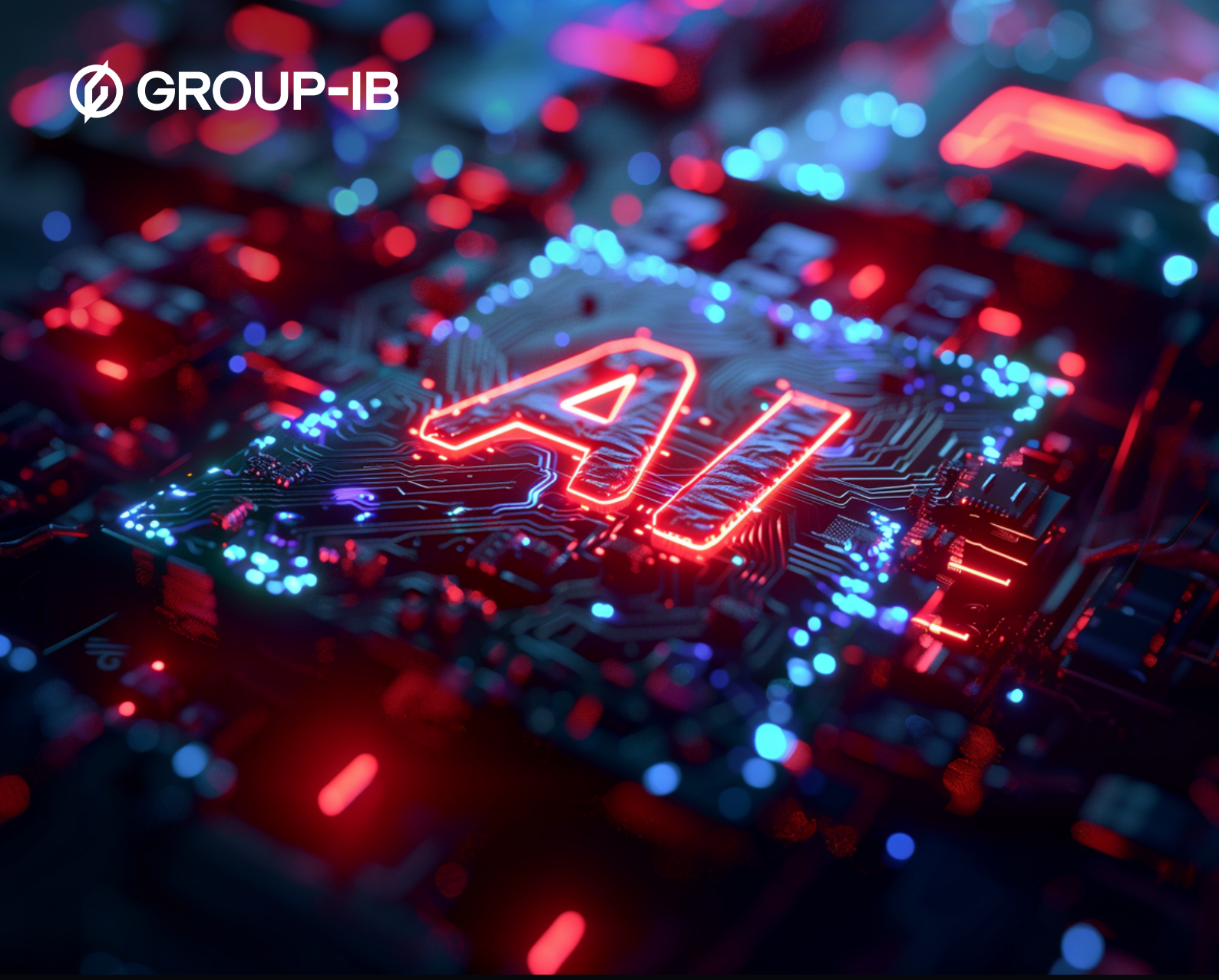
GROUP-IB



GROUP-IB EGUIDE

CYBERSECURITY X AI:
BUILDING CAPABILITIES TO DEFEND ASSETS AND DEFEAT ATTACKERS

There's no denying it: Artificial intelligence has emboldened and empowered cyber criminals, helping them attack faster, more frequently, and with greater impact. But the good news is AI can be a force multiplier for cyber defenders—if you know how to enable it and select the right partner.

TABLE OF CONTENTS

1. INTRODUCTION

Let's start with a quick message from **Group-IB's CEO, Dmitry Volkov**, on how to navigate and utilize the eGuide.

As a cybersecurity service provider for over two decades, we fully understand those of you tasked with steering your organization clear of cybersecurity risks. Faced with unsettling challenges to maintain an ever-resilient posture, you might have already dived deep to understand AI's effects and impact on you, your security team, and your interactions with other organizations, groups, people, and communities.

Building an effective cybersecurity defense is always challenging, complex, and critical to any organization. AI's integration into the cybersecurity world is unquestionable. Many of you might have already spent hours in boardrooms discussing its fantastic potential to help lighten your workloads and meet the growing demands of maintaining security. But it's important to note that AI is the ultimate double-edged sword. It offers incredible opportunities but also presents major challenges. Gartner provides an excellent context for this:

> "Gartner sees generative AI becoming a general-purpose technology with an impact similar to the steam engine, electricity, and the internet. The hype will subside as the reality of implementation sets in. Still, the impact of generative AI will grow as people and enterprises discover more innovative applications for the technology in daily work and life."

That's a heady prediction coming from the publisher of the highly respected Gartner Hype Cycle, which puts widely promoted industry trends into reality-based contexts.

However, we believe AI already has a deep and potentially groundbreaking impact in its use within the cybersecurity landscape. The tectonic plates of AI and cybersecurity aren't just shifting—they are crashing violently into each other, creating a critical sense of urgency for cybersecurity professionals, business stakeholders, C-suite executives, and board members. AI-powered cybersecurity won't be an aspiring initiative for long, but a pressing need businesses need to build strategies and tactics to develop effectively and agilely.

Here's what to expect from this eGuide.

First, let us tell you what this content is not:

- ✕ It is not a deep dive into the technical issues of AI and cybersecurity. Of course, our experts can give personalized advice to anyone looking for technical insights.
- ✕ It is not a "scare story" designed to frighten organizations and their stewards into making rash, unwise, and ill-planned moves.
- ✕ It is not a promotional piece but an informative resource.

