

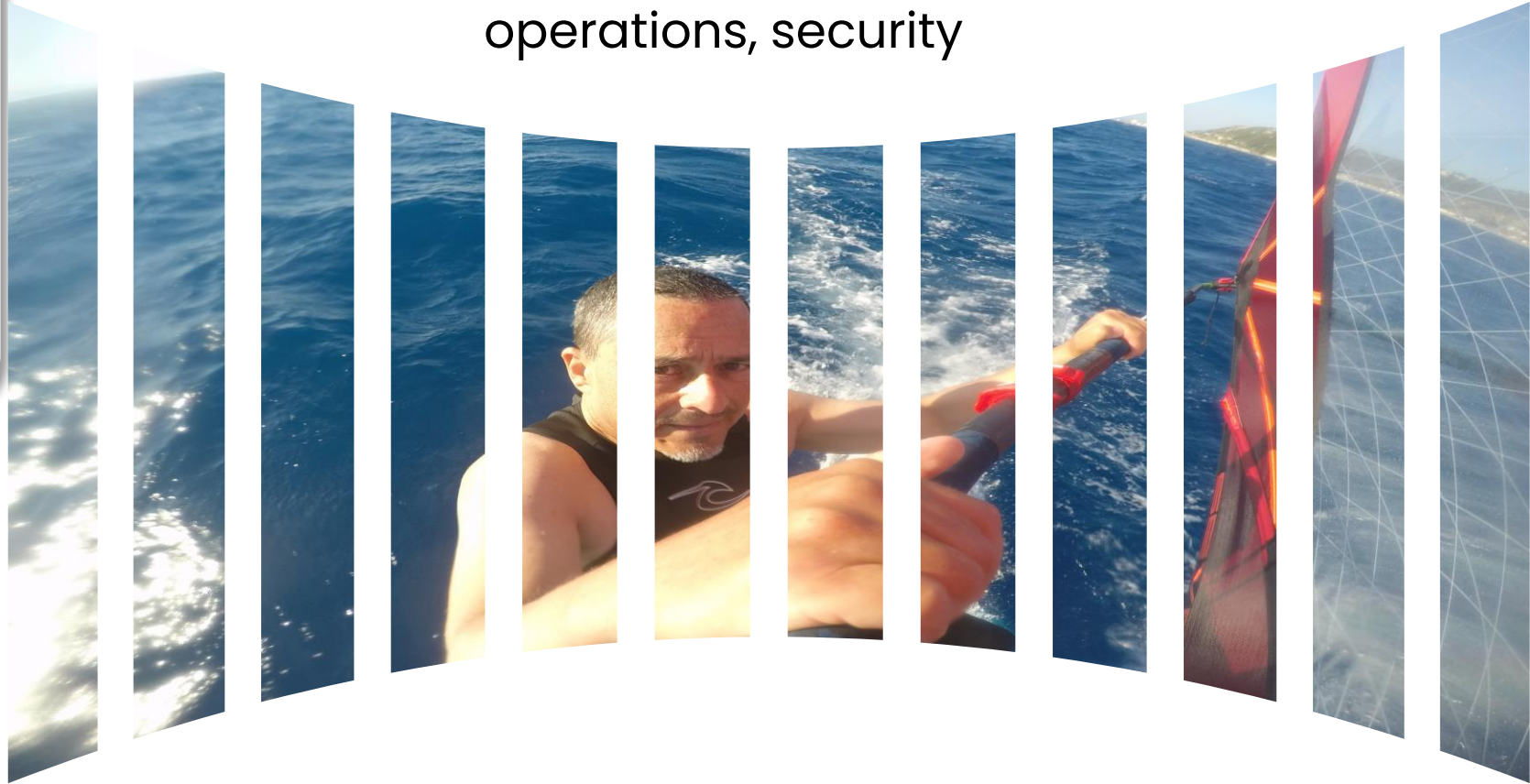
Pini 
Cohen
CTO, EVP STKI

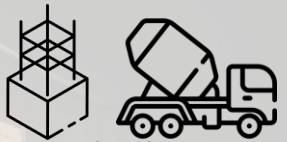
Enable Growth by Infrastructure Cybersecurity, Operations & Development

Who am I?

