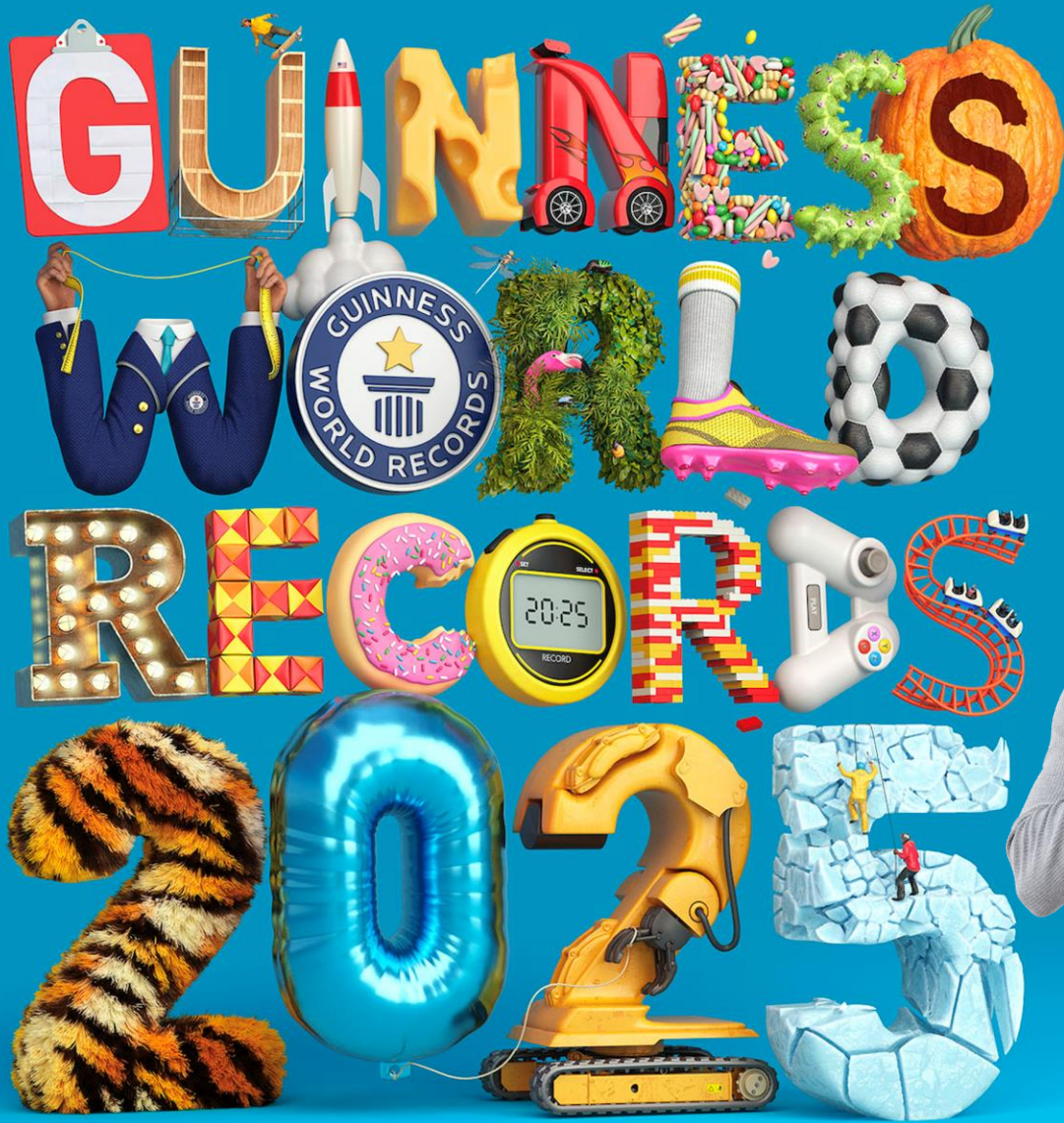




Highlights from STKI Staffing Ratio Research

STKI Staffing Ratios Research ToC (70+ slides) Infra-Cyber-Ops

- 👤 Employees per IT staff member
- 👤 Infra-Cyber-Ops general metrics
- 👤 Infra-Cyber-Ops PMO
- 👤 Cyber
- 👤 Permissions
- 👤 Observability (monitoring)
- 👤 Storage
- 👤 System (Windows, Linux, VDI-TS)
- 👤 NOC-ITOC
- 👤 Help Desk and PC
- 👤 DBA
- 👤 Network and Net-Sec
- 👤 Containers
- 👤 DevOps
- 👤 Public Cloud
- 👤 SAP Basis
- 👤 Demographics + research methodology



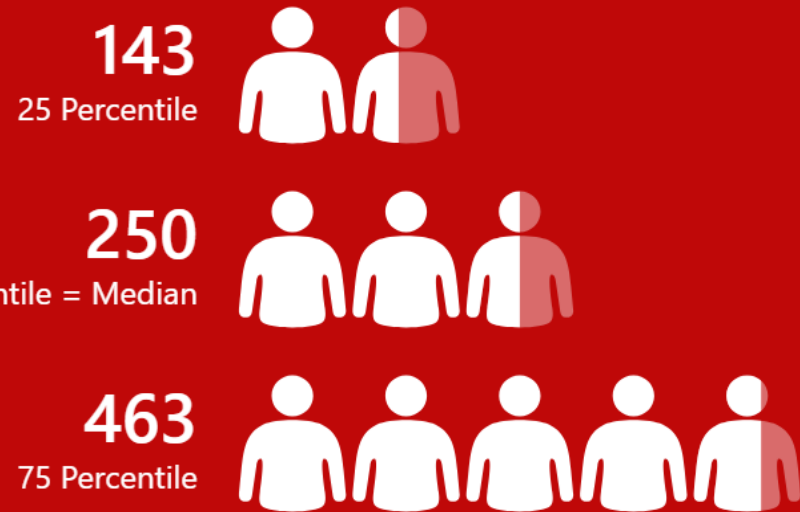
Thank you

for answering the
longest survey in
the world



Number of IT employees

Source : STKI Research



Including full time contractors

Demographics: Number of employees

Source : STKI Research

2250
25 Percentile



5000
50 Percentile = Median



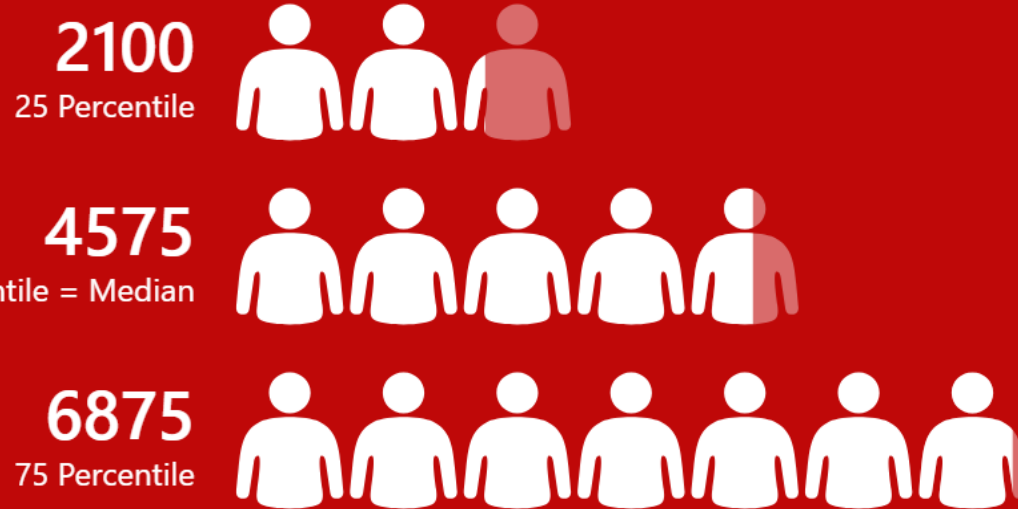
7950
75 Percentile



This does not include “partners” like external doctors in Health, insurance agents in Insurance, etc.

Number of employees that use computers, handhelds, etc.

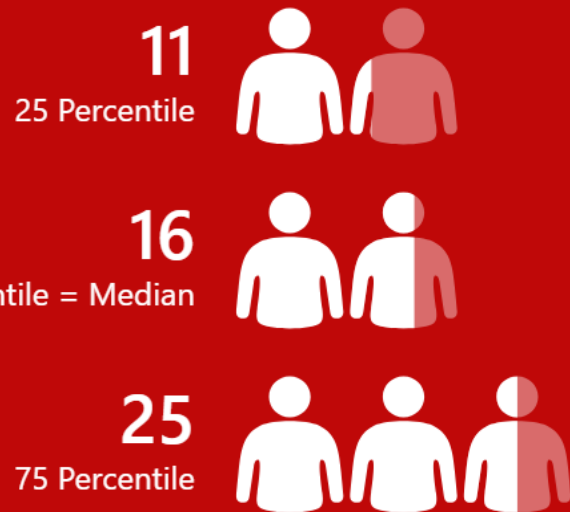
Source : STKI Research



This does not include “partners” like external doctors in Health, insurance agents in Insurance, etc.

Number of employees (using computers) per IT staff member

Source : STKI Research



This does not include “partners” like external doctors in Health, insurance agents in Insurance, etc.

Survey methodology

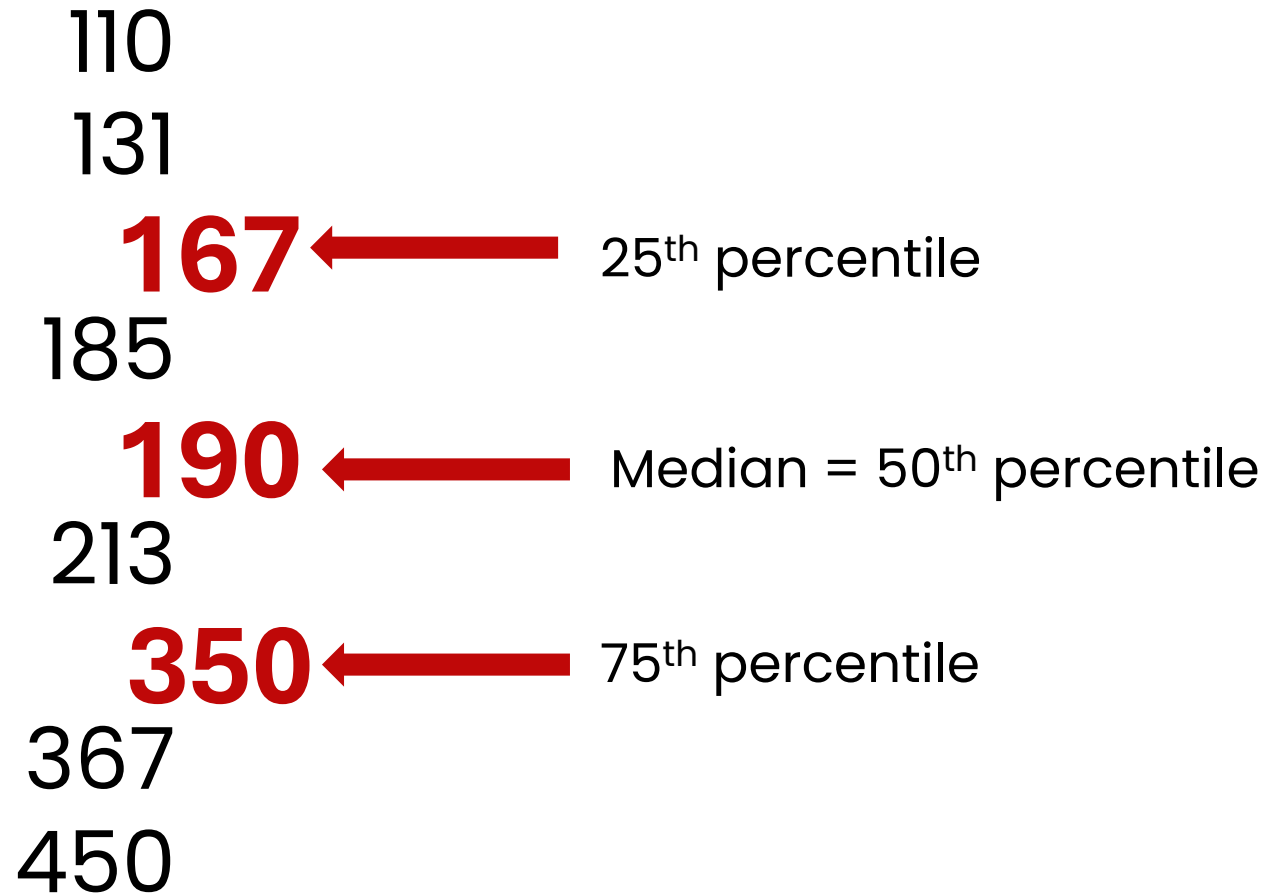
- 👤 Question to Org A – “how many Windows OS do you support?”, “How big is your Windows team?”
- 👤 Answer: “3500 Windows OS’s” , “ 10 FTE (Full Time Employee) in the team”
- 👤 The Ratio is 350 Windows OS per FTE team in Windows team

Survey methodology

- 👤 Org A : The ratio is 350 Windows OS per FTE team in Windows team
 - 👤 Org B: The ratio is 190
 - 👤 Org C: The ratio is 131
 - 👤 Org D: The ratio is 167
 - 👤 Org E: The ratio is 450
 - 👤 185, 213, 110, 367, etc...
- | |
|-----|
| 350 |
| 190 |
| 131 |
| 167 |
| 450 |
| 185 |
| 213 |
| 110 |
| 367 |

Survey methodology

110
131
167
185
190
213
350
367
450



Number of employees (using computers) per IT staff member



What influences the team size?

- 👤 # of components taken care (#of servers)
- 👤 # of layers, component types
- 👤 Minimum team is needed anyway
- 👤 # of sites – locations of DC and branches
- 👤 # of separate LANS
- 👤 # of employees
- 👤 # of clients that access information systems
- 👤 # of partners (insurance agents, independent doctors)
- 👤 Regulation
- 👤 Are we in implementation (or replacement) project now?
- 👤 Ability of IT organization to change
- 👤 Merges and acquisitions
- 👤 Legacy systems (not part of the survey but influencing it)
- 👤 # of technology's / vendors are in use
- 👤 Agility and time to market needed by IT
- 👤 Agility of IT procurement
- 👤 Usage of Outsourcing
- 👤 Usage of public (and "on premise") cloud
- 👤 Need of IDF classification / connection to the internet
- 👤 How critical is the infrastructure / organization?
- 👤 How complex is the organization (types of employees, type of customers, # of business processes)? Stability of the above



What influences the team size?