Here's what you can expect from this piece:

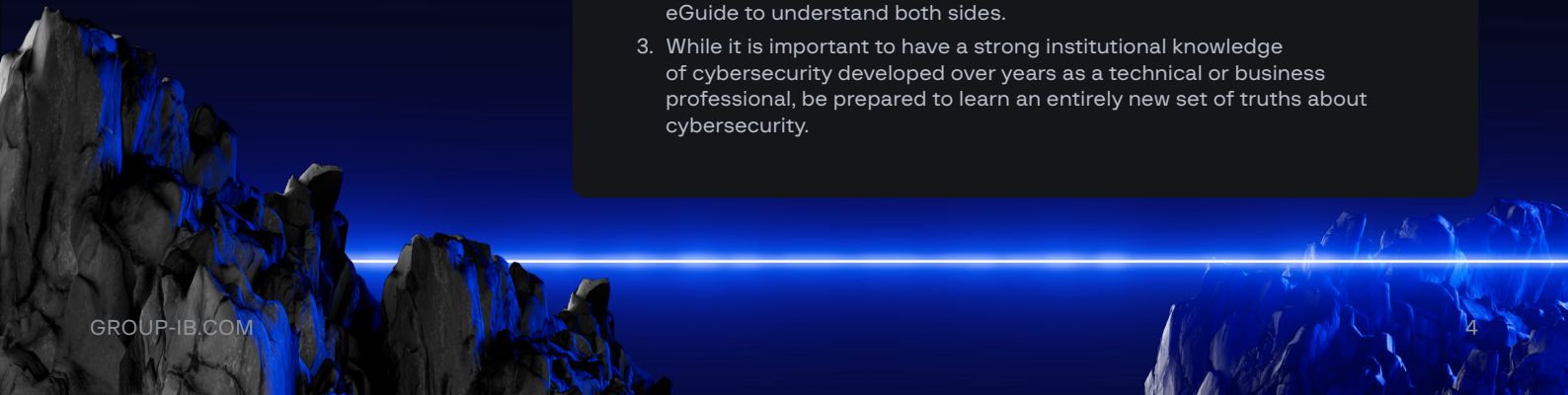
- ✓ Information about the key issues, challenges, and opportunities in the intersection of AI and cybersecurity.
- ✓ Industry-expert perspectives and ideas from consultancies and market research firms.
- ✓ A data-enhanced narrative that leverages relevant and actionable research statistics to provide evidence and context for those perspectives and ideas.

You'll see that we close each section with a short summary called **"Three Things to Consider,"** including actionable steps your organization can take to better prepare for AI-powered cybersecurity.

Thank you for taking time out of your busy day to learn more about these issues.

Three Things to Consider:

1. At the risk of stating the obvious, AI is changing everything. But the changes we've seen recently are nothing compared to what will take place in the very near future and beyond.
2. The relationship between cybersecurity and AI is an important one: It represents a clash and a collaboration, and it's essential for readers of this eGuide to understand both sides.
3. While it is important to have a strong institutional knowledge of cybersecurity developed over years as a technical or business professional, be prepared to learn an entirely new set of truths about cybersecurity.



2.

WHY AI'S IMPACT ON CYBERSECURITY IS HUGE

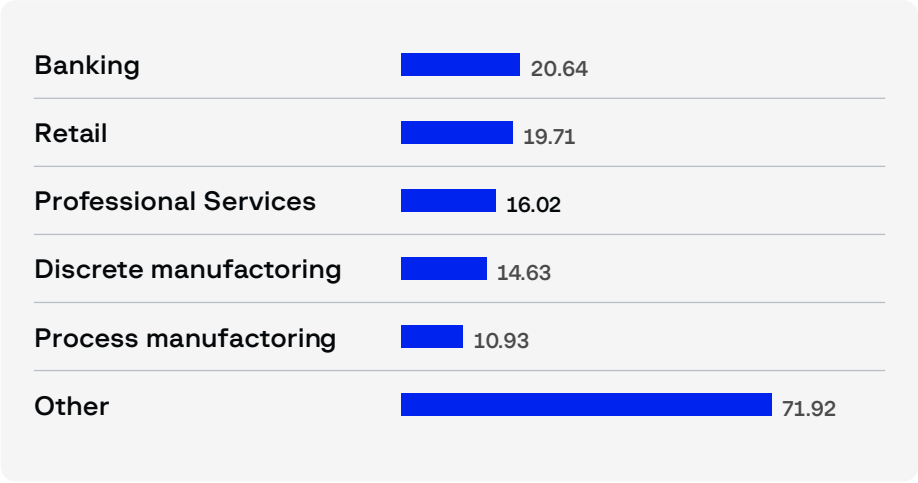
The idea of AI having outsized influence over an organization's cybersecurity strategy is not new. For more than a decade, security professionals have been exposed to attackers' use of effective tools such as automation, runbooks, and scripts to plot and execute malicious content and exploits. Initially, the impact was fairly limited because the tools hackers used either did not scale in terms of attack vectors or did not unleash substantial mayhem before being detected.

But the situation has clearly changed—and it's not only because the tools are now more sophisticated and more capable of causing significant damage before security defenses kick in. It's also because hackers have become much more comfortable and adept with these new methods of attack.

To understand how AI became such a force in the cybersecurity realm, let's take a step back and assess the growth and development of both AI and cybersecurity.

For a long time, AI was a curiosity, something examined in boutique research labs on university campuses or in sandbox projects of major corporations' R&D centers. Expert systems, as AI was familiarly called in the late 20th century, handled basic levels of inference, rule-based reasoning, and entry-level domain knowledge. Scientists envisioned expert systems having utility in use cases such as first-generation credit scoring and music genre preferences.

Today, those relatively crude and limited-function precursors to what is now known as **Generative AI (GenAI)** have morphed into a powerful force reshaping knowledge, content, and decision-making in every industry. In fact, research indicates billions of dollars are spent annually on AI-based systems in dozens of different industries. Five different industries—banking/financial services, retail, professional services, discrete manufacturing, and process manufacturing—are each spending more than $10 billion annually on AI solutions.



Global spending on AI 2023, by industry – © Statista, 2024

For many years, computer scientists and security analysts have understood the growing sophistication of AI meant it would have widespread utility in one of the biggest segments of the entire IT industry landscape—cybersecurity.

As we wrote in a blog earlier: "Artificial intelligence had its big bang moment in the '90s, revolutionizing almost every sector. So, how could cybersecurity escape its influence? The rapid integration of AI into cybersecurity has paved the way for efficiency, agility, automation, and data analytics to take over operations."

After all, cybersecurity is now a massive market segment, expected to approach $200 billion in global expenditures by the end of 2024 and eclipse $300 billion in just five years.

GenAI has captured the lion's share of interest and visibility in cybersecurity because of its wide use in information security research, training, and simulation due to its ability to create cyber-attack scenarios and more, all discussed in great detail in our previous blog. In fact, many statistics in this eGuide specifically speak to GenAI's current and forthcoming impact on cybersecurity.

However, numerous other forms of AI have burst onto the scene with similar levels of impact and importance, each with its own unique influence on cybersecurity. For instance, **Predictive AI**, as the name implies, is well suited for predicting how, where, and when cyber-attacks will threaten an organization. It is also good at helping users spot and analyze patterns, making it a great fit for organizations looking to predict behavior that may indicate threats or even actual attacks. **Causal AI** is also rapidly gaining adoption because it helps organizations understand and create models for cause-and-effect patterns—not only for possible attacks but for the most appropriate responses.

Explainable AI (XAI) serves as a crucial pathway for teams and organizations to comprehend the logic or rationale behind AI-generated decisions, such as alerts and recommendations. By providing transparency, XAI enables prompt, effective, and well-calculated decisions, minimizing potential biases that can arise in manual decision-making processes.

At Group-IB, we recognize the significance of this aspect and have dedicated efforts to incorporate explainability into our fraud protection technologies.