Networks, Storage, Backup DR, Servers,
Legacy servers, transactional and
analytical DBMS,
Integration (Messaging, ETL, ESB, API MNG,
IPaaS), Middleware (BRMS, FTP),
Development technology, Architecture,
Operations, Observability, ITSM-IT Help
Desk, Cloud IaaS, Cloud PaaS, Cyber
Security) Low Code Development Platforms

EVP and CTO covering infrastructure,
development technologies,
operations, security





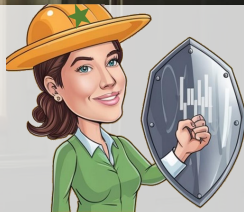
Defining IT

DORA metrics
Cross measurement



The Builder

Cloud native technologies
GenAI in Cyber Ops Infra
DevEx Developer Experience technologies
IDP (Internal Development Portal)



The Protector

Cloud Security
SASE Secure Access Service Edge
DC skill shortage



The Operator

SRE (Site Reliability Engineering)
Error Budgets
New Infrastructure Organization

Summary

HIGH PERFORMERS

AGENDA

The foundation of Defining IT Department: Measurement

IT is data-driven based on business-oriented metrics (OKR).

IT should be measured by business related metrics.



Example of Cloud thinking suitable for all (on premise) organizations:

DORA (DevOps Research & Assessment) Metrics

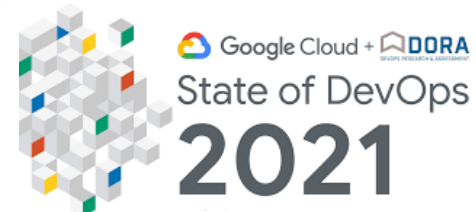
Deployment Frequency

12 deployments per week

Change Failure Rate – the ratio of the number of deployments that caused a failure to the total number of deployments

Change Lead Time – the time from when a developer starts writing code for a feature (or a change) to when that change is released to end user

Mean Time To Recovery (MTTR)



High-performing organizations adopt the DORA metrics as a central framework for measuring technological performance. The DORA metrics are applied to all actions and processes within the organization.



IT KPIs /OKR - Measure what Matters



Pini Cohen
CTO, EVP & Senior
Analyst @ STKI



Galit Fien
EVP & Senior
Analyst @ STKI

כפי שאמר פיטר דרוקר "אם אתה לא יכול למדוד את זה - אתה לא יכול לנהל את זה".
הרי שגם ב- IT המדידה היא חשובה וקריטית.
אולם נשאלת השאלה מה אפשר, מה רלוונטי ומה נכון למדוד ב- IT.
זאת במציאות משתנה, מציאות שבה המדדים שהיו רווחים שנים כבר לא בטוח
שהם מתאימים בעידן הענן, הפיתוח האג'ילי וכד'.

מפגש שולחן עגול הוא מפגש של לקוחות אשר דנים בנושא אשר נקבע מראש,

סדר יום למפגש:

הרצאת פתיחה STKI על מגמות במדדי IT.

דיון בין משתתפים המפגש (ללא יועצים או ספקים) בנושאים הבאים:

- מי מבצע את המדידה ב- IT וכיצד משתמשים בה.
- איזה מדדים הפסיקו להיות רלוונטיים – עמידה בתקציב או הזמן למשל?
- כיצד מודדים ערך מפרויקטי IT?
- מהי שיטת ה- OKR – Objectives and Key Results
- האם ישנם מדדים רוחביים - שמודדים פיתוח-תשתיות-סייבר וכד' באופן מאוחד?
- דוגמאות וטיפים למדדים איכותיים בתחומי ה- IT - פיתוח, תשתיות, סייבר, תפעול, BI וכד'.

למפגש מוזמנים:

CIO, OCIO, מנהלי פיתוח, מנהלי תשתיות-תפעול, CISO, מנהלי BI

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

18.12.24
10:00 - 13:00

משרדי STKI
המנים 72 בני ציון

High-performing organizations use cross-measurement to bring together different interests within the organization.



