Cyberint

H2 2024 Battlecards

Cyberint

Impactful Intelligence

Competitive Overview

	Cyberint	Recorded Future	ZEROFOX	KELA	INTEL471	GROUP-IB	SOCRadar	digital shadows_	INTSIGHTS A RAPID7 COMPANY
Attack Surface Management	🟢	◓	◓	◓	◓	🟢	◓	◓	●
Phishing Protection	🟢	🟢	🟢	●	●	🟢	◓	🟢	🟢
Brand Protection	🟢	🟢	🟢	🟢	◓	🟢	◓	🟢	🟢
Social Media Monitoring	🟢	🟢	🟢	●	●	🟢	◓	◓	◓
Data Leakage Detection	🟢	🟢	🟢	🟢	◓	🟢	◓	🟢	🟢
Deep & Dark Web Chatter	🟢	🟢	🟢	🟢	🟢	🟢	◓	🟢	🟢
Malware Intelligence	🟢	🟢	◓	●	🟢	🟢	◓	🟢	◓
Vulnerability Intelligence	🟢	🟢	◓	◓	◓	🟢	◓	🟢	◓
Supply Chain Intelligence	🟢	🟢	◓	◓	◓	◓	◓	◓	🟢
IoC Feeds	🟢	🟢	◓	◓	🟢	🟢	◓	◓	🟢
Fidelity & Context of Alerts	🟢	◓	◓	◓	◓	◓	◓	◓	◓
Takedown Services	🟢	◓	◓	◓	●	◓	◓	◓	◓
Quality & Speed of Support	🟢	◓	◓	◓	◓	◓	◓	◓	◓

🟢 strong capability ◓ capability provided ● not provided

Recorded Future®

FOUNDED: 2009
HEAQUARTERS: Boston, MA, USA
EMPLOYEES: ~1,050
FUNDING: $70 Million (Series E)

50K FOLLOWERS

COMPANY OVERVIEW

Recorded Future is a privately-held threat intelligence vendor founded in 2009. Over the years, Recorded Future has raised $70 Million over 7 rounds. In May 2019, Recorded Future was acquired by private equity firm Insight Partners for $780 Million.

Recorded Future is widely considered the market leader in cyber threat intelligence. In November 2022, Recorded Future announced in a press release that they had reached $250 Million in annual recurring revenue with more than 1,500 customers around the world.

ADDITIONAL RESOURCES

- https://www.recordedfuture.com/
- https://www.linkedin.com/company/recorded-future/
- https://www.crunchbase.com/organization/recorded-future
- Threat Intelligence datasheet
- Attack Surface Intelligence datasheet
- Brand Intelligence datasheet
- Vulnerability Intelligence datasheet

RECORDED FUTURE WEAKNESSES	CYBERINT DIFFERENTIATORS
Recorded Future is a powerful platform but it requires a lot of time and resources to properly configure and manage it.	Cyberint's platform is deployed instantly with very little configuration. It's low-touch and customers spend 30 min/day in app on average.
Recorded Future has over 1,500 customers, but this often means they don't provide top-tier support and services to their customers.	Cyberint provides a named analyst to customers and this person acts as an extension of your SOC. We provide superior support.
We've heard from former and current Recorded Future customers that their feeds and alerts can be noisy, with many false positives.	We triage alerts to ensure there are very few false positive alerts being sent to customers. We also add context to alerts for faster response.
Recorded Future provides a strong platform but it's very expensive if you deploy all of the modules you need to get full risk coverage.	We focus on providing value with a platform that covers many use cases, provides highly targeted alerts, and can be used efficiently.
Recorded Future provides services but they're expensive and, because they are such a large vendor, their response times are often slow.	Our analysts are cyber experts, our support is the best among all competitors, and our takedown services are faster & more effective.

OBJECTION HANDLING

Doesn't Recorded Future have more sources, more data, and better deep & dark web coverage?

- No company has 100% coverage for every source on the deep and dark web. Sometimes, they may pick something up that we miss. Other times, we will pick something up that they miss.

If Recorded Future is the market leader in this space, why should we go with Cyberint?

- With Cyberint, you get targeted, contextualized alerts with extremely high-fidelity. Plus we provide much better, more responsive support with a named analyst, and our takedown services are faster and more effective. Our product is also less costly and it takes much less time to fully manage our platform..

ZEROFOX®

FOUNDED: 2013
HEAQUARTERS: Baltimore, MD, USA
EMPLOYEES: ~650
FUNDING: $154 Million (Series D)

in **19K FOLLOWERS**

COMPANY OVERVIEW

ZeroFox is was founded as a digital risk protection and deep and dark web monitoring vendor in 2013. Over the years, ZeroFox has made 4 major acquisitions: Cyveillance, a threat intelligence vendor in October 2020; IDX, an incident response firm in December 2021; Vigilante, a DRP and dark web monitoring vendor in October 2022; and LookingGlass Cyber Solutions, an external attack surface management vendor in April 2023.

ZeroFox was acquired by a private equity firm for just $350 Million in January 2024, far below their value at time of IPO.

ADDITIONAL RESOURCES

- https://www.zerofox.com/
- https://www.linkedin.com/company/zerofox/
- https://www.crunchbase.com/organization/zerofox
- Global Threat Intelligence datasheet
- Adversary Disruption datasheet
- Brand Protection datasheet
- Deep & Dark Web Monitoring datasheet
- ZeroFox List Pricing Doc

ZEROFOX WEAKNESSES	CYBERINT DIFFERENTIATORS
ZeroFox is strong in brand protection and social media monitoring but they acquired an external ASM company and bolted it on to their platform.	Cyberint released our ASM module in 2017. It was developed in-house and is natively integrated with all other product capabilities.
ZeroFox provides solid deep and dark web monitoring but their coverage of malware logs and exposed credentials is not very strong.	One of Cyberint's strengths is malware logs & leaked credentials. Each month, we collect >160K malware logs & >17 Million leaked credentials.
ZeroFox doesn't provide supply chain intelligence or 3rd party risk management, which is essential to understanding & mitigating external cyber risk.	Cyberint's Supply Chain Intelligence module continuously monitors partners and suppliers for risks using open, deep and dark web intel.
In general, ZeroFox's technology is great for a limited set of use cases but they're missing key components and their support is not top-tier.	Cyberint provides coverage for a wide range of use cases and our analysts are highly trained experts that serve as an extension of your SOC.
ZeroFox was recently acquired by a private equity firm, creating a lot of uncertainty around the company's future. Can you rely on them?	Cyberint is (and always has been) focused on the combination of CTI, DRP, and EASM. We're leading this market and growing very quickly.

