Ontinue

Using AI For Effective SecOps Collaboration

AI Powered MXDR

The Pace of Change is Immense

ChatGPT

The hype train sets off. Everyone is now talking about “AI”

▲

Pre Nov 2022

Humans use Google

GPT-4

Everyone is now a “Prompt Engineer”

▲

March 2023

Hot topic and the investment funds start flowing

Everything GPT

The wave has hit, the age of synthetic data is here

▲

Today

Rapid release of projects, tools, and new companies

© Ontinue 2023

Vocabulary to Change the World

AI Centaurs

4th Industrial Revolution

LangChain

Chaining

Synthetic Data

Prompts

LLM

AutoGPT

Stable Diffusion

Hallucinating

Azure Open AI Service

ChaosGPT

Agents

GPT4

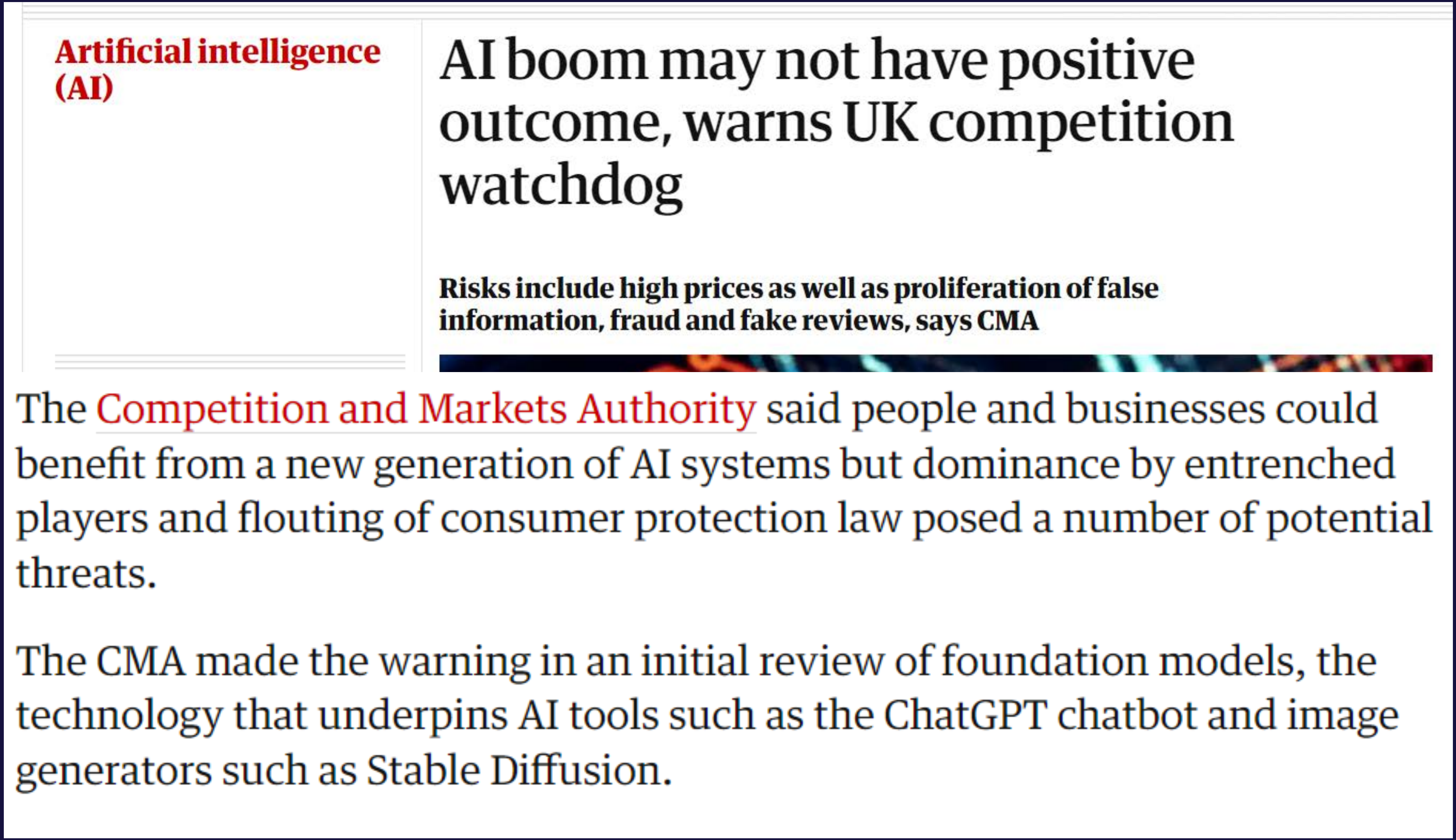
ChatGPT

GAN

ION IQ

Knowledge Amplification

© Ontinue 2023



Artificial intelligence (AI)