Similar to cybersecurity, the application of AI is multifaceted. In a recent gathering of international leaders, the United Kingdom's National Cyber Security Centre highlighted AI's potential to make cybersecurity more effective:

> "While it is essential to focus on the risks posed by AI, we must also seize the substantial opportunities it presents to cyber defenders. For example, AI can improve the detection and triage of cyber-attacks and identify malicious emails and phishing campaigns, ultimately making them easier to counteract."

But there is little doubt AI represents the ultimate double-edged sword in cybersecurity. The World Economic Forum added:

> "While AI is being utilized to enhance cybersecurity operations and improve network monitoring and threat detection, it is also being leveraged by threat actors to enhance their attack capabilities and methods … the race between offensive and defensive AI has never been closer or more important."

The impact of cyber attacks on individuals, businesses, governments, communities and entire nations is undeniable. And AI is making it more likely—and more profitable—for hackers to use the technology, from extorting school districts with ransomware to taking down another nation's power grid.

Why?

As you'll see in the next two sections, there are powerful forces that have made AI both a huge threat to our cybersecurity and an exciting opportunity for a more formidable, scalable, and efficient defense. The reasons why include:

- The transformation of what was once the domain of theoretical research into a massive commercial opportunity, driving incredible advances in performance, functionality, and ease of use.
- The relentless improvement in computing price/performance puts the wherewithal to drive AI in the cybersecurity world within the budgets of organizations of all sizes, as well as that of individual hackers.

But the ultimate reason AI is such a powerful force on both sides of the cybersecurity equation is a simple one: the primacy of data. The hackers want it and are becoming more resourceful and innovative in exploiting it, and the defenders have adopted a "defense at all costs" mindset, sparing no effort to use technologies such as AI in every way possible. The more data we create, consume, share, analyze, and use, the higher the stakes for hackers and defenders alike.

Three Things to Consider:

1. The fates of AI and cybersecurity are inevitably and inextricably linked, perhaps never to be separated.
2. AI may be the single most important defining force for the future of cybersecurity.
3. Organizations should not slow down their use of AI for fear that hackers will use it against them—quite the contrary, in fact. AI must become a more central part of all organizations' business functions.

3. AI-ENHANCED THREATS AND CHALLENGES

Adversaries come in all shapes and sizes, as everyone knows. However, they tend to share commonalities: they are sly, highly motivated, persistent, and unquestionably interested in substantial monetary returns from their efforts. It's those common factors that make them so dangerous.

Cybercriminals increasingly work in a highly collaborative manner, either as part of an organized cybercrime ring or in a loose federation of attackers, readily sharing techniques, tools, and illicit information on underground forums and dark web marketplaces. These forums serve as a marketplace for buying and selling malware, exploits, and stolen data, but they also facilitate collaboration in terms of building target lists, listing vulnerabilities, and most potent exploit schemes.

But one aspect of AI has dramatically heightened the concern shared by CISOs, SecOps teams, IT professionals, business stakeholders, and board members: AI makes it much easier for relatively inexperienced adversaries—often with limited technical and financial resources—to attack the largest organizations in the world.

Of particular concern is the ability of hackers to automate their attack methodologies for faster, more repetitive attacks. In the 2023/2024 Hi-Tech Crimes Report published by Group-IB, we wrote about the growing influence of "hacktivists," who call attention to a social or political cause instead of generating cyber-attacks for financial gain, and who often do so with the help of supporters. To quote that report, in situations in which the hackers carry out defacement attacks, "The frequency with which defaced pages are posted (in some cases as often as several dozen times per day) suggests that … such groups carry out mass exploitation of widely known vulnerabilities for which public exploits are available."

This is a key point echoed by numerous industry analysts. According to Dave Gruber, principal analyst in TechTarget's Enterprise Strategy Group's cybersecurity practice, "Automation has created the concern that AI will make it easier for less-skilled adversaries to participate in malicious activities, increasing the volume of attacks." Gruber adds that security teams are also keenly worried about the speed and diversity of AI-generated phishing tactics.

Gartner sees the growing influence of AI in cybersecurity attacks too: "Enterprises must prepare for malicious actors' use of generative AI systems for cyber and fraud attacks, such as those that use deep fakes for social engineering of personnel, and ensure mitigating controls are put in place."

The aforementioned Hi-Tech Crime Trends Report also details how sophisticated hackers have become in their use of digital tools such as AI in their attack methods, revealing that: "Some threat actors take open-source LLMs from public repositories … and adopt the knowledge-based approach, a methodology for training AI models that involves creating a structured database of information and using it to inform the system's decision-making process and re-train the system."

Of course, the rapidly growing popularity and utility of LLMs such as ChatGPT make them easy tools for hackers to exploit. The statement follows substance as Group-IB's Threat Intelligence team recently uncovered in its dark web marketplace investigation more than 100,000 ChatGPT credentials were stolen from compromised devices. A large number of user devices infected with information stealer malware that have access to OpenAI accounts have been put up for sale on underground markets.

"Many enterprises are integrating ChatGPT into their operational flow. Employees enter classified correspondences or use the bot to optimize proprietary code," commented Dmitry Shestakov, head of threat intelligence at Group-IB. According to the security expert, if threat actors manage to obtain account credentials, ChatGPT's standard configuration's retention of all conversations could unintentionally provide them with a wealth of sensitive intelligence.

Adjusting your AI defenses to be stronger than AI counterattacks

Undoubtedly, attackers gravitate toward AI models for capabilities such as technical consultation, scam creation, intelligence gathering, and maintaining their anonymity. Adversaries are integrating AI into their workflows to scale their threats' impact, innovate their threat methodologies, and create new revenue streams. This has been made much easier for them due to the wider availability of inexpensive (and free) AI tools. They are also utilizing AI to execute hacking toolkits and are building malicious tools for exploits and digital espionage while brainstorming attack techniques, tactics, and procedures (TTPs).

AI-generated malware is used to exfiltrate data from AI services, substantially broadening the scope and impact of data theft. In fact, bad actors are actually copying LLMs in order to commit crimes. FraudGPT and DarkBard are stark examples of this trend. Even the popular ChatGPT tool has been victimized by attackers who spotted and exploited several security vulnerabilities in third-party APIs and plug-ins.

Group-IB's analysis has surfaced an alarming trendline toward significant increases in the number of ChatGPT credentials for sale. For instance, during a five-month period in the second half of 2023, more than 130,000 unique hosts with access to OpenAI were compromised; that figure represented a 36% spike in the number of infected devices when compared to the prior five months. As we revealed in the Hi-Tech Crimes Report, this sharp increase in the number of ChatGPT credentials for sale is due to the overall rise in the number of hosts infected with information stealers, data from which is then put up for sale on markets or in UCLs.

Unquestionably, this is highly concerning to organizations of every nation and industry. For instance, the chaos is already ensued with some of these tactics:

- Financial services firms being hit with an avalanche of fraudulent transactions facilitated by AI-driven deepfake images posed as legitimate customers.
- A sophisticated cybercriminal group leverages AI to identify zero-day vulnerabilities in popular software products and write exploits to compromise many networks. This advanced AI-driven attack demonstrates the potential dangers posed by the malicious use of artificial intelligence in the cyber threat landscape.

