

AI IMPLICATIONS ON IT

**AI implications on IT:
Cyber, Infrastructure,
Operations, Development**

Pini Cohen



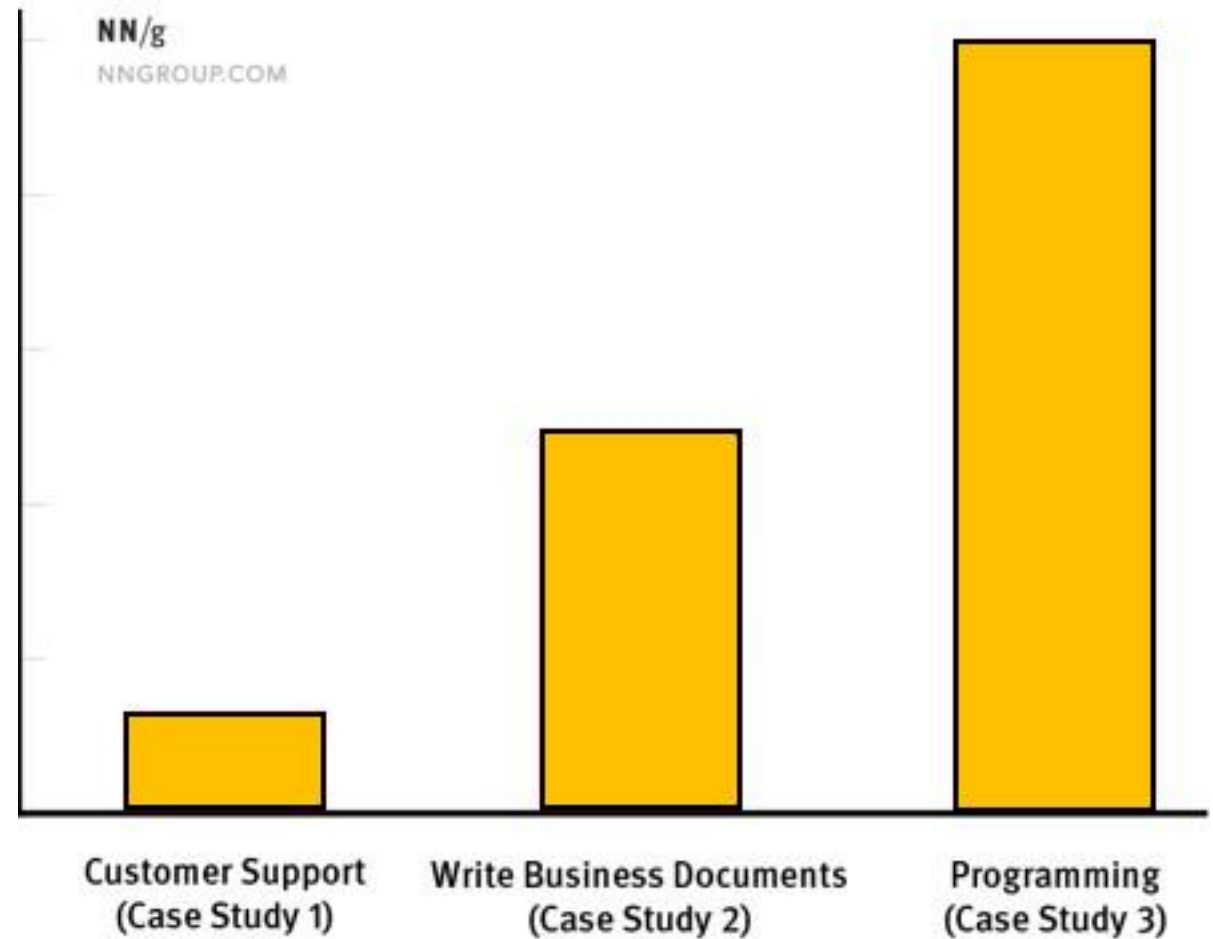
**We
Want AI**

In IT, the need for AI comes from the fields



**AI increases
productivity
especially in
programming**

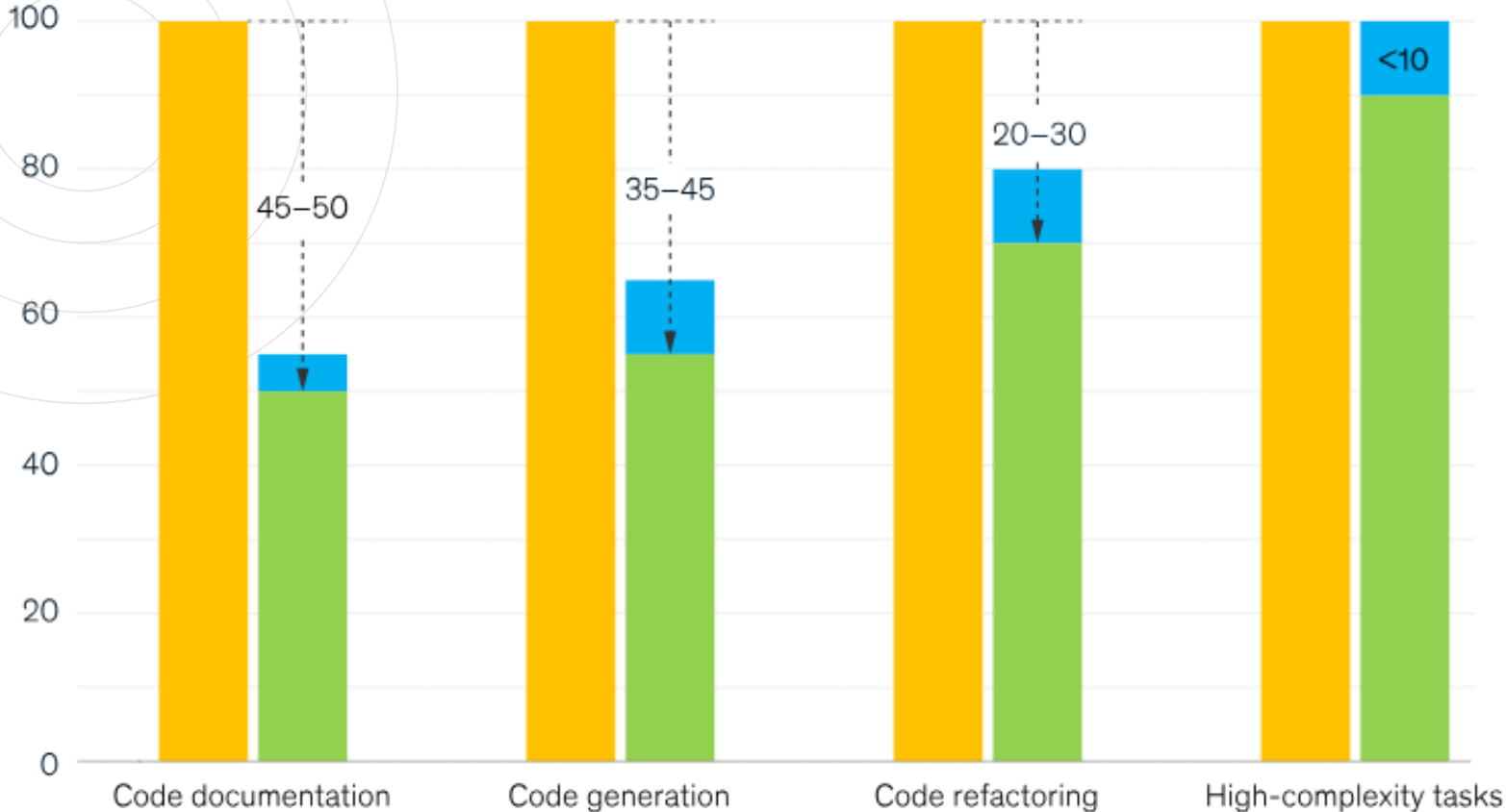
Productivity Increases with AI



<https://www.nngroup.com/articles/ai-tools-productivity-gains/>

Task completion time using generative AI, %

Without generative AI With generative AI



**Generative AI
can increase
developer speed,
but less so for
complex tasks**

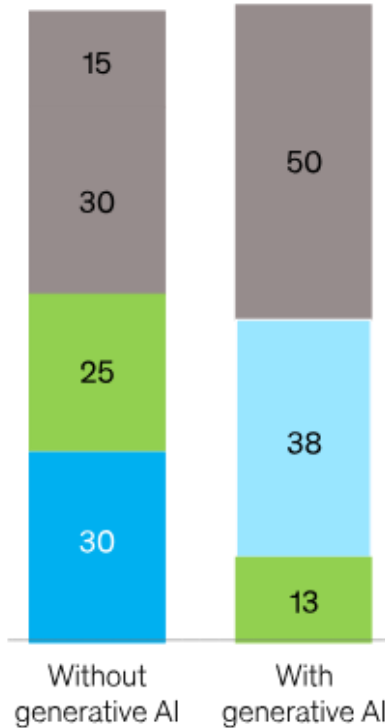
Developers are happier

Generative AI tools have potential to improve the developer experience.