AI boom may not have positive outcome, warns UK competition watchdog

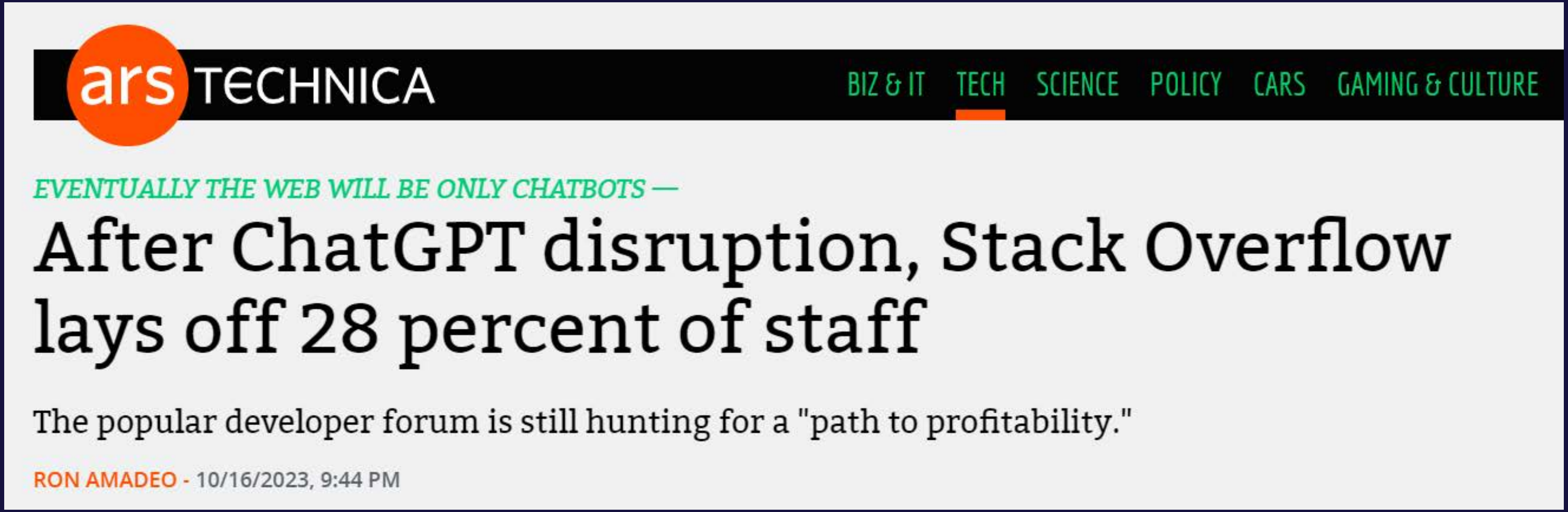
Risks include high prices as well as proliferation of false information, fraud and fake reviews, says CMA

The Competition and Markets Authority said people and businesses could benefit from a new generation of AI systems but dominance by entrenched players and flouting of consumer protection law posed a number of potential threats.

The CMA made the warning in an initial review of foundation models, the technology that underpins AI tools such as the ChatGPT chatbot and image generators such as Stable Diffusion.

https://www.theguardian.com/technology/2023/sep/18/ai-uk-competition-watchdog-cma

© Ontinue 2023



EVENTUALLY THE WEB WILL BE ONLY CHATBOTS —

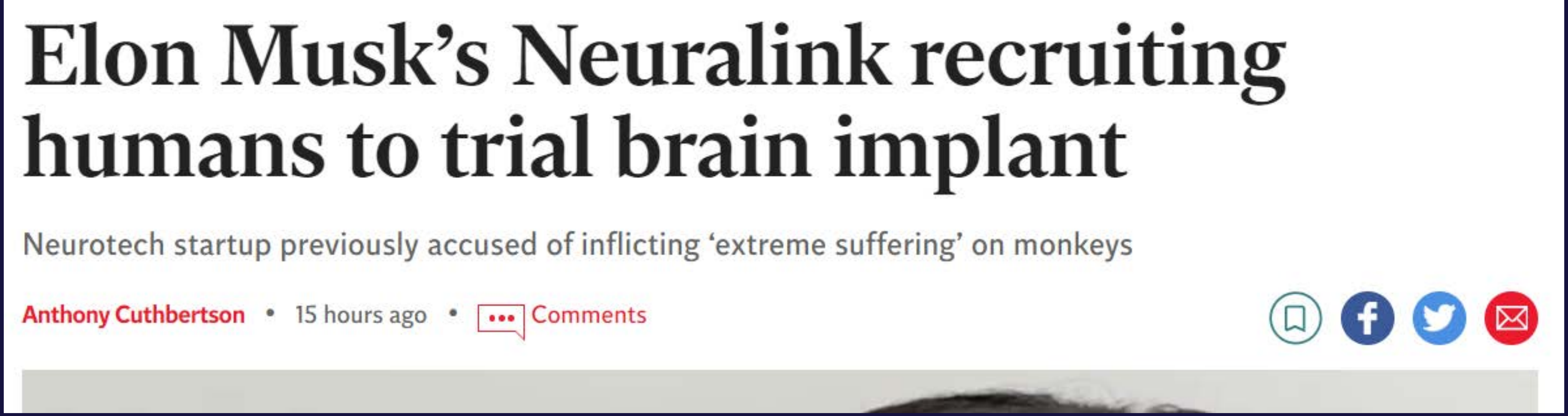
After ChatGPT disruption, Stack Overflow lays off 28 percent of staff

The popular developer forum is still hunting for a "path to profitability."

RON AMADEO - 10/16/2023, 9:44 PM

© Ontinue 2023

https://arstechnica.com/gadgets/2023/10/after-chatgpt-disruption-stack-overflow-lays-off-28-percent-of-staff/