OBJECTION HANDLING

ZeroFox is telling us they have superior capabilities in social media monitoring and phishing protection. How would you respond to that?

- Cyberint provides multi-layered phishing protection through lookalike domain detection, detection of phishing sites via misuse of logos, deep and dark web monitoring to detect phishing kits, and the Phishing Beacon, which immediately detects clones of your official web pages. We also detect impersonation on social media platforms, including Twitter, Instagram, Facebook, and LinkedIn.

ZeroFox has been around longer and they're a bigger vendor. Why should we choose you over them?

- Cyberint continues to innovate and improve our product and its capabilities. While we aren't as big, we have a team of veteran cyber experts who act as an extension of your team and keep you secure.

SOCRadar®
Extension to Your SOC Team!

FOUNDED: 2018
HEAQUARTERS: Delaware, USA
EMPLOYEES: ~120
FUNDING: $5 Million (Series A)

in **13K FOLLOWERS**

COMPANY OVERVIEW

SOCRadar was founded by a team of Turkish cybersecurity professionals but incorporated in Delaware, USA. In February 2023, SOCRadar announced that they raised $5 Million in a Series A round. They have not made any acquisitions and all of their technology appears to be built in-house.

SOCRadar's strategy is to push "democratized threat intelligence" and undercut all competitors on the market, providing value through a decent (though not exceptional) product sold at a very low price point.

ADDITIONAL RESOURCES

- https://socradar.io/
- https://www.linkedin.com/company/socradar/
- https://www.crunchbase.com/organization/socradar
- SOCRadar Platform white paper
- Threat Intelligence datasheet
- Attack Surface Management datasheet
- Digital Risk Protection datasheet

SOC RADAR WEAKNESSES	CYBERINT DIFFERENTIATORS
SOCRadar claims to cover a huge number of use cases but, from what other prospects have told us, they aren't particularly strong in any of them.	Cyberint provides excellent coverage for many external cyber risk use cases. We have had more time to develop and evolve as a company.
SOCRadar is relatively new to the market and their product isn't very mature. It might be a great platform in the future but they're still developing.	Cyberint was founded in 2010 and the first iteration of the product was released in 2014. Now, it's a mature and advanced platform.
Many prospects we've spoken to have voiced hesitations about putting their trust in SOCRadar and relying on them for visibility & support.	Cyberint is trusted by hundreds of brands around the globe, including many Fortune500 companies. We have many reference customers.
If you're interested in support and services, SOCRadar probably isn't the right solution for you – we've heard they are not strong here.	One of our differentiators is the quality of our cyber experts. Our support is faster & more in-depth, and our services are the best available.
SOCRadar makes big claims in their marketing materials but they have never been recognized as a leader by industry analysts like Gartner or Frost.	Cyberint has been recognized by all the top analysts. We were named 2023 ERMM Company of the Year by Frost & Sullivan.

OBJECTION HANDLING

SOCRadar's proposal came in at a far lower price point. Why should we pay more for Cyberint?

- It only takes one missed threat to result in a large, costly security incident. If you're looking to protect your organization from external cyber risks, it's prudent to pay slightly more for a product that will provide complete coverage, rather than paying less for something that provides partial protection but misses relevant threats that may lead to a breach.

SOCRadar is telling us that their technology and capabilities are equal to yours. How can we be sure that your platform is superior?

- It's very hard to measure one vendor's product against another in an objective, data-driven way. But Cyberint is a more established company – over 100 customers, across many industries and regions. We have many reference customers and have been recognized by the top industry analysts – and for good reasons. We are more mature & more trusted.

digital shadows_

FOUNDED: 2011
HEAQUARTERS: San Francisco, CA, USA
EMPLOYEES: ~90 remaining post-acquisition
FUNDING: $58 Million (Series C prior to acquisition)

17K FOLLOWERS

COMPANY OVERVIEW

Digital Shadows was founded in London in 2011. The focus is and has always been on digital risk protection and dark web monitoring. Digital Shadows announced 54% ARR growth YoY in Aug 2021. 10 months later, they were acquired.

In June 2022, Digital Shadows announced that it would be acquired by ReliaQuest, an XDR /MDR provider, for $160 Million. ReliaQuest has about 1,000 employees and itself has raised $330 Million over 3 rounds. In August 2022, ReliaQuest completed the acquisition of Digital Shadows and announced threat intel features in the Grey Matter platform.

ADDITIONAL RESOURCES

- https://www.reliaquest.com/platform/digital-risk-protection/
- https://www.linkedin.com/company/reliaquest-threat-research/
- https://www.crunchbase.com/organization/digital-shadows
- Digital Shadows overview datasheet
- Threat Intelligence datasheet
- Brand Protection datasheet
- Data Leakage Detection datasheet

DIGITAL SHADOWS WEAKNESSES	CYBERINT DIFFERENTIATORS
Digital Shadows is a great platform but since they've been acquired by Reliaquest, they are more focused on XDR than threat intelligence.	Cyberint is and always has been laser-focused on combining threat intel with attack surface management & brand protection capabilities.
For attack surface management, Digital Shadows relies on Shodan, a free & open source tool, so the results are often not comprehensive or complete.	Cyberint provides attack surface management, you can get started with just your primary domain. Discovery is automated & continuous.
Digital Shadows' deep and dark web coverage is solid and they have good sources but their alerts can be noisy and they have many false positives.	Cyberint's analysts triage alerts to throw out false positives and add context to the true positives before they are issued to your team.
Many of Digital Shadows' best analysts left after the acquisition so we've heard their support is now quite slow and the quality of service has fallen.	We triage alerts to ensure there are very few false positive alerts being sent to customers. We also add context alerts for faster response.
In recent years, Digital Shadows services have slipped. They don't have a dedicated takedown team in-house so they must outsource takedowns.	Cyberint has a dedicated takedown team with a success rate of over 90%. Most takedowns are completed within 24 to 48 hours of the request.

OBJECTION HANDLING

Digital Shadows is telling us that they have better deep and dark web coverage than Cyberint, with more sources, more data, and better visibility.

- No company has 100% coverage for every source on the deep and dark web. Sometimes, they may pick something up that we miss. Other times, we will pick something up that they miss.

