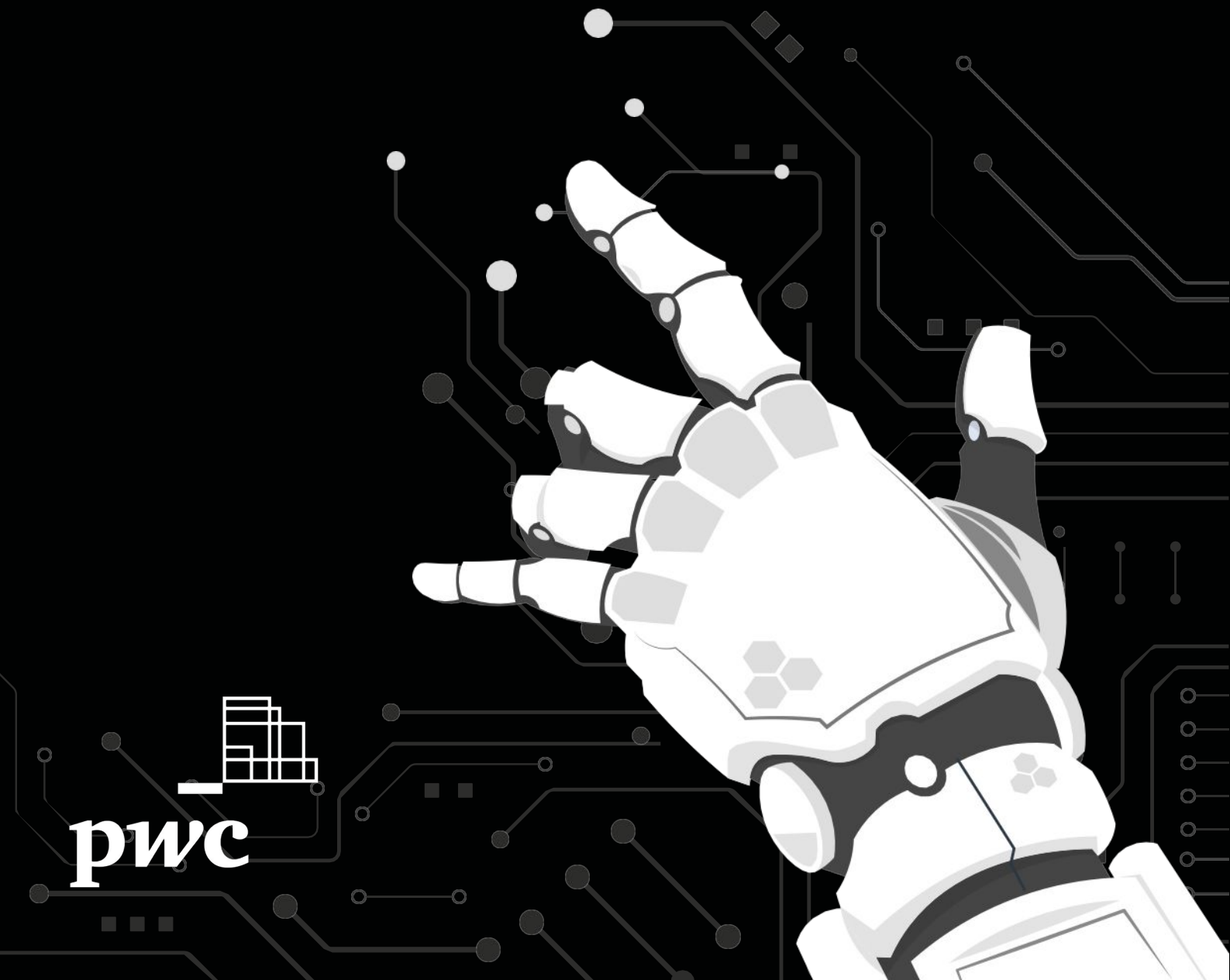
Balancing Power and Protection:

AI in Cybersecurity and Cybersecurity in AI

AI's extraordinary capabilities have the potential to transform cybersecurity, but AI systems must be protected from attacks to prevent harm to people and computing infrastructure.



pwc

Executive Summary

Forms of artificial intelligence (AI) have existed since the 1950s, but the technology is now rapidly expanding at scale for two reasons: more powerful and more affordable computer chips that make it possible for organisations of all sizes to access AI; and the explosion in digital data which provides the information for training AI systems.