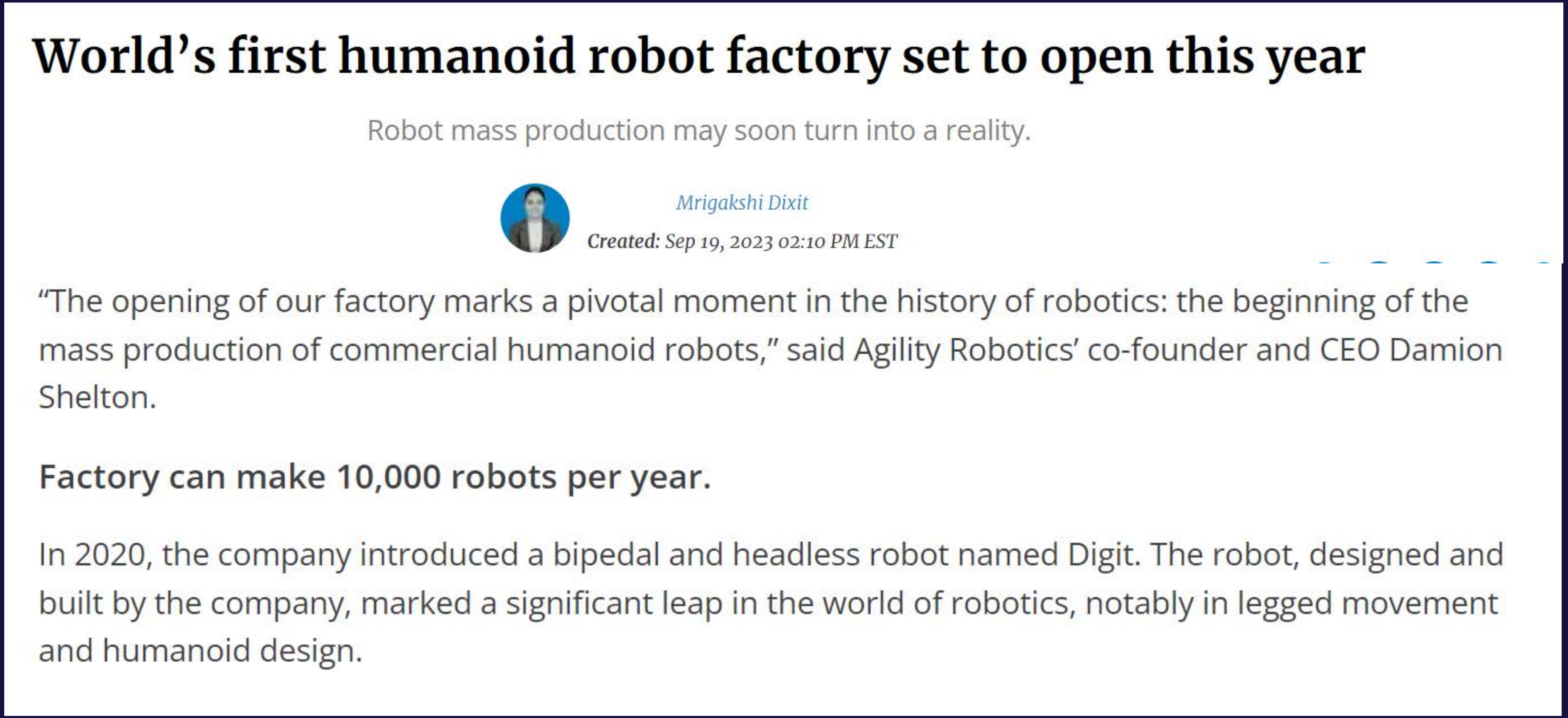
Elon Musk's Neuralink recruiting humans to trial brain implant

Neurotech startup previously accused of inflicting 'extreme suffering' on monkeys

Anthony Cuthbertson • 15 hours ago • Comments

https://openai.com/dall-e-3

© Ontinue 2023



World’s first humanoid robot factory set to open this year

Robot mass production may soon turn into a reality.

Mrigakshi Dixit

Created: *Sep 19, 2023 02:10 PM EST*

“The opening of our factory marks a pivotal moment in the history of robotics: the beginning of the mass production of commercial humanoid robots,” said Agility Robotics’ co-founder and CEO Damion Shelton.

Factory can make 10,000 robots per year.

In 2020, the company introduced a bipedal and headless robot named Digit. The robot, designed and built by the company, marked a significant leap in the world of robotics, notably in legged movement and humanoid design.