- AI being used to create highly coveted cyberattacks on governments and large corporations. Not only is AI used to pinpoint potential entry points, but the technology adapts its behavior to avoid detection and employs encryption, polymorphism (code mutation), and anti-forensic techniques to maintain persistence within compromised systems.

But these examples are not hyperboles. AI is already used to attack cybersecurity defenses and circumvent legitimate security policies and controls.

Three Things to Consider:

1. Adversaries have jumped into the lead over defenders when it comes to leveraging GenAI and similar AI tools.
2. The ease of use and very low cost of AI tools dramatically expand the number of AI-induced attacks because it makes it much easier for less-sophisticated attackers to exploit the technology.
3. The increasingly collaborative nature of hacking makes it easier for attackers to gain important knowledge on how to exploit AI.

4. AI AS A CYBERSECURITY SHIELD

In the previous section, we explored how cybercriminals are using GenAI and other LLMs to execute their malicious intentions, expand their attack vectors, and launch their exploits faster, more frequently, and with more devastating impact. While that may not be the message many executives, board members, and stakeholders want to hear, the harsh reality is that you can't plan a proper defense until you have a full understanding of, and respect for, cyber attackers' methods.

There is good news, however. The cybersecurity industry has made promising strides in using many different facets of AI specifically to fight cyber attacks built through AI manipulations or other illegitimate techniques. Just as earlier iterations of cybersecurity defenses—such as Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), and Extended Detection and Response (XDR)—have helped identify, prevent, and mitigate the impact of attacks, the new breed of AI-empowered solutions acts as an effective and efficient cybersecurity shield.

This defensive framework is intelligent, scalable, cost-efficient, and highly automated. In many cases, AI tools and machine learning (ML) algorithms are integrated into tightly architected cybersecurity platforms that support many sophisticated plug-ins and application programming interfaces to extend the coverage and functionality of AI-powered cybersecurity defenses.

Numerous consulting firms and research organizations express optimism about AI as an exciting technology for cybersecurity defense:

> "Both buyers and providers of cybersecurity services can take advantage of (AI) while remaining protected." (Bain & Company)

> "AI and ML present excellent tools to augment humans and reduce technology costs across cybersecurity capabilities." (EY)

> "We believe that CISOs that use generative AI to improve security processes will have an opportunity to better protect their organizations." (KPMG)

One important step organizations need to take to ensure their use of AI in cybersecurity defense is responsible is to ensure the right security controls are in place. Security Magazine recently reported that many chief information security officers are getting behind an effort to create an AI security framework to help them understand the potential security risks of AI systems. It also notes that proper governance is essential for ensuring a more secure—as well as more responsible—deployment of AI tools and systems.

Other important AI and cybersecurity industry organizations are also taking important steps to ensure proper and secure use of AI. For instance, NVIDIA—considered the leading supplier of AI infrastructure chipsets—released product security policies that encompass its AI portfolio. NVIDIA highlighted several specific recommendations, including:

- Keeping network control and data planes separate.
- Setting appropriate flow controls.
- Using Zero Trust security principles and consistent authentication methods.
- Removing personally identifiable data whenever possible.
- Defining appropriate alerts, tests, and event logs.

Additionally, the Open Worldwide Application Security Project—which evaluates and provides recommendations on the top application security risks—released AI-tailored implementations of key security elements, such as the common vulnerability enumeration method used to identify traditional IT threats. One key part of its recommendations has a tight focus on ensuring AI privacy, which is widely considered a potential security vulnerability for increasingly ambitious AI solutions. Those recommendations cover such issues as usage limitations and purpose specifications, ensuring fairness in handling personal data, limiting data storage timeframes, anonymizing data as much as possible, and following industry privacy standards such as ISO 29100 to demonstrate transparency in privacy, data accuracy, and user consent.

One of the most vital steps in any cybersecurity program is assessing readiness, in which organizations determine their cybersecurity readiness through in-depth and broad-ranging analysis. As you'll see as you read ahead, we've devoted a chapter to assessing and evaluating cybersecurity readiness—and not just in the present but with a particular focus on what's around the corner. This is a critical benefit of using the many forms of AI—GenAI, Predictive AI, Causal AI, machine learning, deep learning and more—to identify potential attack vectors, methodologies, and tactics.

Of course, the well-publicized and often-quoted skills gaps in both cybersecurity and AI have a profound influence in this area. Clearly, organizations need to use technologies such as AI to help extend the capabilities and coverage of their in-house teams. Fortunately, there are several areas in which AI can be an efficient force multiplier of a cybersecurity organization's capabilities:

Fraud detection: AI and ML can help organizations in attack-sensitive industries—such as financial services and retailing—to enhance their digital web and mobile applications, helping them to spot and thwart attempted attacks by utilizing user behavior analysis and biometrics, including keyboard or cursor patterns.

Threat intelligence: AI tools can be used to analyze structured historical data to extrapolate the next likely attack vector of a hacker.

Traffic analysis: AI-powered analytics can easily detect likely threats, enabling monitoring and detection resources to be used more efficiently.

Graph analysis: Automating the examination and interpretation of data on very large graphs is of use in predictive analytics, helping organizations identify correlations and unusual patterns.

Dark web investigation: AI can identify all of an attacker's accounts far more reliably and quickly.

Phishing detection: AI-powered text and image analysis can be used to detect phishing content.

Malware Detection and Analysis: GenAI models can be trained to identify patterns of malicious behavior or anomalous activities in network traffic, aiding in detecting malware (including polymorphic malware that constantly changes code).

Enumerating Tactics, Techniques, and Procedures (TTPs) of Advanced Persistent Threats (APTs) and other actors: It is instrumental in identifying the kill chain, building defenses, and supporting intrusive cybersecurity engagements such as red teaming. Teams can also leverage GenAI to understand threat actors and their attack maneuvers and get answers to critical questions like "Where am I most vulnerable?" through natural language queries.

Patching vulnerabilities: Security teams can utilize GenAI to identify vulnerabilities and automate the generation of security patches. These patches can then be tested for efficacy in a simulated or controlled environment.

Intelligent Response to Cyber Threats: With networks facing growing threats, GenAI enables a shift from rule-based systems to contextual analysis to help join the hidden links that reveal the complete chain of threat activity. LLM models are also employed to develop self-supervised threat-hunting AI, autonomously scanning network logs and data to provide adaptive and dynamic threat responses.

Code generation: GenAI can assist in various SecOps tasks, such as code generation, writing queries, and creating playbooks. Additionally, it can assist in red teaming exercises by generating code to automate the simulation of real-world threats. Through GenAI, security teams can craft scripts and tools to automate diverse attack scenarios, providing a comprehensive security posture assessment. It assists red teams in generating exploit codes during reconnaissance, helping organizations quickly identify weaknesses in their defenses. Furthermore, GenAI enables the swift adaptation and evolution of attack simulations, ensuring ongoing improvement in security testing.