The use cases are everywhere in our daily lives, from email spam filters to virtual assistants. However, as digitisation spreads, the risk of attacks from bad actors accessing connected devices or systems increases, making AI an increasingly important area for cybersecurity. AI will revolutionise cybersecurity, due to its superior ability to scan enormous volumes of data for anomalies and flag up risk.

Organisations with AI capabilities have a challenge to seize the opportunity to reinforce their security, while guarding against AI-enabled systems becoming another point of vulnerability. In recent years, cyber criminals have exploited advances in AI to make their attacks more damaging and more frequent, as organisations around the world have learnt the hard way.

Against this background, 74% of respondents to our 2021 Middle East CEO Survey regard cyberattacks and leaks as a threat to growth this year, up from 68% in 2020. As a result, 43% plan to increase their investment in cybersecurity and data privacy by at least 10% over the next three years. Clearly, a growing proportion of the region's business leaders have grasped that in an accelerating AI race, they have to move fast to stay one step ahead of potential cyber attackers.

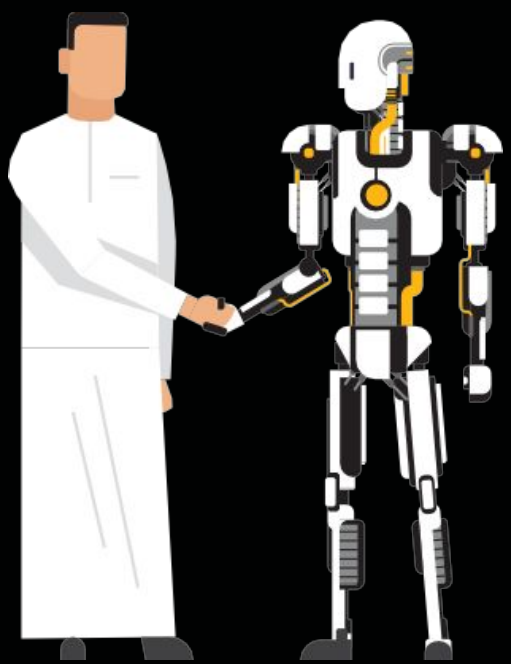
In this report, we set out how organisations can ramp up their cyber defences with AI, while protecting this new and powerful technology against attacks.

What is AI?

Artificial intelligence (AI) is a set of computer science techniques that allow machines to learn from experience, adapt to new inputs and complete tasks in a way that resembles human intelligence. Data is essential to AI – it is impossible to overstate its importance. The way data is chosen, input and processed will determine the decisions the AI system makes and the quality of those decisions.

The three ways an AI system can be trained are supervised learning, in which the user oversees what the machine learns, such as differentiating between a pedestrian and a road sign; unsupervised learning, which is about finding patterns, associations and clusters of data; and reinforcement learning, which starts without data, and teaches the model to solve problems by trial and error. The most common training approach is supervised learning, while the most sophisticated is reinforcement learning.

AI offers remarkable, transformational possibilities for a rapidly expanding range of complex human tasks and activities that can be local, national, or international. For example, AI systems can be trained to detect potential health issues, drive a car, help a restaurant better predict its food demand and optimise a global retailer's supply chain.



Section 1 – AI to support cybersecurity

As digital systems become vital to the running of most organisations, many cybersecurity teams find themselves carrying out multiple tasks with too little time, an uncontrolled flow of data and a shortage of skills. AI can help teams bring these challenges under control by making cybersecurity more advanced and effective in the following key areas:

- Making control systems more accurate at detecting threats
- Accelerating the speed of investigation
- Automating responses
- Coordinating and orchestrating responses

AI can thus strengthen an organisation's cybersecurity defences on every level, from classifying data, through identifying weak points, to blocking spam. At the most complex level, AI can detect malware, fix vulnerable areas before they are attacked, conduct surveillance from a Security Operations Centre (SOC), prevent intrusion and gather threat intelligence by monitoring areas of the internet that may not be directly accessible to all, such as the Dark Web.