Cross
measuring
management



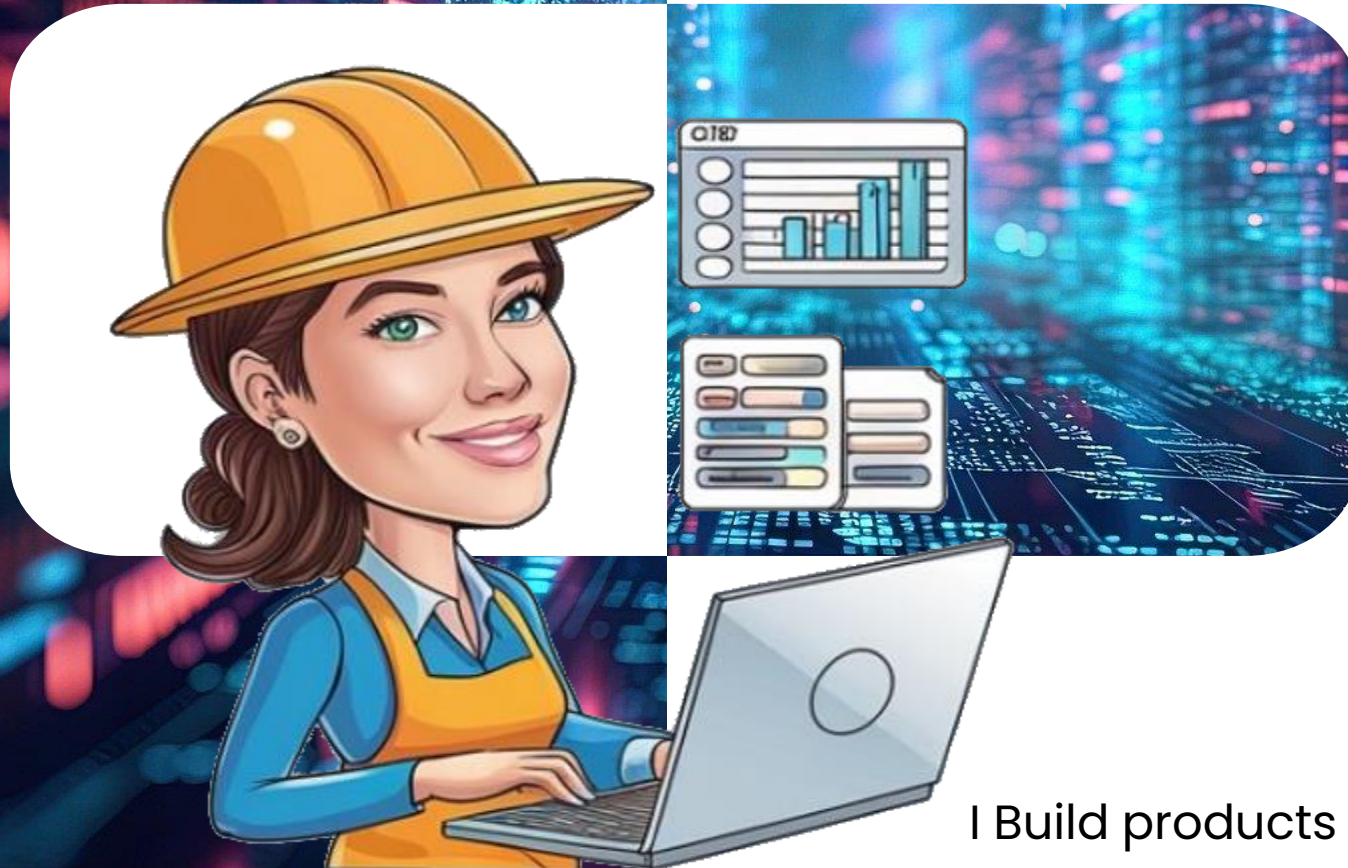
The background of the slide is a photograph of two gladiators in a Roman arena, shaking hands. They are wearing traditional gladiator armor, including metal shoulder guards and arm guards. The arena is filled with spectators, and the Colosseum is visible in the background under a bright sky.

Cross measuring management

Cross-measuring between the development manager (who wants to introduce new software capabilities quickly) and the availability manager (who wants to ensure that every change operates stably and reliably).



