Dark Web Risks

Using AI to Boost Your Cyber Security

With the increasing prevalence of Artificial Intelligence (AI) in how we live, work, and communicate, its impact on cyber security is undeniable.

This eBook explores how AI is revolutionising traditional cyber security and shaping the cyber landscape.

Table of Contents

Introduction

Stephen Hawking once said "Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last unless we learn how to avoid the risks."

In an era of rapid technological advancements and an ever-increasing reliance on digital platforms, cyber security is now a paramount concern for organisations of all sizes.

The complexities of the digital environment have given rise to advanced threats and attacks that require an equally advanced defence. Within this context, Artificial Intelligence has emerged as a powerful tool in the fight against cyber threats.

In this eBook, is based on a panel discussion originally featured at the Future Insight Technology (FIT) 2023 Conference. The four prominent speakers discuss the key challenges, trends, and recommendations surrounding AI in cyber security, each bringing their experience and insights to the discussion.

Meet the Speakers

Gavin Wood has over 25 years of experience driving business transformation, with a recent focus on cyber security as the new CyberLab CEO

cyberlab

Andrew Napier boasts over two decades in telecoms technology, primarily in roles facilitating the sale of MPLS and security solutions.

TalkTalk Business

Adam Hartley Senior Sales Engineer at Forcepoint, brings practical expertise in cyber security solutions to the panel.

Forcepoint

Fraser Howard, Threat Research Director within Sophos Labs, is a seasoned expert in malware research and behavioural protection strategies.

SOPHOS

The Role of AI in Enhancing Cyber Security

Cyber security has become an intricate battleground in the contemporary era. Cyber attacks are more sophisticated and prevalent than ever, driven by highly organised and profit-driven attackers.

The core challenge defenders face lies in the overwhelming volume of data generated by these cyber threats. The number of attacks, malicious files, IP addresses, and command-and-control servers is on a relentless rise. This surge in the volume of cyber security threats necessitates an innovative approach to keep pace.

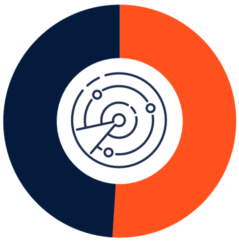
This ever-evolving landscape of cyber threats is where Artificial Intelligence steps in as a game-changer. AI has emerged as a pivotal force in simplifying the work of cyber security professionals and augmenting their capabilities. It revolutionises the traditional approach to cyber security in several fundamental ways.

> *"Already AI. has helped us in that regard. So, it helps us from an automated point of view, from a predictive capability point of view in terms of scaling to meet that volume."*
>
> *– Fraser Howard, Threat Research Director, Sophos*

Automated Threat Detection

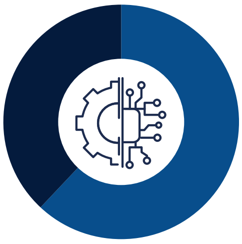
One of the foremost contributions of AI in cyber security is its proficiency in automating the detection of threats. Traditional threat detection methods often involve sifting through colossal volumes of data, which can be time-consuming and labour-intensive. AI systems, on the other hand, excel in processing vast datasets rapidly and identifying anomalies, patterns indicating potential malicious activity, and previously unseen threats.

This automation significantly reduces response times, enabling faster and more effective risk mitigation. In a world where time is a critical factor in combating cyber threats, AI's ability to expedite threat detection is invaluable.



51%

of businesses use AI primarily for threat detection*



62%

of enterprises have fully implemented AI for cybersecurity or are exploring additional uses*

* Source: Strategies against AI cyber attacks worldwide 2021 I Statista

Predictive Capabilities

AI leverages machine learning algorithms to predict potential threats based on historical data and ongoing trends. By analysing past attack patterns, AI systems can foresee potential vulnerabilities and emerging threats before they materialise.

This predictive capability empowers cyber security teams to proactively secure their systems, fortify their defences, and implement mitigations ahead of time. It shifts the paradigm from a reactive stance to a proactive one, allowing organisations to stay one step ahead of cyber adversaries.

Pattern Recognition

AI excels at pattern recognition, a crucial threat identification and classification facet. It can detect real-time patterns that may not have been observed before. By comparing the behaviour of threats to known patterns, AI can accurately classify and respond to attacks. This is particularly valuable in identifying new, evolving threats that do not conform to established attack patterns.

AI's capacity for real-time pattern recognition helps in the swift and accurate classification of threats, enabling quicker responses and reducing the window of vulnerability.