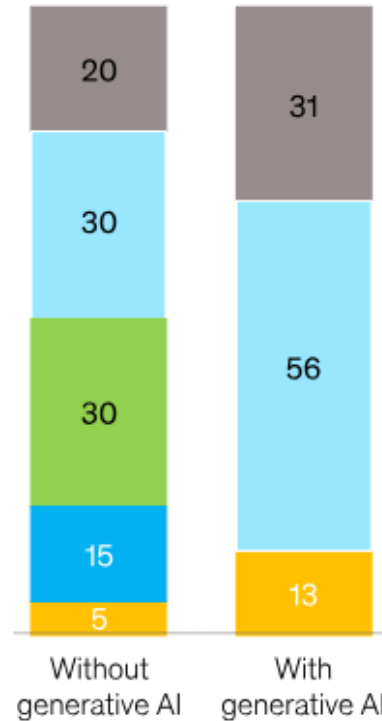
Agreement with statement,
% of respondents

Strongly disagree Somewhat disagree Neither agree or disagree Somewhat agree Strongly agree

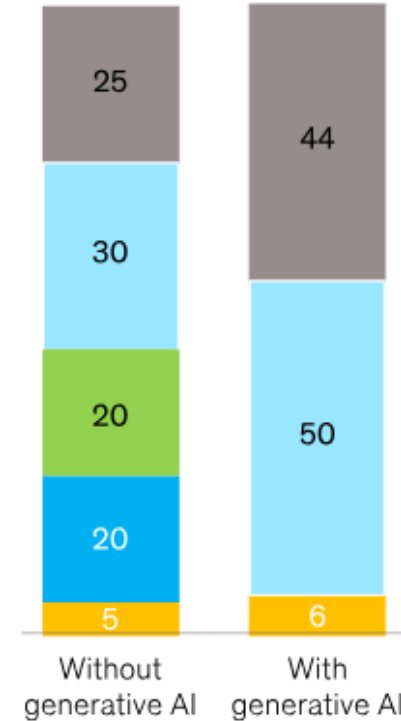
I felt happy



I was able to focus on satisfying and meaningful work



I was in a 'flow' state



Note: Figures may not sum to 100%, because of rounding.

McKinsey & Company

<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/unleashing-developer-productivity-with-generative-ai>

Copyright@STKI_2024 Do not remove source or attribution from any slide, graph or portion of graph



STKI.INFO



create javascript function that tests if a string is palindrome



Sure! A palindrome is a word, phrase, number, or other sequence of characters that reads the same forward and backward. To check if a given string is a palindrome using JavaScript, you can use the following function:

javascript

Copy code

```
function isPalindrome(str) {  
  // Remove non-alphanumeric characters and convert to lowercase  
  const cleanedStr = str.toLowerCase().replace(/^[^a-z0-9]/g, '');  
  
  // Compare the cleaned string with its reverse  
  const reversedStr = cleanedStr.split('').reverse().join('');  
  return cleanedStr === reversedStr;  
}
```

- Code generation or Code Assistant or AI pair programming tools are LLM's trained on code
- Part of the development tools (IDE) in all development process
- What about risks?



