZeroFox or Dataminr didn't scrap it from Facebook specifically. So that's more from like the legal team type of question or approach to be able to help answer that business question.

Of what level of risk are we willing to accept in order to make a data set available to a customer that doesn’t care where it comes from, whether it was actually scraped from Facebook's site or whether it was on a dark web forum or wherever. They want to know what their exposure is.

Because again, from either the cyber perspective or the physical security perspective, they want to know what is my exposure, were my executives in that data set? And how do we mitigate any risk posed to my people, places or things when these data sets are leaked?

Tegus Client

Have you heard about other companies in this space? Like I heard names like Maltego, Cobwebs, Babel Street. Do any of these names ring a bell?

Vice President of Intelligence at Flashpoint

Yes. So Babel Street definitely, they collect a lot of this type of information as well. I'm not familiar with Cobwebs, though I've heard of them. But Maltego is more of like a data-visualization tool like a link-analysis tool, where leveraging data sets like this, like the open source data sets or breach datasets or anything like that. Maltego will enable you to draw correlations within large data sets.

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

So it will actually like create a graph for you and connect the different nodes of the graph based on connections within larger data sets. So it's a really, really great tool for doing link analysis, drawing links and correlations between larger data sets to see if there's any overlaps or connections in the data.

Tegus Client

Understood. And I got another question I was going to ask about. You talked about, at a higher level, how the cyber threat intel and this kind of physical security, did you say that these things are coming together?

Vice President of Intelligence at Flashpoint

Yes. I would say that we've seen and I've personally seen over the past couple of years, kind of more of a fusion of a lot of these types of capabilities where, again, physical security customers are understanding that a lot of the threats that are coming towards their organizations or their employees or whatever are emanating from the same types of communities that these cyber threat intelligence teams are already monitoring.

And so from that sense, there's definitely been, from my perspective, more of a collaboration between the cyber teams who may already be leveraging these types of tools, albeit for different purposes, having those relationships with the physical security teams and understanding who to pass information off to in the event of an imminent threat or anything like that.

Tegus Client

But the buyer for a cyber threat intel is different from the buyer for these kinds of physical security products, correct?

Vice President of Intelligence at Flashpoint

Typically, yes. But it depends on the size of the organization.

Tegus Client

Understood. Have you come across an example where these platforms have probably prevented an incident? Have you heard of any of those examples?

Vice President of Intelligence at Flashpoint

Yes. I wish I could go into details because it's always interesting, right? Because the things that make the news are when things go bad, not really when law enforcement or somebody prevents something before something happens because they don't typically share information about the investigation.

So I can confidently tell you that there are many examples of real-world lives being saved from these types of things. And when those types of events happen or don't happen, for that matter, that's really when the value of these types of platforms and these data sets really shines through.

You can't put a price on being able to say that you prevented a shooting at a school or a shooting at a retail location or a shooting at a synagogue or anything. So I can confidently tell you that there are many examples of preventing incidents and it only strengthens the value prop for the entire market.

Tegus Client

Got it. You talked about vendors like Dataminr that have existed for a long time, right? Is there a segmentation of this market from legacy vendors to newer vendors? Like are the likes of Echosec and others replacing with Dataminr?

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.

Vice President of Intelligence at Flashpoint

I wouldn't necessarily say that they're replacing Dataminr or anything like that. I think it kind of goes back to what I was touching on earlier, where a lot of the buying centers for some of these newer in the space companies have typically been in the cyber threat intel centers, and they're now getting introduced into physical security centers.

So I wouldn't necessarily say that they're going to be replacing a Dataminr or anything like that. But it wouldn't be uncommon if a Dataminr and another one of those types of platforms were sitting side by side so that there's better coverage for those types of threats.

Tegus Client

Can you talk about why somebody would need both the solutions? Like both of them would look at social media or other sources and surface the events, right? What's the use case for both to exist?

Vice President of Intelligence at Flashpoint

Just better depth and coverage. And again, it's going to depend on the size of the organization, their budget and their risk tolerance. And if they want that extra line of defense, it's better to spend more money and get two notifications for the same type of thing than have one vendor miss something. So one vendor may have coverage on slightly different sources or may alert a little bit faster.

Tegus Client

Great. Well, thank you very much for your time. I appreciate the insights. Have a good one.

Tegus is not a registered investment advisor or broker-dealer, and is not licensed nor qualified to provide investment advice. The information published in this transcript ("Content") is for information purposes only and should not be used as the sole basis for making any investment decision. Tegus, Inc. ("Tegus") makes no representations and accepts no liability for the Content or for any errors, omissions, or inaccuracies will in no way be held liable for any potential or actual violations of United States laws, including without limitation any securities laws, based on Information sent to you by Tegus. The views of the advisor expressed in the Content are those of the advisor and they are not endorsed by, nor do they represent the opinion of, Tegus. Tegus reserves all copyright, intellectual and other property rights in the Content. The Content is protected by the Copyright Laws of the United States and may not be copied, reproduced, sold, published, modified or exploited in any way without the express written consent of Tegus.

THIS DOCUMENT MAY NOT BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS INCLUDING RESALE OF ANY PART, UNAUTHORIZED DISTRIBUTION TO A THIRD PARTY OR OTHER METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF TEGUS INC.