In short, AI is revolutionising cybersecurity by allowing systems to **sense**, **think** and **act**:

Sense

Sensors, text analytics, natural language processing and biometrics all help cybersecurity systems to identify unusual or suspicious behaviour within the company's systems.

Think

Machine learning - and particularly deep learning, given the scale of data - allow systems to improve over time, constantly learning patterns of behaviour and reducing the number of false positives or missed attacks.

Act

Automated, orchestrated cybersecurity systems act on threats to close vulnerabilities and alert companies to attempted attacks.

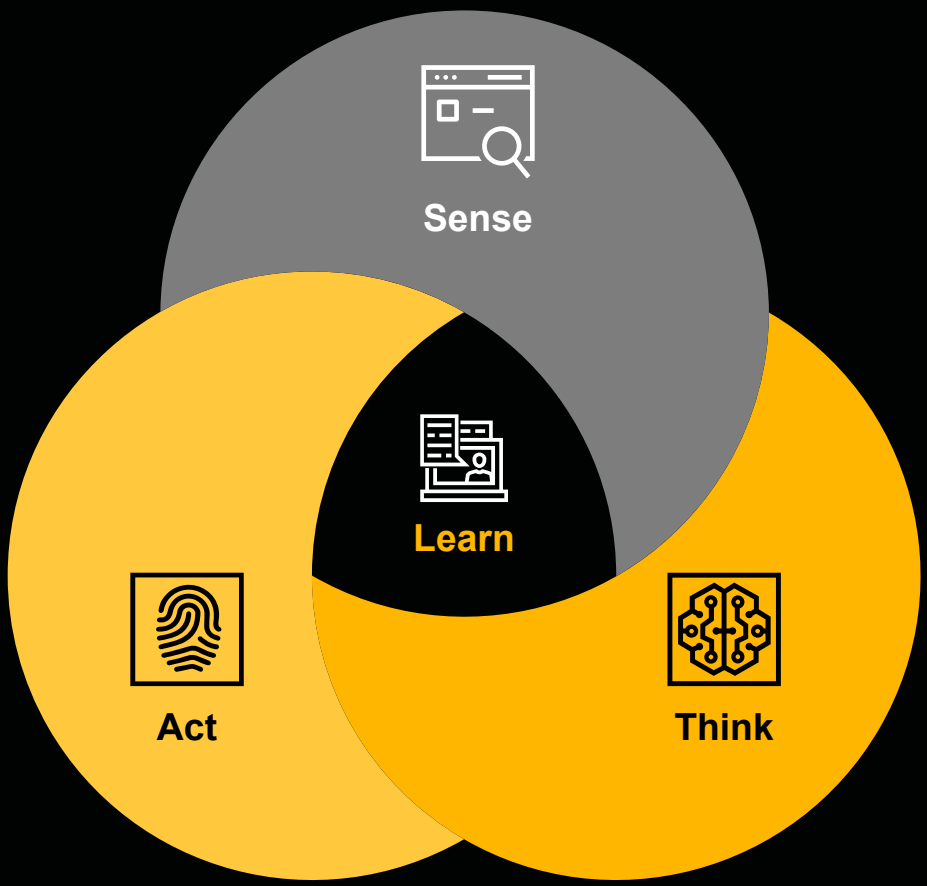


Figure 1: AI is revolutionising cybersecurity. AI systems can be trained to generate alerts for threats, identify new types of malware and protect sensitive data for organisations:

Of course, implementing an AI-enabled cybersecurity system also presents challenges. The first obstacle for many organisations is limited availability of standardised cybersecurity data across all functions for the AI system to learn. AI also creates complex governance questions for organisations: for example, the system can only learn from the data it is given and unconscious bias may influence which data is chosen. AI systems can produce a high number of false positives if data quality is low, or the system has not been trained to understand the context of the actions being analysed, impacting its ability to make the right decisions. AI-based solutions have to be more accurate than rules-based solutions to be viable candidates for replacing them.

Beyond data quality and governance, there is also a shortage of skilled AI professionals, and an even greater shortage of cybersecurity specialists, to put systems in place and help organisations manage them on an ongoing basis.

Thresholds to detect anomalies

Built-in and customisable rules to let security professionals adapt technology to their organisation's unique, complex combinations of software and systems.