- 👤 Size of infra taken care (#of servers)
- 👤 Minimum team is needed anyway
- 👤 # of sites – locations of DC and branches
- 👤 # of separate LANS
- 👤 # of employees
- 👤 # of clients that access information systems
- 👤 # of partners (insurance agents, independent doctors)
- 👤 Regulation
- 👤 Are we in implementation (or replacement) project now?
- 👤 Ability of IT organization to change
- 👤 Merges and acquisitions
- 👤 Legacy systems (not part of the survey but influencing it)
- 👤 # of technology's / vendors are in use
- 👤 Agility and time to market needed by IT
- 👤 Agility of IT procurement
- 👤 Usage of Outsourcing
- 👤 Usage of public (and "on premise") cloud
- 👤 Need of IDF classification / connection to the internet
- 👤 How critical is the infrastructure / organization?
- 👤 How complex is the organization (types of employees, type of customers, # of business processes)? Stability of the above





“Technical Debt”

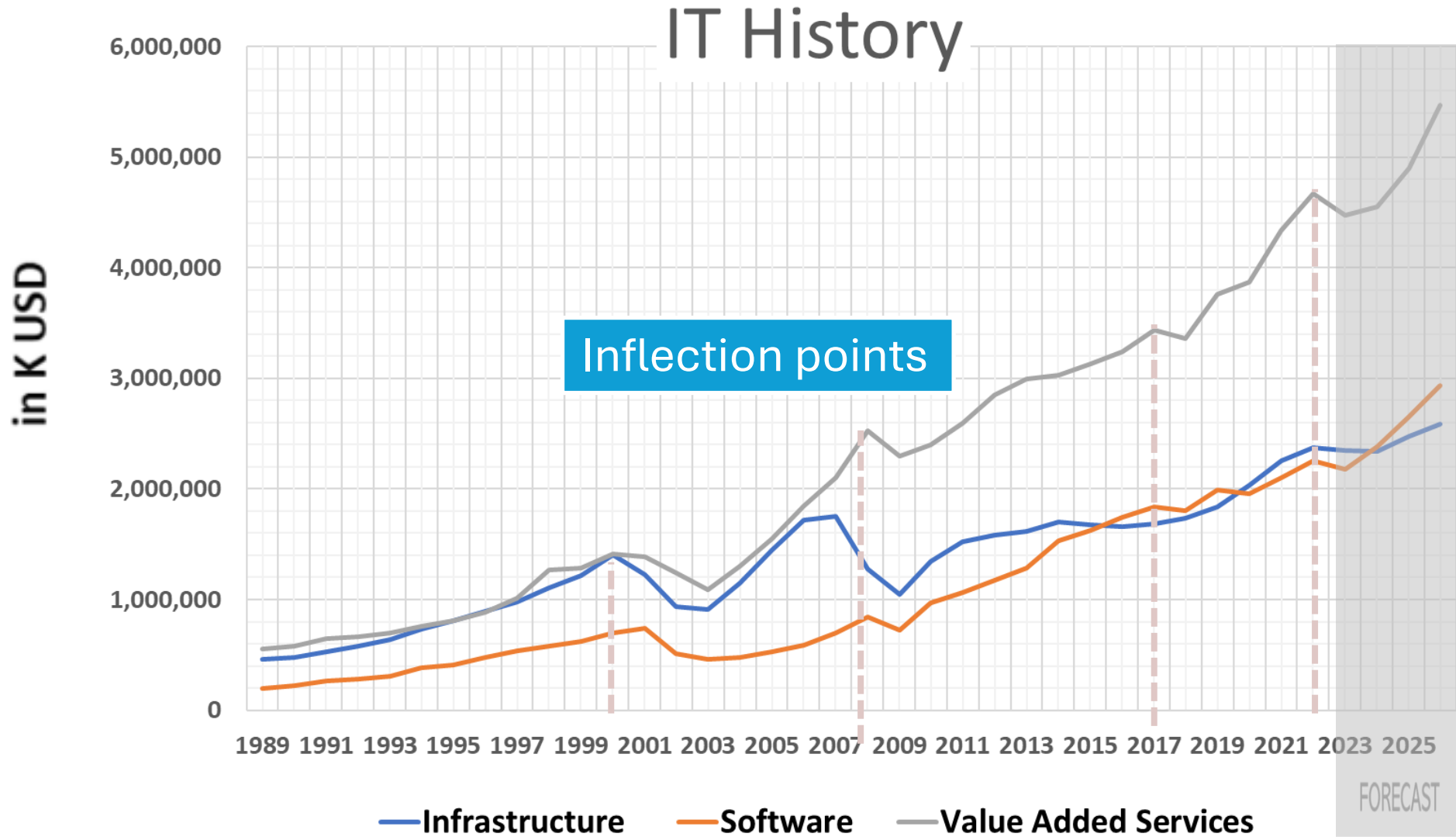
Not In 2024-26 ?



- Outdated infrastructure (software/ hardware)
- Outdated software (several versions behind latest vendor version)
- ERP and/or CRM
- Core systems based on outdated technologies (not in itself broken systems) but are critical to day-to-day operations
- Outdated data management tools (ETL, DW, BI)
- Inability to integrate applications or processes (in-house or partners)
- Missing documentation
- Un-commented configuration
- Un-documented code changes



The IT Market is moving from traditional infrastructure and tools to services (and cloud) – this impacts the FTE ratios



“We are in a cloud project, so we need extra people”

Percent of Infra-Cyber-Ops from total IT employees

Source : STKI Research

22%
25 Percentile



25%
50 Percentile = Median

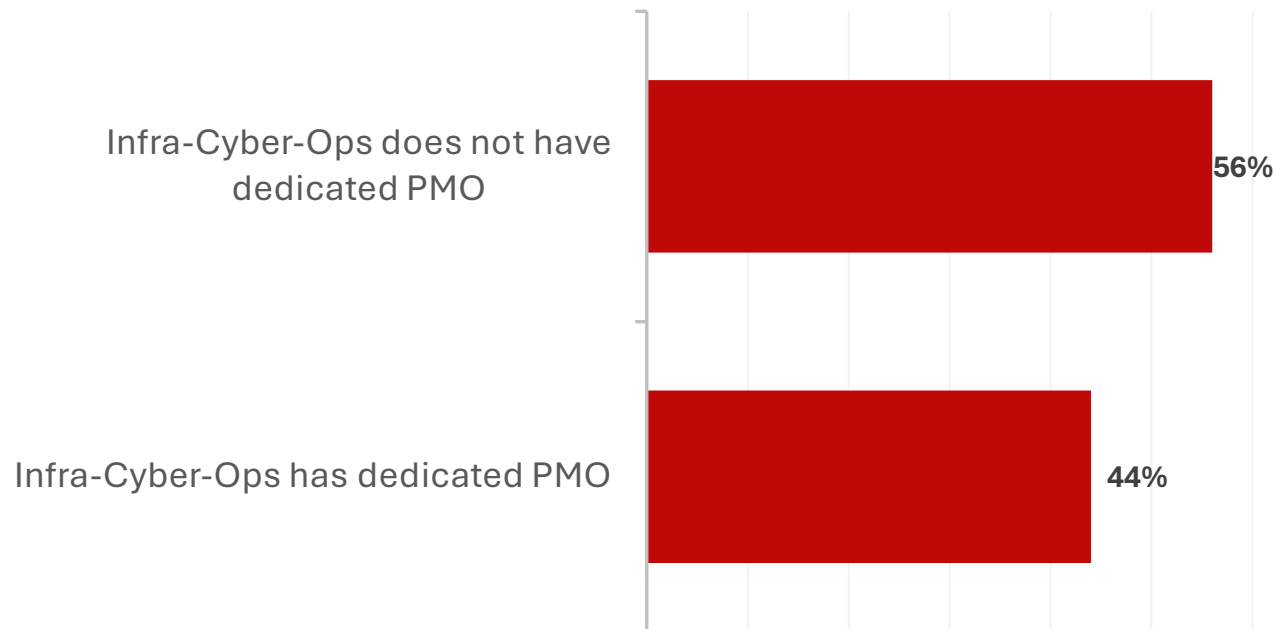


35%
75 Percentile

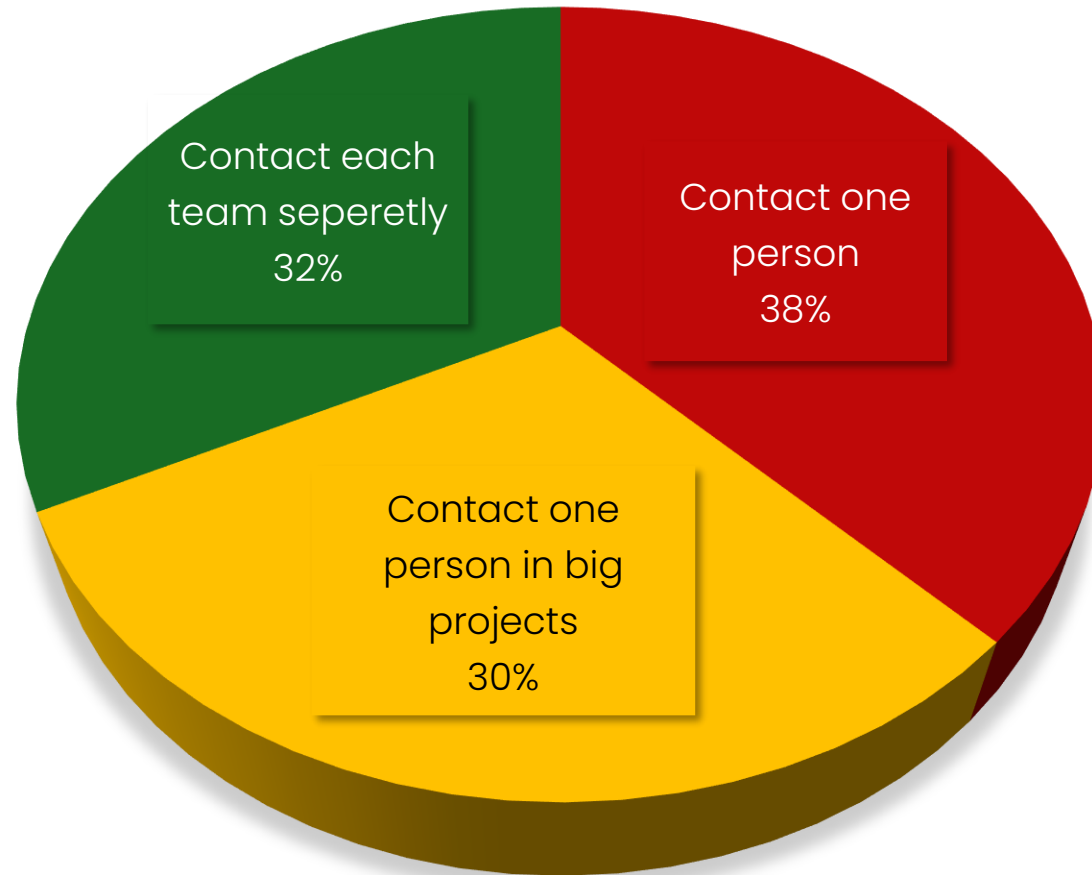


- Totals not including telephony call center , application support , software infrastructure (document management, forms, etc.), HATMAA, HPC, infra procurement,
- SIEM soc might be outsourced (fully or partly)

Does Infra-Ops-Cyber has dedicated PMO services?



How development (products projects) contact the infra-cyber teams?



“One contact” for infra-cyber projects is essential for improving the satisfaction of infra-cyber-ops services

I RECOMMEND

Have a dedicated PMO for Infra-Ops-Cyber

Have one contact person for each product-project

WHY

Infra-Ops-Cyber are different from development projects

Projects (products) hate to move from one person to the other – this might cause “to shadow IT”

Cyber budget from total IT budget in Israeli Enterprises

Source : STKI Research

6%
25 Percentile



10%
50 Percentile = Median



17%
75 Percentile



“Cyber” is defined differently - example - some CIOs consider patches to be part of cyber security, while others may not consider it to be part of cyber security

Sometimes cyber activities are funded by “regulations”

Organizations Increase their cyber budget over the years

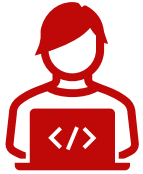


Security (Cyber) Tools Market 2018-2026 – increase!!

	2018		2019		2020		2021		2022		2023		2024		2025		2026
Endpoint related tools	\$43.50	5.75%	\$46.00	15.22%	\$53.00	3.77%	\$55.00	3.64%	\$57.00	3.51%	\$59.00	5.08%	\$62.00	9.68%	\$68.00	7.35%	\$73.00
Network\Web cloud services (FW, WAF, ddos services , etc.)	\$75.00	6.00%	\$79.50	10.69%	\$88.00	4.55%	\$92.00	7.61%	\$99.00	3.03%	\$102.00	3.92%	\$106.00	3.77%	\$110.00	3.64%	\$114.00
data content related tools (DLP, DB FW, DLP Halbana, etc.)	\$32.50	10.77%	\$36.00	2.78%	\$37.00	5.41%	\$39.00	5.13%	\$41.00	4.88%	\$43.00	6.98%	\$46.00	6.52%	\$49.00	6.12%	\$52.00
cyber management tools (SIEM tool, Incident responds, automation)	\$33.00	6.06%	\$35.00	2.86%	\$36.00	2.78%	\$37.00	5.41%	\$39.00	6.41%	\$41.50	13.25%	\$47.00	14.89%	\$54.00	11.11%	\$60.00
Zero Trust including identity, access, SDP software defined perimeter, SASE (secure access service edge) IDM, Access	\$20.00	5.00%	\$21.00	4.76%	\$22.00	4.55%	\$23.00	8.70%	\$25.00	8.00%	\$27.00	11.11%	\$30.00	13.33%	\$34.00	11.76%	\$38.00
Cloud security protection tools (CNAPP CSPM CASB)									\$22.00	13.64%	\$25.00	12.00%	\$28.00	14.29%	\$32.00	12.50%	\$36.00
Other cyber tools (secure development, awareness etc.)	\$11.00	4.55%	\$11.50	4.35%	\$12.00	4.17%	\$12.50	4.00%	\$13.00	3.85%	\$13.50	3.70%	\$14.00	7.14%	\$15.00	13.33%	\$17.00
TOTALS	\$215.00	6.51%	\$229.00	8.30%	\$248.00	4.23%	\$258.50	14.51%	\$296.00	5.07%	\$311.00	7.07%	\$333.00	8.71%	\$362.00	7.73%	\$390.00

Values in Million USD

Cyber security “personas” :



Guidance (CISO)
Budget, priorities, regulations and certifications, PT



Secure
development



SOC
SOC, Security analyst + Incident response
 (“money time”). SOC is big and might be
outsourced



Other – Cyber awareness,
permission team, etc.