Reliaquest is offering to throw in additional capabilities from their portfolio at a very low cost (or no cost). What else can you offer us?

- We provide threat intel, attack surface management, brand protection, phishing protection, social media monitoring, deep & dark web monitoring, vulnerability intel and supply chain intel – it's a single platform for a huge number of external cyber risk use cases.

INTSIGHTS
A RAPID7 COMPANY

FOUNDED: 2015
HEAQUARTERS: New York, NY, USA
EMPLOYEES: ~70 remaining post-acquisition
FUNDING: $71 Million (Series D prior to acquisition)

11K FOLLOWERS

COMPANY OVERVIEW

IntSights is a threat intelligence and digital risk protection vendor based in NYC. Originally founded by two Israelis– former members of the IDF's Unit 8200– Intsights grew quickly. In June 2021, they claimed to have more than 350 customers.

In June 2021, Insights was acquired by Rapid7, a large vendor that first became known as a risk and vulnerability management platform, for $335 Million. Rapid7 itself was founded in Boston in 2000, currently has about 2,800 employees, and has raised $89 Million over 4 rounds. There have been rumors that Rapid7 is exploring a sale to venture capital firms.

ADDITIONAL RESOURCES

- https://intsights.com/
- https://www.linkedin.com/company/intsights/
- www.crunchbase.com/organization/intsights/
- Intsights "corporate overview" datasheet
- Threat Intelligence datasheet
- Rapid7 Security Risk Mitigation with threat intel + XDR

INTSIGHTS WEAKNESSES	CYBERINT DIFFERENTIATORS
Intsights is a great platform but since they've been acquired by Rapid7, they are more focused on XDR & SIEM than threat intelligence.	Cyberint is and always has been laser-focused on combining threat intel with attack surface management & brand protection capabilities.
Intsights doesn't do attack surface management, which means it takes longer to configure & deploy the platform, and no continuous discovery.	Cyberint provides attack surface management, you can get started with just your primary domain. It's a SaaS platform, instant deployment.
Because they're missing full-fledged ASM, it's harder to map threat intel to your digital assets and Intsights's alerts are therefore less targeted.	We map threat intel to your digital assets so you only receive targeted, contextualized alerts about the threats that matter to your business.
Intsights's deep and dark web coverage is solid and they have good sources but their alerts can be noisy and they have many false positives.	Cyberint's analysts triage alerts to throw out false positives and add context to the true positives before they are issued to your team.
Many of Intsights's best analysts left after the acquisition so we've heard their support is now quite slow and the quality of service has fallen.	Cyberint's analysts act as an extension of your SOC. We offer outstanding support, market-leading services, and fast & effective takedowns.

OBJECTION HANDLING

Intsights is telling us that they have better deep and dark web coverage than Cyberint, with more sources, more data, and better visibility.

- Cyberint continuously discovers the open, deep and dark web to map out your external attack surface and detect relevant threats. This process enables Cyberint to provide better visibility and detect threats that Intsights would miss, as they lack the continuous ASM discovery capability.

Intsights is offering to throw in additional capabilities from the Rapid7 portfolio at a very low cost (or no cost). What else can you offer us?

- We provide threat intel, attack surface management, brand protection, phishing protection, social media monitoring, deep & dark web monitoring, vulnerability intel and supply chain intel – it's a single platform for a huge number of external cyber risk use cases.

GROUP-IB

FOUNDED: 2003
HEAQUARTERS: Singapore
EMPLOYEES: ~380
FUNDING: $1 Million (seed funding)

in **50K FOLLOWERS**

COMPANY OVERVIEW

Group-IB was founded in Moscow in 2003 as an investigations, incident response, and digital forensics services company. They eventually moved into the threat intelligence space and, much later, the DRP and ASM categories.

In November 2018, Group-IB moved its headquarters from Moscow to Singapore to avoid negative PR associated with cybercrime coming from Russia. In September 2021, Group-IB's CEO and co-founder was accused of treason and arrested. He remains in jail today. Group-IB continues to face geopolitical challenges and trust issues with customers.

ADDITIONAL RESOURCES

- https://www.group-ib.com/
- https://www.linkedin.com/company/group-ib/
- https://www.crunchbase.com/organization/group-ib
- Threat Intelligence datasheet
- Attack Surface Management datasheet
- Digital Risk Protection datasheet

GROUP-IB WEAKNESSES	CYBERINT DIFFERENTIATORS
Group-IB has strong technology but they don't have a platform. Instead, they have 3 different point solutions that aren't fully integrated.	Cyberint was built from the ground up to combine threat intel, attack surface management and brand protection into 1 platform.
If you want coverage for attack surface management, digital risk protection, and threat intel, you need to buy and manage 3 products.	Because Cyberint's capabilities are all natively fuzed into a single platform, it's easy to manage and doesn't require a large commitment of time.
Group-IB's threat intelligence product has an amazing depth of information but the alerts are noisy and it's hard to get actionable insights.	We map threat intel to your digital assets so you only receive targeted, contextualized alerts about the threats that matter to your business.
Group-IB is having geopolitical challenges, which may present conflicts of interest. Other prospects have expressed concerns about trust.	Cyberint is trusted by hundreds of customers globally, in a number of different industries. We are recognized by the top industry analysts.
Many of Group-IB's analysts are in Moscow so we've heard that communication can be a challenge and support is sometimes sub-par.	Cyberint's analysts act as an extension of your SOC. We offer outstanding support, market-leading services, and fast & effective takedowns.

OBJECTION HANDLING

Group-IB is telling us that they have better deep and dark web coverage than Cyberint, with more sources, more data, and better visibility.

- No company has 100% coverage for every source on the deep and dark web. Sometimes, they may pick something up that we miss. Other times, we will pick something up that they miss.

Group-IB is telling us that Cyberint provides coverage for many use cases but does not excel at any of them. They say Cyberint is a "jack of all trades, master of none" – is that true?

- Cyberint is not the #1 standalone solution for ASM, DRP, or CTI, but by combining all 3 into one platform, each of these 3 capabilities is greatly enhanced and the product provides huge value to customers with a minimal commitment of time. Group-IB has 3 distinct products but no platform.

KELA

FOUNDED: 2009
HEAQUARTERS: Tel Aviv, Israel
EMPLOYEES: ~100
FUNDING: $50 Million (Private equity)

in **8K FOLLOWERS**

COMPANY OVERVIEW

KELA is a relatively new player in the threat intel + digital risk protection + attack surface management space. They've been around since 2009 but just announced the launch of their "cyber intelligence platform" in January 2023.

