STKI Analysis of Cybersecurity Staffing Ratios and Tool Implementation in Israeli High-Tech Sector

Commissioned by aidoc

Pini Cohen
CTO, EVP, STKI
https://www.linkedin.com/in/pinicohen/
pini@stki.info

Table of Contents

Part 1: Staffing ratios

Part 1
Among the factors that influence the cyber security effort:

- Was the company (or its managers) hit by cyber attack before?
- Industry
- International presence (localization – regulations – local sites)
- Mobile vs. Web vs. both
- Consumer vs. B2B
- Sensitive Data
- On premise vs. Cloud single tenant vs. Cloud multi tenants

STKI.INFO

Cyber personal: "Who handles cybersecurity in the organization?"

- Dedicated cyber personal in cyber team Examples: Analyst in SEC Ops team
- Dedicated cyber personal in “none cyber team” Example: DevSecOps engineer, part of DevOps team
- Not Dedicated cyber personal doing “cyber job” (example FW). Other organizations might have dedicated cyber personal for this job
- Cyber effort that is part of other job. Example – “secure development” is part of the developer's responsibility

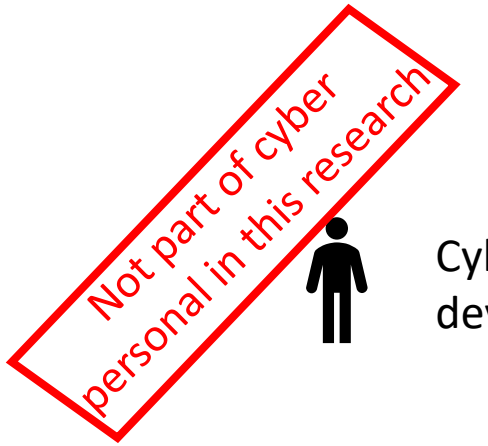
STKI.INFO

Cyber personal: "Who handles cybersecurity in the organization?"

Dedicated cyber personal in cyber team Examples: Analyst in SEC Ops team

Dedicated cyber personal in “none cyber team” Example: DevSecOps engineer, part of DevOps team

Not Dedicated cyber personal doing “cyber job” (example FW). Other organizations might have dedicated cyber personal for this job



Cyber effort that is part of other job. Example – “secure development” is part of the developer's responsibility

In this part the participants were asked (for example)

How many developers are in the company?

How many app sec personal are in the company (in FTE Full Time Employee) ?

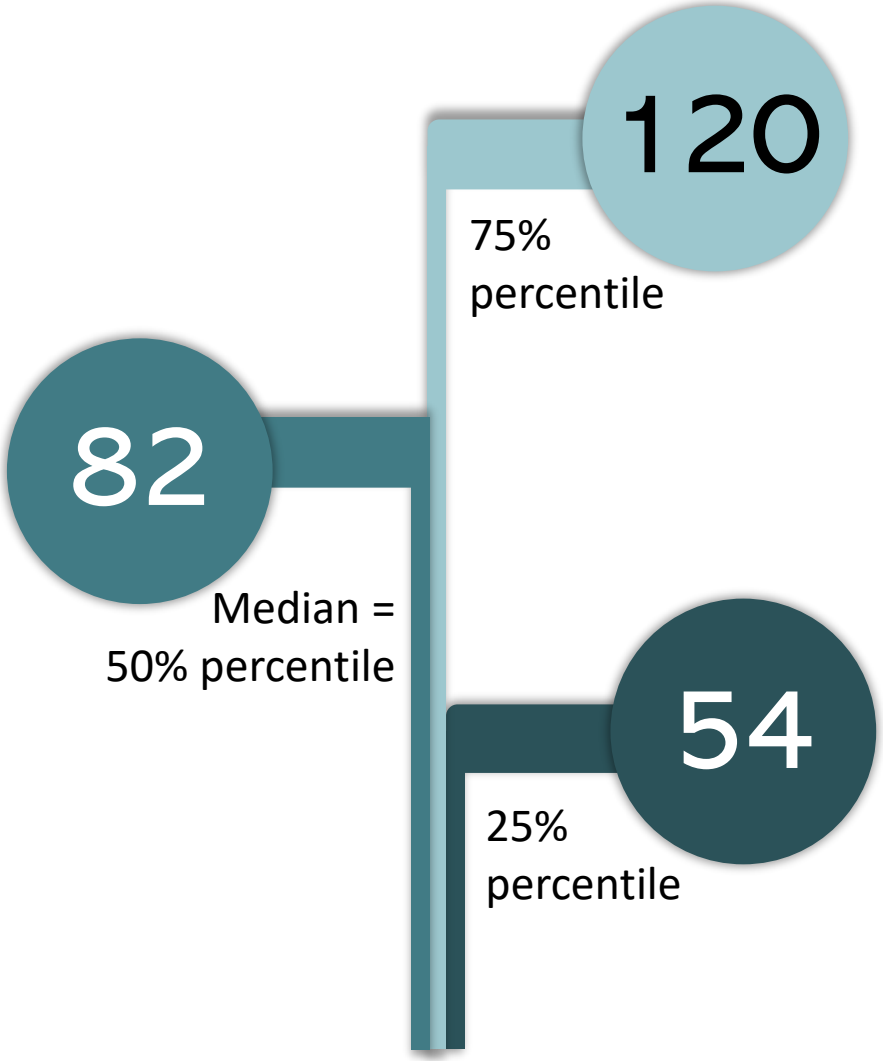
And the metric we've calculated here is: Developers / App Sec personal

Executive summary: Survey Ratios (Median)

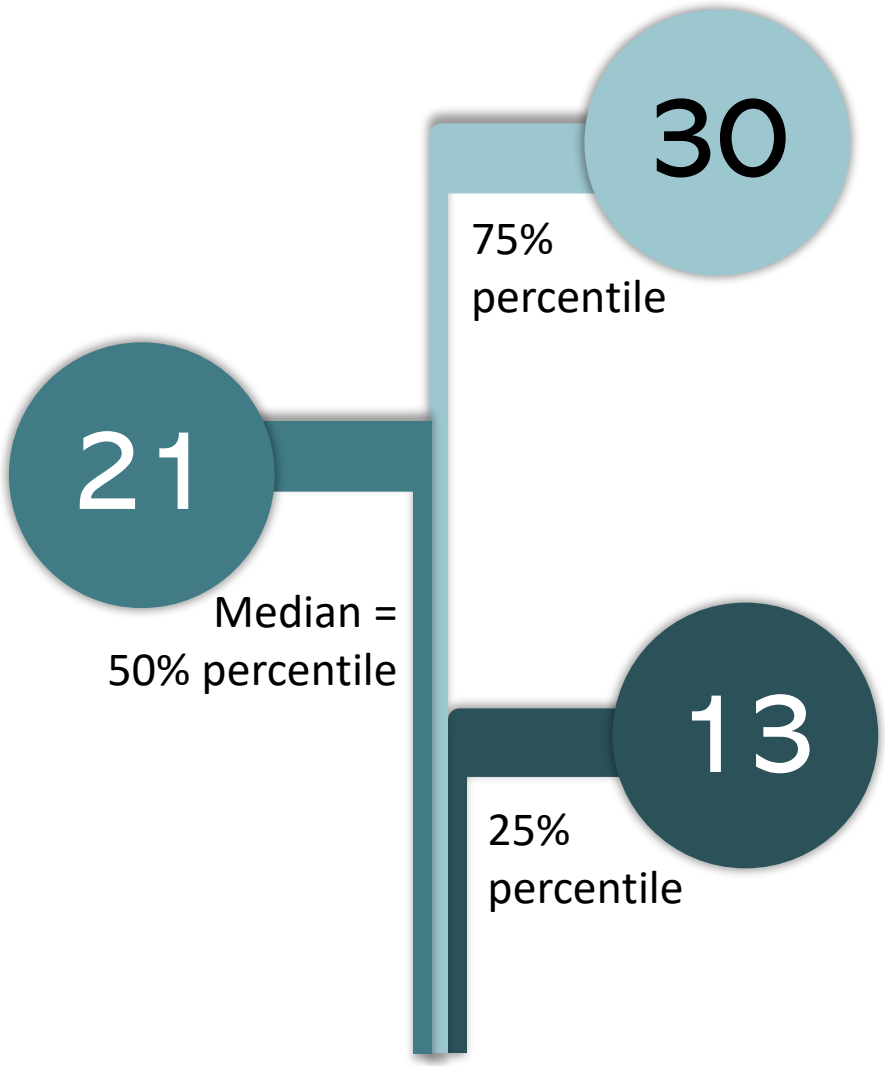
Employees	Per total Cyber Personal is 82
Developers	Per total cyber personal is 21
Employees	Per CISO team member is 302
Sec Ops 0 to 1 FTE	(Full Time Employee)
Employees	Per IT security member is 500 (cloud companies)
Employees	Per APP SEC member is 450
Developers	Per APP SEC member is 125
Employees	Per (Cloud Sec + DevSecOps) (cloud companies): 263
Developers	Per (Cloud Sec + DevSecOps) (cloud companies) : 75