https://openai.com/dall-e-3

© Ontinue 2023

Today’s challenges and ambitions

Fast

Accelerate decision making and lessen the impact of incidents

▲

Slow

Long decision making allows incidents to grow in impact

Proactive

Increase your security posture and reduce signal to noise

▲

Reactive

Chasing fires does not allow teams to get ahead of threats

Efficient

Put your full Microsoft investment to work for you

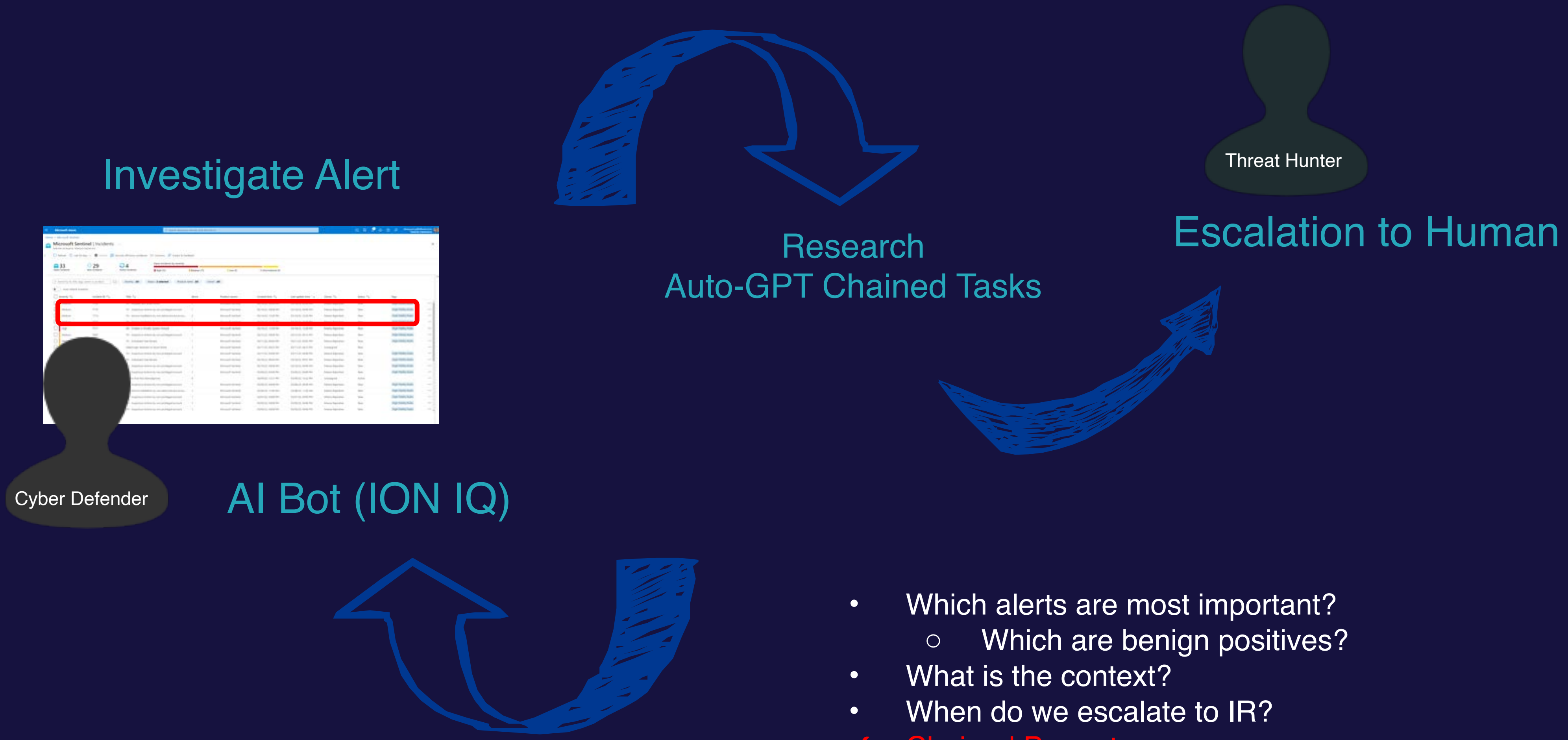
▲

Inefficient

Managing too many tools with too little staff.

© Ontinue 2023

Creating an AI Cyber Defence force multiplier



Investigate Alert

Research
Auto-GPT Chained Tasks

Threat Hunter

Escalation to Human

Cyber Defender

AI Bot (ION IQ)

- Which alerts are most important?
    - Which are benign positives?
- What is the context?
- When do we escalate to IR?
- ✓ Chained Prompts
- ✓ Autonomous Agents

© Ontinue 2023

Microsoft solves a piece of the puzzle

Multi-cloud, multi-device control plane

Microsoft Sentinel

Microsoft Defender - Extended Detection and Response (XDR)

DEFENDER FOR CLOUD

Servers & VMs I Containers I Azure App Service I Network Traffic I SQL I IoT & OT

MICROSOFT 365 DEFENDER

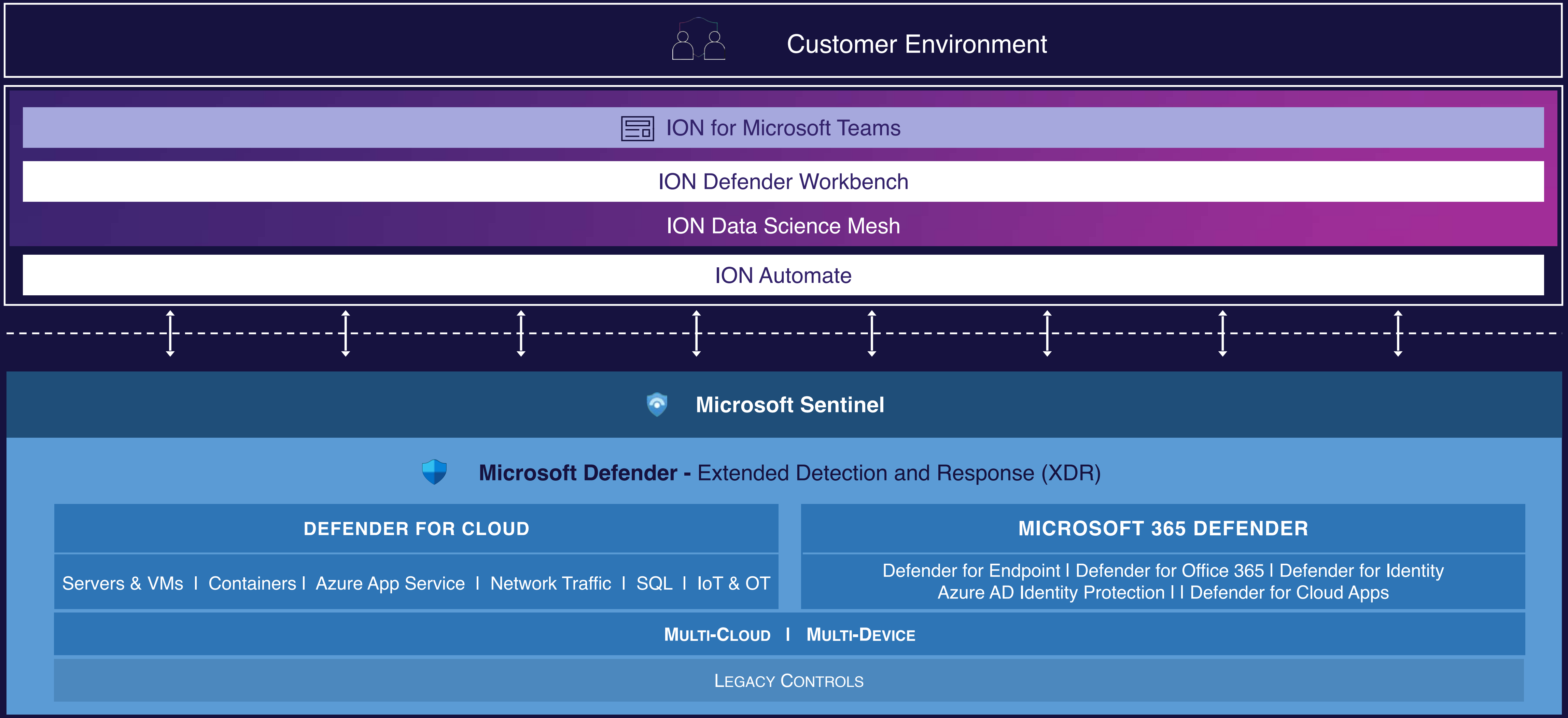
Defender for Endpoint I Defender for Office 365 I Defender for Identity
Azure AD Identity Protection I I Defender for Cloud Apps