Headquartered in Tel Aviv, KELA has many analysts and researchers who were trained in Israeli military units. Over the past year, KELA has been trying to penetrate North American markets, adding new sales directors in the USA. They also have a presence in Japan. They seem to be maturing and appearing more often in competitive deals.

ADDITIONAL RESOURCES

- https://ke-la.com/
- https://www.linkedin.com/company/kela-group/
- https://www.crunchbase.com/organization/kela-group
- KELA IntelAct One-Page datasheet
- KELA RaDark One-Page datasheet
- KELA competitive analysis
- KELA Internal – competitive intelligence & battlecards

KELA WEAKNESSES	CYBERINT DIFFERENTIATORS
KELA provides "asset management capabilities" but they are lacking the automated, continuous discovery that attack surface management needs.	Cyberint automates the process of external attack surface discovery so your new assets are automatically identified and added into scope.
KELA provides strong deep and dark web monitoring but they are missing ASM, phishing, malware intel, and other important use cases.	Cyberint provides excellent coverage for many capabilities and use cases. It's one platform to detect and mitigate all external cyber risks.
Because they're missing full-fledged ASM, it's harder to map threat intel to your digital assets and KELA's alerts are therefore less targeted.	We map threat intel to your digital assets so you only receive targeted, contextualized alerts about the threats that matter to your business.
KELA's deep and dark web coverage is solid and they have good sources but their alerts can be noisy and they have many false positives.	Cyberint's analysts triage alerts to throw out false positives and add context to the true positives before they are issued to your team.
KELA doesn't provide professional services, managed takedowns, investigations, or RFIs, so they are limited in how much they can support you.	Cyberint's analysts act as an extension of your SOC. We offer outstanding support, market-leading services, and fast & effective takedowns.

OBJECTION HANDLING

KELA is claiming they have better deep and dark web coverage than Cyberint, with more sources, more data, and better visibility. Any thoughts?

- No company has 100% coverage for every source on the deep and dark web. Sometimes, they may pick something up that we miss. Other times, we will pick something up that they miss.

KELA is telling us that Cyberint provides coverage for many use cases but does not excel at any of them. They say Cyberint is a "jack of all trades, master of none" – is that true?

- Cyberint is not the #1 standalone solution for ASM, DRP, or CTI, but by combining all 3 into one platform, each of these 3 capabilities is greatly enhanced and the product provides huge value to customers with a minimal commitment of time.

INTEL471

FOUNDED: 2014
HEAQUARTERS: Delaware, USA
EMPLOYEES: ~150
FUNDING: N / A

in **15K FOLLOWERS**

COMPANY OVERVIEW

Intel 471 was founded in 2014 with a strong focus on adversary and malware intelligence. They are known to have excellent IoC feeds, malware intel, and RFI / investigations.

More recently, Intel 471 has been trying to expand their capabilities and feature set to keep up with the market. In November 2022, Intel 471 acquired a small attack surface management vendor called SpiderFoot. Their website also claims that they provide brand protection, compromised credentials detection, third-party risk management, and more.

ADDITIONAL RESOURCES

- https://intel471.com/
- https://www.linkedin.com/company/intel-471/
- https://www.crunchbase.com/organization/intel-471
- Attack Surface Protection datasheet
- Malware Intelligence datasheet
- Vulnerability Intelligence datasheet
- Credential Intelligence datasheet
- Cybercrime Intelligence datasheet

INTEL 471 WEAKNESSES	CYBERINT DIFFERENTIATORS
Intel 471 has a great product but it's more of a niche platform. They're great in IOC feeds & threat actor profiling but they're missing many use cases.	Cyberint provides excellent coverage for many capabilities and use cases. It's one platform to detect and mitigate all external cyber risks.
Intel 471 just acquired an external attack surface management vendor so they are still in the process of integrating that tech into their platform.	Cyberint developed and released an attack surface management module in 2017. It is fully integrated with other capabilities and features.
Intel 471 provides great deep & dark web intel but it isn't targeted or tailored to the customer's assets, so it's lower fidelity and less actionable.	We map threat intel to your digital assets so you only receive targeted, contextualized alerts about the threats that matter to your business.
Intel 471 can be pricey for what the platform provides. And if you want full coverage, you would need to deploy them plus another product.	By providing coverage for so many use cases, Cyberint helps you to consolidate vendors, which saves you time and reduces vendor costs.
We've heard that Intel 471 does great investigations, but they are not as strong in customer support, takedowns, and other services.	Cyberint's analysts act as an extension of your SOC. We offer outstanding support, market-leading services, and fast & effective takedowns.

OBJECTION HANDLING

Intel 471 is telling me they provide attack surface management, deep and dark web monitoring, brand protection, and 3rd party risk management. Why are you saying they only cover a limited set of use cases?

- Intel 471 finalized their acquisition of SpiderFoot, an ASM vendor in early 2023, so the capabilities aren't yet fully integrated. They have only recently started offering brand protection so their capabilities are not mature here. The same is true of 3rd party risk management.

Intel 471 is telling us that Cyberint provides coverage for many use cases but does not excel at any of them. They say Cyberint is a "jack of all trades, master of none" – is that true?

- Cyberint is not the #1 standalone solution for ASM, DRP, or CTI, but by combining all 3 into one platform, each of these 3 capabilities is greatly enhanced and the product provides huge value to customers with a minimal commitment of time.

CYBLE

FOUNDED: 2019
HEAQUARTERS: Atlanta, GA, USA
EMPLOYEES: ~160
FUNDING: $39 Million (Series B)

22K FOLLOWERS

COMPANY OVERVIEW

Cyble's offering includes EASM, CTI, DRPS, vulnerability management, and takedowns. Although officially based in Atlanta, Cyble was founded by a team of tech and cyber entrepreneurs from India. They do the majority of their business in APAC (specifically India, SE Asia, and Japan). Cyble raised $24 Million in a Series B round in August 2023.

They seem to have a strong focus on the channel, as they call themselves a "Partner-First" vendor and much of their social media marketing is focused on their partner program.

