

Martin Holste

Field CTO Cloud and AI, Trellix



GenAI Test

Q1

How manual is your GenAI?

- a) I have to write a prompt to use it
- b) It alerts me to a problem
- c) It makes decisions and can automatically take action based on playbooks

Writing effective prompts can take time - GenAI can make decisions and proactively take action without you ever having to write a prompt

Q2

How many alerts does your team investigate in a day?

- a) 10%-20%
- b) 20%-50%
- c) 50%-80%
- d) 100%

Did you know that GenAI can investigate 100% of your alerts

Q3

What data sources does your GenAI use today?

- a) Endpoint telemetry only
- b) A couple telemetry sources
- c) Everything that comes into our environment

For broadest coverage have GenAI use more telemetry and data sources

Q4

How easily can you get an audit trail for your GenAI so you know it's not hallucinating?

- a) No problem
- b) Would take some work, but I think we could do it
- c) No idea, it's a black box

You should be able to see how GenAI is using your data, so you can trust its analysis

Q5

How fast is your GenAI at investigating every alert?

- a) We don't use it for investigation
- b) It investigates critical alerts I tell it to look at
- c) It gives a full investigation to every alert that comes in and tells me in minutes if I need to look at it

For the biggest impact your GenAI should give every alert a full investigation within minutes

Importance of GenAI



Trellix^{Wise}

*Let's take a
look*



The Trellix logo is centered on a blue background with a green-to-blue gradient at the top. The logo consists of the word "Trellix" in a white, sans-serif font. The background features a pattern of white, wavy lines that resemble a trellis or a stylized grid, which is more prominent in the top and bottom sections of the image.

Trellix