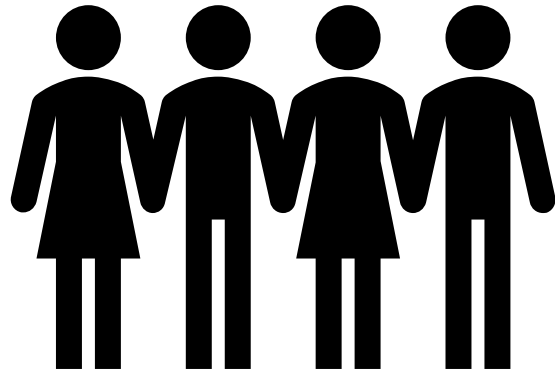


Cyber products (implementing the cyber
products)

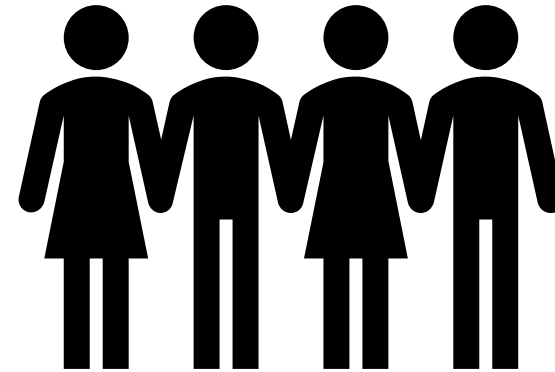


IT controller (who controls the CISO?)
conducting a different set of PT’s

The big divide



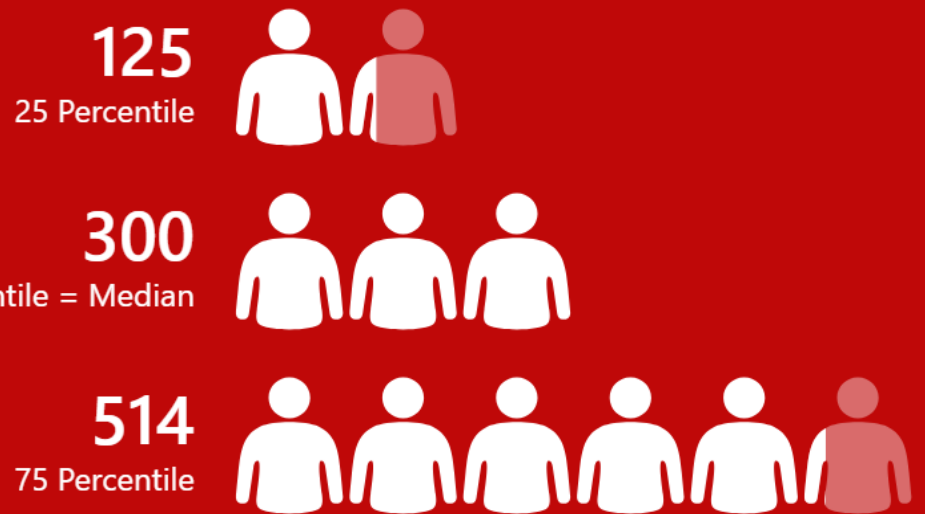
regulated / finance organizations



not regulated organizations

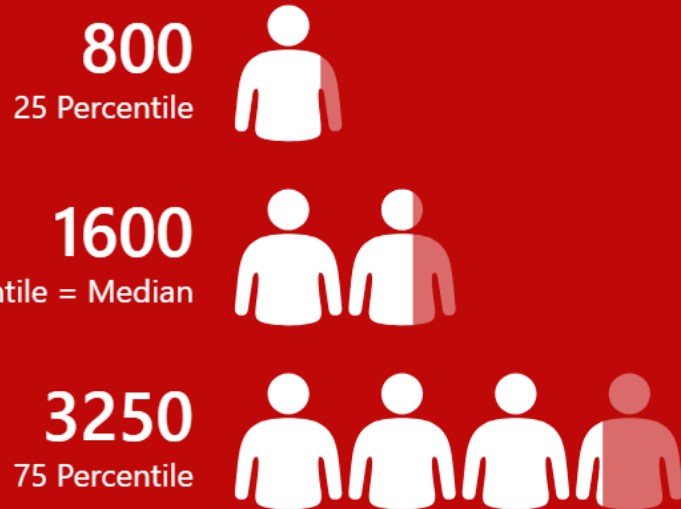
Number of Employees (using computers) per **guidance department (CISO)** staff member in **regulated / finance** organizations

Source : STKI Research



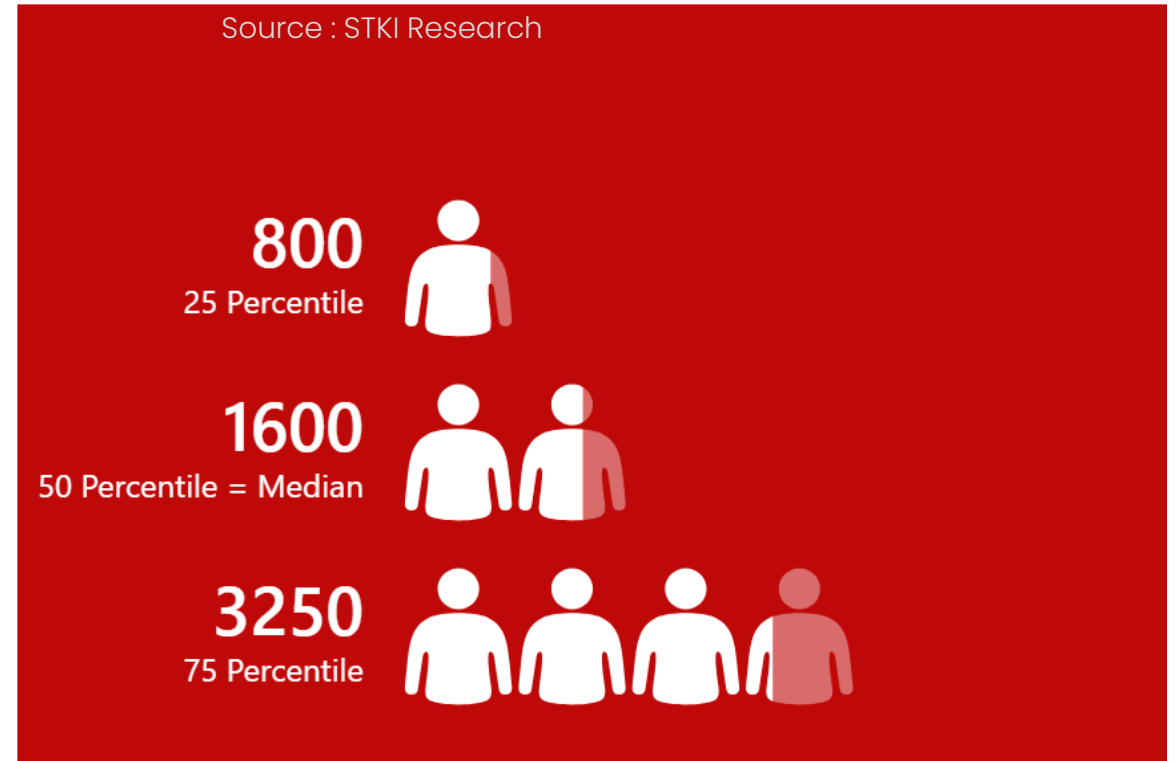
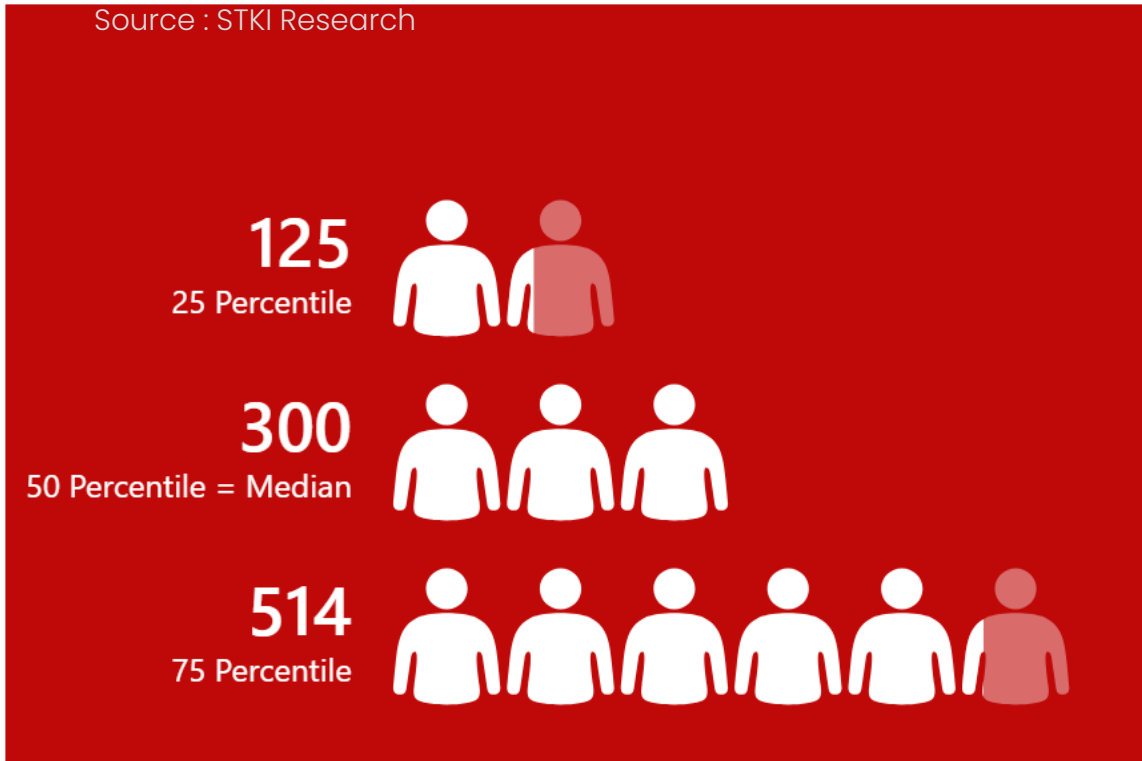
Number of Employees (using computers) per **guidance department (CISO)** staff member organizations **not regulated organizations**

Source : STKI Research



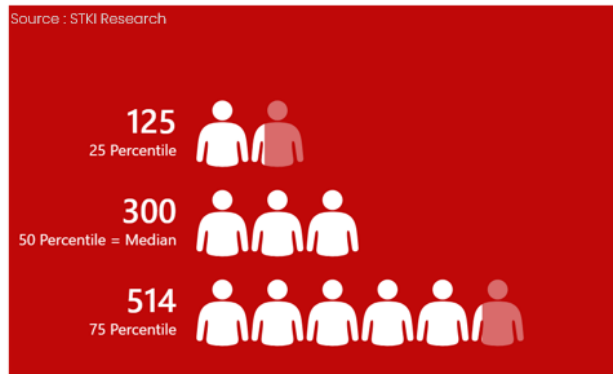
regulated / finance organizations

not regulated



The difference between regulated and not regulated organizations has decreased over the years

Number of Employees (using computers) per guidance department (CISO) staff member in **regulated / finance** organizations



2017

Cyber personnel

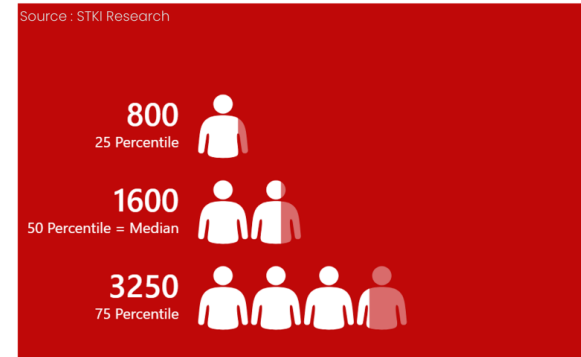
- Number of employees (that use computers) divided to total number of cyber related IT personnel for **regulated** orgs (regulations over 50% of cyber budget):

Per FTE	# employees / # cyber personnel
25 percentile	106
Median	133
75 percentile	158

- Cyber personnel include: guidance, cyber analysts, cyber operations, permissions team
- First level soc personnel not included, insurance agents (not employees) are not included

Source: STKI

Number of Employees (using computers) per guidance department (CISO) staff member organizations **not regulated organizations**



2017

Cyber personnel

- Number of employees divided to total number of cyber related IT personnel for **non-regulated** orgs (regulations is less than 50% of cyber budget):

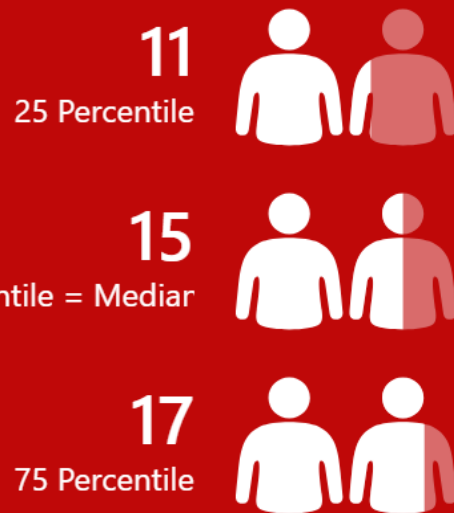
Per FTE	# employees / # cyber personnel
25 percentile	656
Median	1125
75 percentile	1792

- First level soc personnel not included (mainly soc service in non-regulated orgs.)