STKI.INFO

Employees / total Cyber Personal



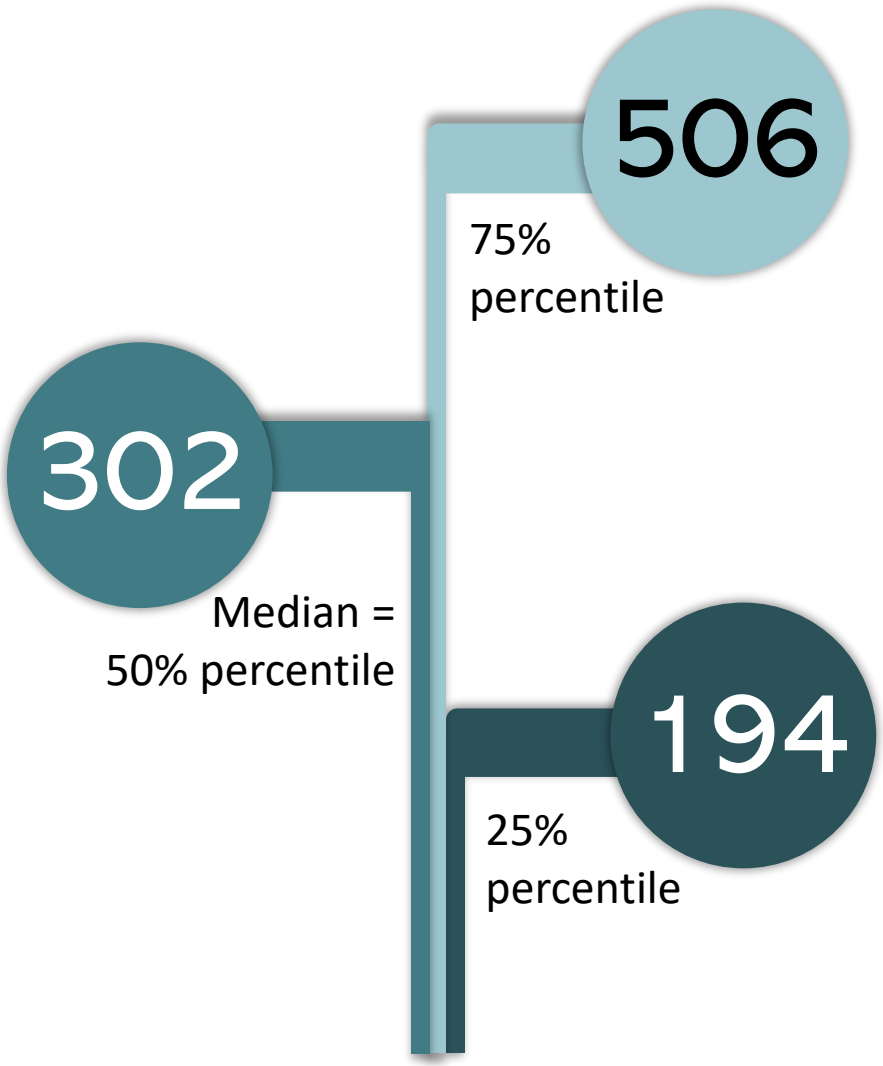
Developers / total cyber personal



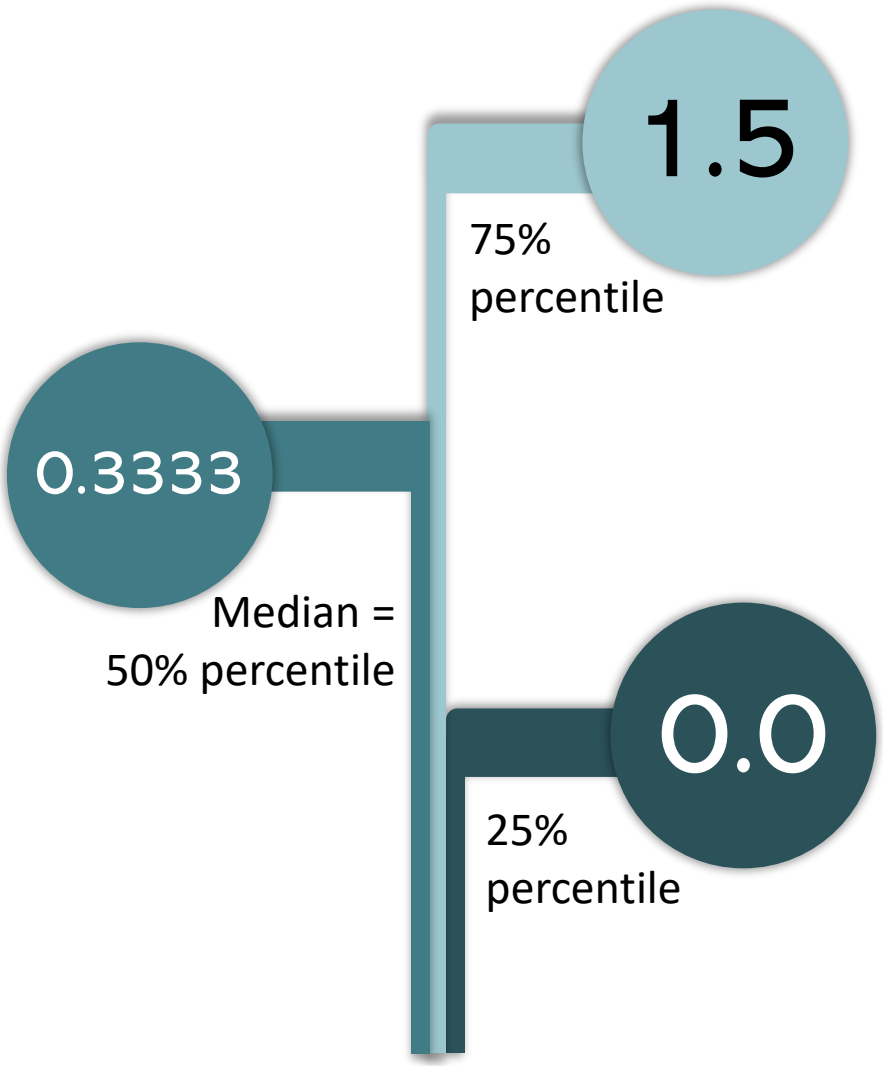
Employees / CISO team

including regulations, architecture, PT, Awareness

Not including DPO

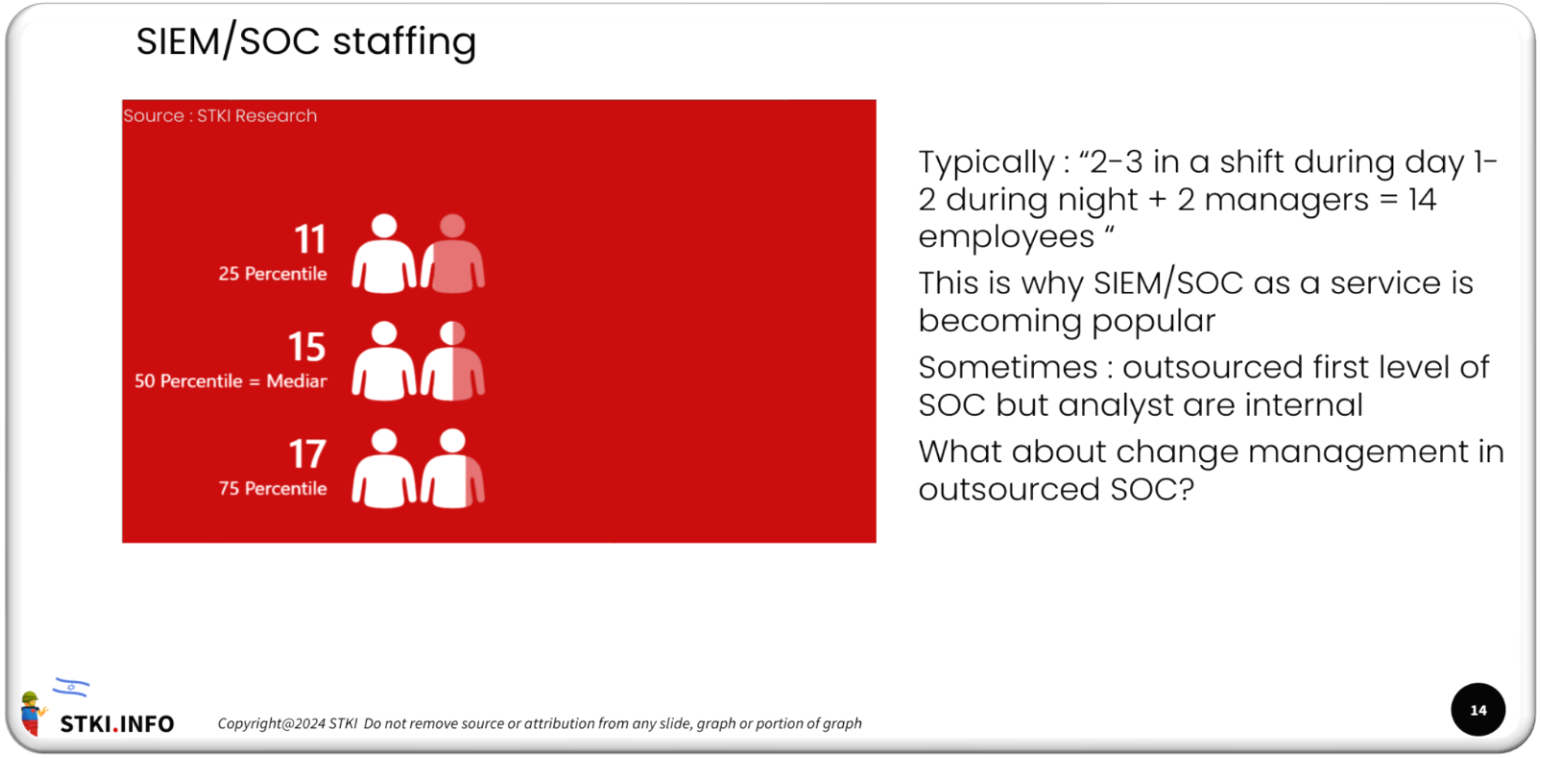