Using AI and ML also provides other significant benefits to create a more robust, flexible, and intelligent cybersecurity defense shield. For instance, these tools enhance **security protocols** by creating complex security configurations for network-connected devices. **Training and simulation** is another area in which AI tools efficiently augment often-overworked in-house cybersecurity staff, quickly and automatically generating training materials,including simulations based on historical data and rapidly changing industry trends on attack vectors.

Data loss prevention is an additional critical activity with which AI can help immeasurably. New tools interpret frequently confusing and contradictory contexts for numerous data types, creating processes, rules, and procedures to further prevent sensitive and personal information from being exfiltrated inappropriately.

In each of these cases, one of the most important goals is to ensure organizations can get out in front of attacks—to stop them before they execute malware, exploit endpoints, infiltrate networks, and move laterally throughout the enterprises.

To understand and explore AI's diverse and amazing use cases for upgrading your cybersecurity practices to the next level, contact Group-IB domain experts for a complete and tailored picture for your business.

It's vital to understand that although these sophisticated and innovative tools help immeasurably, they cannot manage every cybersecurity task without expert intervention and help. Human intelligence is still an essential component of using GenAI most effectively. AI tools are great at reacting to new attack vectors and innovative new threats, but employees of technology partners can often be the key factors in preventing a security threat from becoming a security incident. Having a well-resourced and highly trained team of cybersecurity professionals at a CISO's disposal as an outsourced resource also helps bridge the critical, huge, and still-expanding cybersecurity skills gap.

Three Things to Consider:

1. Even though attackers often gain the initial advantage in using new tools such as GenAI, defenders can more than make up the difference if they understand how to leverage the technology in key areas, such as threat intelligence, analytics, and anomaly detection.
2. AI is a powerful force multiplier in extending an organization's cyber defenses, but it must be extended and complemented with well-trained, AI-proficient cybersecurity experts.
3. Assessing readiness is a critical benefit in using AI as part of comprehensive cybersecurity hygiene.

5.

BEST PRACTICES IN ASSESSING CYBERSECURITY READINESS FOR TODAY AND TOMORROW

Putting in place the right AI tools, processes, and teams requires more than just a checklist of activities for cybersecurity readiness. It requires detailed planning for both the short and long term, a well-resourced and properly orchestrated rollout and deployment, and the development of metrics to test and ensure the efficacy of AI-powered cybersecurity.

With that in mind, here are a few specific best practices organizations can use when deciding how to incorporate AI in their cybersecurity strategy and how to use the technology to properly determine their cybersecurity readiness.

1. **Threat intelligence should be a primary use case for AI**. Threat intelligence feeds are often under-leveraged in many organizations' cybersecurity frameworks, but using AI as part of threat intelligence gives a more finite and precise understanding of what threats are evident, where they are attacking, and how they should be remediated.
2. **Automation, especially in detection and response, is essential to getting the most from AI-powered cybersecurity**. While tools such as Endpoint Detection and Response, Managed Detection and Response, and Extended Detection and Response are all starting to use AI to some degree to speed cybersecurity actions, full-blown automation is greatly enhanced by AI tools. This not only speeds up detection and response but also makes it less likely to result in false positives or an endless array of alert triage.
3. **Data quality really matters**. AI systems need to connect to a wide range of high-fidelity data sources in order to be properly trained on threats, attack vectors, and response methodologies.
4. **Anomaly detection is much more accurate and actionable with AI tools**. Detecting and interpreting unexpected data behavior or unusual activities in networks or logs is cumbersome and difficult using even fairly recent tools. AI, however, is faster and more accurate in spotting precursors to actual attacks.
5. **Don't overlook the human factor**. In fact, having experienced, well-trained, and creative people working closely with AI tools is the best way to ensure you get the most from your cybersecurity AI investments. AI-proficient analysts can take digital forensics and analytics a step further by providing contextual perspective and making judgment calls in increasingly complex situations.
6. **Selecting the right tools and the right partner isn't just a technology decision**. You need a diverse, well-rounded team of contributors to make these evaluations. In addition to technical team members such as CISO, CIO, CTO and their teams, include key stakeholders from lines of business including those most likely to benefit from AI-powered cybersecurity. Be sure to also include representatives from finance, legal, human resources, and compliance/governance.

7. **Establish, review, and refine governance and policies frequently**. In many instances, this is going to be uncharted territory, so it will pay to be flexible and responsive to new lessons learned about AI usage governance.
8. **Don't build an AI framework**. Start with security objectives and build an appropriate GenAI security strategy.
9. **Continuous monitoring is critical**. Be sure to continually monitor cyber threat intelligence—facilitated by AI and machine learning, of course—in order to stay ahead of Zero Day threats, advanced persistent threats, and emerging threats created and augmented by adversarial AI tools and intentions.

To help you further assess the state of your organization's readiness in utilizing AI for cybersecurity requirements, we have developed an online Readiness Assessment tool.

About the Group-IB AI-Readiness Survey

Click here to easily navigate the self-driven survey; we're confident you'll get a useful insight into how well-positioned your organization is in using AI for effective cybersecurity. The survey is carefully designed to evaluate AI's relevance to your business, integration of AI into your existing infrastructure, your current maturity level and expertise, and identify the specific use cases for which AI can be implemented.

After the survey, you will receive a comprehensive score across these areas, providing valuable insights into your readiness for AI adoption. This score will inform the next steps, guiding you toward recommended actions tailored to your organization's needs and empowering you to prioritize and plan your AI initiatives effectively.

START THE SURVEY

Three Things to Consider:

1. Using AI to enhance an organization's cybersecurity readiness is a strategic decision—but it's not a strategy in and of itself. It's a starting point for a broader cybersecurity strategy.
2. Don't try to do everything at once. While using AI to create more effective and efficient cybersecurity, it's wise to start with a few use cases to build success and momentum.
3. In the words of legendary college basketball coach John Wooden: "Be quick but don't hurry." There is a sense of urgency here, but don't rush into decisions. Better to take a little time and get it right.