MULTI-CLOUD I MULTI-DEVICE

© Ontinue 2023

ION I Technology

Enabling your existing technology investments to do more



Customer Environment

ION for Microsoft Teams

ION Defender Workbench

ION Data Science Mesh

ION Automate

Microsoft Sentinel

Microsoft Defender - Extended Detection and Response (XDR)

DEFENDER FOR CLOUD

Servers & VMs I Containers I Azure App Service I Network Traffic I SQL I IoT & OT

MICROSOFT 365 DEFENDER

Defender for Endpoint I Defender for Office 365 I Defender for Identity
Azure AD Identity Protection I I Defender for Cloud Apps

MULTI-CLOUD I MULTI-DEVICE

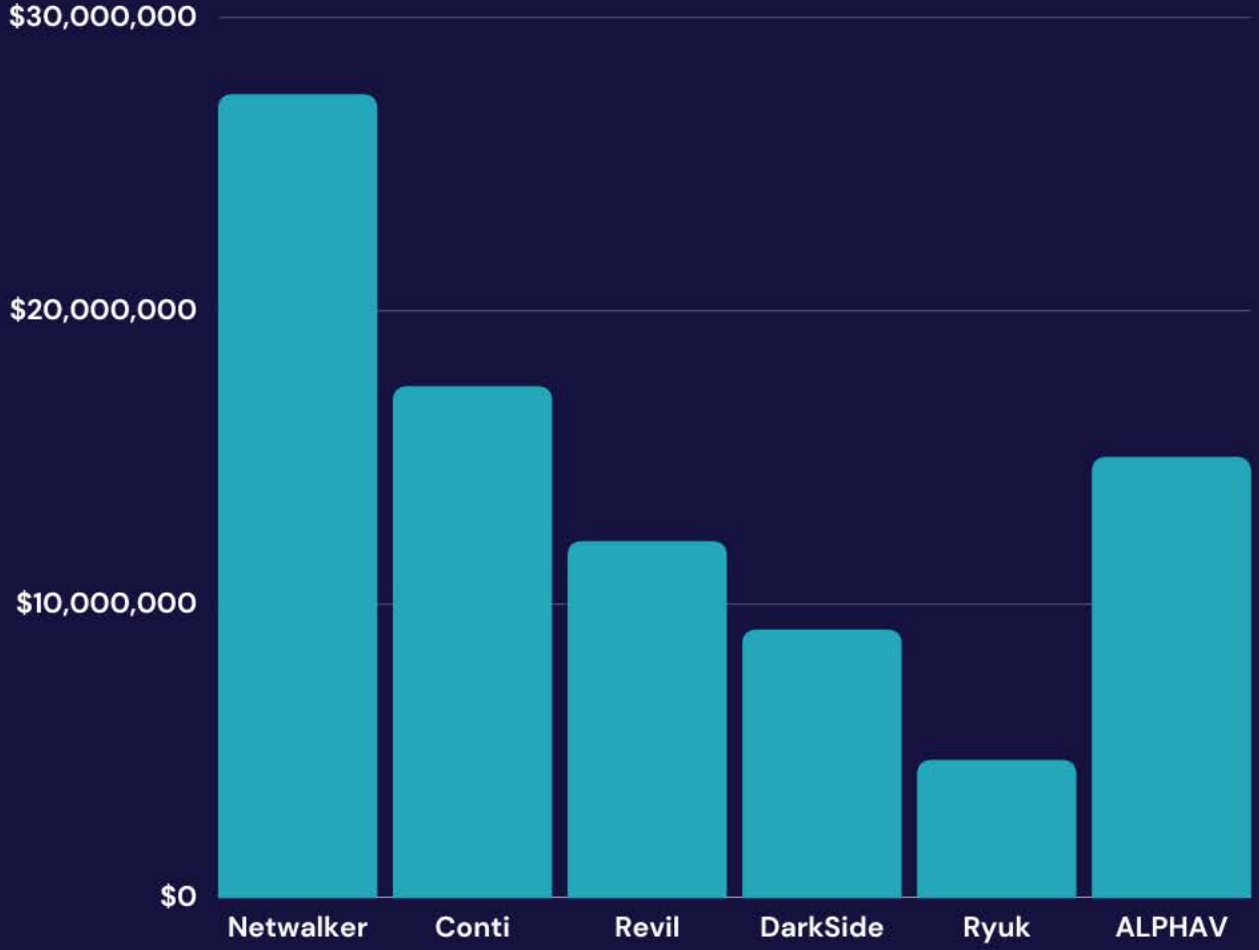
LEGACY CONTROLS

© Ontinue 2023

Battle of the Bots

Are we heading towards Utopia or Armageddon?

© Ontinue 2023



Making Money!