Source: STKI

SIEM/SOC staffing

Source : STKI Research



Typically : “2-3 in a shift during day 1-2 during night + 2 managers = 14 employees ”

This is why SIEM/SOC as a service is becoming popular

Sometimes : outsourced first level of SOC but analyst are internal

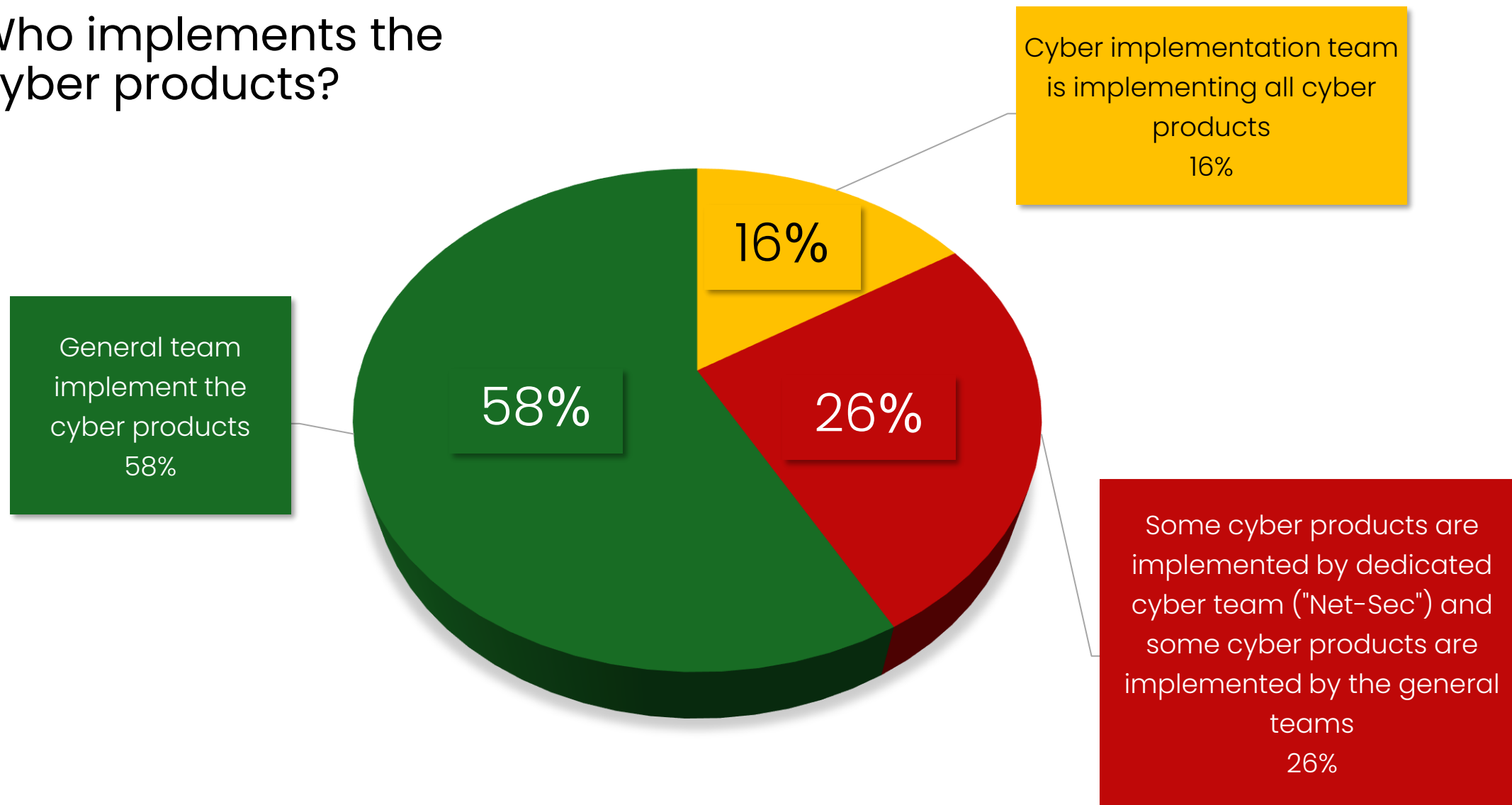
I RECOMMEND

Put special attention to change management and its implications on the external SOC

WHY

The external SOC must be part of every change in production

Who implements the cyber products?



I RECOMMEND

Cyber is everywhere and should be implemented at all levels (all teams) and not by a dedicated cyber team

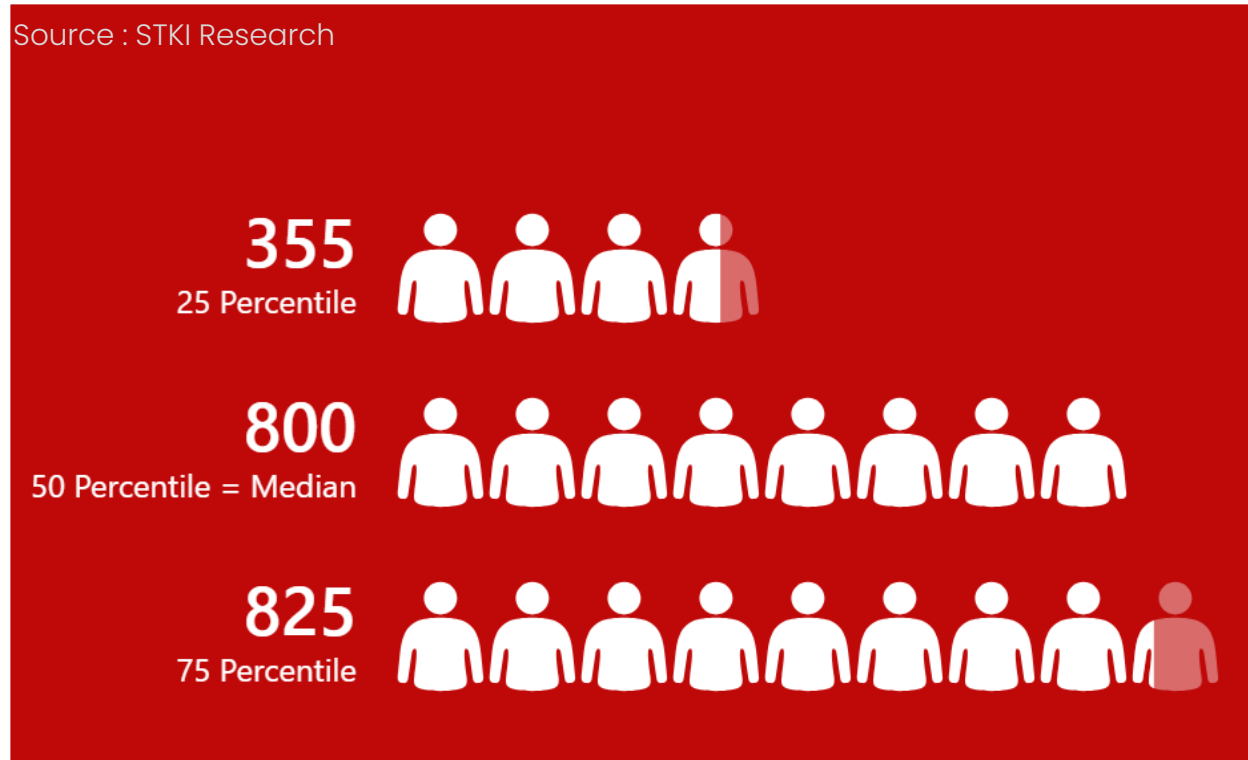
Users should create “Cyber Guild”

WHY

We need one responsible team per each technology part

Number of production server (Windows+Linux) per observability (monitoring) staff member.

Source : STKI Research

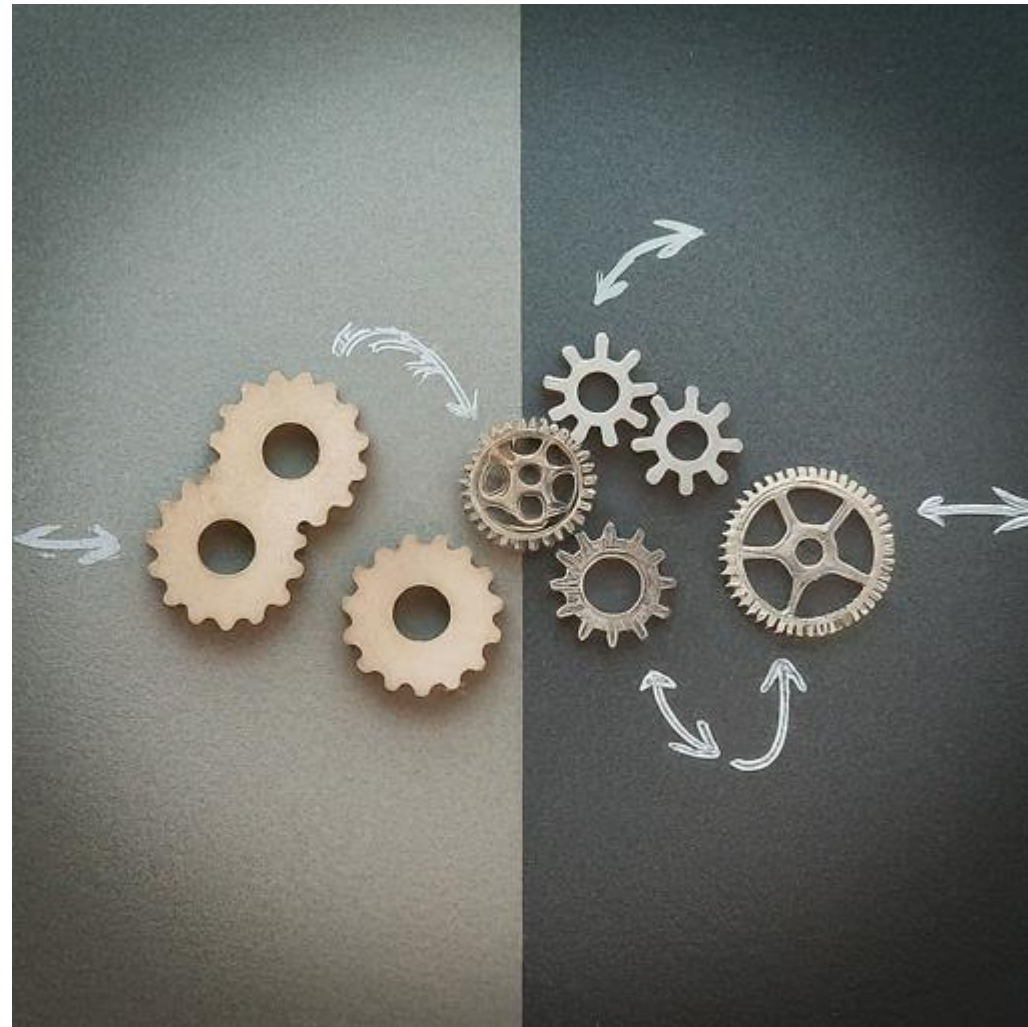


This is for building the observability maps not for looking at the maps (NOC ITOC)
Legacy servers are not counted (AS400 MF)

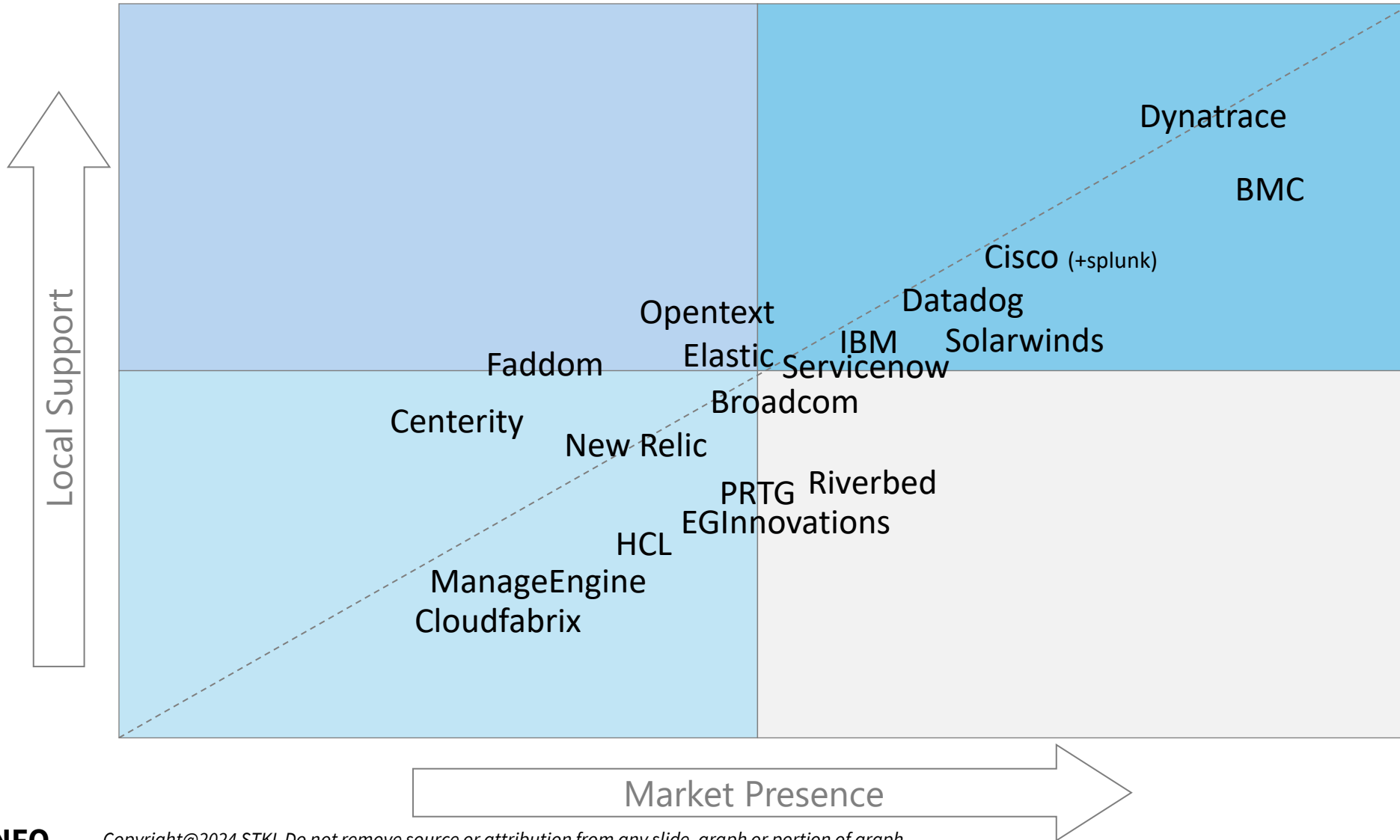
Observability
(monitoring) projects
has the highest
chance to fail



Good operations
(availability) based on
advanced observability
is **90% process** and only
10% technology