ADDITIONAL RESOURCES

- https://cyble.com/
- Q2 2023 Ransomware report
- Customer Success Story – Large EdTech platform
- Cybercrime Surveillance whitepaper
- The role of early threat intelligence whitepaper

CYBLE WEAKNESSES	CYBERINT DIFFERENTIATORS
Cyble is a late-comer to the threat intel, digital risk protection, external attack surface management space. They are not a leader in these categories.	Cyberint pioneered the combination of CTI, DRPS and ASM in 2017 & we've been improving upon all of these capabilities ever since.
Cyble doesn't focus on the detection of malware infections or leaked credentials– but stolen credentials is the #1 attack vector, year after year.	Cyble has very strong capabilities for detecting exposed credentials. We find more than 17M sets of leaked creds every month.
Cyble is an up-and-coming vendor but they're still relatively new to threat intel, so they have limited sources and visibility into the deep and dark web.	Cyberint was founded in 2010 and has specialized in deep and dark web threat intel ever since. We have thousands of sources.
Cyble doesn't have any public reference customers. They have very few mentions from industry analysts like Gartner. Why take a chance?	Cyberint is a globally recognized threat intel leader, with many reference customers plus many mentions from Gartner, Forrester, Frost, etc.
Cyble's team is no doubt talented but do they have extensive, nation-state level intelligence experience? Are they world-class experts?	Cyberint's team is made up of cyber experts, many of whom served in elite cyber units in the Israeli military and/or intelligence services.

OBJECTION HANDLING

It seems like both you and Cyble provide a similar product with coverage for the same use cases, but they are offering us a significantly lower price point. Why should we go with Cyberint?

- It might seem like Cyble ticks all of the right boxes but, ultimately, you get what you pay for and their coverage for every use case is not as robust as Cyberint's. It only takes one undetected threat to lead to a very costly security incident, so why take a chance on the least expensive solution?

CYFIRMA
DECODING THREATS

FOUNDED: 2017
HEAQUARTERS: Singapore
EMPLOYEES: ~90
FUNDING: $18 Million (Series B)

6K FOLLOWERS

COMPANY OVERVIEW

Cyfirma was founded in Singapore in 2017 and has a strong focus on developing business in India, Singapore, Malaysia, Thailand, Indonesia, Taiwan, and Japan. Their offering includes external attack surface management, digital risk protection, threat intelligence, and a mobile application that reports to defend against malware and other threats.

While we have not competed against Cyfirma in a large number of deals, we are starting to see them come up more and more often in APAC. From what we understand, their competitive pricing is a main selling point.

ADDITIONAL RESOURCES

- https://www.cyfirma.com/
- DETECT – Digital Risk Protection Datasheet
- DECYFIR – Threat Intel / EASM Datasheet
- Southeast Asia Threat Landscape Report

CYFIRMA WEAKNESSES	CYBERINT DIFFERENTIATORS
Cyfirma is still new to the threat intel, digital risk protection, external attack surface management space. They are not a leader in these categories.	Cyberint pioneered the combination of CTI, DRPS and ASM in 2017 & we've been improving upon all of these capabilities ever since.
Cyfirma doesn't focus on the detection of malware infections or leaked credentials– but stolen credentials is the #1 attack vector, year after year.	Cyberint has very strong capabilities for detecting exposed credentials. We find more than 17M sets of leaked creds every month.
Cyfirma does not seem to offer any sort of takedown service. If they do not, then the offering is limited – detection is helpful but not sufficient.	Cyberint has a dedicated takedown team with a success rate of over 95%. Over 70% of takedowns are completed within 72 hours.
Cyfirma has not received much recognition or favorable rankings from industry analysts like Gartner, Frost & Sullivan, and Forrester.	Cyberint is a globally recognized threat intel leader, with many reference customers plus many mentions from Gartner, Forrester, Frost, etc.
Cyfirma's team is no doubt talented but do they have extensive, nation-state level intelligence experience? Are they world-class experts?	Cyberint's team is made up of cyber experts, many of whom served in elite cyber units in the Israeli military and/or intelligence services.

OBJECTION HANDLING

It seems like both you and Cyfirma provide a similar product with coverage for the same use cases, but they are offering us a significantly lower price point. Why should we go with Cyberint?

- It might seem like Cyfirma ticks all of the right boxes but, ultimately, you get what you pay for and their coverage for every use case is not as robust as Cyberint's. It only takes one undetected threat to lead to a very costly security incident, so why take a chance on the least expensive solution?

BlueVoyant

FOUNDED: 2017
HEAQUARTERS: New York, NY, USA
EMPLOYEES: ~600
FUNDING: $525 Million (Series D)

53K FOLLOWERS

COMPANY OVERVIEW

The BlueVoyant Platform includes Managed Detection & Response, Supply Chain Defense, Digital Risk Protection, and Professional Services. Though primarily an MDR provider, it seems they've recently increased focus on DRP, data leak detection, supply chain intel, and vulnerability management. They've been actively targeting Cyberint's accounts in APAC.

BlueVoyant also has a strong focus on the channel. They've received the "Microsoft Security U.S. Partner of the Year" award two years running, in both 2022 and 2023.

ADDITIONAL RESOURCES

- https://www.bluevoyant.com/
- Digital Brand Protection Solution Brief
- Dark Web Investigations Solution Brief
- Supply Chain Defense Solution Brief
- Data Readiness Assessment Solution Brief
- Supply Chain Defense High Volume Monitoring

BLUEVOYANT WEAKNESSES	CYBERINT DIFFERENTIATORS
BlueVoyant is primarily an MDR provider. They offer digital risk protection and supply chain security but this is not a main focus for them.	Cyberint pioneered the combination of CTI, DRPS and ASM in 2017 & we've been improving upon all of these capabilities ever since.
BlueVoyant is not a threat intelligence provider so they have limited sources and visibility into the deep and dark web. It's simply not in their DNA.	Cyberint was founded in 2010 and has specialized in deep and dark web threat intel ever since. We have thousands of sources.
BlueVoyant provides ASM and brand protection, but what about IoC feeds, malware intel, threat actor tracking, CVE intel, & intel data lake use cases?	Cyberint has a comprehensive threat intelligence platform. Get strategic, operational, and tactical intelligence with a single product.
BlueVoyant claims to offer unlimited takedowns but how effective are their takedown services? What kind of SLAs can they commit to?	Cyberint has a dedicated takedown team with a success rate of over 95%. Over 70% of takedowns are completed within 72 hours.
BlueVoyant is has received recognition as an MDR provider but they've never been mentioned as a DRP or CTI vendor in a Gartner or Forrester report.	Cyberint is a globally recognized threat intel leader, with many reference customers plus many mentions from Gartner, Forrester, Frost, etc.