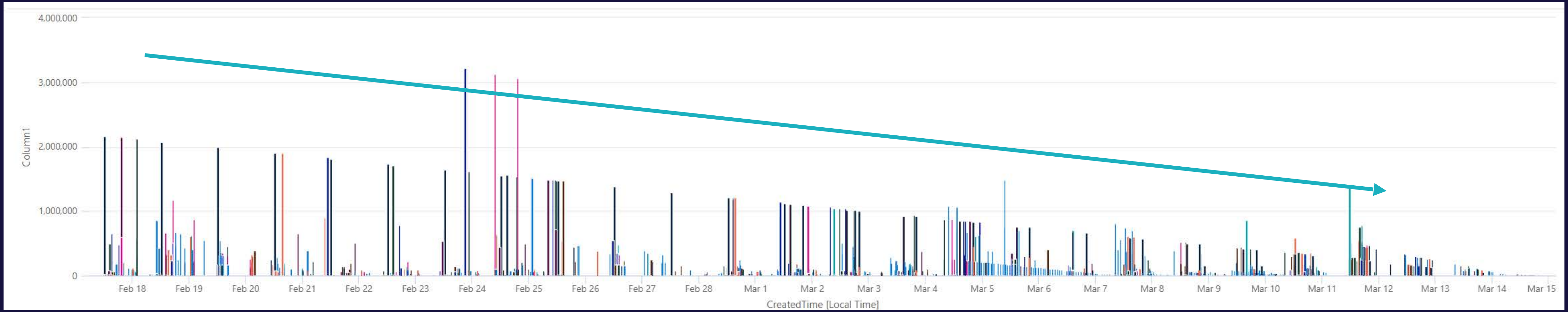
Ransomware gangs have been hitting the jackpot against the West, for over 10 years. $500m+ war chest...