SOC operations FTE (Full Time Employees) for cloud companies



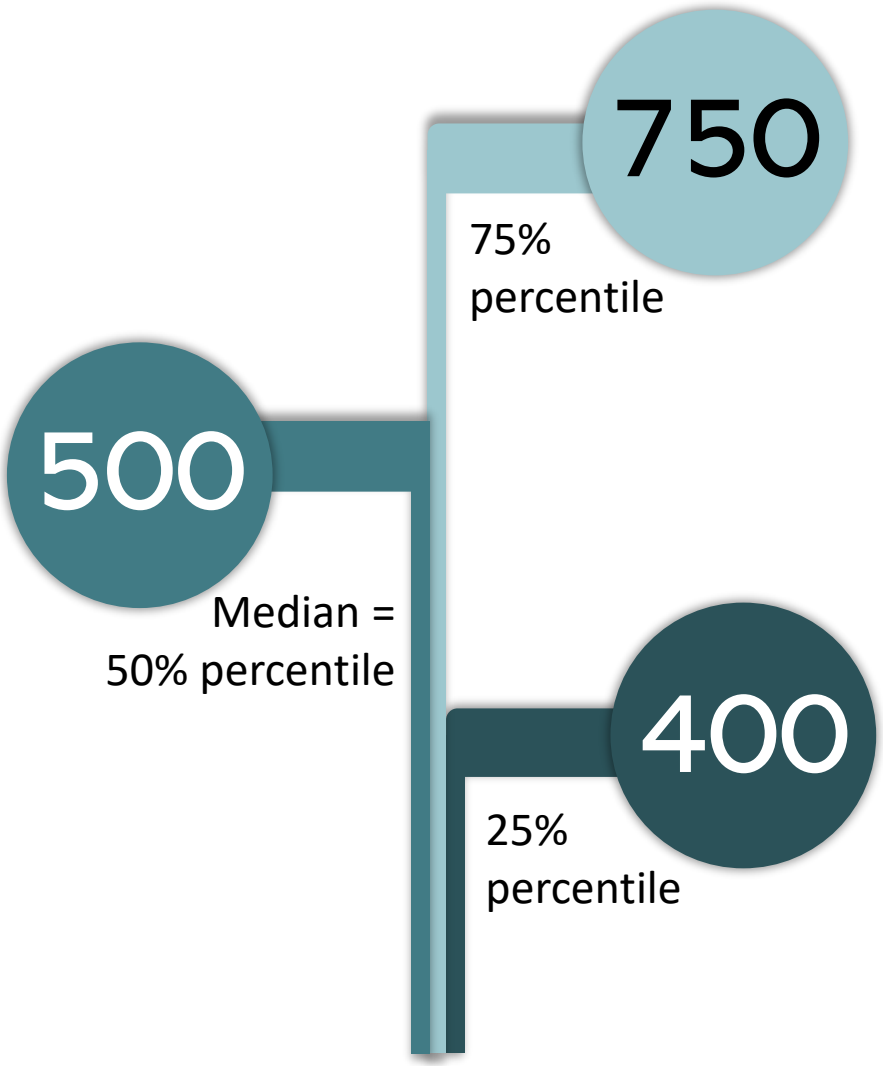
Many organization use MSP for SIEM\SOC

Big difference from SIEM/SOC in the STKI staffing report for enterprises:

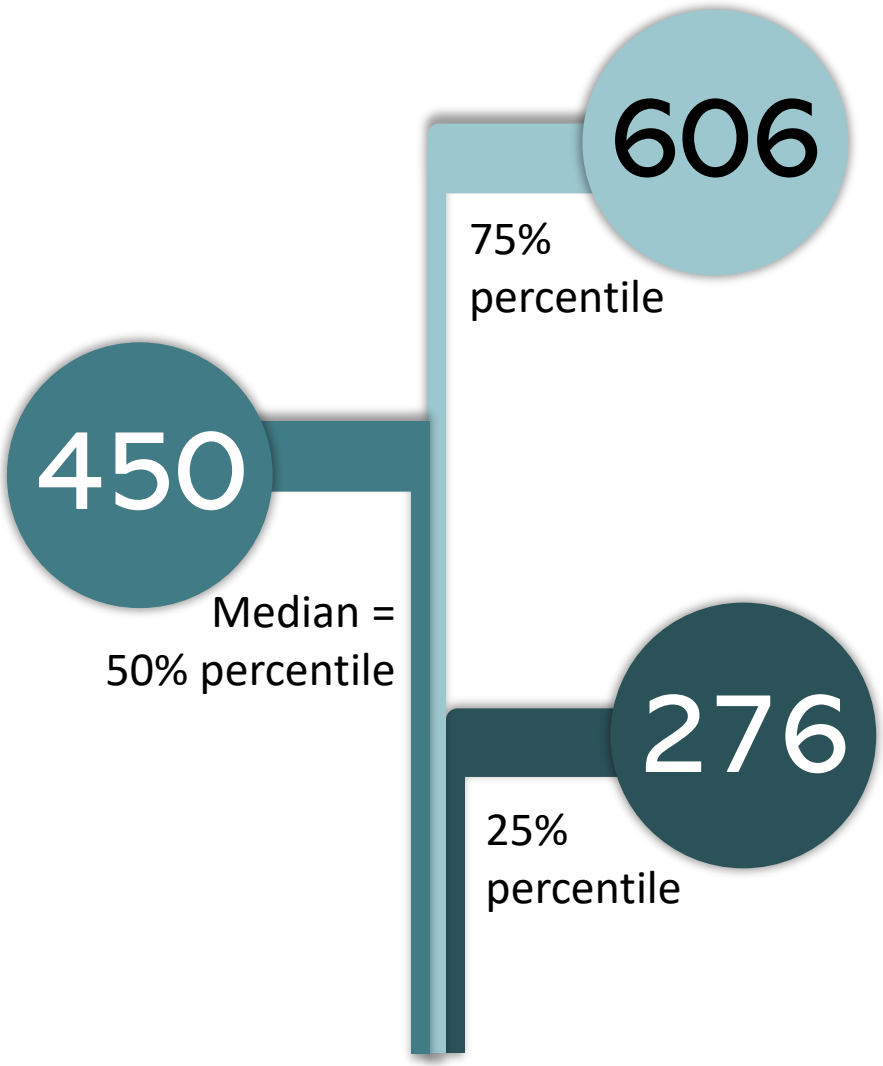


Source: STKI https://www.stki.info/_files/ugd/0b88a6_537d843d77ec423c9c46fdfde7d0436f.pdf

