AI MONDAY®

#AIMonday

Herzlich Willkommen

Mit KI geschützt, nicht überlistet – Sicherheit mit Augenmaß

LinkedIn Gruppe:
AI Monday Heidelberg-Mannheim

Supported by

BASF NEXT MANNHEIM dfki ai

srh Gründer-Institut der Hochschule Heidelberg innoWerft

KI LAB Heidelberg Technologiepark Heidelberg dataconsulting hip:com e.V.

Powered by

DAIN STUDIOS

appose

AI MONDAY®

AI Security – more important than ever

Speaker

Martin Schöpper

Deputy CISO BASF

Supported by

BASF

NEXT MANNHEIM

dfki ai

srh Gründer-Institut der Hochschule Heidelberg

innoWerft

KI LAB Heidelberg

Technologiepark Heidelberg

e dataconsulting

hip:com e.V.

Powered by

DAIN STUDIOS

appose

#AIMonday

AI Security – more important than ever

How do we work with AI and use it to our advantage?

1. Threat Landscape disrupts through AI

2. Governing AI via regulations

3. AI as an opportunity in Security

Facts, Numbers, and Figures

Attacks are increasing in numbers and frequency with broader attack surface

Global Cyber Security Situation

38%
…increase of global cyberattacks have been observed[1]

$4.45 Mio
…is the average total cost of a data breach[2]

74%
…of companies had potential data breaches during the past 12 months[3]

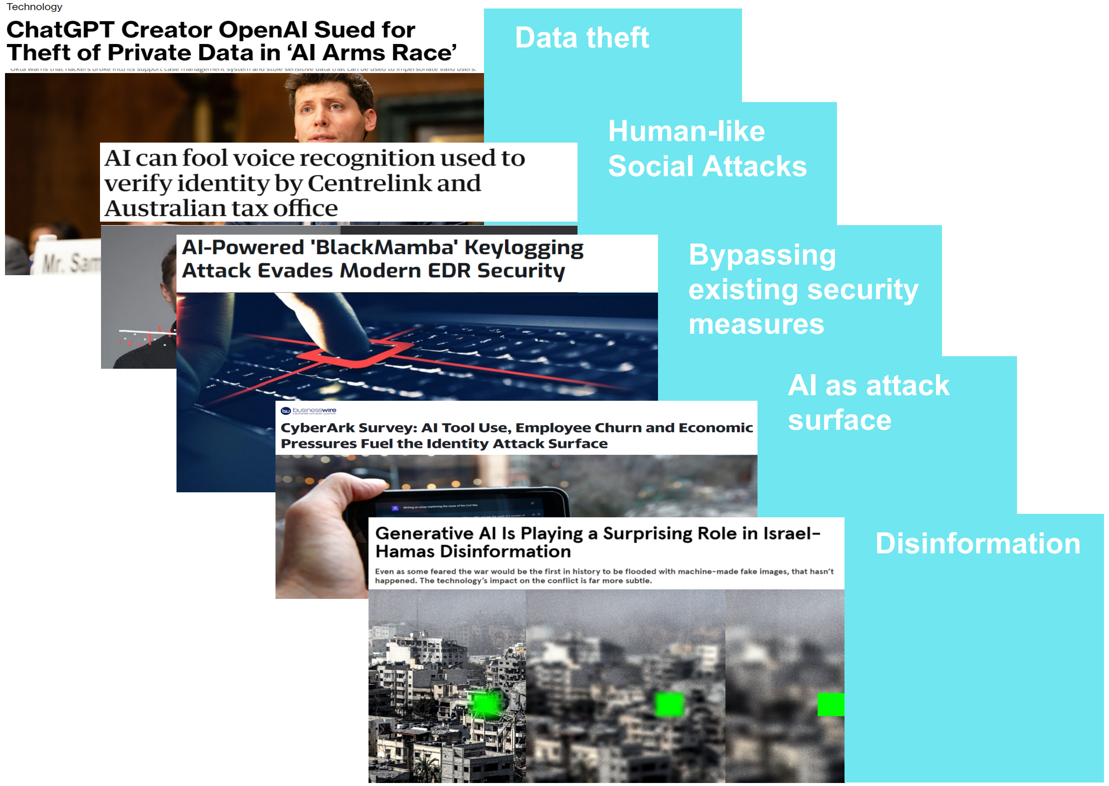
52%
…of all security breaches involved some form of customer PII[2]

[1] Check Point Research Report 2023
[2] IBM Security Report 2023
[3] Forrester Top Cybersecurity Threats 2023

#AIMonday

Changes on the AI Threat Landscape

2023: AI as a broad threat for organizations



Technology

ChatGPT Creator OpenAI Sued for Theft of Private Data in 'AI Arms Race'

Okta warns that hackers broke into its support case management system and stole sensitive data that can be used to impersonate valid users.

Data theft

AI can fool voice recognition used to verify identity by Centrelink and Australian tax office

Human-like Social Attacks

AI-Powered 'BlackMamba' Keylogging Attack Evades Modern EDR Security

Bypassing existing security measures

CyberArk Survey: AI Tool Use, Employee Churn and Economic Pressures Fuel the Identity Attack Surface

AI as attack surface

Generative AI Is Playing a Surprising Role in Israel–Hamas Disinformation

Even as some feared the war would be the first in history to be flooded with machine-made fake images, that hasn't happened. The technology's impact on the conflict is far more subtle.