#HACKTHEPLANET

© Ontinue 2023

Effort savings from AI & Automation

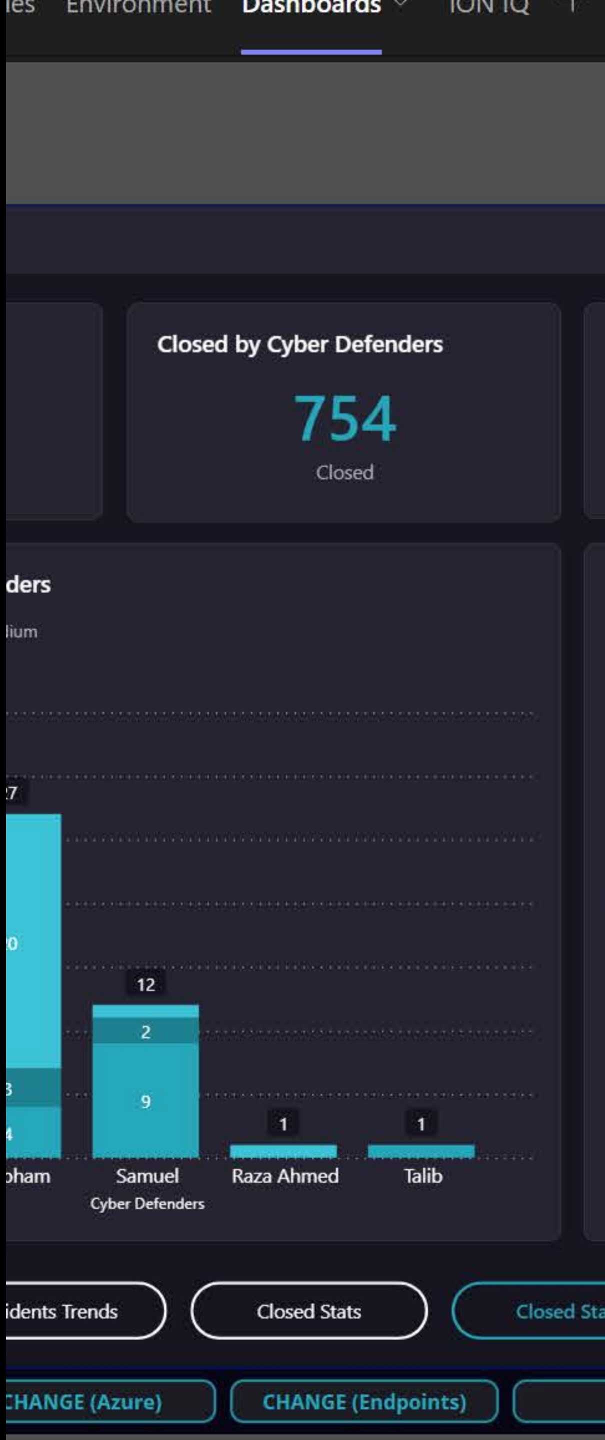
#DoMoreWithLess



Time to close alerts for reduced over time

© Ontinue 2023

Show Me The Future

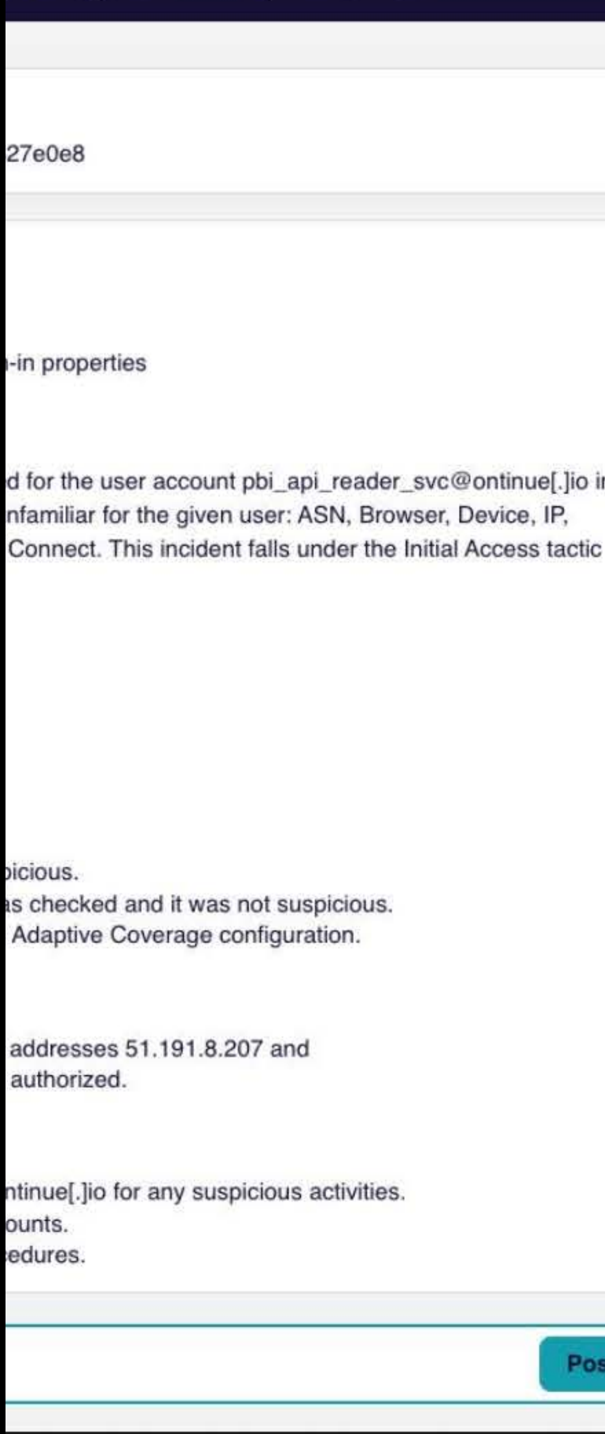


Closed by Cyber Defenders

754

Closed

ION IQ - AI Powered Incident Summarization



27e0e8

-in properties

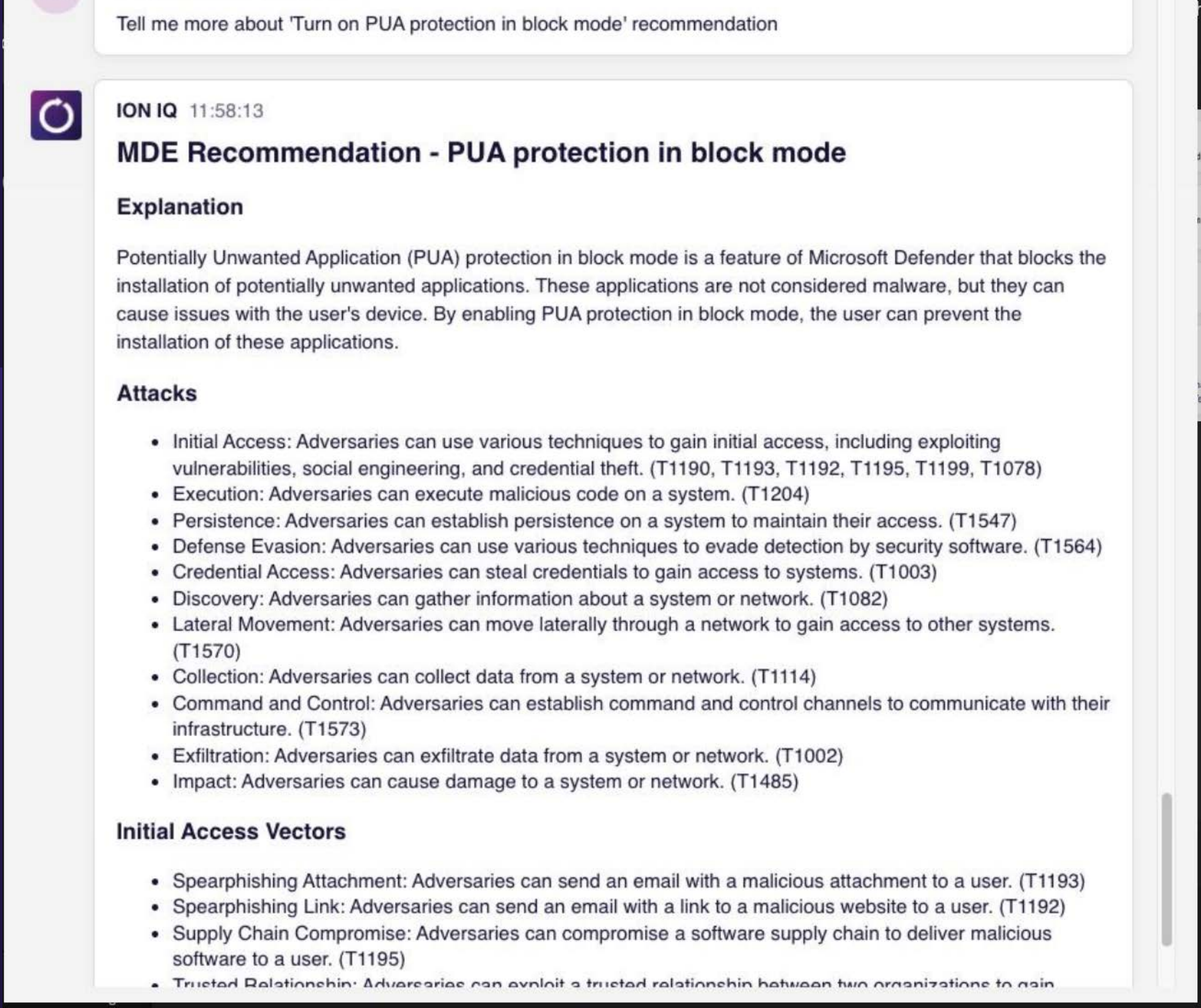
d for the user account pbi_api_reader_svc@ontinue[.]io i
nfamiliar for the given user: ASN, Browser, Device, IP,
Connect. This incident falls under the Initial Access tactic

icious.
s checked and it was not suspicious.
Adaptive Coverage configuration.

addresses 51.191.8.207 and
authorized.

ntinue[.]io for any suspicious activities.
ounts.
edures.