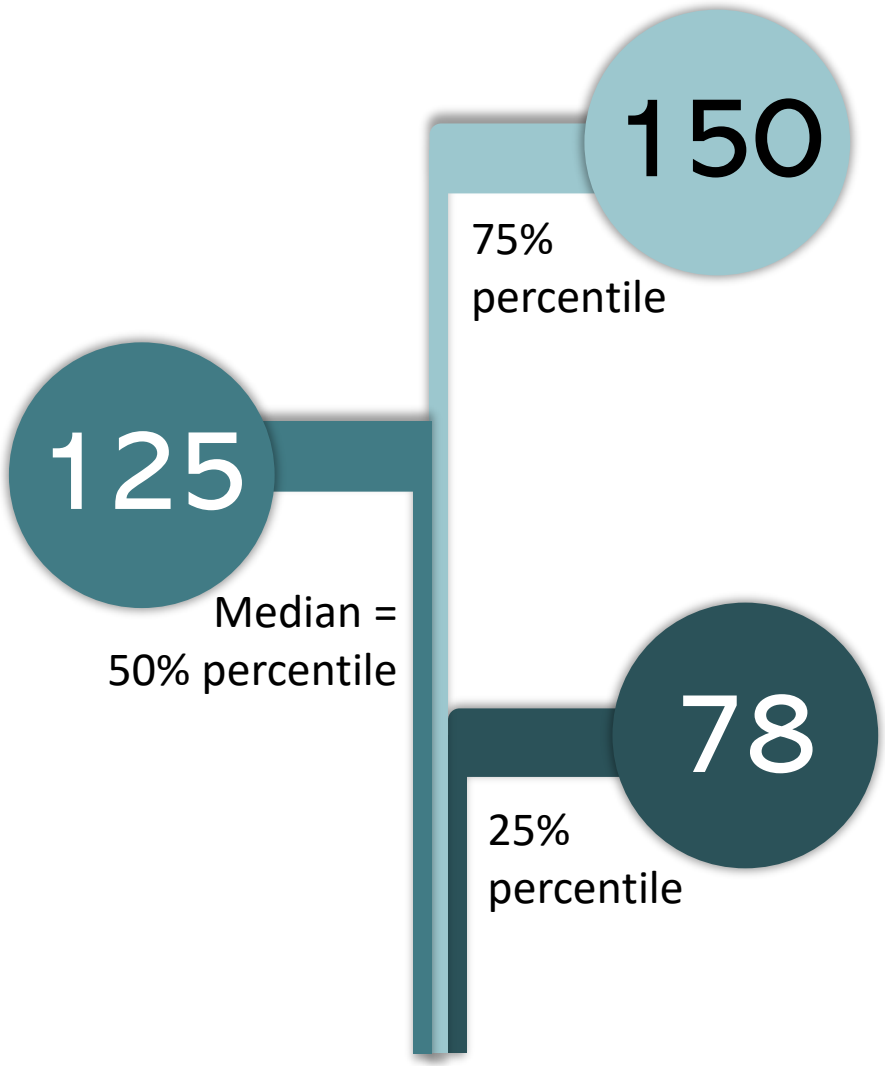
Employees / IT security Team for cloud companies



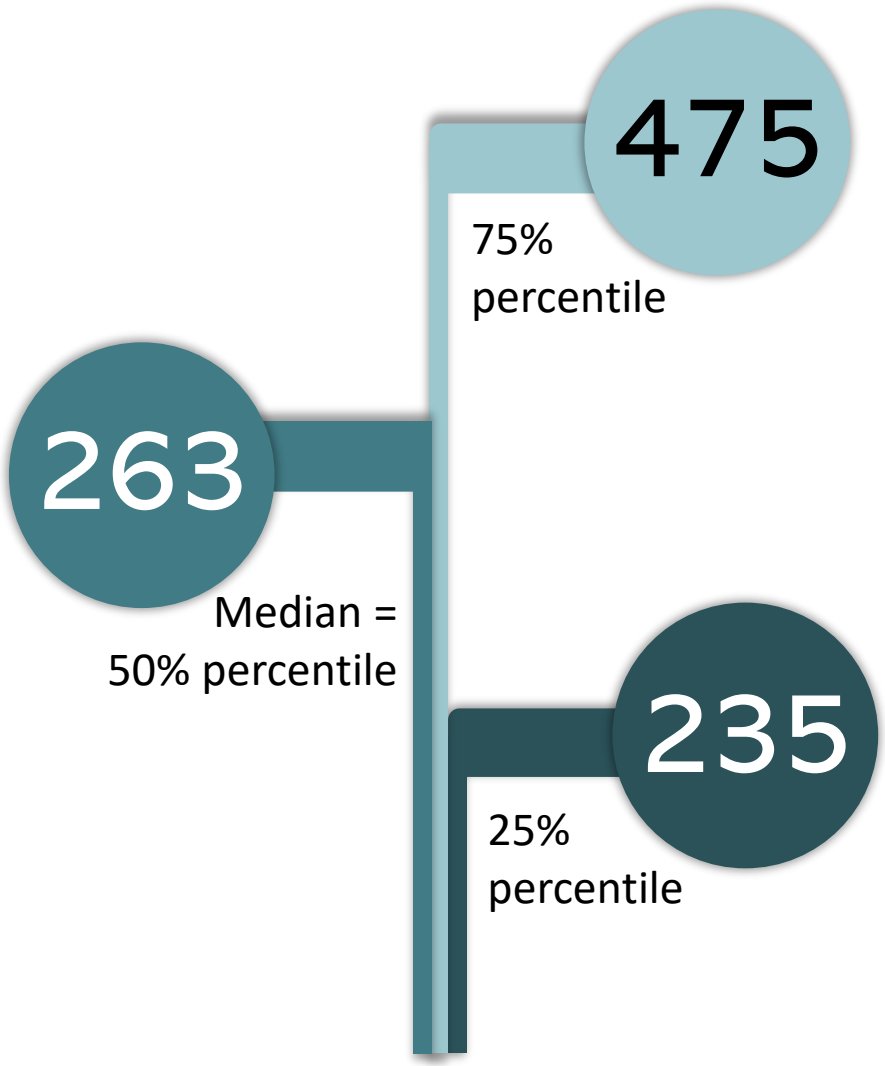
Employees / APP SEC personal



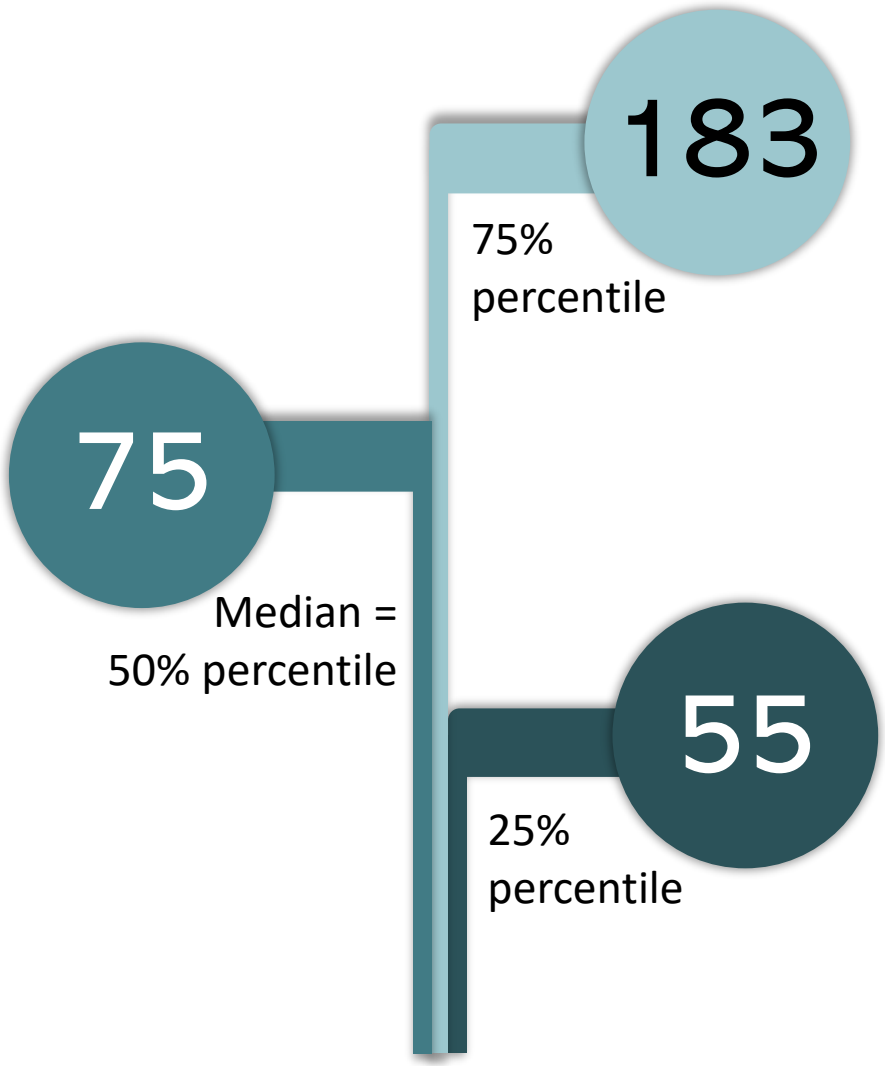
Developers / APP SEC personal



Employees / Cloud Sec + DevSecOps (for cloud companies)



Developers / Cloud Sec + DevSecOps (for cloud companies)



Developers’ effort for cybersecurity (SDLC) is between 5% and 10% for total development effort

DevOps effort for cybersecurity is between 15% and 25% of total DevOps effort

IT effort for cybersecurity is between 10% and 20% of total IT effort

Security Architecture

In all small-medium companies the CICO is responsible for security architecture (of product and IT)

For bigger companies product security architects and/or IT security architects might be part of R&D or IT (hence the CISO org. will be smaller)

Security Sales Enablement team (or InfoSec)

A "security sales enablement" team empowers sales professionals with the knowledge, tools, and content necessary to effectively communicate a company's cybersecurity posture and address potential customers' data safety concerns.