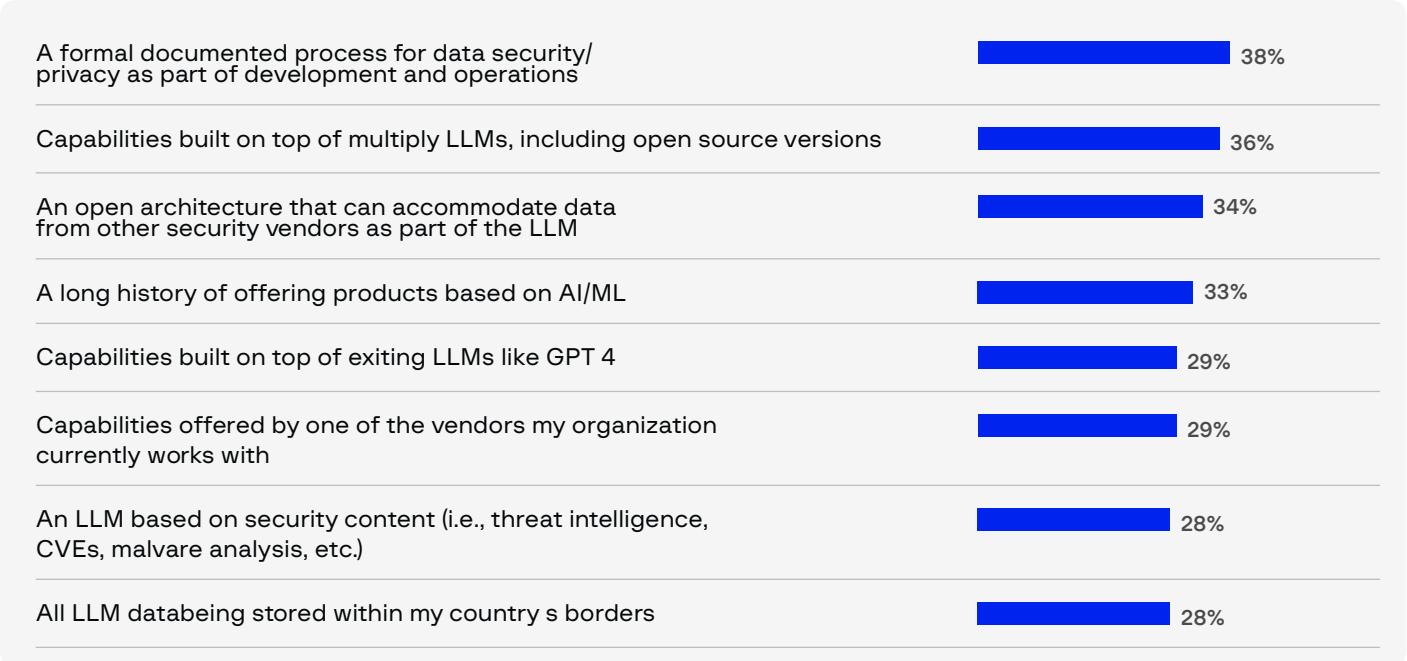
6. EVALUATING AND SELECTING THE RIGHT PARTNER FOR AI-ENABLEMENT—ABOUT GROUP-IB

Cybersecurity has long been said to suffer from "tools sprawl," the phenomenon describing the widespread proliferation of security solutions. This has usually been a byproduct of the breakneck pace of new threats introduced within the IT landscape, forcing organizations to evaluate and select tools for those problems and to determine the best partners with whom to work.

AI-powered cybersecurity isn't likely to be any different since this emerging area requires new kinds of solutions that are effective (able to protect against sophisticated threats) and efficient (able to do so as quickly, inexpensively, and with as little drain on cybersecurity resources as possible).

When determining which products, services, and vendors to use to leverage an AI-powered cybersecurity framework, it is essential to keep the top requirements in mind.

Enterprise Strategy Group polled IT and cybersecurity executives from around the world on their top needs in this process, and their findings made it clear that multiple capabilities are required. Topping the list is having a formal, documented process for data security and privacy as part of the DevOps model (38%); followed by capabilities built on top of multiple LLMs (36%), having an open architecture that can accommodate data from other security vendors; and possessing a long history of offering products based on AI and ML (33%).



Generative AI for Cybersecurity, Enterprise Strategy Group, 2024

Therefore, any organization looking to team with a solutions provider to deliver state-of-the-art solutions—as well as the ability to service and support those solutions—should look for a partner with such capabilities as:

- A history of supporting AI across a number of cybersecurity use cases, such as ransomware, phishing, and bot protection; dark web monitoring; and data leak prevention.
- A wide range of AI-powered services, such as digital forensics, incident response, and high-tech crimes investigation.
- AI-powered and AI-aware products in areas such as attack surface management, threat intelligence, fraud protection, and business email protection.

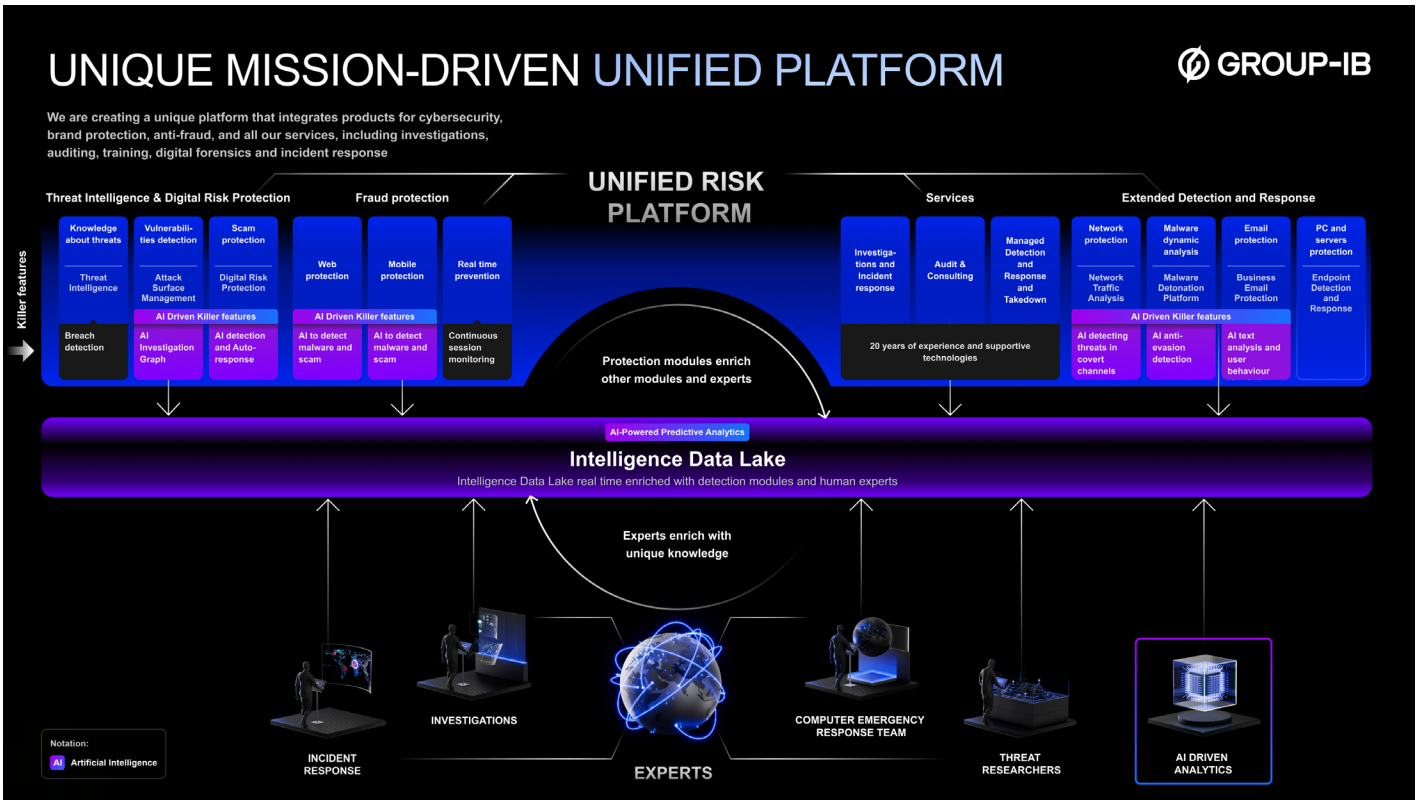
ESG's Dave Gruber noted a number of other important skills and experiences organizations should look for in this era of AI-driven threats and defenses. These include the ability to put in place methods of helping organizations identify potential internal uses of AI tools; offering to help customers develop and manage their AI governance programs; and possessing a deep understanding of LLMs, including how to leverage open models within their own security stack.