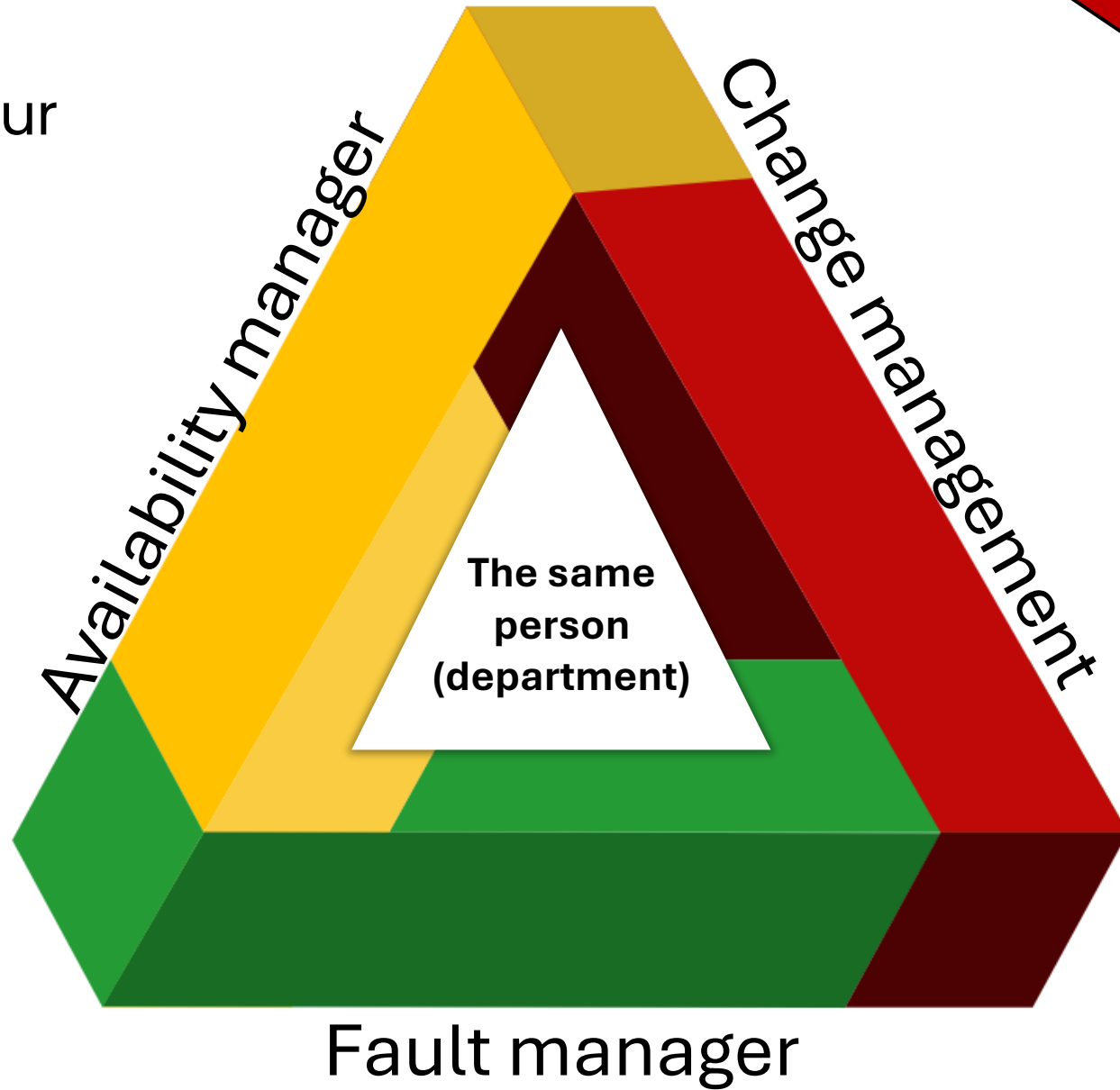


Israel enterprise Observability (monitoring) brands market presence 2024



This diagram is not “apples to apples” comparison – it contains all kind of Observability types: infra (traditional), APM, AIOps, MOM, Discovery, Cloud, etc.

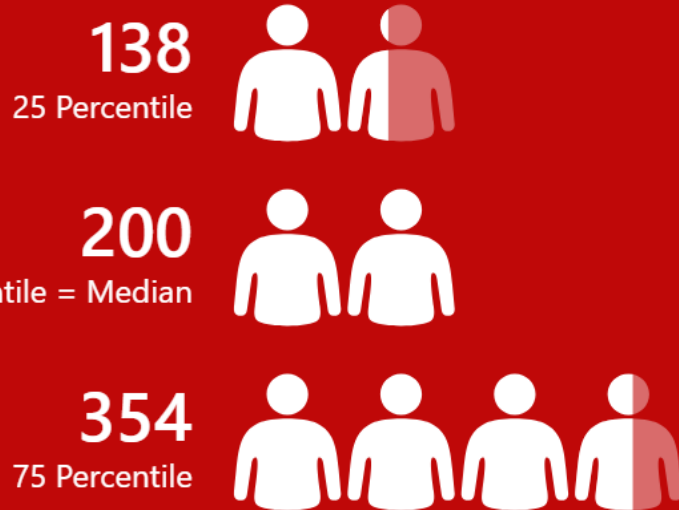
Want to improve your
IT availability ?
This is your holly
triangle



Lots of material /
presentation on this
subject by STKI

of Windows servers (all:prod+dev+test) per Windows system staff member

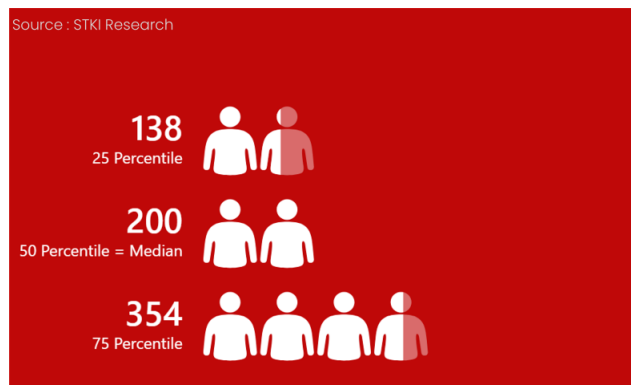
Source : STKI Research



Windows team includes Windows servers, AD, exchange/365, VMWARE ESX VDI-TS

Increase in metric from last survey (all servers)

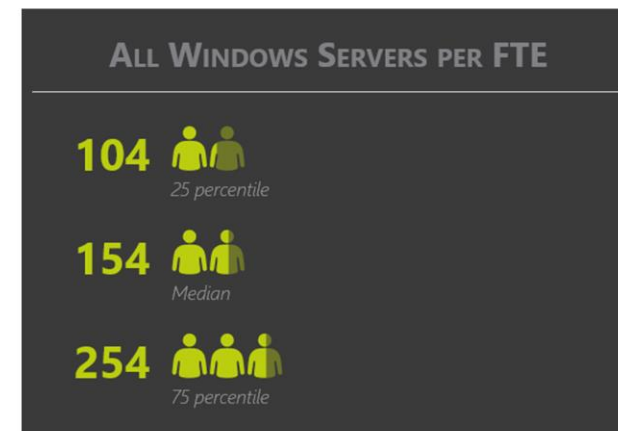
of Windows servers (all:prod+dev+test) per Windows system staff member



Windows team includes Windows servers, AD, exchange/365, VMWARE ESX VDI-TS

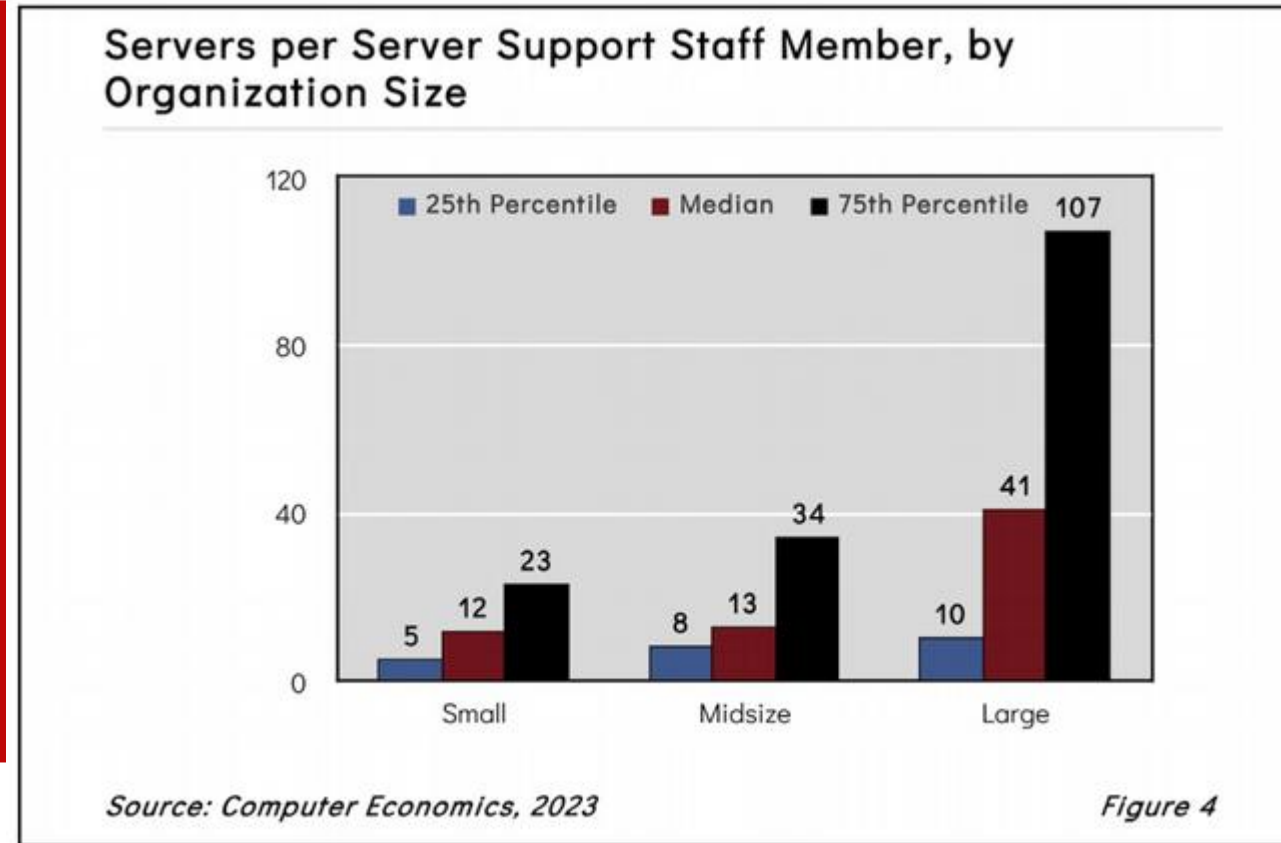
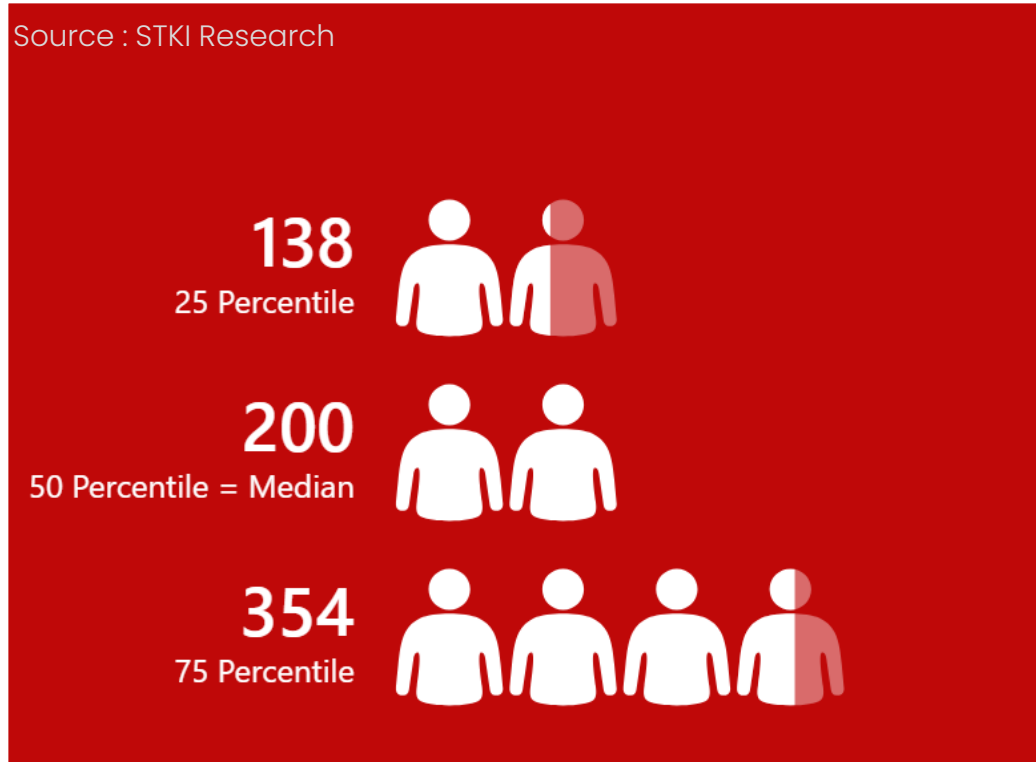
- Number of Windows Servers (logical) per System member
 - Server is either physical or virtual
 - This includes SBC\VDI (Citrix\WTS\Jetro) support
- For development environment's ratios can grow up to 700 servers per FTE
- Organizations with 100% identical servers in branches can get ratios up to 1700 servers per FTE
- Sometimes (separate) virtualization team gives services to both Windows and Linux

Source: STKI



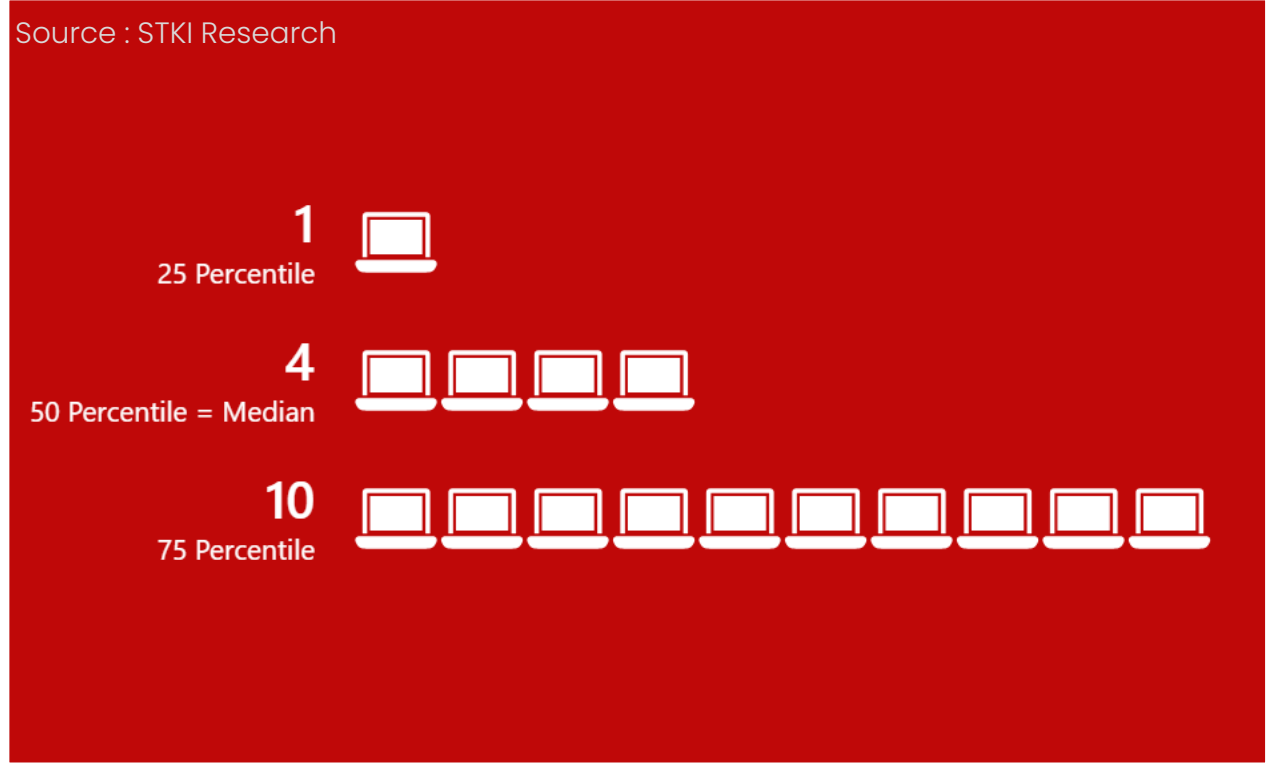
of Windows servers (all:prod+dev+test) per Windows system staff member compared to Computer Economics

Source : STKI Research



we use a broad definition for server support staff that includes all personnel who support the server and storage infrastructure, whether data center enter or cloud infrastructure, including system administrators, system programmers, system engineers, storage administrators, cloud architects, and facility engineers. It also includes computer operators, job schedulers, production control personnel, disaster recovery administrators, and other ancillary functions supporting the compute and storage infrastructure.