Only in large companies

Large variety of in effort in this field – many (large) company do not have this team but when exist it might be big team

In this research “Security Sales Enablement” is considered part of CISO but it might also report to others

DPO is not part of CISO

In most cases it will be part of the Legal Department

Miscellanies

- In some small companies IT is reporting to the CISO
- In small – medium companies PT outsourced and is managed by the CISO
- In large companies there might be dedicated PT team and/or PT personal that manages the outsourced PT. They might be part of R&D (and not part of CISO)
- DevSecOps might report to CISO and might report to R&D
- APPSEC might report to CISO and might report to R&D
- Cyber security in R&D is :
  - Cloud security (build the cloud so it is secure)
  - DevSecOps (secure pipelines)
  - App Sec (code security)

The most significant trend is AI (by CISO's):

- Secure usage of AI
- Protect the organization from AI attacks
- How to use AI in the "day to day" work?

The most significant Usage of AI is in the SIEM SOC

- Reduce / Replace the first level in soc operations
- Replace totally the SOC ?

Other trends

- Application Security
- New generation of DLP (based on AI)
- Password-less access
- Browser security
- Risk based vulnerability
- Product consolidation (platforms)

Part 2: Products Usage and vendors in Israeli High-Tech companies

In this part the participants were asked for each product category:

Do you use a product in this category?

In your perspective, who is the market leader in Israel in this category and who follows?

Even if the participant is not using a tool in this category

Categories are:

EDR	App Sec	File sharing
Secure Browsing	Email Security	SOAR
CSPM	DNS security	NHI
Threat Intelligence	SASE / SSE	Awareness tools
Vulnerability Management	Device management	Compliance assistance
SIEM	IDP	Third party risk management

All users have EDR

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for EDR tools

CrowdStrike is leading the pack with significant lead

SentinelOne and Microsoft Defender

PaloAlto Cortex

Israel High-tech market Browser Security

	Using dedicated tool	Not using dedicated tool
All organizations:	**60 %**	**40%**
Larger organizations:	**50 %**	**50%**

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for

Browser Security Tools

PaloAlto is leading the pack followed by Island

Seraphic and LayerX

All users have CSPM Cloud Security Posture Management

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for CSPM

According to the survey results, Google Wiz is the clear leader, significantly ahead of the competition

Orca and Palo Alto Networks follow in the next tier

Upwind and Cloudwize positioned behind

Crowdstrike rounds out this ranking

Israel High-tech market Threat Intelligence

All organizations:		
No	Service	Product
22 %	29%	49%

Larger organizations:		
No	Service	Product
2 %	36%	52%

STKI.INFO

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for Thread Intelligence tools and services

According to the survey results, Recorded Future is the leader

CyberInt (by Checkpoint)

Kela

Mediant (by google)

Luminar (by Cognyte), ClearSky, Digital Shadows, Crowdstrieke, IntSights (Rapid7) sharing the same positioning

Israel High-tech market dedicated Vulnerability Management tools

	Using dedicated product	Not using dedicated product
All organizations:	**62 %**	**38%**
Larger organizations:	**60 %**	**40%**

Companies with no “dedicated vulnerability management” product are using CSPM or EDR, etc.

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for

Vulnerability Management tools

According to the survey results, Tenable (Nesses Vulcan) is the leader

Google (Wiz) if following

Orca Acunetix Palo Qualys Crowdstrike Rapid7 Pentera sharing the same positioning

Israel Hightech market DLP

All organizations:

Not using
44 %

Using
28%

Partly
28%

Larger organizations:

Not using
41 %

Using
59%

Quit a few negative responses on DLP adoption

STKI.INFO

Israel Hightech market SIEM tool

All organizations use SIEM tool

All organizations:

Owned by organization

95 %

owned by soc provider (as a service)

5%

Israel High-tech market SOC strategy

All organizations:

SOC is Operated by org

39 %

SOC is Operated by MSP

16%

SOC is Operated by org with MSP

45%

Larger organizations:

SOC is Operated by org

61 %

SOC is Operated by org with MSP

39%

STKI.INFO

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for SIEM tools

According to the survey results, Cisco (Splunk) is the clear leader

Microsoft, PaloAlto (inc. Qradar) and Elastic

Crowdstrike, Google Sumologic

And closing the ranking are Datadog, Rapid7 and Exabeam

Israel Hightech market SOC service (MSP) mentioned

Trustnet Citadel 2Bsecure WeAnkor

Other MSP mentioned:

Bezeqint , Qmasters

Israel Hightech AppSEC

All use APP SEC tools

DAST is the less used while SAST and Component CSA are the most used

Container security is also considered as part of APP SEC

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Application Security Vendors (all types of tools - SAST DAST SCA, etc):

According to the survey results, Checkmarx, Snyk and Synopsys are the leaders

Google Wiz, Arnica, PaloAlto and OX Security

Then lots of other tools including Coverity (Synopsys) , Github, Veracode, Mend, JFrog, Bright, Oligo, Backslash and SonarQube

Israel Hightech Email Security dedicated tools

All organizations:	Using dedicated tool	Not using
	93 %	7%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Dedicated email security tools

According to the survey results, Fortinet (Perception Point) is the leader, with small edge over Proofpoint.

Cisco, Checkpoint and Abnormal

Forcepoint, Ironscales and PaloAlto

Israel High-tech Email DNS security

All organizations:

Using

47 %

Not using

53%

Larger organizations:

Using

58 %

Not using

42%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for

DNS security

According to the survey results, Cisco is the clear leader

Cloudflare

ThreatStop and PaloAlto

All users utilize VPN, ZTNA or SASE/SSE

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for **ZTNA and SASE/SSE services**

According to the survey results, Cato is the clear leader

PaloAlto

Zscaler

Cloudflare

Netskope

Cisco

Checkpoint (Perimeter81) and Fortinet

Israel High-tech market Device management - All have

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Device Management tools:

According to the survey results, results Microsoft Intune is the leader

Kandji (for Macs)

by Jam f (for Mac) and JumpCloud (for both Mac and PC)

Israel Hightech market IDP Identity Provider - All have

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for IDP (Identity Provider Services)

According to the survey results, Okta is the clear leader

Microsoft EntraID

OneLogin and Google

Israel Hightech market SOAR tools

All organizations:	Using	Not using
	69 %	31%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for SOAR tools

According to the survey results, Torq is the clear leader

PaloAlto (Demisto)

Tines

Splunk, Google, Crowdstrke and BlinkOps that share the same positioning.

Israel Hightech market Honeypots (deception) tools

All organizations:

Using

19 %

Not using

81%

Larger organizations:

Using

25 %

Not using

75%

Some users utilize open source solutions

Israel Hightech market Secure file sharing tools

All organizations:	Using	Not
	87 %	13%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for File Sharing services:

According to the survey results, Google (drive) and Box are the clear leaders

Microsoft (Onedrive) and Kiteworks

DocuSign, Egnyte, Dropbox and GoAnywhere that share the same positioning

Israel Hightech market NHI Non Human Identities tools

All organizations:

Using **31 %**

Not using **69%**

Larger organizations:

Using **39 %**

Not using **61%**

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for **NHI**

Non Human Identities

Astrix Security , Clutch

Axonius Silverfort, Oasis, and Okta

ALL

Israel High-tech market use Employee Awareness Tools or Services

STKI.INFO

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative positioning for

Employee Awareness tools & services

According to the survey results, KnowBe4 is clear leader

Dcoya (Ninjio) and Ironscales, Consienta, Wizer and Riot that share the same positioning.

Hoxhunt

ALL

Israel High-tech market use Password Management tools or Services

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Password Management tools

1Password

According to the survey results, 1Password is the clear leader

LastPass

Keeper

IBM (Hashicorp)

Bitwarden

Cyberark

Israel Hightech market Compliance Automation

All organizations:

Using

38 %

Not using

62%

Larger organizations:

Using

22 %

Not using

78%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Cyber Compliance Automation:

DRATA

anecdotes

According to the survey results, Drata and Anecdotes are the clear leaders.

Cypago

Scytale and Vanta that share the same positioning.

Israel Hightech market Third Party Risk Management

All organizations:

Using

62 %

Not using

38%

Larger organizations:

Using

56 %

Not using

44%

Perception survey conducted among couple of dozens CISOs from Israeli high-tech companies to assess the relative

positioning for Third Party Risk Management tools

Panorays

According to the survey results, Panorays is the clear leader

Rescana and BitSight that share the same positioning

Sling Score, Security Scorecard and Commugen that share the same positioning

Part 3 Research Methodology and Participant Demographics

Research Methodology and Participant Demographics

The survey included diverse participants from various industries.