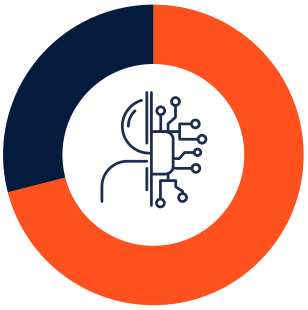
Efficient Decision-Making

With the sheer volume of data cyber security professionals must handle, AI provides invaluable assistance in expeditious decision-making.

The ability to process and interpret data at remarkable speeds is a force multiplier for security teams. AI systems can swiftly assess the information, analyse its relevance, and make informed decisions in a fraction of the time it would take a human operator. This reduces the workload on cyber security professionals and ensures that responses to cyber threats are accurate and timely.

AI is not merely a tool; it's a transformative force that elevates cyber security measures to a new level of efficacy. By automating threat detection, predicting potential vulnerabilities, excelling in pattern recognition, and expediting decision-making, AI is poised to revolutionise the way we defend against cyber threats. This intersection of technology and cyber security is where the future of digital defence lies, and organisations must harness the full potential of AI to navigate this intricate battleground successfully. particularly valuable in identifying new, evolving threats that do not conform to established attack patterns.

AI's capacity for real-time pattern recognition helps in the swift and accurate classification of threats, enabling quicker responses and reducing the window of vulnerability.



71%

organisations spend more on AI and machine learning for cyber security than two years ago

AI in Cybersecurity: Statistics, Example & Trends in 2023 (businessdit.com)

Get Started Now

See how Sophos MDR can drive business value and superior outcomes for your organization.

Speak with an Expert

Addressing Key Challenges

Integrating Artificial Intelligence into your cyber security brings immense potential improvements. Yet it also introduces several significant challenges that organisations must address to harness the full benefits of AI in cyber defence. These challenges encompass various dimensions:

Alignment of Processes and Training

One of the fundamental challenges is aligning existing processes and training with AI-driven cyber security solutions. While AI can automate tasks and enhance productivity, organisations must ensure their established processes are compatible with these new technologies.

It's not just about deploying AI tools; it's about adapting workflows and procedures to leverage the full potential of AI capabilities. This requires a fundamental shift in the way cyber security professionals operate. Businesses must transition from traditional approaches to ones that are more AI-centric.

Adam Hartley, a Senior Sales Engineer at Forcepoint stated the importance of integrating the work of humans in collaboration with AI. When talking about how AI performs without human supervision he said, "It's about making things aware and adaptive of the environment to take proactive actions, but also making sure that they're risk aware."

Moreover, training is critical. Users must understand how AI systems work, their limitations, and potential risks. Training programs should be tailored to ensure cyber security professionals can effectively integrate AI into their daily operations.

If you need guidance or support with integrating AI into your Cyber Security protocol, contact CyberLab.

AI Review Councils and Training Initiatives

As discussed in the Future Insight in Technology Panel, organisations like Forcepoint have introduced AI Review Councils to assess every tool used.

An increasing number of organisations are recognising the importance of AI Review Councils. These councils evaluate AI-driven tools, ensure they align with business objectives, and comply with ethical standards.

Furthermore, training initiatives should be an integral part of the AI integration process. Cyber security professionals and other staff members who interact with AI-driven systems need to be educated about the role and capabilities of AI, and how to work effectively with these systems.

Privacy Concerns and Data Control

Privacy is another critical concern when implementing AI-driven cyber security solutions. An illustrative example would be an AI-powered language tool, such as Grammarly. Adam Hartley had this to say while talking about AI tools we may be using every day, without knowing.

"I use Grammarly for everything. It's on a desktop, it's in Google and in office, but the free version of Grammarly takes every bit of information that I touch in emails, documents, and it wasn't until we reviewed this months ago and found that it takes that into its AI model to interpret, for better spelling and for grammar across that. So, if you think of Grammarly as an AI language tool to help you day in and day out, having AI that could be malicious."

While these tools offer significant benefits, they also raise concerns about data privacy. Free versions of such tools may collect and analyse user data, potentially exposing sensitive information.

Organisations must exercise caution and consider the implications of AI tools on data privacy. They should carefully evaluate third-party AI tools and vendors to ensure that sensitive data is protected and that AI-driven processes align with privacy regulations and organisational policies.

Shadow IT and Uncontrolled AI

Organisations must be vigilant about Shadow IT, especially as AI becomes more pervasive.