The Builder Technologies



I Build products that customers love



Cloud native
is the standard
in all IT activities
(even on premise)



THE BASIC
THINGS
IN LIFE





Partial list of aspects



Cloud repatriation is the process of moving applications, data, or workloads from public cloud environments back to on-premises infrastructure or private clouds

Cloud repatriation is the process of moving applications, data, or workloads from public cloud environments back to on-premises infrastructure or private clouds

According to IDC's Server and Storage Workloads Survey, only 8-9% of companies plan full workload repatriation

Cloud Repatriation

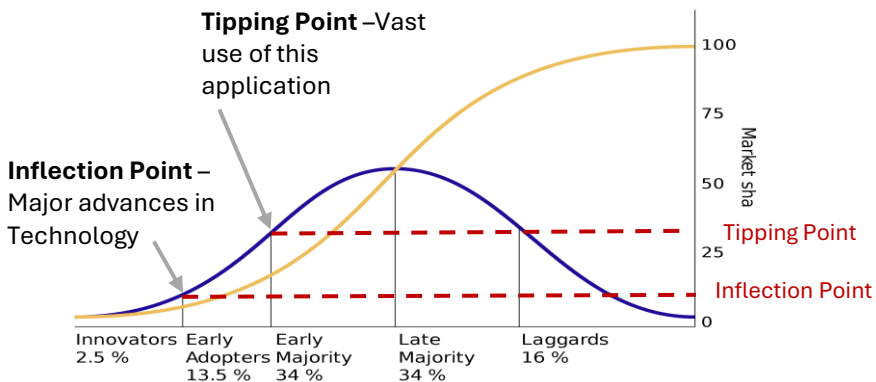
<https://cloudian.com/blog/cloud-repatriation/>



Technology status in Israeli

Enterprise IT

(cloud native status is different)



	Inflection point	Tipping point
Cloud	✓	✓
Microservices	✓	✓
Event Driven	✗	✗
Sserverless	✓	✗
IaC Infra as Code	✗	✗
IDP Internal Development Portal	✗	✗
GITOPS	✓	✗
DEVSECOPS	✗	✗
Observability-based monitoring	✗	✗
GraphQL	✗	✗
LCDP Low Code used by IT	✓	✗
LCDP Low Code used by the Business	✗	✗
FINOPS	✓	✗
SASE Secure Access Service Edge	✗	✗
Unified data infrastructures	✗	✗
NVME	✓	✗
Storage backup ransomware feature	✓	✓
Quantum ready cyber tools	✗	✗



Which problem Monorepo solves?

Polyrepos - the code of team A,B,C is managed separately

When shared library is modified, each team must independently update the shared library in their repository

This leads to different services running different versions of the library, causing compatibility issues



Web Assembly (WASM) is a binary instruction format for a stack-based virtual machine.

It is supported by all major browsers, ensuring compatibility and performance.

It is designed as a portable compilation target for high-level languages like C, C++, and Rust.

WASM enables high-performance applications on web pages.

WASM can run alongside JavaScript, enhancing web application capabilities.

Introduction to Web Assembly



Example Scenario for using Web Assembly (same page)

In a web-based image editing application: Web Assembly might handle: Image processing algorithms, filters, and transformations.

JavaScript would manage: User interface, file uploads, displaying the processed images, and coordinating the overall application flow.



OpenTelemetry is an open-source observability framework.

It provides tools for generating, collecting, and exporting telemetry data.

Supports metrics, traces, and logs for monitoring applications.

Integrates with various backend systems for data analysis.

Aims to provide a standard for observability across services.