Various Code Assistance tools

- On Premise vs. Cloud service
- Personal vs. Enterprise versions
- Different languages
 - The quality of result is based on the volume of code it was trained on.
Including Teraforms, Selenium
- Different missions:
 - Write code
 - Write tests
 - Find bugs
 - Document / explain code
 - Refactor / improve
 - Modernize code



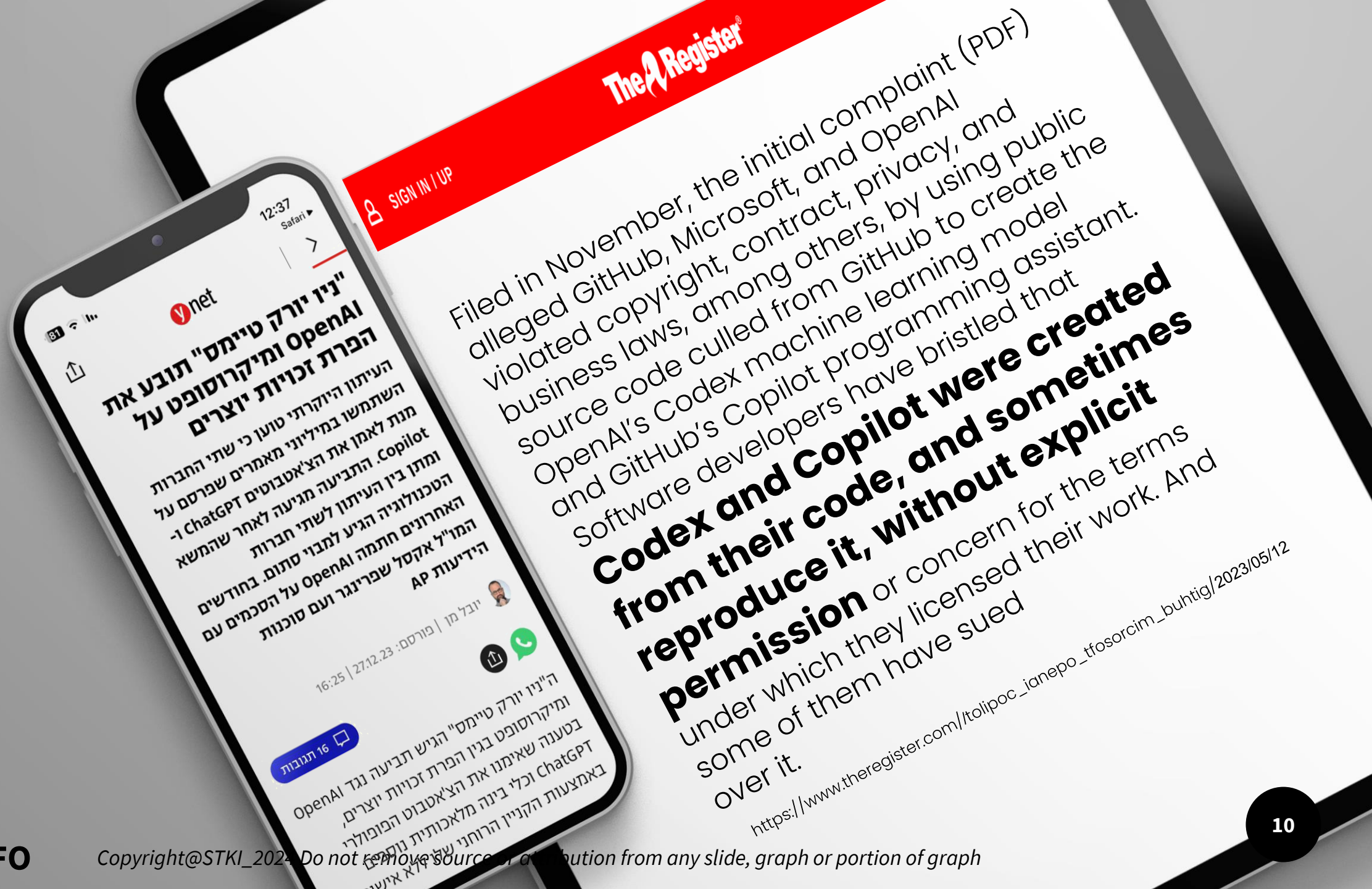
Israeli Enterprise Code Assistance perspective

- Comes from the field (the programmers)
- Productivity increase between 15% (at the beginning) up to 40% (in some organizations)
- Quality of code is improved
- Learning curve for getting the best results from the tool
- Like code you get from off-shore programmers – takes some time until you trust it
- Lots of potential in documentation and unit testing
- Not suitable for all situations (defense, core IP of company, etc.)