'Shadow IT' refers to using IT systems and services within an organisation without explicit approval. Many products now incorporate AI elements outside the organisation's knowledge or control. This creates challenges in assessing the risk associated with AI components embedded within everyday software and applications, even in browsers or office software. Organisations need mechanisms to identify and manage these uncontrolled AI elements to mitigate potential risks and ensure they do not compromise security.

Use of AI to Conduct Cyber Crime

Cybercriminals are increasingly using AI to conduct attacks that are more efficient, effective, and evasive. AI can learn to spot patterns in behaviour, understanding how to convince people that a video, phone call or email is legitimate and then persuading them to compromise networks and hand over sensitive data.

There are several types of cybercrimes that are being facilitated by AI, such as phishing attacks, malware attacks, DDoS attacks, and deep fakes.

The Human Element

Despite the increasing role of AI in cyber security, the human element remains paramount. It's not about replacing humans with AI but ensuring that your staff can work safely and efficiently with AI tools. The organisation's workforce must be part of the decision-making process regarding AI implementation. This human-AI collaboration is crucial, especially when AI systems require human judgment in complex, unforeseen, or ambiguous scenarios. Effective communication between humans and AI systems is essential to make the most of AI-driven cyber security solutions.

"The biggest threat to a business for AI is that someone uploads something from their business into that A.I. and loses control of it. So, if, for instance, a person in AI is trying to modify their code to make it more efficient, your code and intellectual property is then in that AI model and anyone can query it." - Adam Hartley, Senior Sales Engineer - Forcepoint

Summary of Key Challenges

Integrating AI into cyber security represents a significant shift in how organisations defend against cyber threats. While there is immense potential for AI to improve cyber security, addressing key challenges is vital to ensuring its successful implementation. These challenges encompass aligning processes, establishing AI Review Councils, addressing privacy concerns, managing uncontrolled AI, and recognising the continued importance of the human element. Overcoming these challenges is essential for organisations to harness the full potential of AI in cyber security while maintaining security, privacy, and ethical standards.

> *"You've got to be ready for any possibility at any time. And suppose you're getting AI. based attacks inbound. In that case, you have to have something very capable of dealing with large, volumetric and complicated and potentially completely new as well, because today, day I can make something up that no one's ever seen before."*

Andrew Napier - Head of Cloud & Security Product Services - Talktalk Business

Future Trends in AI and Cyber Security

The future of AI in cyber security holds several exciting possibilities and trends that organisations must be aware of to stay ahead of the evolving threat landscape. These trends will shape the way AI is utilised in the cyber security domain:

Enhanced Automation

AI will continue to evolve and enhance automation in cyber security. Automation will be pivotal in handling routine and time-consuming tasks, allowing security professionals to focus on more strategic and complex issues.

Scenarios will arise wherein AI-driven systems can automate responses to common threats. This automation is essential to reduce response times and to ensure that security teams can proactively address emerging threats. To stay ahead of the curve, organisations should invest in AI systems capable of swiftly identifying and mitigating threats, thereby increasing the overall efficiency and effectiveness of their cyber security operations.

Transparency and Trustworthiness

As AI gains prominence in cyber security, transparency will be increasingly emphasised.

Organisations and cyber security professionals will need to seek to understand how AI systems function, their decision-making processes, and the training data used. This transparency is critical for building trust in AI systems, especially when making high-stakes decisions. Internal stakeholders and external entities, including regulators and customers, are more likely to trust transparent AI systems. Therefore, organisations should prioritise transparency in developing and deploying AI-driven cyber security solutions.

Outsourcing Security

Smaller organisations and those without dedicated cyber security teams may increasingly outsource their security to specialised vendors with AI capabilities.

The growing shortage of cyber skills and professionals has pressured businesses to find competent security experts. As a result, many companies need help to recruit and retain in-house cybersecurity talent, given the competitive job market and high demand for such expertise.

These vendors can offer a global perspective on threats and better protect against complex attacks. With a team of experts who continuously monitor the evolving threat landscape, they can provide insights and threat intelligence that small organisations often struggle to access on their own. This external perspective is invaluable, as it brings a broader understanding of emerging threats and trends that could potentially affect businesses.

Outsourcing cyber security can efficiently bolster security efforts, especially when dealing with rapidly evolving threats. Cyber threats are constantly changing and becoming more sophisticated, making it increasingly difficult for internal teams to keep up. Specialised vendors have the resources and expertise to adapt to these changes swiftly, offering a proactive stance against emerging threats. This is particularly beneficial for smaller organisations that might need more resources to maintain an in-house team capable of rapid response.