Group-IB is at the forefront of understanding AI's use by adversaries and how to harness AI and ML to improve cyber defense against them. Since our founding nearly two decades ago, we have created and constantly innovated our solutions for real-world cybersecurity problems, many of which have been accelerated by the use of AI technology.

With our extensive expertise built in threat hunting, threat intelligence, digital forensics, auditing and consulting, and training and education, working with hundreds of organizations around the world on a wide range of AI-enhanced threats and attacks. Our continuously monitoring security operations center provides rapid incident response, using sophisticated AI tools and ML algorithms to speed up the time to defend against emerging threats.

A vendor-neutral managed security solutions provider (MSSP), Group-IB holds expert status in integrating new, state-of-the-art AI-powered solutions with legacy technologies and tools, enabling the creation of seamless webs of cybersecurity across geographies, industries, and use cases. We have worked with a number of high-profile organizations in both public and private sectors to monitor, identify, defend against, and remediate the impact of AI-driven threats (see sidebar "Real-World Success Stories").

At the heart of Group-IB's stable of solutions is our Unified Risk Platform, a powerful ecosystem of AI-driven technologies that scan and analyze an organization's risk profile in real-time and offer tailored and complete defenses against known and emerging threats across a single user interface. This is both effective and efficient in providing end-to-end security coverage.



Group-IB Unified Risk Platform - an ecosystem of AI-powered cybersecurity technologies for future-proof cybersecurity

Group-IB's original platform ecosystem has been further expanded to include even more functionality, combining the recent AI upgrades, including:

Fraud Protection

Group-IB Fraud Protection is an advanced solution designed to detect all types of fraud and counteract sophisticated fraud schemes that your business faces, regardless of the industry.

AI x Fraud Protection

- In-depth user activity analysis across devices with the combination of deep, supervised, and unsupervised machine learning.
- Advanced behavioral fraud detection for comprehensive user protection including monitoring different data-sets through device fingerprints, IP addresses, malware signatures and fraudster profiles.
- Preventative Proxy protects web and mobile applications from various types of bot activities.

Digital Risk Protection

Group-IB Digital Risk Protection platform leverages advanced technologies to detect the illegitimate use of logos, trademarks, content, and design layouts across the digital surface.

AI x Digital Risk Protection

- Automated monitoring of digital assets
- Neural-based detection for precise detection of up to 90% of the violations
- AI algorithms, trained with more than a decade's worth of collected data enhance phishing and scam website detection efficiency
- AI-driven advice and actions for takedowns including effective communication channels, requests to regulators, cease-and desist processes, so you don't have to spend time interacting with regulators to the take the malicious resources down.

Attack Surface Management

Group-IB Attack Surface Management is designed to discover, assess, and help manage your organization's attack surface. The tool provides full visibility of all Internet-facing assets, identifies vulnerabilities, and prioritizes remediation tasks to strengthen security.

AI x Attack Surface Management

- Agentless SaaS solution with automated IT asset discovery
- Continuous mapping of an organzations' attack surface
- Predictive intelligence of potential threats based on historical data and emerging threat patterns, allowing organizations to prepare and protect themselves against future attacks.
- Automated vulnerability assessment with control suggestions to reduce response times.
- Automated, detailed and actionable reports for critical security issues and trends.

Threat Intelligence

Group-IB Threat Intelligence provides unparalleled insight into your adversaries. Integrate the intelligence to maximize the performance of every component of your security ecosystem. Equipping your team with Group-IB's strategic, operational and tactical intelligence streamlines security workflows and increases efficiency.

AI x Threat Intelligence

- An augmented Threat Intelligence module that supports a more extensive array of contextual awareness in the Graph Network Analysis tool.
- Real-time threat data, including trending threats vulnerabilities and threat actors' activities to be operationalized instantly.
- Automated identification of risky events through an extensive database of Indicators and Compromise (IOCs).
- Automated alerts for immediate notification of vulnerabilities discovered or exploited by threat actors
- Custom threat-hunting rules tailored to your industry, prioritizing threat detection requirements pertaining to your business.

Managed Extended Detection and Response (MXDR)

Empowered with network traffic analysis, malware detonation, threat intelligence, and ML models for event correlation, Group-IB Managed XDR works seamlessly across networks, endpoints, email and network storages. This integrated approach makes your security operations more effective than a siloed solution involving multiple discrete products.

AI x Managed Extended Detection and Response (MXDR)

- Advanced ML models for event correlation across networks, endpoints, and the cloud are used to identify and attribute anomalous activity across the entire perimeter.
- AI optimizations for improved detection of "malware-free" attacks
- Automated incident response activities to avoid manual digging through scattered alerts.
- Effective threat mitigation through actionable intelligence specific to each industry's priority.
- An upgraded version of its Managed Extended Detection and Response (MXDR) capability, now supporting Linux and MacOS systems, as well as an extended remediation capability for Windows EDR.

Group-IB's key differentiator is its ability to combine extensive R&D resources with the collective knowledge, intelligence, and innovation of its industry-leading security experts and analysts to solve problems by building solutions based on not just the latest but future-coming security challenges, needs and technology developments.

REAL-WORLD SUCCESS STORIES

Group-IB has helped numerous organizations solve problems caused or accelerated by the use of adversarial AI technologies and processes. Recent representative examples of organizations that have benefitted from their relationship with Group-IB include:

- Security Lab, which partnered with Group-IB for an MDR service to identify new attack vectors for emerging security incidents, contain any attacks, define the duration of any compromise, and determine if any persistence remained after an attack.
- Libertex Group, which used Group-IB's audit and consulting services to augment limited internal resources and manpower to identify and address security incidents threatening its online financial services trading.
- Tier-1 global bank, which integrated Group-IB's Threat Intelligence into its existing infrastructure, the bank gained the ability to constantly profile threat actors, swiftly detect advanced attacks and techniques, flag network anomalies at their first indication, and respond to emerging threats with unmatched speed.
- Sorint.SEC, a trusted cybersecurity service provider and Group-IB's official partner leveraged our proprietary Threat Intelligence for enriched and tailored insights capable of outsmarting the dynamic landscape of cyber threats and adversaries for its customers.

Three Things to Consider:

1. Choosing a provider of AI-powered cybersecurity solutions is just as important as selecting the right tool—probably even more so.
2. With its extensive research and development capabilities, Group-IB is at the forefront of analyzing how hackers use GenAI and ML algorithms to attack organizations' security defenses … and how to thwart them.
3. Group-IB has a proven track record in providing cybersecurity solutions across a wide range of use cases and industries.

7. CONCLUSION AND NEXT STEPS

The rapidly intersecting paths of AI and cybersecurity represent the ultimate double-edged sword. Organizations that adopt AI in its various flavors will gain a force multiplier that will help them in many ways—in everything from driving sharper and more actionable threat intelligence to identifying attempts to manipulate credentials and steal identities. That said, AI is the same kind of force multiplier for hackers, attackers, and rogue adversaries looking to exfiltrate data and wreak havoc on organizations, people, and communities.