Risks with Code Assistant Tools

- Content / code is leaked and reused by the AI tool:
 - Credentials (Keys, User-Password)
 - IP (code or text with user stories, product details, documentation, company secrets)
- Infected code is suggested by the AI tool or library names “invented” by hallucinations become backdoor for cyber attacks
- AI is exposing organization vulnerabilities (internal threat)
- The code suggested by AI includes opensource code or other IP
- Who has the rights for the code that was generated by the developer and the code assistance tool?
- The model was trained on content that has IP rights





Solutions to the code assistance tools



Defending the New LLM Frontier:
End-to-End Security for the
Generative AI Era



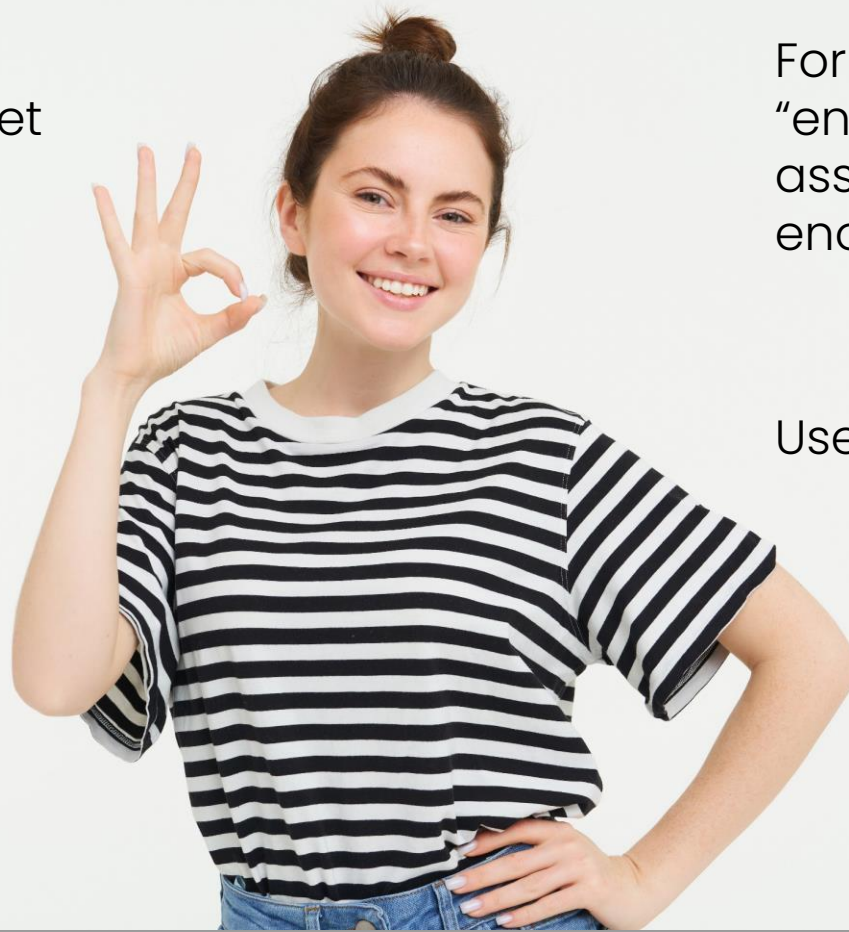
- Use DLP when prompting
 - Need to integrate the DLP to the IDE / Web Gui
 - Is the DLP configured to code/software scenarios?
- Log the code assistance activities
- Use open-source security and license compliance management tools
 - Need to integrate the DLP to the IDE / Web guy
- Use on premise installations
- Use "Enterprise Edition" cloud solutions



STKI Recommends

Enterprises should evaluate their risk in the different vectors and set their policy to the different activities domains

Enhance the security awareness program with AI related topics



For most of the enterprises the “enterprise edition” of code assistant offering might be good enough for the near future

Use risk mitigation AI tools

Evaluate AI risks and solutions every 6 months

How will the future look like? Convergence!!

Recommendations specific to the organization – not “connect to Kafka” as it's done in GitHub but “connect to Kafka” in your organization – using RAG (Retrieval Augmented Generation)



How will the future look like?

Convergence!!