OBJECTION HANDLING

BlueVoyant is offering us unlimited takedowns. Their offer is also a similar price point to Cyberint. Can you provide unlimited takedowns?

- Cyberint has a dedicated, in-house takedown team that has maintained a success rate of >95% over the past 6 quarters, across thousands of takedowns. While we don't offer unlimited takedowns, our services are superior in terms of speed and efficacy. Takedowns are performed by Cyberint employees.

BlueVoyant says they have mature deep and dark web monitoring capabilities. They say it's the same as yours. How can you prove you are stronger?

- Cyberint was founded as a threat intel and deep and dark web monitoring vendor. Our team is made up of intelligence experts, many of whom worked at government-level organizations. You can explore the raw intel and intel data lake to see the breadth of intelligence that we collect (40M+ items/month).

BITSIGHT

FOUNDED: 2011
HEAQUARTERS: Boston, MA, USA
EMPLOYEES: ~800
FUNDING: $400 Million (Series E)

33K FOLLOWERS

COMPANY OVERVIEW

Bitsight was founded in 2011 as a Security Ratings Service and Third-Party Risk Management vendor. While they have historically relied on basic external IT security checks and vendor questionnaires to assess risk, they have more recently started talking about external attack surface management, continuous monitoring, and deep and dark web intelligence.

In some cases, Bitsight interfaces with vendors to inform them of risks and threats that have been discovered (Cyberint does not do this and has no plans to). Bitsight also excels at providing risk reports that can be shared with an organization's leadership.

ADDITIONAL RESOURCES

- https://www.bitsight.com/
- Third-Party Risk Management
- Vendor Risk Management
- Attack Surface Analytics Datasheet

BITSIGHT WEAKNESSES	CYBERINT DIFFERENTIATORS
Bitsight is a solid product but focused on different use cases, mainly compliance (e.g. vendor approval procedures, internal GRC policy requirements, etc.)	Cyberint's Supply Chain Intel is focused on giving you the intel you need to stop attacks and breaches at 3rd parties from affecting your org.
Bitsight's focus is on point-in-time security posture. They use questionnnaires, which makes it hard to verify the responses provided by suppliers.	Cyberint's Supply Chain Intel provides continuous open, deep and dark web intelligence on your trusted vendors, partners and suppliers.
Attack Surface Management is new use case for Bitsight, so their capability is not mature. ASM is a 'side project' and not a primary area of expertise.	Cyberint developed and released an attack surface management module in 2017. It is fully integrated with other capabilities and features.
Bitsight uses basic ASM scans & questionnaires, but their visibility into threats on the deep and dark web, like malware and leaked creds, is limited.	Cyberint was founded in 2010 and has specialized in deep and dark web threat intel ever since. We have thousands of sources.
Bitsight's basic reports are cost effective but upgrading vendors to the continuous monitoring status consumes a lot of budget for security teams.	Cyberint's Supply Chain Intel module provides continuous monitoring with alerts sent to your SOC in real time, all at a lower price point.

OBJECTION HANDLING

Bitsight is an established 3rd party risk management vendor. They seem much more mature than Cyberint. Why should we choose you over them?

- We provide very different capabilities. If your main use case is compliance and meeting internal policy requirements, you may be better off with Bitsight. But if you want to stop breaches caused by insecure 3rd parties, we are the better choice.

Bitsight works with vendors to help resolve and remediate some of the security issues they've detected. Does Cyberint do something similar?

- At Cyberint, we are focused on keeping your business secure, not the 3rd party's. While contacting vendors may seem like a useful process, from what we've been told by former customers, it is rarely effective. Just because Bitsight contacts a vendor regarding a security issue does not mean the 3rd party will respond or cooperate with them.

Security Scorecard

FOUNDED: 2014
HEAQUARTERS: New York, NY, USA
EMPLOYEES: ~530
FUNDING: $300 Million (Series E)

27K FOLLOWERS

COMPANY OVERVIEW

SecurityScorecard was founded in 2014 as a third-party risk management and security ratings services vendor. They compete directly with Bitsight, RiskRecon, Black Kite, UpGuard, etc.

Like these other competitors, SecurityScorecard primarily uses external IT security assessments combined with vendor questionnaires to assign risk scores. Recently, they have also started to add new solutions to their offering: Automatic Vendor Detection, Attack Surface Intelligence, and Cyber Risk Intelligence.

ADDITIONAL RESOURCES

- https://securityscorecard.com/
- Third-Party Risk Management Datasheet
- Attack Surface Intelligence Datasheet
- Cyber Risk Intelligence Datasheet
- Executive-Level And Board Reporting Datasheet

SECURITY SCORECARD WEAKNESSES	CYBERINT DIFFERENTIATORS
SecurityScorecard is a security ratings service, focused on procedural use cases: vendor approval, M&A due diligence, reporting, compliance, etc.	Cyberint's Supply Chain Intel is focused on giving you the intel you need to stop attacks and breaches at 3rd parties from affecting your org.
Security Scorecard's risk assessment is based almost exclusively on basic ASM checks, which are important, but overlooks many crucial risk factors.	Cyberint's Supply Chain Intel provides continuous open, deep and dark web intelligence on your trusted vendors, partners and suppliers.
Continuous monitoring is limited to periodic ASM scans, not real-time intel and deep and dark web visibility to detect attacks and breaches in real time.	Cyberint's Supply Chain Intel provides continuous monitoring using open, deep and dark web intelligence with real-time alerting.
SecurityScorecard says they have threat intel but do they have this capability? Or is it just data bought from 3rd party vendors? How robust is the intel?	Cyberint was founded in 2010 and has specialized in deep and dark web threat intel ever since. We have thousands of sources.
SecurityScorecard is very strong at providing periodic reports on 3rd party vendors and partners but they don't alert you to real risks in real time.	Cyberint's Supply Chain Intel module send alerts directly to your SOC when a trusted 3rd party is attacked or breached, giving you time to react.

OBJECTION HANDLING

SecurityScorecard is an established 3rd party risk management vendor. They seem more mature than Cyberint. Why should we choose you over them?

- We provide very different capabilities. If your main use case is compliance and meeting internal policy requirements, you may be better off with Bitsight. But if you want to stop breaches caused by insecure 3rd parties, we are the better choice.

SecurityScorecard works with vendors to help resolve and remediate some of the security issues they've detected. Does Cyberint do something similar?