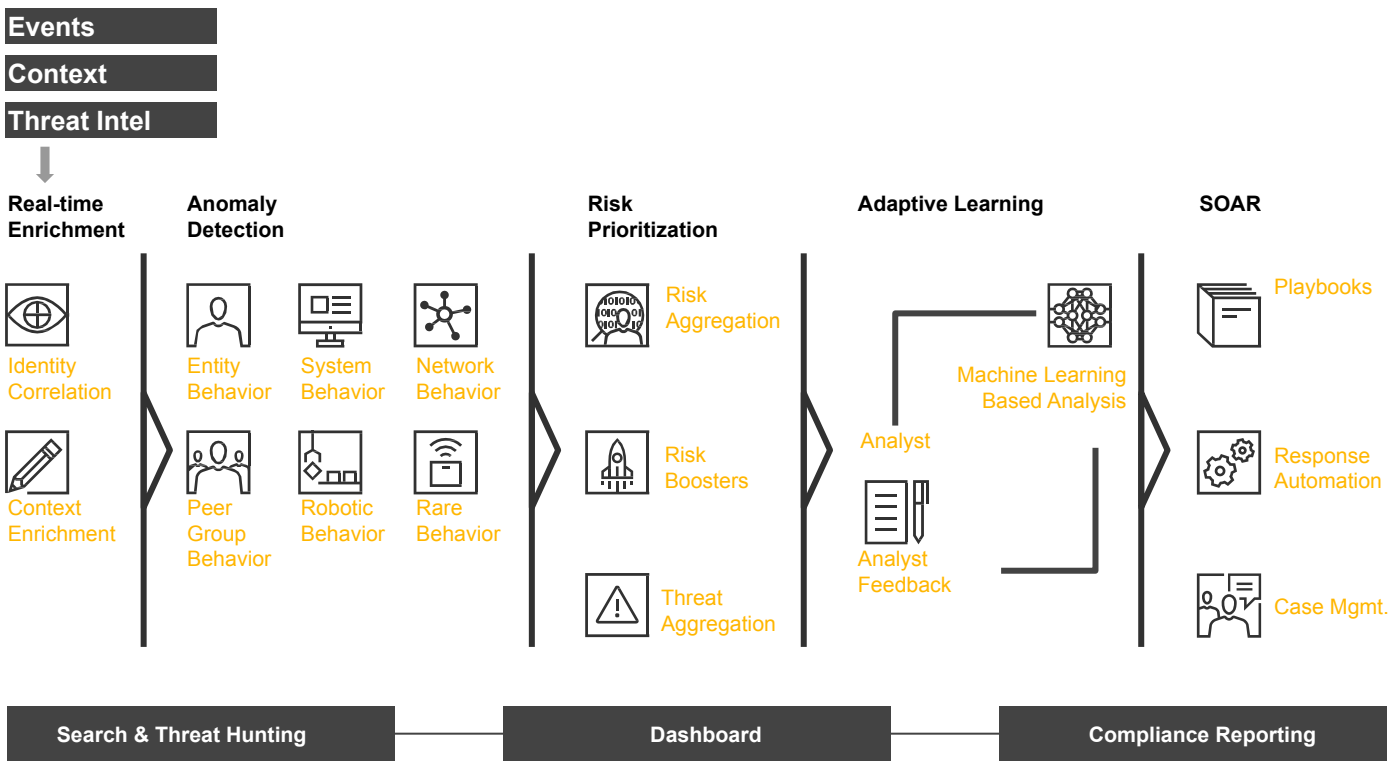
Built-in AI models created by machine learning algorithms, that go beyond rules to address complex relationships and learn the peculiarities of an enterprise's threat surface.

External, importable AI models that let a community of enterprises share knowledge.

Case study: The use of AI to protect a smart city (Security Convergence)

By using AI, organisations can reduce the Mean Time To Detect (MTTD) and Mean Time To Repair (MTTR) when confronted by physical and cybersecurity attacks. In the context of smart cities, security convergence between the physical and cyber realm can be realized through data collected from sensors across an urban area, using technologies such as drone feeds, Lidar sensors and smart cameras, can be correlated centrally to identify a potential threat and automatically launch the correct response to validate, contain or mitigate it. That could mean sending a drone to validate a Lidar sensor alert or sending a robot dog to prevent a crime as soon as feeds from smart cameras confirm a robbery attempt or a street fight.