AI code assistance tools will take the design documents of the product / project with its epic, user stories etc. , give advise, prepare a plan and budget for the product / project and code it

Milestone ZERO

ENGINEERING LEADERSHIP | BLOG POST

Will AI Replace Software Engineers Soon? No. In 20 Years? Maybe

August 24, 2023
Greg Vilines

מאגר החקיקה באתר האינטרנט
פרויקט מסמך אפיון

same forward and backward. To check if a given string is a palindrome using JavaScript, you can use the following function:

```
javascript
function isPalindrome(str) {
  // Remove non-alphanumeric characters and convert to lowercase
  const cleanedStr = str.toLowerCase().replace(/[^a-z0-9]/g, '');

  // Compare the cleaned string with its reverse
  const reversedStr = cleanedStr.split('').reverse().join('');
  return cleanedStr === reversedStr;
}
```



Programming will never be the same



(image: james steidl)



AI implications on Cyber: new era for fishing, targeted attacks and fraud (Deep Fake)



**New era for smart
modified malware
created by anyone
who wants**

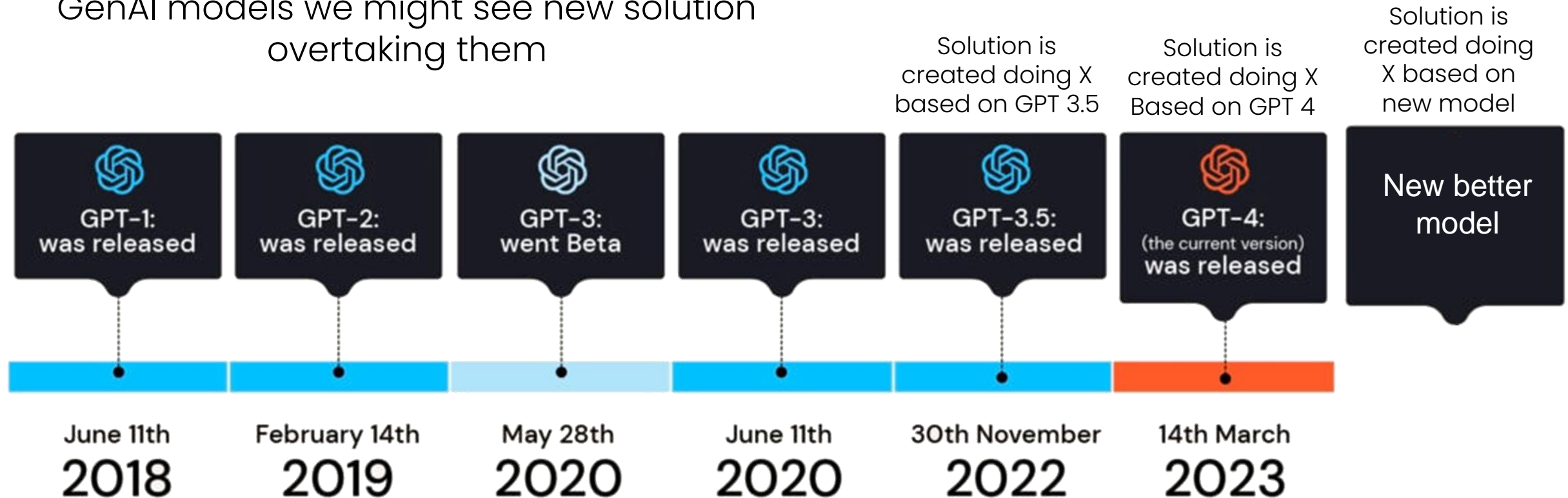


New era of Cyber tools that are smarter



Will we see instability in solutions/vendors?

When solution can not adopt easily to new GenAI models we might see new solution overtaking them



New era of infra- system-cyber “experts”

“create a storage pool named SAP_PROD that uses the APPS volume group and is mounted on the /dev/APPS directory, verify that the pool was created, mount the storage pool, check if the sizes reported are as expected and if AutoStart is configured correctly”

How will the new tech expert will look like?



Implications

- Productivity boost
- Quality improved
- Increase the need for testing environment so we can test the GenAI scripts
 - Who will build the testing environment? Answer: GenAI
 - Cloud is the first choice for building the testing environment
- Dynamic and Self Healing + resource optimization (cost savings)





How will your team look like?

- Will we need smaller team?
- Will you merge several team together?
- Will you need more experienced team members?
- Will you need less experienced team members?
- Will it be easier to replace team member?
- How will you use outsourcing?