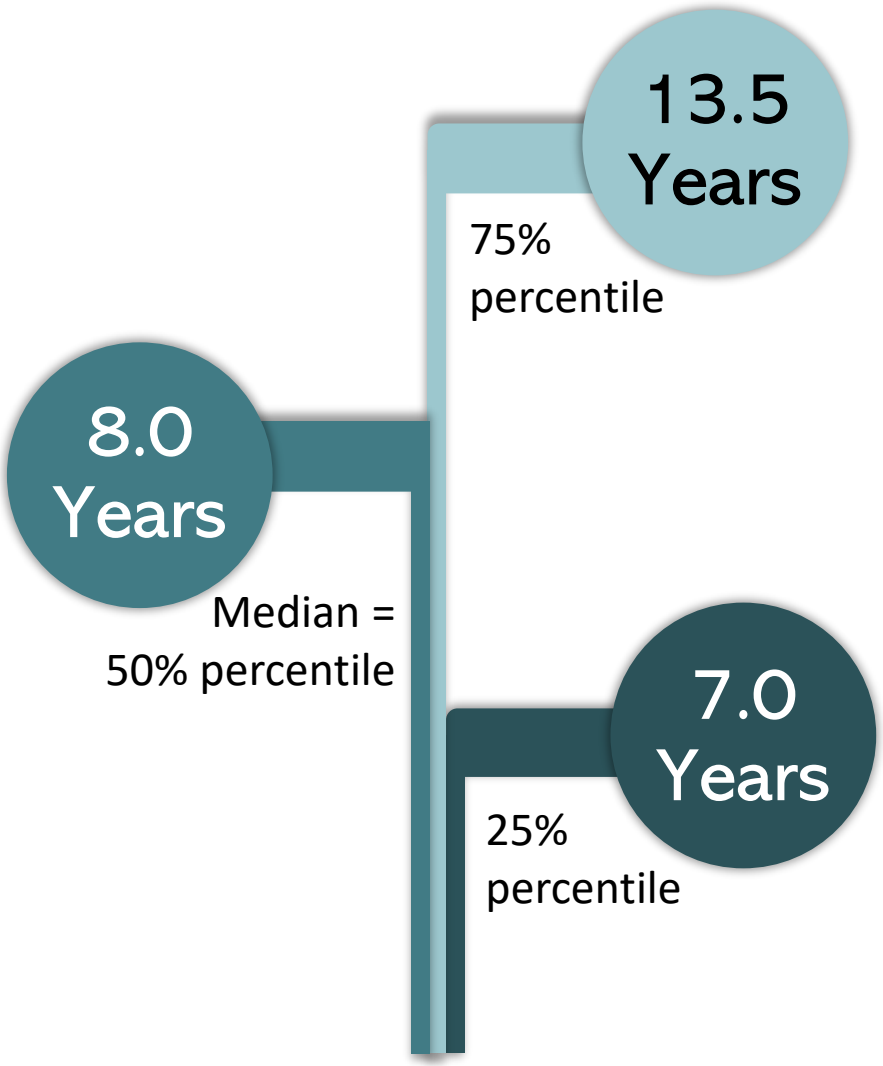
Data collected from dozens of CISOs in Israeli high-tech companies.

Focus on understanding cybersecurity practices and tools.

Insights were gathered on company size

Analysis aimed at identifying trends in cybersecurity adoption

How old is the company in years



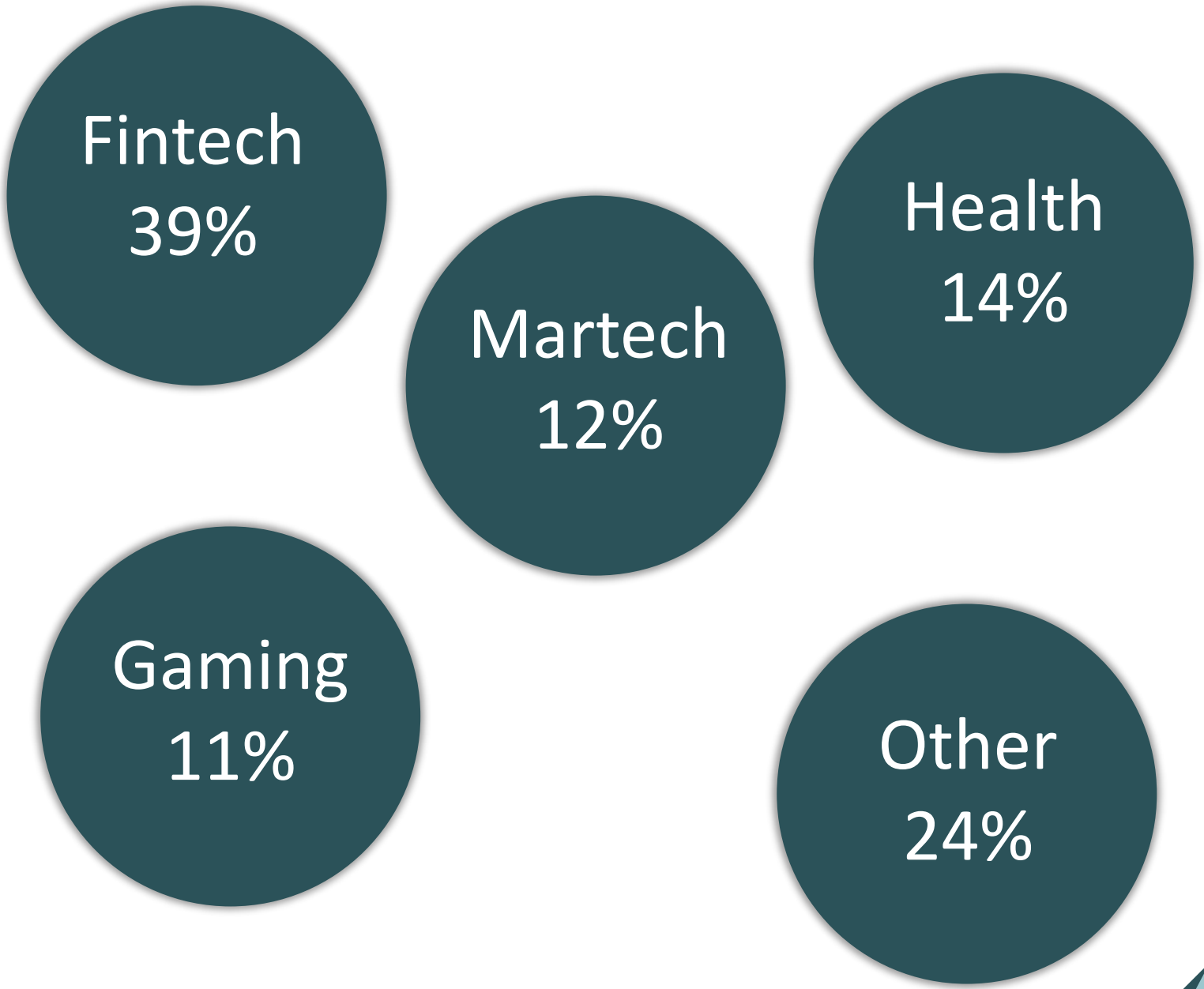
Private :

62.5 %

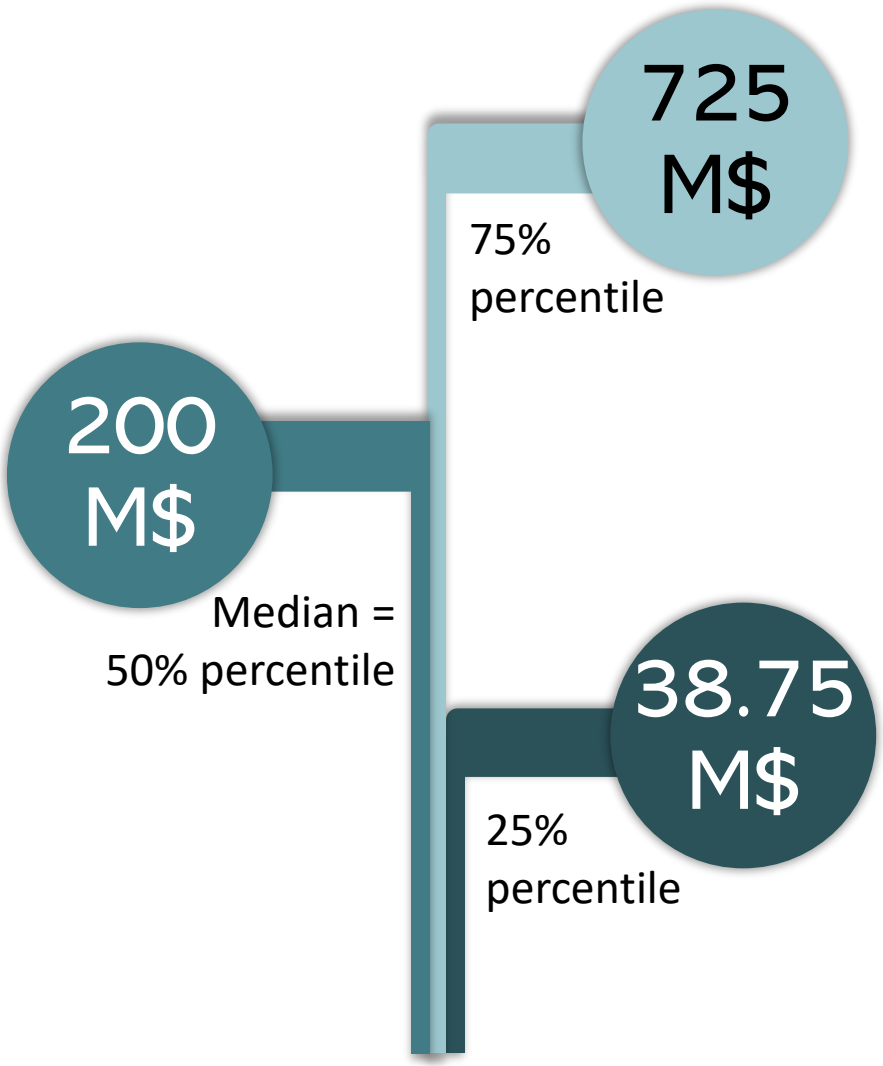
Public :