How many Windows VM are created/modified per week?



What percent from Windows team effort is dedicated to cyber?

Source : STKI Research


20%
25 Percentile



21%
50 Percentile = Median



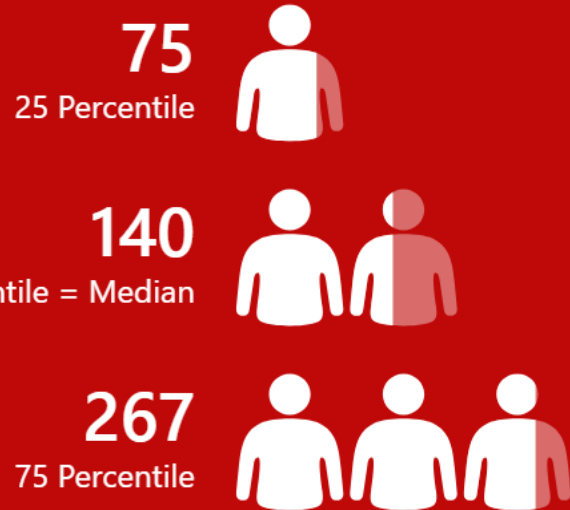
34%
75 Percentile



“Cyber” is defined differently - example - some CIOs consider patches to be part of cyber security, while others may not consider it to be part of cyber security

of production Linux servers per Linux system staff member

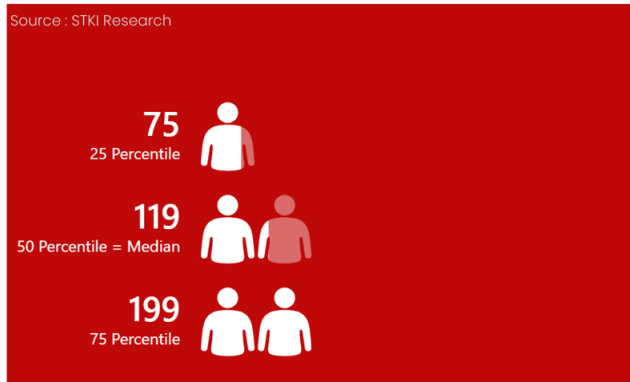
Source : STKI Research



Linux server team is mainly only responsible for Linux servers

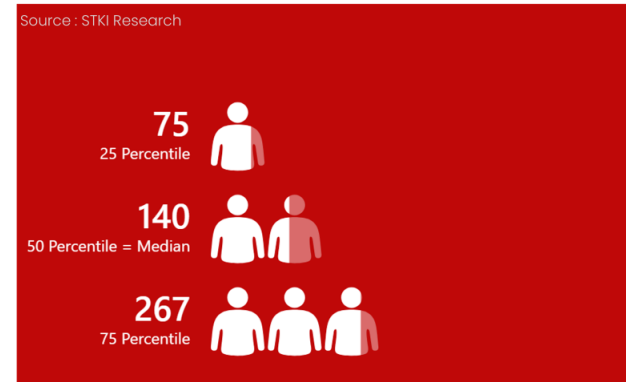
Windows vs. Linux – and the winner (in efficiency) is Linux but “Windows team” is also responsible for AD, Exchange/365, VDI

of Windows servers (production) per Windows system staff member



Windows team includes Windows servers, AD, exchange/365, VMWARE ESX VDI-TS

of production Linux servers per Linux system staff member



Linux server team is mainly only responsible for Linux servers

How many Linux VMs are created/modified per week?

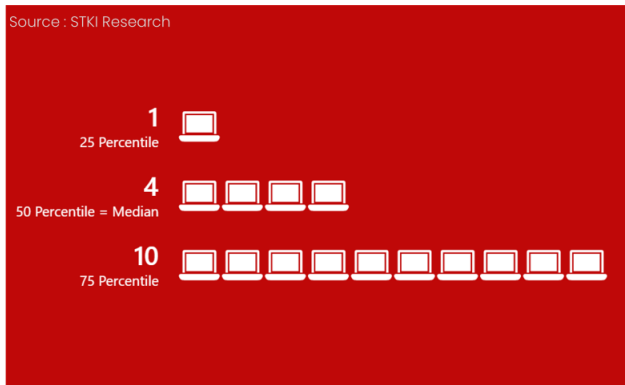
Source : STKI Research



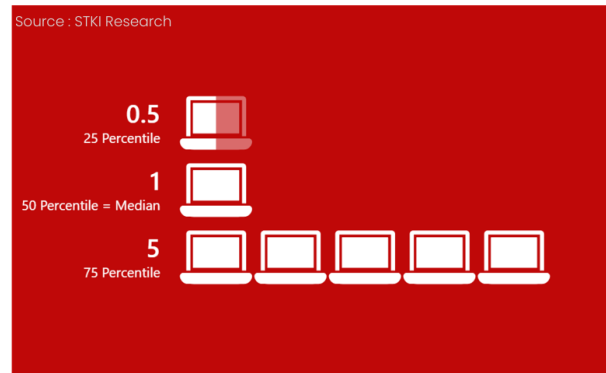
Linux enviroment is more stable than Windows

Linux environments are more stable than Windows in enterprise IT

How many Windows VM are created/modified per week?



How many Linux VMs are created/modified per week?




Linux environment is more stable than Windows

Percent of effort from Linux team dedicated to cyber

Source : STKI Research


5%
25 Percentile



9%
50 Percentile = Median



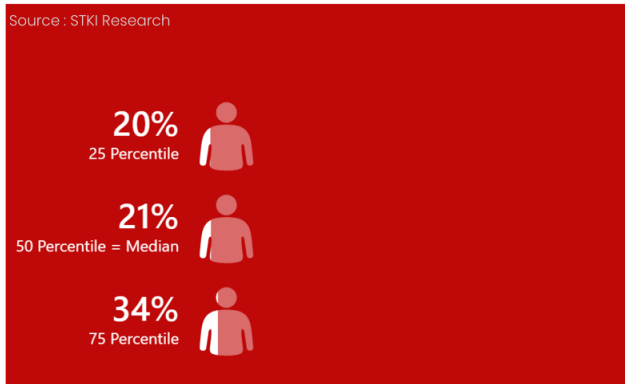
14%
75 Percentile



“Cyber” is defined differently – example – some CIOs consider patches to be part of cyber security, while others may not consider it to be part of cyber security

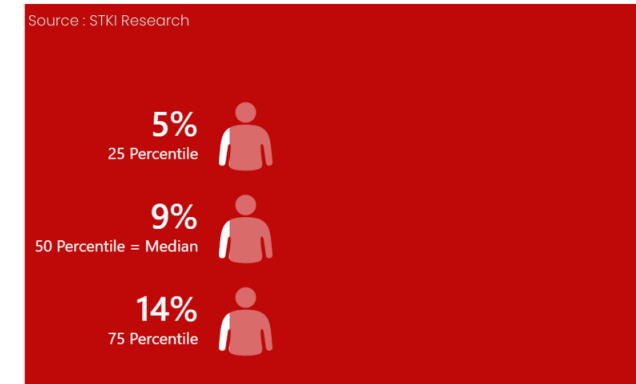
Windows environment require more cyber related effort than Linux environments in Enterprises

What percent from Windows team effort is dedicated to cyber?



“Cyber” is defined differently - example - some CIOs consider patches to be part of cyber security, while others may not consider it to be part of cyber security

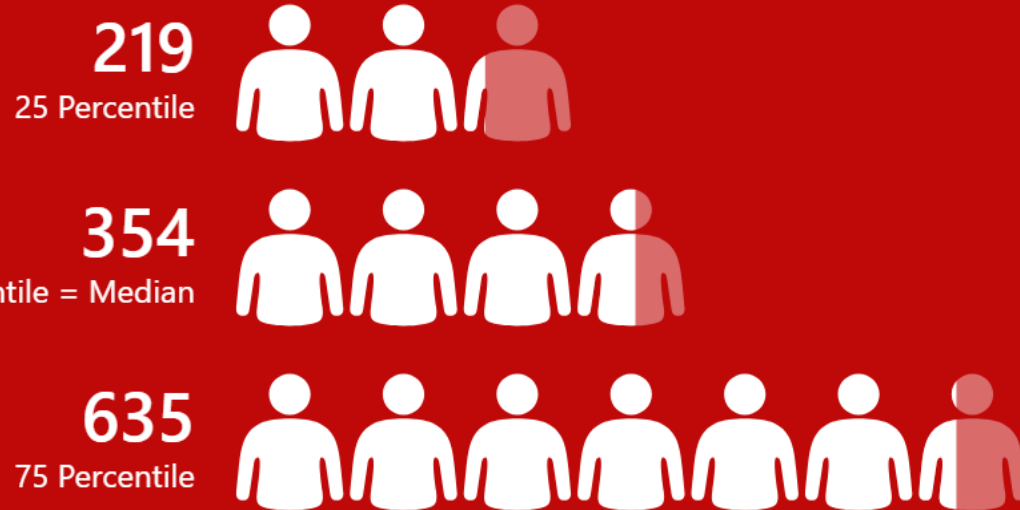
Percent of effort from Linux team dedicated to cyber



“Cyber” is defined differently - example - some CIOs consider patches to be part of cyber security, while others may not consider it to be part of cyber security

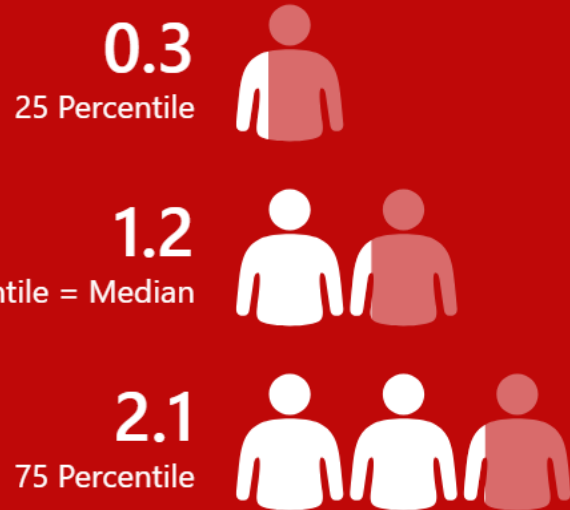
Employees per second level support (PC technicians) staff member

Source : STKI Research



Second level support (PC technicians) per site (location)

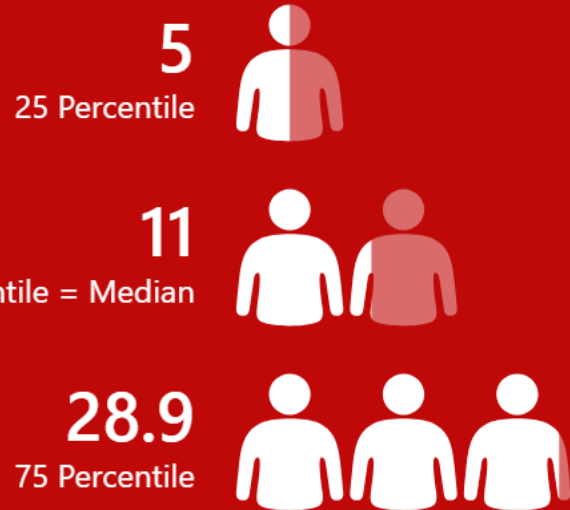
Source : STKI Research



Isolated network are not counted as locations

Employees per site (location) per second level support (PC technicians) staff member

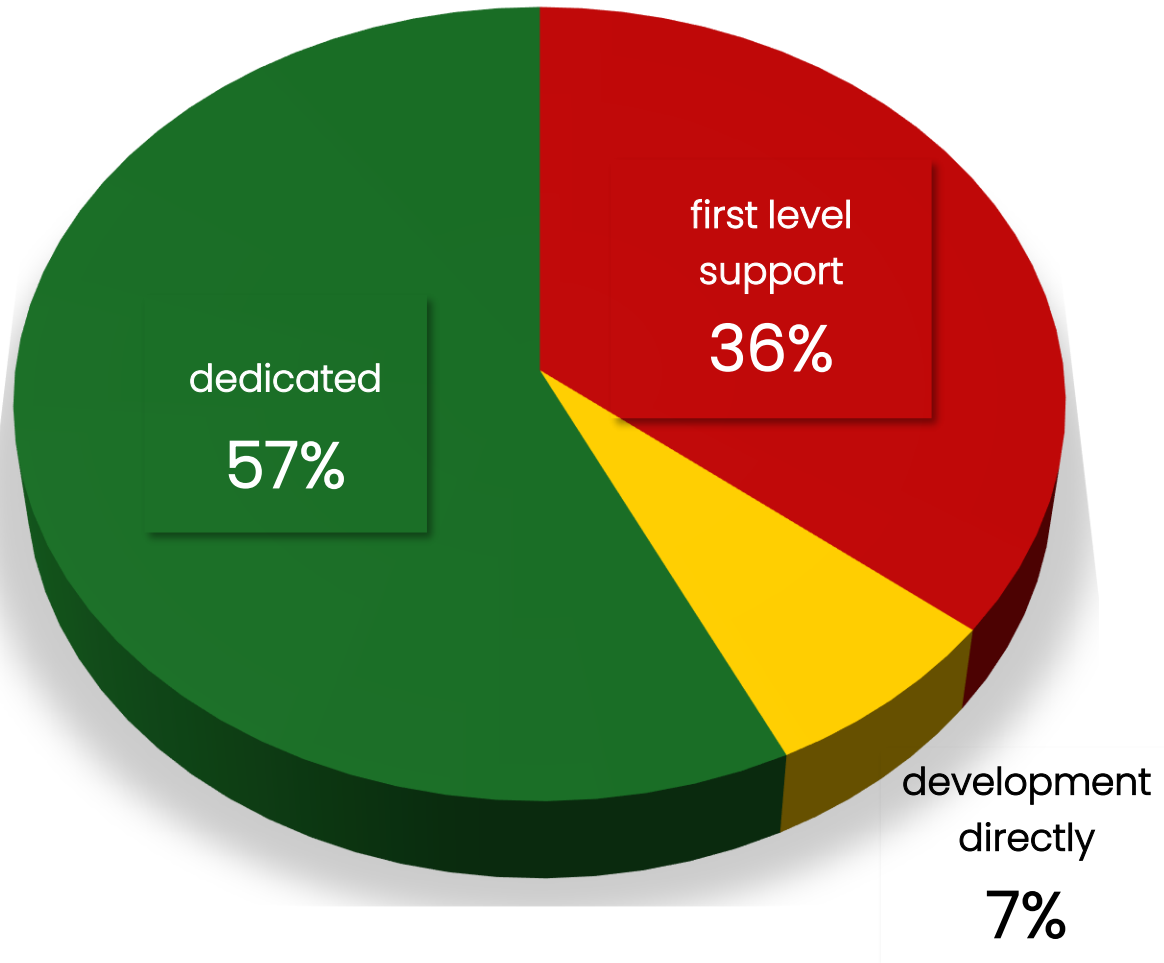
Source : STKI Research



75 Percentile more likely to have thin clients

Isolated network are not counted as locations

Who gets the application related tickets?

