guys. If you can connect with that one, maybe this is you guys as you can see, it's not very good.

engineer a nation state malware, working on a presentation in a realistic style. So that's you researcher sitting on a beanbag in front of a pool in the desert in a fancy hotel trying to reverse

So Dall-e two can create an image from text. In that example, we can see a cybersecurity

although they're pretty famous. The rst one is Dall-e two. The second one is GPT three and the

think I did. We did. Gal and I. Let's begin those three logos or logos for three fairly new tools,

So rst of all, I need to say that our code is in Jupyter Notebooks and PyTorch. So if any one of

Dean Langsam:

transcript may contain errors.

audio le

Quiver – Using Cutting Edge ML to detect interesting command lines for Hunters:

automatically transcribed by Sonix

This presentation was featured live at

About LABScon

programming, data visualizations, and Bayesian modeling.

Gal Braun is a data scientist at SentinelOne, working on Data Science & Machine

learning focused on explainability, representation learning, and visualizations.

About the Presenters

Command Lines for Hunters

Cutting Edge ML to Detect Interesting

LABScon Replay | Quiver – Using Cutting Edge ML to detect interesting command lines for Hunters

Camila Scajola- Mora - YY Labs

LABSCON

JUNE 26, 2023

Quiver | Using Cutting Edge ML to Detect Command Lines for Hunters

JUNE 26, 2023

Still, the output is not perfect. Capturing the nature of language, these projects can generate text, images, and code that provide

DALL-E2 is known to take an input prompt in human language and draw a stunning

image with impressive matching results; GPT3 and similar projects can create an

Quiver – QUick Verier for Threat HuntER – is an application aimed at understanding

command lines and performing tasks like Attribution, Classication, Anomaly

Detection, and many others.

Imagine giving a command line to an input prompt and getting the probability of it

being a reverse shell, by an Iranian actor, or maybe used for cybercrime. A single

same way other languages can. And the application can be as versatile as we want.

Command lines are a language in themselves and can be taught and learned the

innite amount of text seemingly written by a real person, while Github's Copilot can

image with impressive matching results; GPT3 and similar projects can create an

With the

and

being

added value to a user. Now, they even understand command lines!

What do GPT3, DALL-E2, and Copilot have in common? By grasping the structure and

of language, these projects can generate text, images, and code that provide

With

and

being

added value to a user. Now, they even understand command lines!

What do GPT3, DALL-E2, and Copilot have in common? By grasping the structure and

of language, these projects can generate text, images, and code that provide