The onus is on organizations to use AI better than the bad guys.

Organizations need to be smarter and more nimble, innovative, and persistent in using AI to thwart the rapid-fire succession of attacks, especially considering the fast-expanding set of attack vectors across endpoints, data centers, edge sites, and the cloud. This means security, IT, business teams, C-suite executives, and boards of directors must work together to come up with the right strategies and tactics to fully leverage AI as a core element of cybersecurity defense. They must also develop a full understanding of what the hackers are doing with AI and how they're doing it.

This requires comprehensive, long-term planning including the proper use of technology, processes, policies, and personnel. It also requires an organizational commitment to devoting sufficient budget and staff resources to get the job done. Short cuts are a recipe for disaster when your adversaries' tools are equal to your own—you must devote the right resources to the task to be able to leapfrog your potential attackers.

A foundational component of a successful cybersecurity strategy is acknowledging and accepting that all organizations—even the biggest and best-resourced in the world—will need expert help with that security. That's why special attention must be paid to understanding where organizations need the most help and support to overcome the inevitable head start the attackers have enjoyed … and that's not going to be solved by just buying the right tools.

Organizations need to identify, evaluate, select, and work hand in glove with technology partners with extensive experience—and not just experience using AI for cybersecurity but how adversaries have used AI to attack organizations like their own. Experienced, market-proven cybersecurity veterans such as Group-IB offer the edge regarding next-generation defenses. Two of the company's biggest differentiating factors are the industry-first work in digital forensics, cybercrime investigations, and incident response services and our recurrent and significant partner network with some of the top law enforcement agencies, which has enabled Group-IB to feed our data lake with very unique insights and information that ultimately cascades into our Unified Risk Platform, and provides even our private sector clients and partners with a distinctive edge in their cybersecurity posture and protection.

Our “globalized presence, but localized expertise” is supported by our mission-critical Digital Crime Resistance Centers (DCRCs) is each region of operation that help businesses with the most relevant insights and jurisdictional support to beat cybercrime and reveal the threat actors, cybercriminal groups and their tactics behind APTs and other threats.

We work round-the-clock as not just your cybersecurity provider, but a true business partner to help organizations ensure long-term security, sustainability for their business, their employees, and all their digital assets.

You can get started today by taking our AI Readiness Assessment, which will summarize your current AI maturity and recommend actions tailored to your organization's needs, empowering you to prioritize and plan your AI initiatives more efficiently and effectively.

If you’d like help to revamp your strategy to become even more resilient, our experts are on hand, to offer you support and the most sound expertise.

Let us guide you from where you are now to where you want to be next. Become AI-empowered with Group-IB!

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+
Successful investigations of high-tech cybercrime cases

300+
employees

600+
enterprise customers

60
countries

$1 bln
saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

120+
patents and applications

7
Unique Digital Crime Resistance Centers

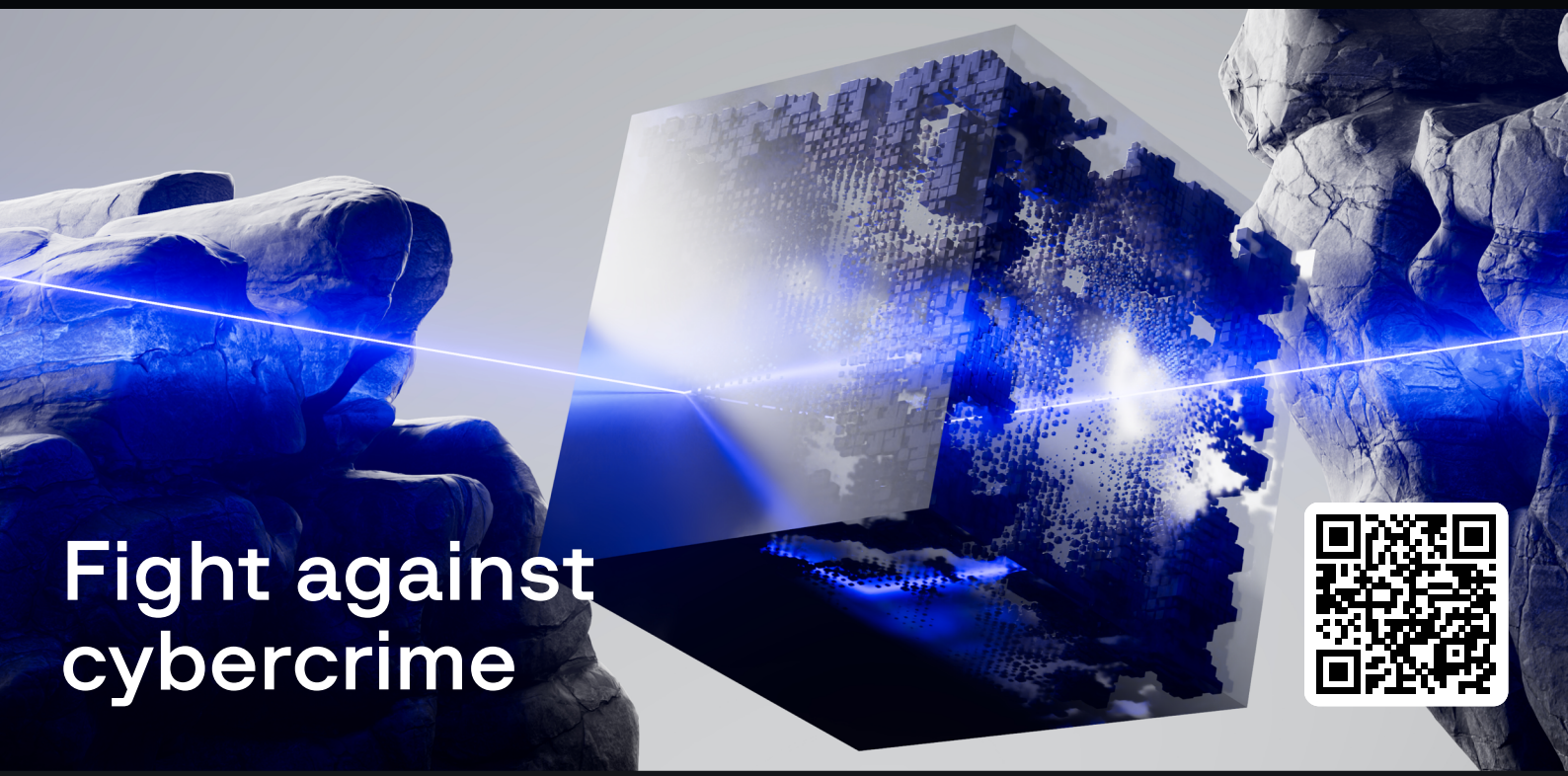
* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL
EUROPOL
AFRIPOL

Recognized by top industry experts

FORRESTER®
Aité Novarica
kuppingercole ANALYSTS
Gartner
IDC
FROST & SULLIVAN



Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785