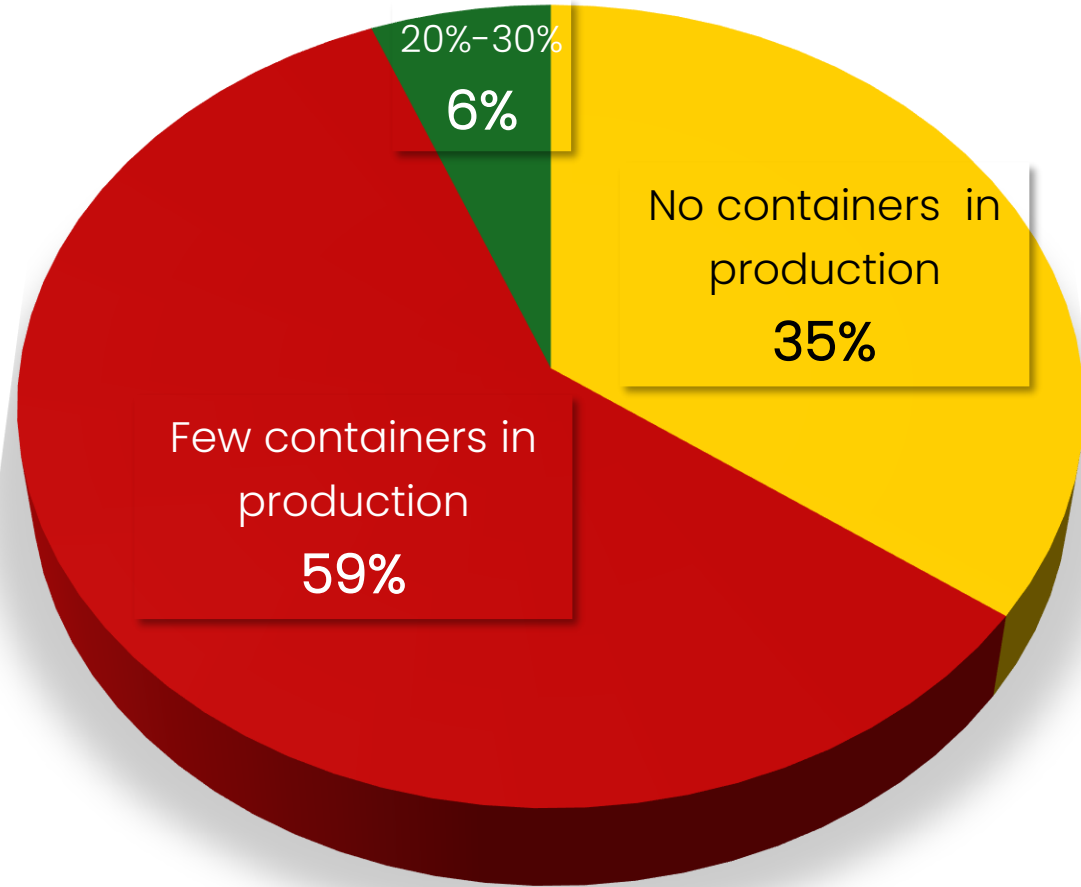


In most cases the first level support will answer all calls

In case the ticket is not solved by the first level support or dedicated team (if exists) it will always go to the development

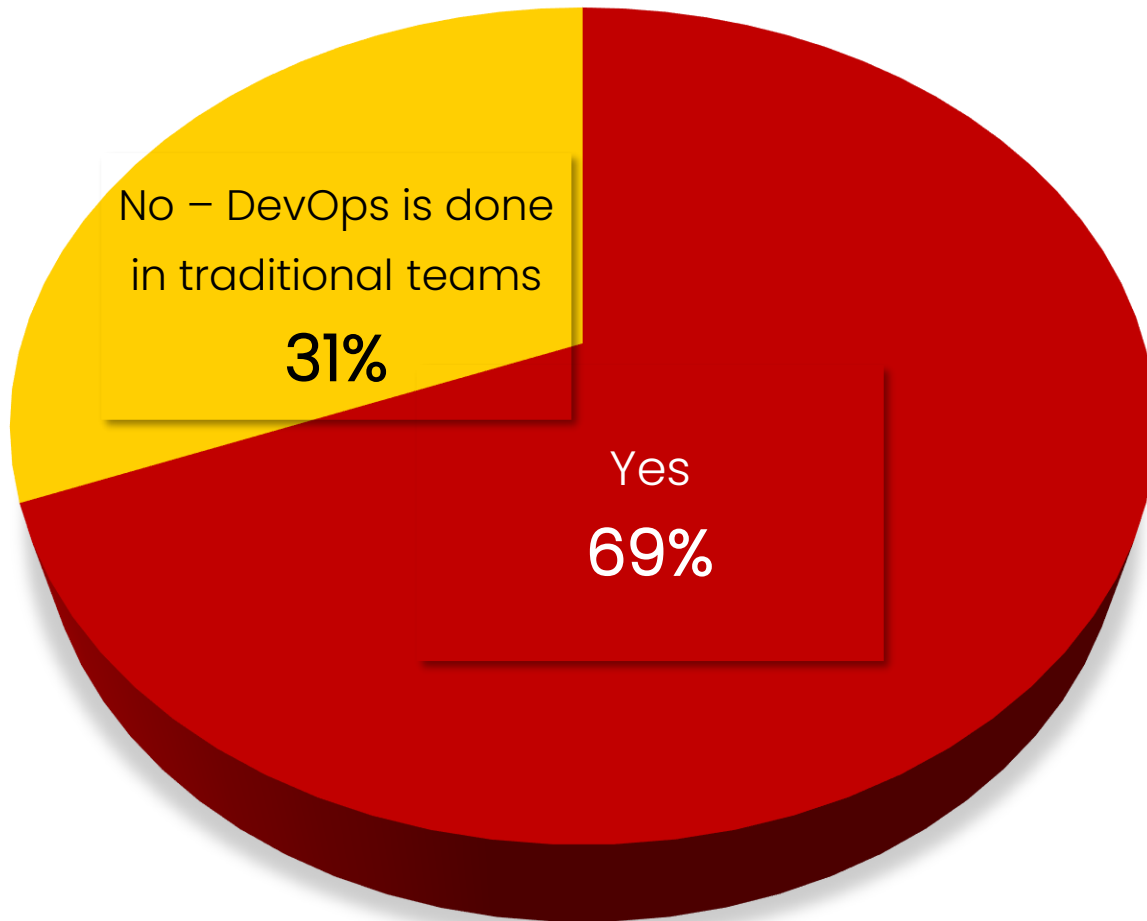
Sometimes the "dedicated application support team" is part of "applications" and of even the business unit and not part of infra-ops

Percent of production system based on containers



OEM (products) based on containers are not included

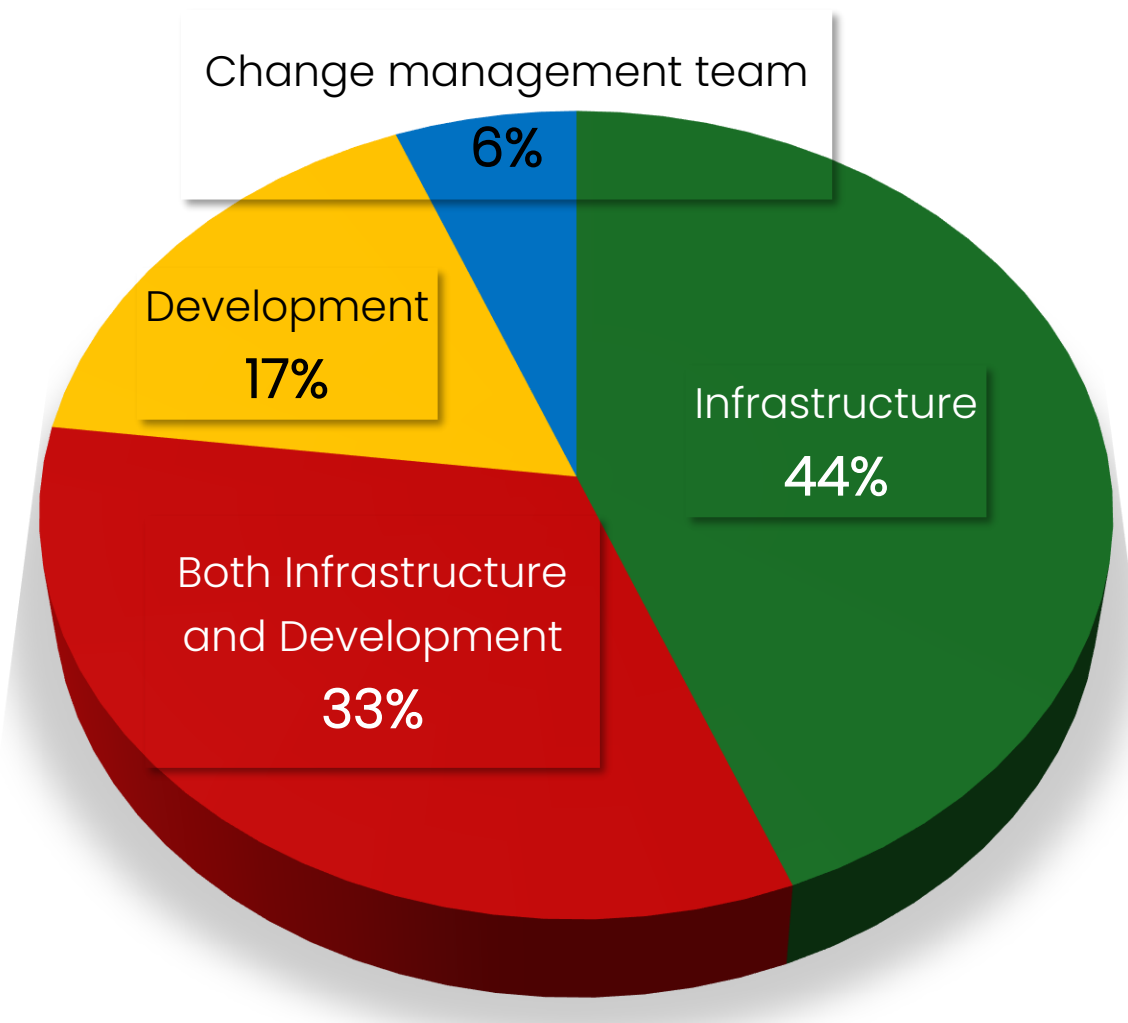
Is there dedicated DevOps team?



Even if DevOps team exist - not all DevOps related effort is done in this team

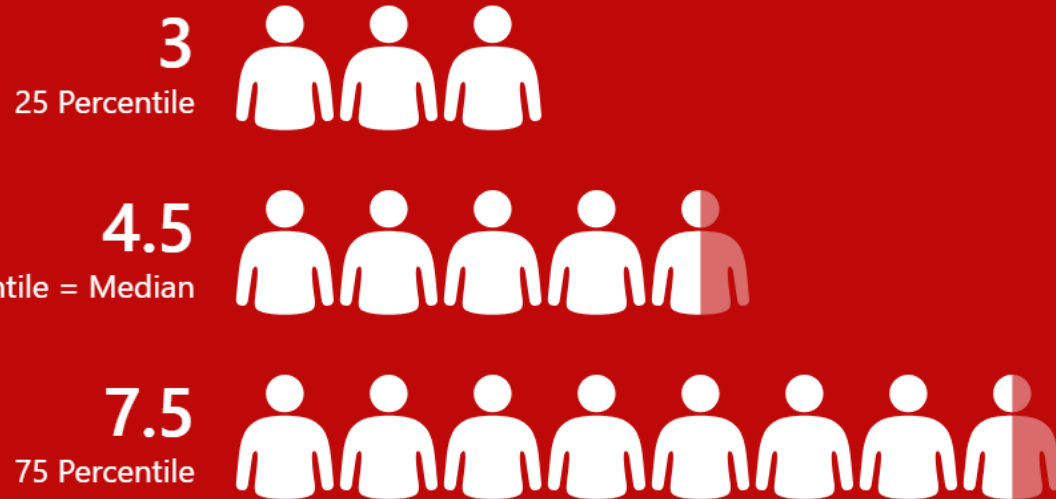
DevOps team reporting structure

New metric



How big is the DevOps team

Source : STKI Research



Devops is "app DevOps" (pipelines),
infra DevOps (IaC) or both
sometimes DevOps is part of "Cloud"

Cloud effort is done in (percent)



Sometimes cloud is part of devops ,
Sometimes devops is part of cloud
Sometimes devops=cloud

Traditional Infrastructure-Ops.-Cyber pre-cloud Organization:



System



Cyber



Storage



Networking



DBA



Monitoring

The Traditional Way

In the cloud, all is done by the same person
(done with Infrastructure as Code IaC - based on landing zones)



Current situation in most enterprises



System

Cyber

Storage

Networking

Cloud

“completely different technologies” (example containers)

“the skills are so different”

“out core teams are so busy they can not handle more things”

“we outsource this part”