Only time will tell!

Work & Life will never be the same



(image: james steidl)



הזמנה לסקר תשתיות

Employees per total support staff members

EMPLOYEES PER SUPPORT STAFF MEMBERS

162



25 percentile

192



Median

250



75 percentile

Source: STKI

B	A
כמה CI מטופלים ע"י סביבת השו"ב? לשאול על ניטור אפליקטיבי - כמה אחוז מהאפליקציות בארגון מנוטרות APM	18
מה נפח האחסון לשימוש בארגון (אחסון שמערכות ההפעלה "רואות") כולל HCI, כולל אחסון שמופעל בזמן DR	19
כמה משרות אחסון/גיבוי+DRP יש?	20
במידה ורלוונטי, מה אחוז הטיפול בסייבר מסך עבודת צוות האחסון\גיבוי\DR?	21
כמה שרתי Windows יש בארגון (כולל וירטואליים)?	22

אתם מוזמנים לשולחות עגולים

- שיפור הממשק בין מרכז התמיכה בנושא סייבר (SOC) לבין מרכז התמיכה הטכנולוגי (Help Desk)
- המשכיות עסקית בכל תרחיש – האם נדרש שינוי תפיסה?
- הזמינות והשרידות של מסדי הנתונים הארגוניים
- יישום פתרונות שליטה ובקרה (observability) מבוססי AI



בניית אסטרטגית API כתשתית ליצירת חדשנות

כולנו בתפילה לשוכם של החטופים ולשלומם של חיילינו.
צוותי האינטגרציה והקישוריות מאפשרים כבר שנים את הפעילות העסקית המנוגת של הארגון.
הצוותים משתמשים בטכנולוגיות מוכחות ותהליכים בשלים אך עם זאת הצוותים נדרשים לשנות את דרכי הפעולה הותיקות שלהם.
הצורך באינטגרציה מהירה של שירותים, הצורך בשליטה מיטבית וניראות על המוני API, הצורך של הגדרת ושימוש מהירה של API על ידי המפתחים, הניראות של איזה API משפיע על איזה API ומהו הפוליסה המופעל כרגע על הממשק – כל אלה (בין היתר) הם הבסיס לארכיטקטורת ממשקים מודרנית.

הפעם, שמחים להתארח במשרדי Google Cloud
יגאל אלון 98 ת"א, קומה 12

סדר יום למפגש:
10:00 - הרצאת פתיחה - STKI
10:45 - הרצאת Google Cloud - הטמעת חדשנות ויעילות תפעולית באמצעות API שאלות ותשובות
11:30 - דיון בין משתתפי המפגש (ללא השתתפות Google Cloud)

- עד כמה ה-API הם חלק מתשתית הממשקים הארגונית המנוהלת
- האם יש עדיין הקמה של ממשקים חדשים בטכנולוגיה מסורתית או שרוב הממשקים החדשים נוצרים כ-API?
- כיצד ניתן לשלוט על הממשקים וה-API בתוך הארגון ומחוצה לו באופן מאוחד?
- האם יש ניסיון במוניטוריזציה של ממשקים?
- כיצד ניתן להשיג רמת אבטחה גבוהה בממשקים הפנים והחוץ ארגוניים באופן נוח?
- כיצד ניתן לשלב את הממשקים הפנים ארגוניים לממשקים בין העננים ובין העננים ל-SDC?

REGISTER NOW!

למפגש מוזמנים:
מנהלי אינטגרציה \ קישוריות \ ממשקים , CTO, ארכיטקטים, מנהלי פיתוח, מנהלי דיגיטל
המפגש מיועד ללקוחות STKI USERS (כל ספקים), נא לא לשלוח יועצים, אלא אם הם עובדים 100% מזמן בארגון.

31.01.2024
10:00 - 13:00
חניה בתשלום: חניון ברח' תובל 4 ת"א

Thank you Inbal Raanan!!





thank
you

Good luck with planning your future
**AI Implementation in development,
Infrastructure, Operations and Cyber**



[image: james steidl]



TO BE CONTINUED



Lunch

13:20–14:20

Break

6

**Organization
2024**

14:20–15:00 Galit

Fein

7

**AI-powered
Knowledge Worker**

15:00–15:30 Einat

Shimoni

THE END