- At Cyberint, we are focused on keeping your business secure, not the 3rd party's. While contacting vendors may seem like a useful process, from what we've been told by former customers, it is rarely effective. Just because Bitsight contacts a vendor regarding a security issue does not mean the 3rd party will respond or cooperate with them.

BLACK KITE

FOUNDED: 2016
HEAQUARTERS: Boston, MA, USA
EMPLOYEES: ~110
FUNDING: $36 Million (Series B)

in **9K FOLLOWERS**

COMPANY OVERVIEW

Founded in 2016, Black Kite is a relatively new player in the security ratings services and third-party risk management space. They call their product a "Third Party Risk Intelligence" platform.

Black Kite's main differentiators appear to be: taking brand impersonation risks (e.g. phishing) and other threats (e.g. exposed credentials) into account alongside ordinary attack surface issues; estimating "the probable financial impact if a third-party vendor, partner or supplier experiences a breach"; and automatically mapping risk assessment results to compliance frameworks.

ADDITIONAL RESOURCES

- https://blackkite.com/
- Black Kite 3rd party risk management recorded demo
- Black Kite automated compliance mapping recorded demo
- Third-Party Breach Report 2023
- Centralizing Supply Chain Security Whitepaper
- University of Kansas Case Study
- Ellie Mae Case Study
- Carlsberg Case Study

BLACK KITE WEAKNESSES	CYBERINT DIFFERENTIATORS
Black Kite is focused on compliance with various industry standards and frameworks. This is useful but it is a very different use case from Cyberint.	Cyberint's Supply Chain Intel provides continuous open, deep and dark web intelligence on your trusted vendors, partners and suppliers.
Black Kite is providing a valuable product but it doesn't seem like it's built for InfoSec professionals – it's really a tool for GRC and auditing teams.	Cyberint's Supply Chain Intel module is built by InfoSec pros, for InfoSec pros. It is focused on helping customers to stop incidents & breaches.
Quantifying risk in terms of dollars and cents is a great feature but this doesn't necessarily help the InfoSec team to keep their organization secure.	Cyberint's Supply Chain Intel module provides the real-time info you need to stop a breach at a 3rd party from causing a breach at your organization.
Black Kite claims to detect brand impersonation (e.g. phishing sites) and other threats (e.g. exposed credentials) but threat intel is not their strength.	Cyberint has advanced threat intel and impersonation detection capabilities, which is all used to evaluate your vendors and suppliers.
Black Kite is still a relatively new vendor in the 3rd party risk management space. They haven't been mentioned in reports from Gartner, Forrester, etc.	Cyberint is a globally recognized threat intel leader, with many reference customers plus many mentions from Gartner, Forrester, Frost, etc.

OBJECTION HANDLING

Black Kite says that they also assess 3rd parties using threat intelligence and detect risks like phishing, exposed credentials, malware infections, and so on. How are you different from them?

- It's not clear where Black Kite is getting their intelligence from but, as they aren't a CTI provider, it's very likely they are simply buying data from a 3rd party vendor. Cyberint, on the other hand, is strongly focused on CTI, DRPS, and EASM.

We really like that Black Kite can quantify risk in terms of dollars and cents. Is this something that's on your roadmap?

- We are focused on providing intel that prevents insecure 3rd parties from causing a breach at your organization. Quantifying risk is useful but it's not part of the vision for Cyberint's Supply Chain Intel module. We give you the intel you need to protect your organization's networks, systems, and data.

MANDIANT®

NOW PART OF Google Cloud

FOUNDED: 2004
HEAQUARTERS: Alexandria, VA, USA
EMPLOYEES: ~2,200
FUNDING: n/a (acquired by Google Cloud)

in **177K FOLLOWERS**

COMPANY OVERVIEW

Mandiant was founded in 2004 as a digital forensics and incident response services firm. The founder, Kevin Mandia, started the company after co-authoring "Incident Response & Computer Forensics," one of the first and most foundational books on DFIR.

Mandiant rose to prominence after publishing a report in Feb. 2013 on APT1, a state-sponsored threat group based in China. In Dec. 2013, Mandiant was acquired by FireEye for $1 Billion but was later divested in June 2021 when FireEye was acquired by a private equity firm. In March 2022, Google Cloud acquired Mandiant for $5.4 Billion.

ADDITIONAL RESOURCES

- https://www.mandiant.com/
- Threat Intelligence Demo
- Threat Intelligence Datasheet
- Attack Surface Management Demo
- Attack Surface Management Datasheet
- Digital Risk Protection Demo
- Digital Risk Protection Datasheet

MANDIANT WEAKNESSES	CYBERINT DIFFERENTIATORS
Mandiant's focus as a threat intel provider is on sharing IoCs and tracking state-sponsored threat groups, but this is not targeted intelligence.	Cyberint is focused on Impactful Intelligence: true positive, relevant alerts directly related to your organization and its digital assets.
Mandiant is very strong in DFIR and some aspects of threat intel, but digital risk protection and attack surface management is not their primary focus.	Cyberint is the leader in the external cyber risk management market, which is the intersection of CTI, DRP, and EASM (see Frost&Sullivan report).
Mandiant sells products and technology but doesn't do much to help customers who don't pay very significant fees for a managed service option.	Cyberint offers a partnership. You get a dedicated analyst that works alongside your team to help your organization stay secure.
Mandiant is now owned by Google Cloud so they are part of a massive organization. Customers are one among many and don't get much support.	Cyberint is deeply invested in the happines and success of our customers. A dedicated customer success manager will support your account.
Mandiant does not offer Takedown services yet (they are planning on adding this to their offering). So you are left to manage takedowns independently.	With Cyberint, you can request a takedown with one click. We have a dedicated takedown team in-house that has a success rate of >95%.

OBJECTION HANDLING

Mandiant is a large, trusted cybersecurity vendor. Why should we select Cyberint over Mandiant?

- Mandiant is a great vendor but they aren't innovating and staying at the forefront of the market the same way Cyberint is. We also have a stronger commitment to customer success.

Mandiant seems to have a more advanced threat research function. Can the Cyberint team operate at the same level of excellence?

- Mandiant is focused on operational intel (IoCs) and strategic intel (tracking APTs) whereas Cyberint is focused on providing impactful intelligence – alerts about the threats you need to respond to ASAP.

What can Cyberint offer that Mandiant cannot?

- Cyberint helps organizations detect, assess, prioritize, and respond to external cyber risks. This includes everything from phishing and leaked creds to misconfigurations and 3rd party risks.