Maintaining a balance between internal and external expertise ensures that outsourced security aligns with the organisation's specific needs and goals. While external vendors provide a wealth of security expertise, it's crucial for organisations to maintain internal oversight and control. This approach enables a customised security strategy that addresses the unique requirements and risk profile of the business. By working in collaboration with external security providers, organisations can ensure that their security posture is effective. and tailored to their specific operational and compliance needs.

> *"And we're seeing that around a few of the vendors in the history of cyber, but also in other streams as well; we've been able to make their products adaptive without needing a human or logic. I don't think we're quite there to trust it, and I think that that is the big ultimate deciding factor. If this becomes a trend, do people trust AI to come up with the right answer and the action rather than? At the moment I don't trust GPT to come up with a rhyming slang that actually rhymes."*

Adam Hartley
Senior Sales Engineer,
Forcepoint

Behaviour-Based Analytics

AI-driven systems increasingly rely on behaviour-based analytics to detect and respond to threats by assessing known patterns, identifying anomalies in real time, and swiftly detecting deviations from the norm. As discussed, this approach is instrumental in identifying previously unseen threats and attacks, and it's vital in a rapidly evolving threat landscape where new attack vectors emerge regularly.

Continued Evolution of AI Models

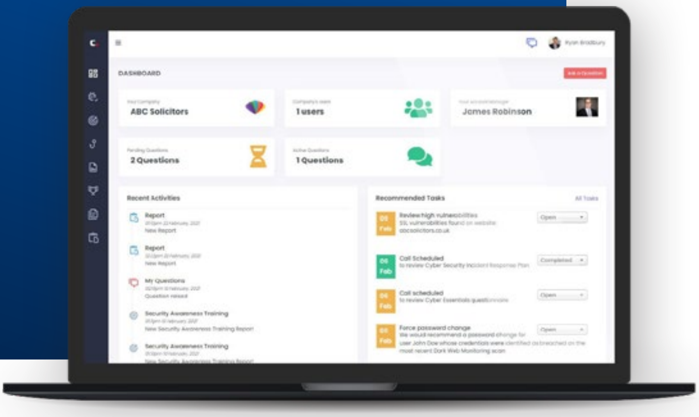
AI models will continue to evolve to become more trustworthy and resilient. The transcripts highlight the importance of eliminating unconscious bias in training data to ensure that AI doesn't inherit human biases. As AI becomes integral to cyber security, organisations must continuously update, refine, and evaluate their AI models to remain practical and ethical.

The need for organisations to regularly review and improve AI models to address any emerging issues, including bias and performance concerns, will continue to grow.

The future of AI in cyber security is promising but also presents complex challenges. The trends discussed in the transcripts, including enhanced automation, behaviour-based analytics, transparency, outsourcing security, and the evolution of AI models, will shape the cyber security landscape in the coming years. Organisations must adapt and prepare to embrace these trends to stay resilient in the face of evolving cyber threats. By staying informed and leveraging these trends effectively, organisations can harness the full potential of AI in cyber security and maintain a robust defence against an ever-changing threat landscape.

CyberLab Control: Cyber Security As A Service

Protect your business from cyber threats with Cyberlab Control – our automated cyber security portal.



Delivering a suite of powerful tools including automated phishing simulations, dark web data breach monitoring, and security awareness training, all wrapped up in a user-friendly portal with expert guidance and support.

1m+	10k+	1k+
Data Breaches Identified	Domains Monitored	Customers Protected

Learn More   Get Free Trial

Conclusion

As we move forward, it's clear that robust cyber security is paramount as the cyber security sector becomes increasingly complex and threats grow more sophisticated. Enter Artificial Intelligence (AI), a game-changer, automating threat detection, enhancing predictive capabilities, and expediting decision-making. The advancement of AI isn't just a technological advancement; it's a fundamental shift in our approach to cyber security.