This is wrong because



System

Cyber

Storage

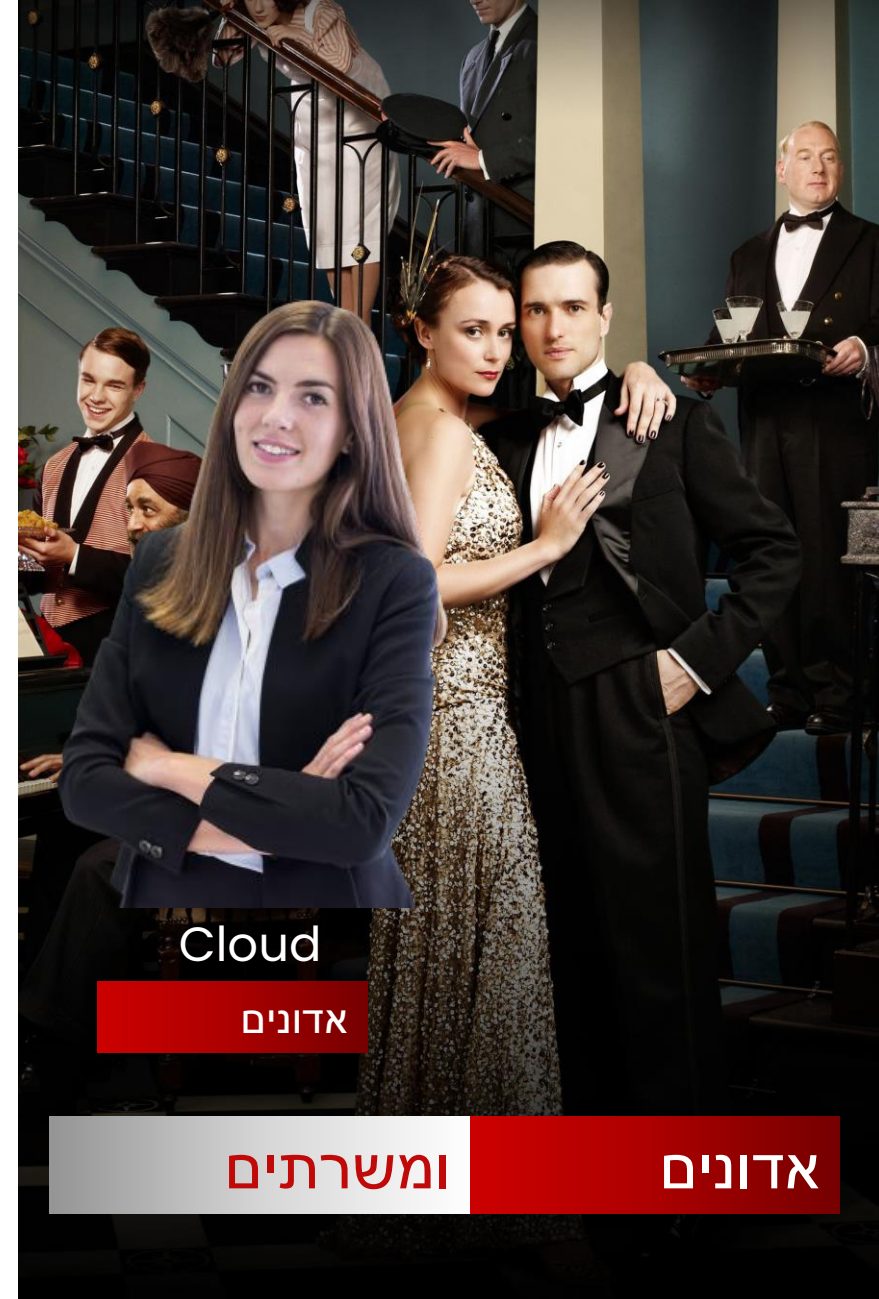
Networking

ומשרתים

ומשרתים

ומשרתים

ומשרתים



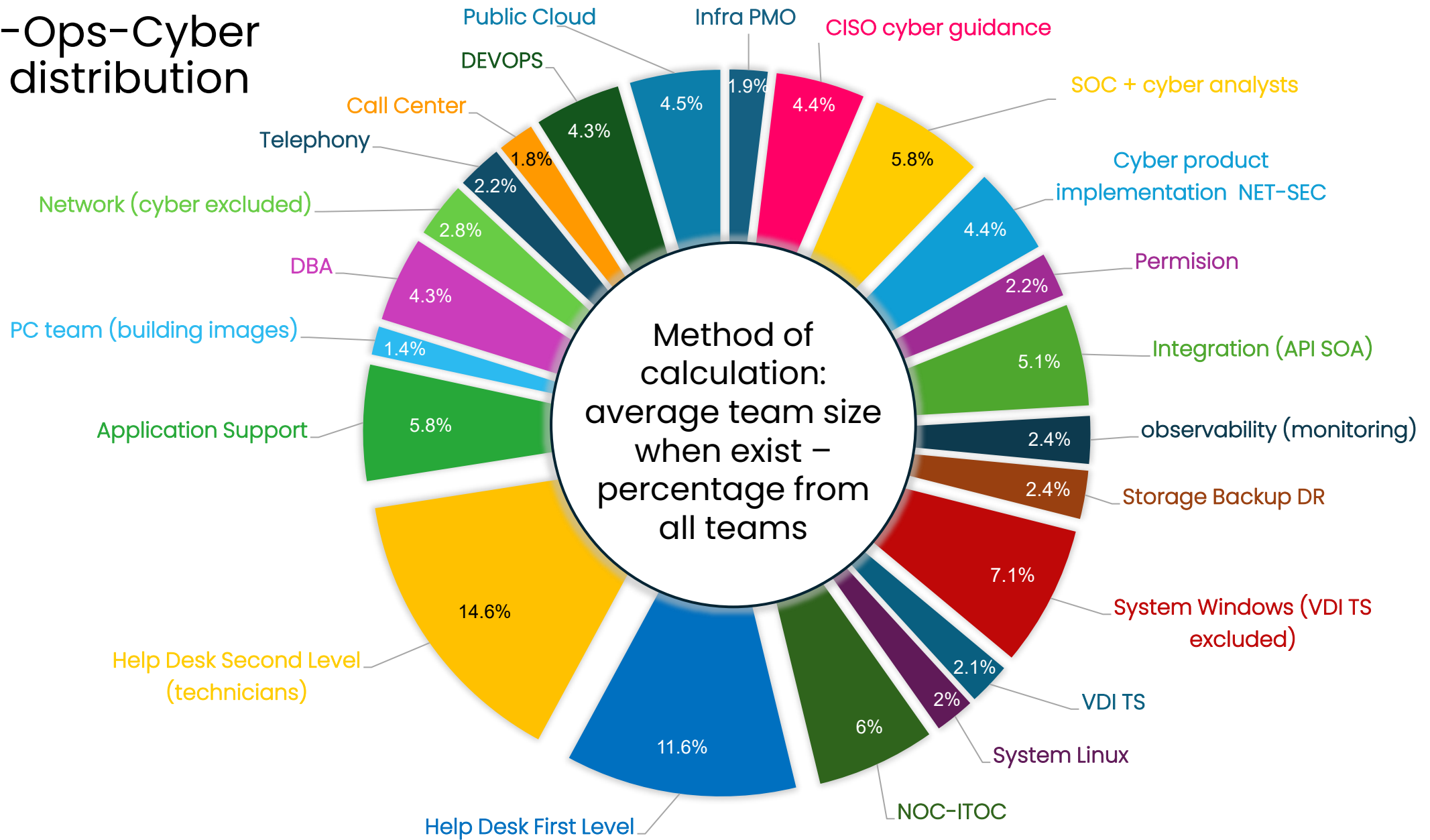
Cloud

אדונים

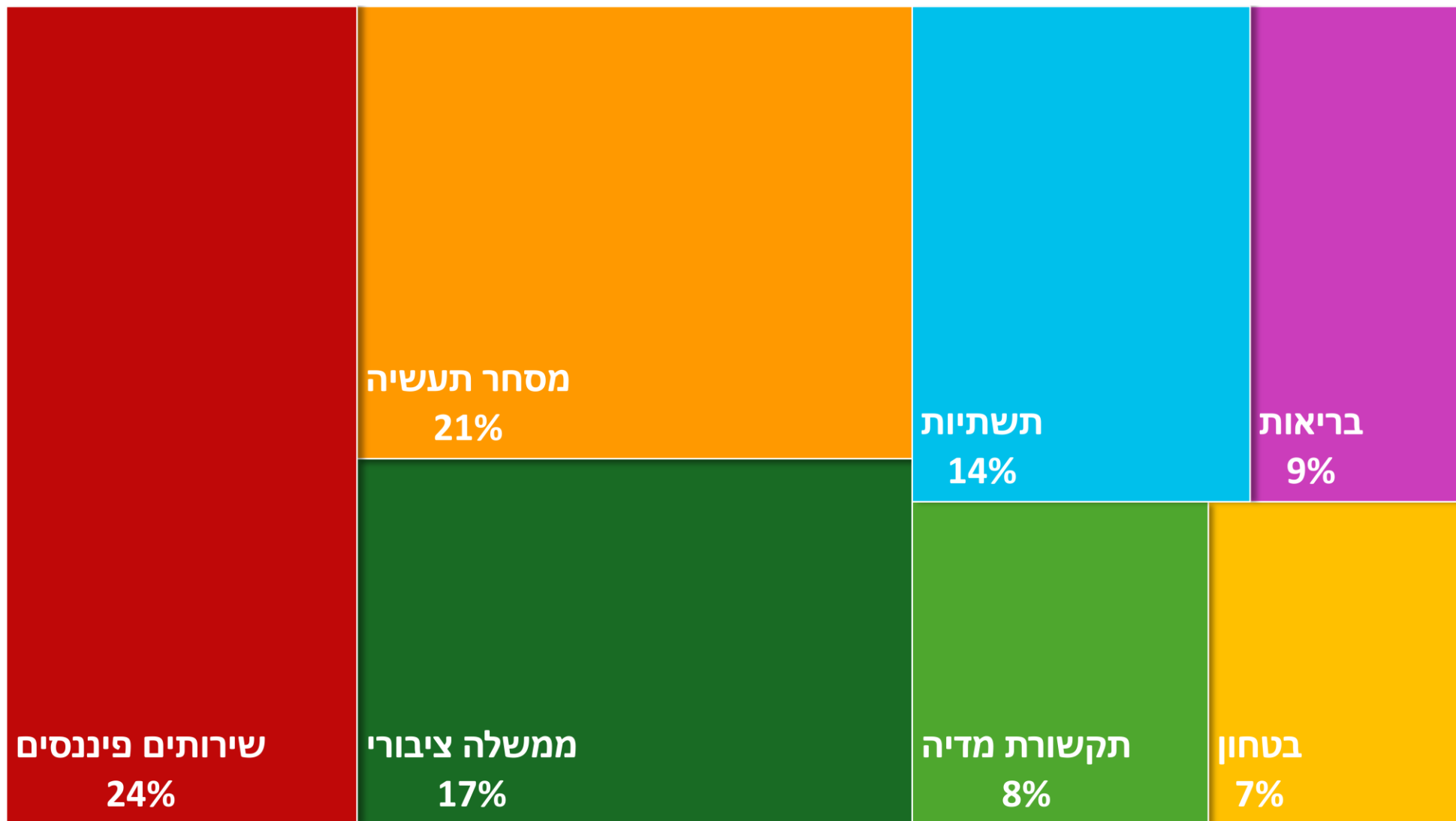
ומשרתים

אדונים

Infra-Ops-Cyber staff distribution



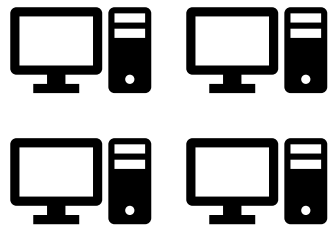
SURVEY DEMOGRAPHICS



Final word : How will the next (cloud based) research look like?

In the cloud, fully IaC (Infrastructure as Code, auto scale is prevalent,) what important is # of layers, component types and not # of components taken care (#of servers)

How do you measure the # of component types / layers?



In the cloud – the same level of effort



Please talk to us about new ideas for the staffing research





שיפור תהליכים והתייעלות בתשתיות ה-DC

יום ד' 03.07.24 10:00-13:00

בית STKI, המנים 72 בני ציון

סדר יום:

- הרצאת פתיחה STKI
- הרצאת אורח: כיצד ניתן לחסוך 15% באופן מיידי בתקציב השרתים (AMD ו-Dell Technologies)
- שאלות ותשובות למציגים
- דיון בין משתתפי המפגש ללא נוכחות ספקים בנושאים הבאים:
 - מהם האתגרים הגדולים ביותר בניהול ותפעול סביבות DC?
 - איזה תצורות שרתים מסייעות יותר להורדת עלויות: שרתי BLADE למול פיצות, שרתי AMD למול אינטל וכד'.
 - כיצד ניתן למקסם את התועלת מאוטומציה בכדי לשפר את יעילות העבודה.
 - איזה כלים או תהליכים ניתן לאמץ מסיביבת הענן לסביבת ה-DC
 - מבנה ארגוני עדכני ותהליכי עבודה של צוותי הסיסטם
 - טיפים ורעיונות לשיפור התפעול והורדת עלויות

לקוחות נכבדים,

אחרי שעברנו לענן ונתנו ל-AI לעשות את כל המשימות שלנו (כשאנחנו משחקים מטקות בים...), הגיע הזמן לחזור למציאות שבה 80% יותר מפעולות הארגון מתבצעות ב-DC באמצעות התשתיות המסורתיות - שרתים, אחסון, תקשורת וכד'.

ארגונים מחפשים את הדרך להתייעל ולשפר תהליכים בסביבת ה-DC כי האתגרים של החצים תקציביים, עומס עבודה ומחסור בכ"א גדולים מתמיד.

מפגש שולחן עגול הוא מפגש שבו לקוחות דנים בנושא שנקבע מראש.

למפגש מוזמנים CTO, מנהלי תשתיות, מנהלי סיסטם ומנהלי רכש. נא לא לשלוח יועצים (אלא אם עובדים 100% משרה בארגון)

אסטרטגיות הסבה מ- Power Builder



Pini Cohen
CTO, EVP & Senior Analyst @ STKI

סביבת ה- Power Builder מהווה מרכיב משמעותי בפורטפוליו של חלק לא מבוטל מארגוני ה-IT המובילים בישראל. הסביבה בשלה יוציבה ומספקת את פונקציונליות הנדרשת אולם עקב האכילס בסיטואציה הוא נושא הכ"א שמוביל לפערי ידע והמשך גם לחוסר אפשרות להתקדמות של המערכות ועד למצב של בעיות זמינות. מפגש שולחן עגול הוא מפגש של לקוחות אשר דנים בנושא אשר נקבע מראש.

סדר יום למפגש:

הרצאת פתיחה STKI

הרצאת אורח - יאיר שייב ONE - מיגרציה של מערכות Power Builder הלכה למעשה שאלות ותשובות

דיון בין משתתפי המפגש בנושאים הבאים (ללא השתתפות ספקים-המציגים):

- מה האתגרים הטכנולוגיים והתפעוליים בהמשך הפעלת מערכות מבוססות PB?
- באיזה מקרים ניתן להכשיר אנשים לעבודה ב-PB?
- כיצד ניתן להעביר את הידע הטמון במערכות PB הותיקות למערכות חדשות?
- מה הניסיון הנצבר מהסבת מערכות PB?
- האם ניתן לבצע את פרויקט ההסבה באופן הדרגתי?

למפגש מוזמנים:

למפגש מוזמנים מנהלי פיתוח, CIO, PMO, CTO

המפגש מיועד ללקוחות STKI USERS (לא ספקים), נא לא לשלוח יועצים, אלא אם הם עובדים 100% מזמנם בארגון.

22.07.24
10:00 - 13:00

משרדי STKI
המנים 3 בני ציון



Thank you