37.5%

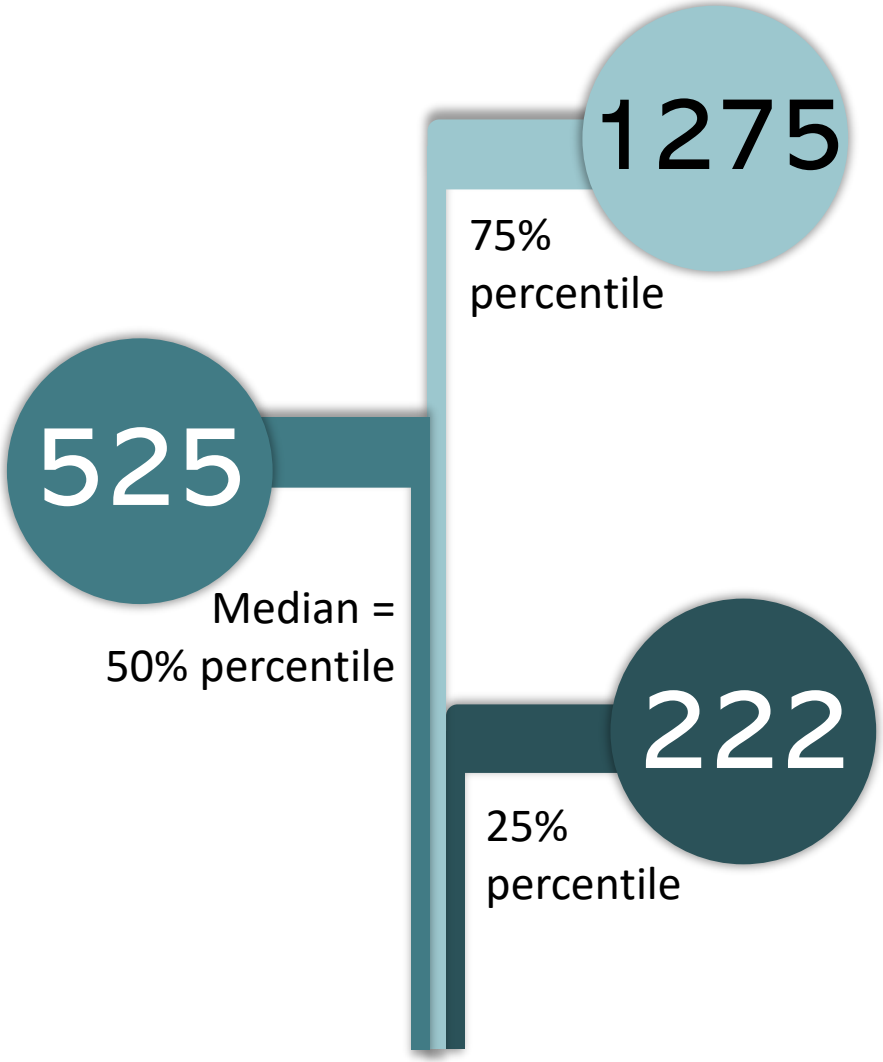
Industry



Revenues



Number of Employees



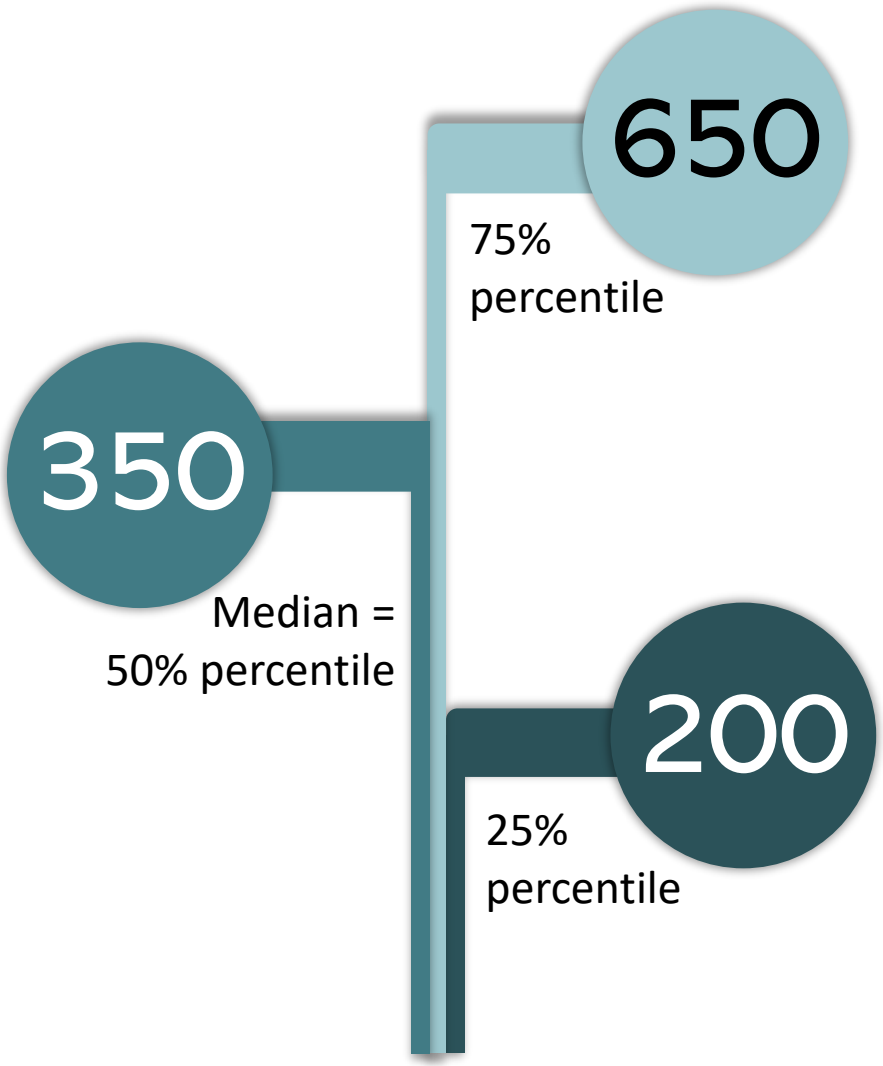
Cloud companies :