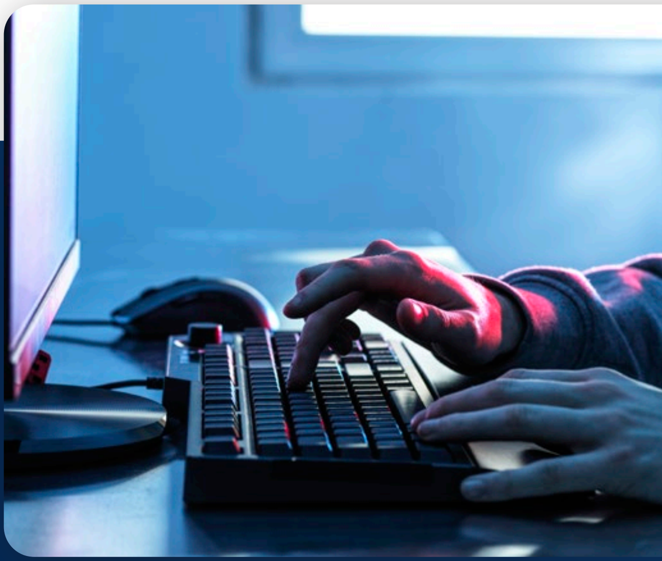
AI's multifaceted role significantly bolsters AI's multifaceted role significantly bolsters traditional security measures. It automates threat detection, reducing response times and enabling faster, more precise risk mitigation. Its predictive capabilities empower teams to identify vulnerabilities and emerging threats proactively. AI excels in pattern recognition, accurately classifying threats, even those deviating from established attack patterns. It expedites decision-making by rapidly processing vast datasets, lightening the load on cyber security professionals and ensuring timely responses.

This intersection of technology and cyber security is where the future of digital defence lies. AI isn't merely a tool; it's a transformative force that elevates security measures to a new level of efficacy, enabling us to adapt to the evolving threat landscape.

Yet, integrating AI into cyber security poses challenges, necessitating a fundamental shift in operations, the establishment of AI Review Councils, and careful consideration of privacy and security impacts. The human element remains irreplaceable, and collaboration between humans and AI is crucial for success.

Looking ahead, exciting trends in AI and cyber security include enhanced automation, behaviour-based analytics, transparency, trustworthiness, and the increasing prevalence of outsourcing security for smaller organisations. Staying informed and adaptable is essential in a world of continuously evolving digital threats.

To navigate this transformative landscape effectively or seek guidance on integrating AI into your cyber security protocol, we encourage you to contact our experts at Cyberlab. The future of AI in cyber security holds immense promise, and together, we can fortify our digital defences for the challenges that lie ahead.



Our People. Our Platform. Protects You.

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reenforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk I cyberlab.co.uk

Awards and Accreditations

CREST.

VA

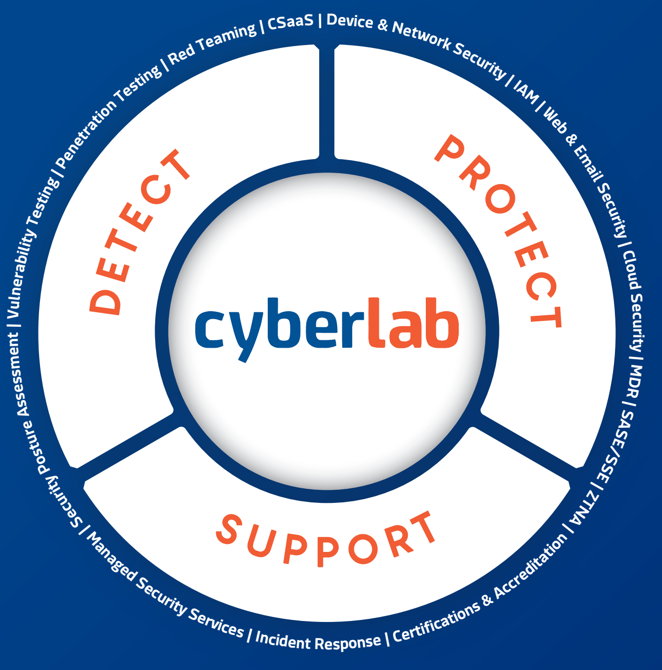
PEN TEST

IASME CONSORTIUM

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS


Red Teaming | CSaaS | Device & Network Security | IAM | Web & Email Security | Cloud Security | MDR | SASE/SSE | ZTNA | Certifications & Accreditation | Incident Response | Managed Security Services | Security Posture Assessment | Vulnerability Testing | Penetration Testing
DETECT
PROTECT
SUPPORT
cyberlab

cyberlab

cyberlab.co.uk

© 2023 CyberLab is a trading name of Cyberlab Consulting Limited registered in England & Wales No. 12392586.Registered Office: Bridgford House, Heyes Lane, Alderley Edge, SK9 7JP. Cyberlab is a registered trademark.