FORTRA™

FOUNDED: 1982 (formerly HelpSystems)
HEAQUARTERS: Minneapolis, MN, USA
EMPLOYEES: ~3,000
FUNDING: n/a (acquired by H.I.G. Capital)

in **28K FOLLOWERS**

COMPANY OVERVIEW

Fortra is a cyber vendor based in Minneapolis that offers a broad product portfolio, including DRP. Their capabilities include domain protection, phishing protection, social media monitoring, account takeover prevention, and data leak detection (e.g. credentials).

While they offer many capabilities, many of them were recently acquired. Fortra (formerly HelpSystems) acquired Digital Defense in Feb 2021 for vulnerability management; Phish Labs in Oct 2021 for brand protection; and Alert Logic in Mar 2022 for MDR. It's more of a private equity conglomerate than a true cybersecurity solutions provider, as they haven't built much technology in-house.

ADDITIONAL RESOURCES

- https://www.fortra.com/
- https://www.phishlabs.com/
- https://www.digitaldefense.com/
- https://www.alertlogic.com/
- https://www.digitalguardian.com/
- Frost & Sullivan: Fortra is 2022 Company of the Year for DRP
- Fortra: Cybersecurity Solutions Portfolio Overview
- Fortra: Frontline Vulnerability Management Datasheet

FORTRA WEAKNESSES	CYBERINT DIFFERENTIATORS
Fortra acquired many vendors to stitch together their cybersecurity capabilities: Phish Labs, Digital Defense, Alert Logic, Digital Guardian, and more.	Cyberint is a true innovator and has pioneered the combo of CTI, EASM, and DRP for years. All tech is built in-house and natively integrated.
Fortra provides many DRP use cases: domain protection, phishing protection, social media monitoring. What about EASM and 3rd party risks?	Cyberint provides an advanced EASM module that continuously identifies exposures and risks, plus the Supply Chain Intelligence module.
Fortra collects malware logs & leaked creds but how extensive is their visibility? Deep & dark web monitoring and CTI doesn't seem like their focus.	CTI and deep & dark web are in Cyberint's DNA. We provide operational, strategic, and tactical intelligence, plus continuous DDW monitoring.
Fortra has suffered a major security incident in 2023– the GoAnywhere campaign and following communication failures. Can you trust them?	Cyberint is a cyber vendor that always puts security first, for our own organization and for our customers. We are a vendor that can be trusted.
Fortra doesn't seem to offer Takedown services (or if they do, it's certainly not a focal point). So you are left to manage takedowns independently.	With Cyberint, you can request a takedown with one click. We have a dedicated takedown team in-house that has a success rate of >95%.

OBJECTION HANDLING

We're only interested in digital risk protection use cases. Why should we go with Cyberint over Fortra?

- Cyberint has been a leader in the DRP space for years, as recognized by industry analysts (Gartner, Forst, etc.) as well as our customers. We provide full DRP coverage for all impersonation use cases.

Fortra is offering us a lower price point as compared to Cyberint. Can you work with us on the pricing?

- Cyberint's pricing is aligned with the value we provide to our customers. We can offer discounts to make the price more competitive but, at the end of the day, you get what you pay for and Cyberint provides an extremely robust, valuable platform.

SpyCloud

FOUNDED: 2016
HEAQUARTERS: Austin, TX, USA
EMPLOYEES: ~200
FUNDING: $170 Million (Series D)

9K FOLLOWERS

COMPANY OVERVIEW

SpyCloud was founded in 2016 as an account takeover and fraud prevention vendor. Most of their capabilities revolve around deep and dark web monitoring and leaked credentials. In August 2023, they raised $110 Million in a Series D round.

SpyCloud now positions their product as a “cybercrime analytics platform” that provides “identity-centric solutions that scale to outpace criminal innovation.” The use cases are still focused on account takeover (for consumers and employees), fraud prevention, and DDW monitoring. In their marketing materials, they have a heavy focus on integrations and automated remediation capabilities.

ADDITIONAL RESOURCES

- https://spycloud.com/
- https://spycloud.com/resources/spycloud-labs/
- SpyCloud: Enterprise Protection Solution Brief
- SpyCloud: Employee ATO Prevention Datasheet
- SpyCloud: Session Identity Protection
- SpyCloud: Compass Ransomware Prevention Datasheet

SPYCLOUD WEAKNESSES	CYBERINT DIFFERENTIATORS
SpyCloud claims to have hundreds of billions of credentials but most of that is old, irrelevant data. How are their ongoing collection capabilities today?	Cyberint collects tens of millions of malware logs each month, totaling nearly 100 Million sets of leaked creds per month on an ongoing basis.
SpyCloud provides deep and dark web monitoring and some intelligence related to exposed credentials, but what about strategic intelligence?	Cyberint provides many strategic intelligence modules: threat landscape, threat actor + malware + CVE intel modules, plus reports.
Malware logs and compromised credentials represent just one attack vector. What about phishing, malicious apps, fraudulent social profiles?	Cyberint has been a leader in digital risk protection for years and provides extensive coverage against all impersonation use cases.
SpyCloud doesn’t fully map out your external attack surface or check for common security risks, such as unpatched software with exploitable CVEs.	Cyberint provides an advanced ASM capability that continuously discovers your external assets, detects exposures, and alerts you to major risks.
SpyCloud doesn’t appear to offer ‘takedowns’ or purchase of compromised credentials from marketplaces and other dark web forums.	Cyberint has an in-house takedown team for more traditional takedowns, plus a CTI team with avatars on the dark web to buy leaked creds.

OBJECTION HANDLING

SpyCloud is primarily focused on detecting leaked credentials. Doesn’t that mean they’re stronger than Cyberint in this particular use case?

- No, one of Cyberint’s strengths is collecting InfoStealer logs, each of which can contain dozens, hundreds, or even thousands of set of leaked creds.

SpyCloud provides many more integrations than you. This makes their offering more attractive.

- We’re happy to develop the native integrations you need to select Cyberint. It’s a one-time effort that will enable you to procure the stronger platform and, in the long run, get more value.

SpyCloud has a more robust fraud prevention offering. What capabilities does Cyberint offer here?

- Many of the use cases that Cyberint covers eliminate threats before they can evolve into fraud: fake social media profiles, phishing sites, malware log collection, DDW monitoring, leaked creds, etc.

Thank You!

cyberint.com