ION IQ – Localized Security Recommendations



Tell me more about 'Turn on PUA protection in block mode' recommendation

ION IQ 11:58:13

MDE Recommendation - PUA protection in block mode

Explanation

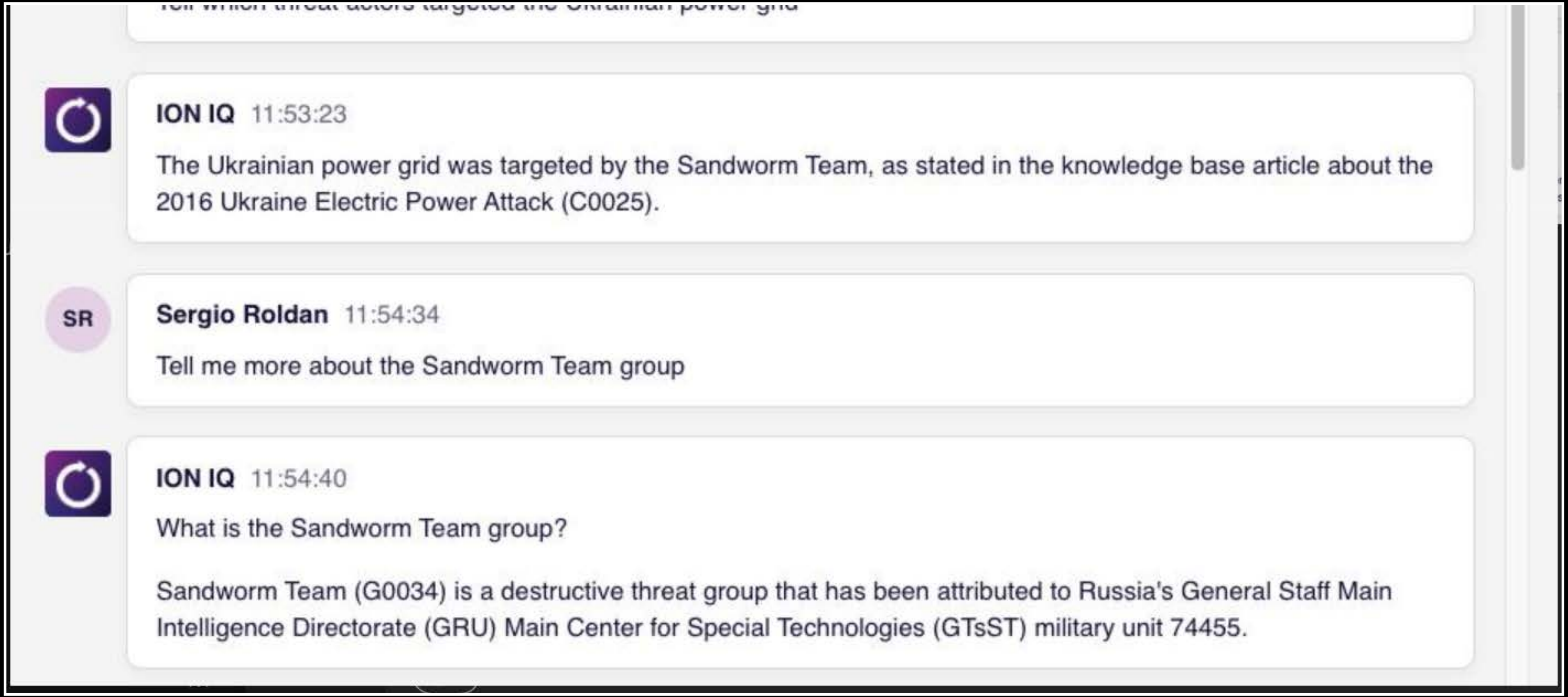
Potentially Unwanted Application (PUA) protection in block mode is a feature of Microsoft Defender that blocks the installation of potentially unwanted applications. These applications are not considered malware, but they can cause issues with the user's device. By enabling PUA protection in block mode, the user can prevent the installation of these applications.

Attacks

- Initial Access: Adversaries can use various techniques to gain initial access, including exploiting vulnerabilities, social engineering, and credential theft. (T1190, T1193, T1192, T1195, T1199, T1078)
- Execution: Adversaries can execute malicious code on a system. (T1204)
- Persistence: Adversaries can establish persistence on a system to maintain their access. (T1547)
- Defense Evasion: Adversaries can use various techniques to evade detection by security software. (T1564)
- Credential Access: Adversaries can steal credentials to gain access to systems. (T1003)
- Discovery: Adversaries can gather information about a system or network. (T1082)
- Lateral Movement: Adversaries can move laterally through a network to gain access to other systems. (T1570)
- Collection: Adversaries can collect data from a system or network. (T1114)
- Command and Control: Adversaries can establish command and control channels to communicate with their infrastructure. (T1573)
- Exfiltration: Adversaries can exfiltrate data from a system or network. (T1002)
- Impact: Adversaries can cause damage to a system or network. (T1485)

Initial Access Vectors

- Spearphishing Attachment: Adversaries can send an email with a malicious attachment to a user. (T1193)
- Spearphishing Link: Adversaries can send an email with a link to a malicious website to a user. (T1192)
- Supply Chain Compromise: Adversaries can compromise a software supply chain to deliver malicious software to a user. (T1195)
- Trusted Relationship: Adversaries can exploit a trusted relationship between two organizations to gain



Tell which threat actors targeted the Ukrainian power grid

ION IQ 11:53:23

The Ukrainian power grid was targeted by the Sandworm Team, as stated in the knowledge base article about the 2016 Ukraine Electric Power Attack (C0025).

Sergio Roldan 11:54:34

Tell me more about the Sandworm Team group

ION IQ 11:54:40

What is the Sandworm Team group?

Sandworm Team (G0034) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.

ION IQ – Threat Actor Awareness

© Ontinue 2023

Ontinue

© Ontinue 2023