Disinformation

2024: AI as specific threats from use cases

DPD error caused chatbot to swear at customer

19.01.2024 BBC NEWS

Air Canada's chatbot gave a B.C. man the wrong information. Now, the airline has to pay for the mistake

16.02.2024 CTV NEWS

Employee tricked to transfer millions in deepfake video conference

04.02.2024 CNN

Morris II: Zero-click worm that target GenAI-powered applications

01.03.2024 WIRED

Governing AI via regulations

- **Limiting creativity** and a technology in **development**?
- How do you decide **what data do you give to the model**?
- How does AI decide what is a threat in real life? – **Ethical considerations**
- **“We need to understand to protect”** – still possible?

AI as an opportunity in Security

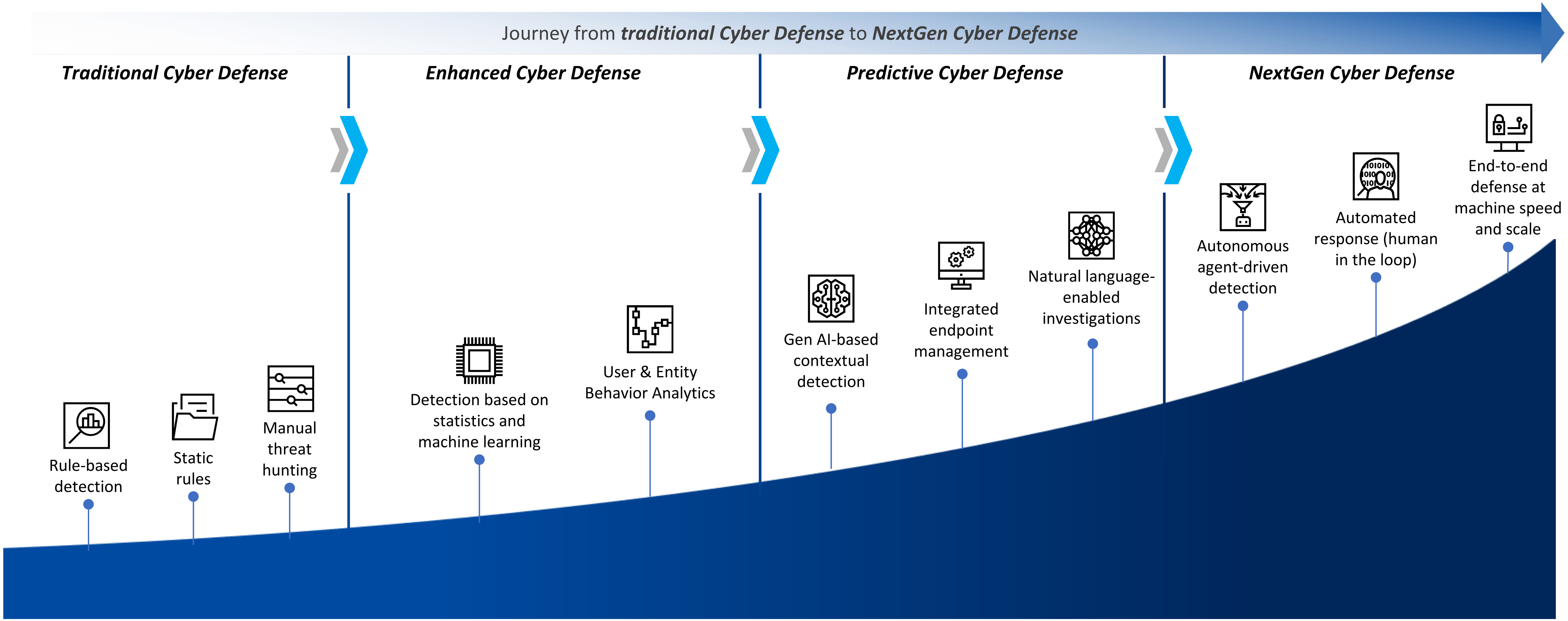
- Optimize **threat detection and data security** response time through AI
- **Cybersecurity and AI are Inseparable** – essential for maintaining robust and resilient defenses.
- **Removing human error** & establishing better decision making

#AIMonday

#AIMonday

Futuristic AI-enabled Cyber Security Defense

Traditional cyber defense needs a mind shift towards an AI-driven and autonomous approach



Journey from ***traditional Cyber Defense*** to ***NextGen Cyber Defense***

Traditional Cyber Defense

- Rule-based detection
- Static rules
- Manual threat hunting

Enhanced Cyber Defense

- Detection based on statistics and machine learning
- User & Entity Behavior Analytics

Predictive Cyber Defense

- Gen AI-based contextual detection
- Integrated endpoint management
- Natural language-enabled investigations

NextGen Cyber Defense

- Autonomous agent-driven detection
- Automated response (human in the loop)
- End-to-end defense at machine speed and scale

AI MONDAY®

#AIMonday

Thank you!

Find me here!

LinkedIn: [Martin Schöpper | LinkedIn]

Supported by

BASF NEXT MANNHEIM dfki ai

srh Gründer-Institut der Hochschule Heidelberg innoWerft

KI LAB Technologiepark Heidelberg dataconsulting hip:com e.V.

Powered by

DAIN STUDIOS

appcose