Figure 2 below shows the use of automation in operations where the security orchestration, automation and response (SOAR) platform utilises machine learning (ML) to take decisions:



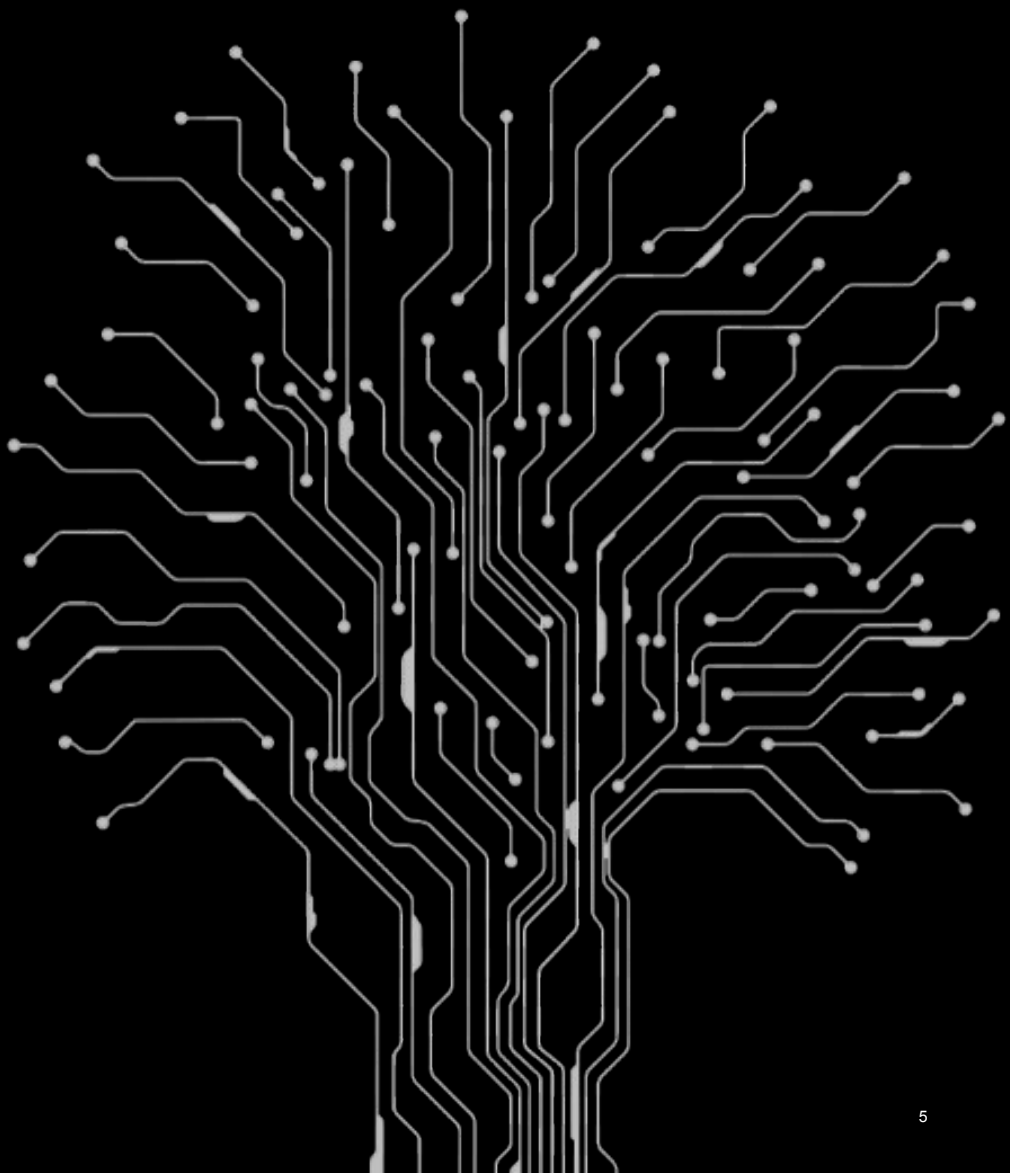
Section 2 – Cybersecurity for AI: Who guards the guards?