84 %

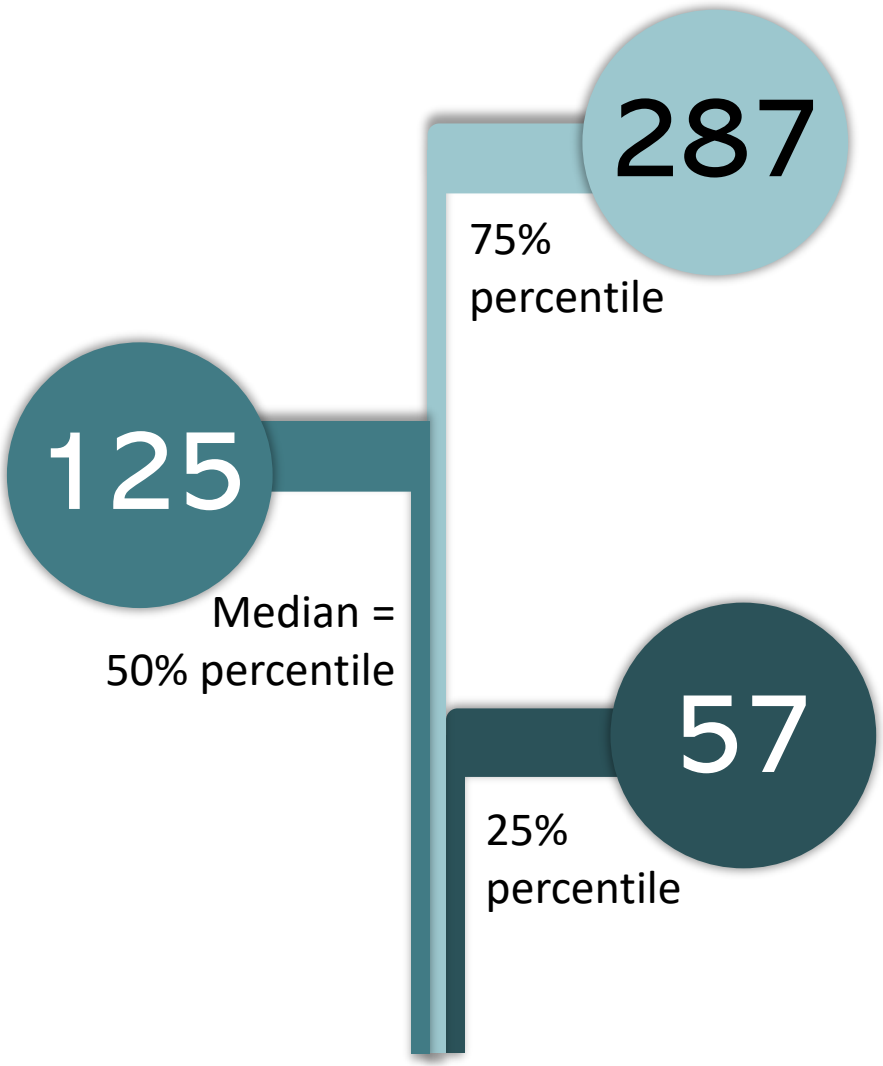
Not cloud companies :

16%

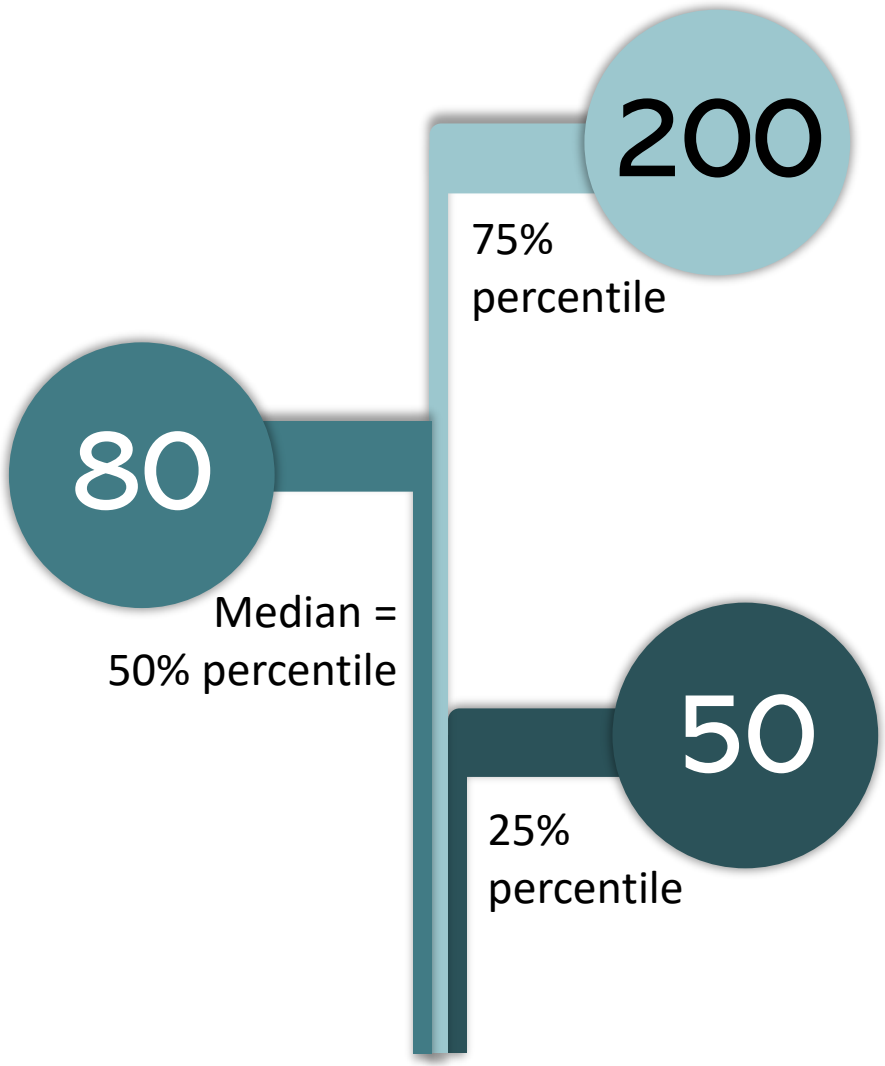
Number of Employees for cloud companies



Number of Developers



Developers for cloud companies



Survey methodology

Question to Org A – “How many Full Time Employees are in your APP SEC department?” “How Many Developers?”

Answer: “3500 Developers , 10 FTE (Full Time Employee) in the APP SEC team”

The Ratio is 350 Developers per each APP SEC team member

Survey methodology

Org A : The ratio is 350 Developers per each APP SEC team member
Org B: The ratio is 190

Org C: The ratio is 131

Org D: The ratio is 167

Org E: The ratio is 450

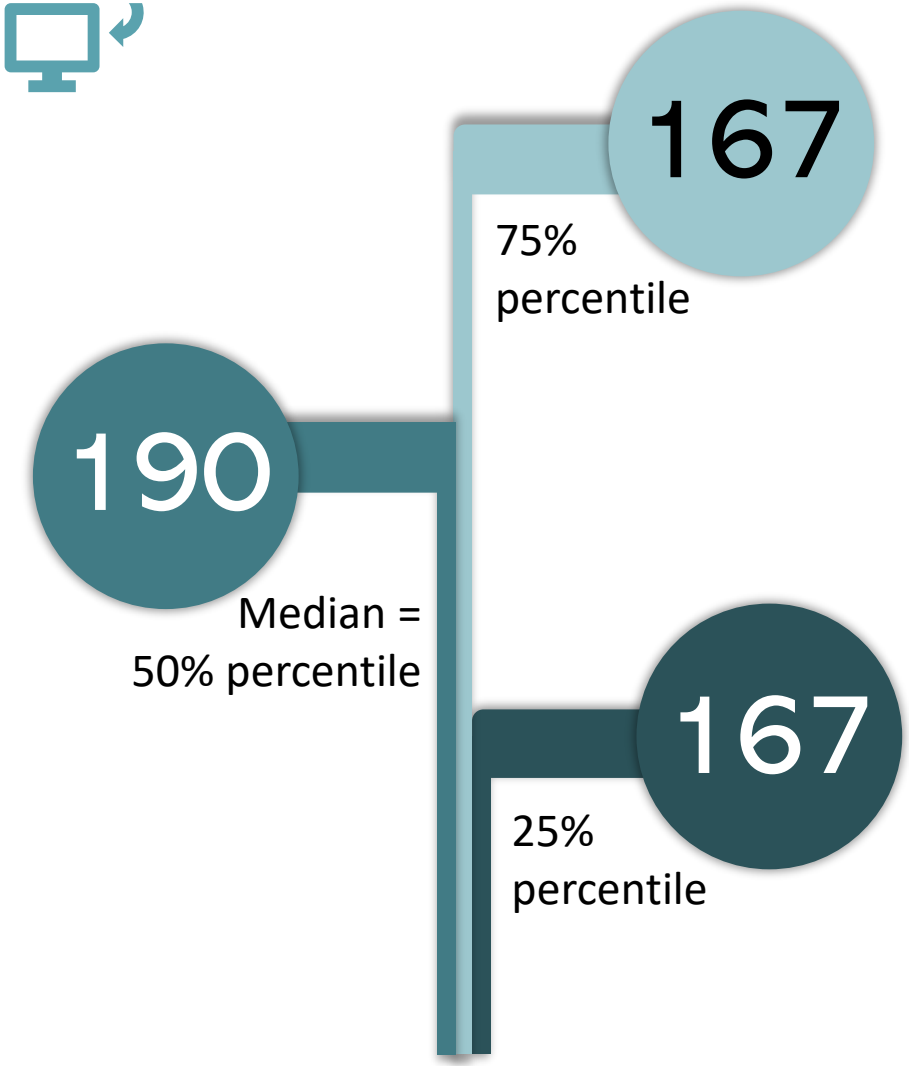
185, 213, 110, 367, etc…

Survey methodology

110
131
167
185
190
213
350
367
450

110
131
167 ← 25th percentile
185
190 ← Median = 50th percentile
213
350 ← 75th percentile
367
450

Survey methodology



Pini Cohen
CTO, EVP, STKI
https://www.linkedin.com/in/pinicohen/
pini@stki.info