Unfortunately the ‘good guys’ are not the only people to have realised the potential of AI. Cyber criminals are also deploying AI offensively to identify and target vulnerable organisations, accelerate the pace of cyber attacks, and automate processes such as removing their digital fingerprints from internal systems.

Organisations must therefore ensure that they have strong cybersecurity measures in place to protect AI systems in every function, including the AI in their cybersecurity defences. There are three main AI threat vectors: data, input and model, which attackers can either extract or manipulate. They may manipulate the data the AI system is learning from by ‘poisoning’ it, or extract data to obtain confidential information, or learn more about the logic of the AI system.

The autonomous vehicle sector offers a notable example of such manipulation. Attackers can manipulate the behaviour of smart cars by sticking small amounts of tape on red traffic lights so that the AI system controlling the car does not recognise them, and the vehicle runs through the stop sign.

To protect their AI systems from cyber attacks, organisations must control who has access to the system, validate the data being sent to the AI system to mitigate against the threat of it being ‘poisoned’ by bad actors, and train AI systems to learn from previous attacks and avoid future manipulation.



Section 3 – The future of AI and cybersecurity

AI is essential for organisations that are serious about ramping up their cybersecurity to keep pace with ever-more sophisticated and damaging threats in an increasingly digitised world. The benefit of foresight is the priceless cybersecurity asset that AI unlocks via data collection, selection and analysis. At the same time, AI itself must be protected from bad actors.

As Figure 3 below sets out in detail, applying machine learning to data analysis improves threat detection before a problem occurs and gives organisations the time they need to successfully neutralise incoming threats. AI can also play an integral role in detecting and preventing phishing scams, and efficiently scanning for potential vulnerabilities in corporate IT systems.

Developers are also leveraging AI to improve biometric authentication by eliminating weaknesses in the process. Meanwhile, by analysing network traffic dynamics, AI can generate and recommend policies and procedures to fit an organisation's specific situation, including studying patterns to improve behavioural analytics.

In the ideal future cybersecurity system, AI will be used to augment every dimension.

Improving Cyber Threat Detection With Machine Learning

- In cybersecurity, foresight is priceless.
- Detecting cyber attacks in advance can give organisations the time they need to successfully neutralize these incoming threats.

AI-Fueled Phishing Detection and Prevention

- Aland machine learning play an integral role in m aling phing attacks
- These technologies can identity and track over 10,000 active phing sources
- They also allow for swift distinction between take and valid

Making Vulnerability Management Easier

- Just this year, Over 2,000 unique cybersecurity vulnerabilities have been recorded
- Managing these with only humans would be practically impossible.
- AI opens up an easier approach

More powerful Password Protection and Authentication

- Password have always been one of the weakest components of security control
- Biometric authentication is seen as a potential alternative for the future.
- Developers are and AI to go biometric authentication and inte any weakness so that More robust

Automated Network Security

- Network Security operations lakes up a monumental amount of time and human effort to us and manage
- AI can bring automation to tedious tasks enabing streamlined and united operations reducing the margin of error

More Robust Behavioral Analytics

- Similar to our other examples. AI and machine learning can also be employed to improve behavioral analytics by studying patterns

If your organisation is considering leveraging the potential that AI can offer, you need to consider security from the very beginning. PwC can help you:

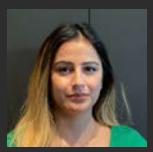
1. Set your AI security foundation (for example, aligning security considerations to your AI strategy, framework, and processes)
2. Develop and implement the use-cases that can help you leverage AI to secure your infrastructure
3. Train your employees to help them better understand emerging AI security threats

Key Contacts

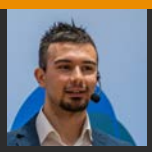
Simone Vernacchia
Partner
Digital Infrastructure & Cybersecurity Lead
PwC Middle East

Ali Khan
Director
Consulting Technology - Cybersecurity
PwC Middle East

Mohammed Saty
Senior Manager
Consulting Technology - Cybersecurity
PwC Middle East



Shallika Sharma
Manager
Consulting Technology - Cybersecurity
PwC Middle East



Semih Kumluk
Digital Training Manager
PwC's Academy Middle East

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 6,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.