Tools that support OpenTelemetry include SigNoz, Jaeger, Prometheus, Honeycomb, Datadog, New Relic, Splunk, Dynatrace, Logit.io, AppDynamics, AWS Distro for OpenTelemetry, Lightstep, Uptrace, Grafana, and Zipkin (partial list)

Introduction to OpenTelemetry

```
attributes": {  
  "http.method": "GET",  
  "http.scheme": "http",  
  "http.server_name": "127.0.0.1",  
  "http.host": "localhost:8082",  
  "http.target": "/server_request?param=testing",  
  "net.peer.ip": "127.0.0.1",  
  "net.peer.port": 48240,  
  "http.flavor": "1.1",  
  "http.route": "/server_request",  
  "http.status_text": "OK",  
  "http.status_code": 200
```



Application Health :

Error events, exceptions, warnings, and health checks

Performance Metrics :

Response times, throughput, resource utilization, and SQL query performance

Application Instrumentation: adding code to an application to monitor its performance, collect metrics, and generate logs

User and System Interactions:

User actions, logins, logouts, form submissions, and system events like startup, shutdown, and restarts

Security and Audit :

Security events, authentication, authorization, and sensitive data access logs

Business and Operational Metrics:

Business process events, integration points, background jobs, and infrastructure changes



High performance organization

Writing Application

Instrumentation based on OpenTelemetry standard



How do I use GenAI in infrastructure operations security?



1 GENAI usage in Infra-Security-Ops departments

Ask the public GenAI questions

- ❑ “Write a Dockerfile for my project”
- ❑ The GenAI might ask for relevant details

Can you write a Dockerfile for this project?



Certainly! To write a Dockerfile for your project, I need some information about your project's requirements. Here are a few questions to help me understand what you need:

1. **Programming Language and Version:** What programming language is your project written in? If it's, say, Python, do you need a specific version of Python?
2. **Dependencies:** Do you have any dependencies? For instance, if it's a Python project, do you have a `requirements.txt` or `Pipfile`?
3. **Build Steps:** Are there any specific build steps you need to follow, like running a build command?
4. **Entry Point:** What is the command to run your application?
5. **Port:** If your application runs on a specific port, which port is it?
6. **Additional Configurations:** Any other configurations or environment variables you need to set?

Once I have this information, I can create a Dockerfile tailored to your project.

🔊 📄 ↻ ⌵

Relevant feedback

“we use less consulting since we use GenAI in infra-cyber-ops”



2

GENAI usage in Infra-Security-Ops departments

Use the GenAI tools provided by the traditional vendors

Example Cisco AI Assistant:

- Update the firewall rule 'Allow_HTTPS' to include port 8443
- Create a basic security policy for FTD with default deny and allow outbound web traffic
- Set up a site-to-site VPN between our main office and branch office networks
- What access control rules are disabled?
- I want to understand my Edge ACP access control policy, can you tell me more about it?
- Create a new firewall rule to block all incoming traffic from IP address 192.168.1.100



3

GENAI usage in Infra-Security-Ops departments

Use dedicated agentic infra-cyber-ops tools that assist in heterogeneous environment

The code assistant* for DevOps

*Assists vs. Delegates

These tools learn your environment (talk to cloud, KUB engine, Git repositories, Slack, Jira, read YAML files, etc.)

Kubiya prompt examples:

- ❑ Provide Terraform code to provision an S3 bucket in AWS
- ❑ Run the Terraform code to create the S3 bucket
- ❑ Update the configuration file in GitHub with new environment variables
- ❑ Grant temporary access to the production database for the next 2 hours
- ❑ Create a new development environment for the mobile app project



Aiden (OpsVerse) prompt examples:

- ❑ Create an end-to-end CI/CD pipeline for my Java application using Jenkins and Kubernetes
- ❑ Write a shell script to automate our daily backup process
- ❑ Explain the root cause of the increased latency in our API gateway over the last 24 hours
- ❑ Create a monitoring dashboard in Grafana to visualize our key performance metrics
- ❑ Analyze our current infrastructure and suggest optimizations for cost reduction

OPSVERSE™

The Builder – DevEx Developer Experience



I Build products that customers love



What is Developer Experience (DevEx)

Developer Experience (DevEx) refers to the overall experience of developers while working on their tasks.

A positive DevEx boosts productivity, efficiency, and job satisfaction for developers.

Good DevEx involves streamlined tools, clear documentation, and supportive infrastructure.

Organizations with strong DevEx tend to have lower developer turnover rates.

Investing in DevEx can lead to faster development cycles and higher quality software.



Galit Fein about modern team structure:

“Ideally, development teams are autonomous and self-sufficient, managing their entire software lifecycle independently”

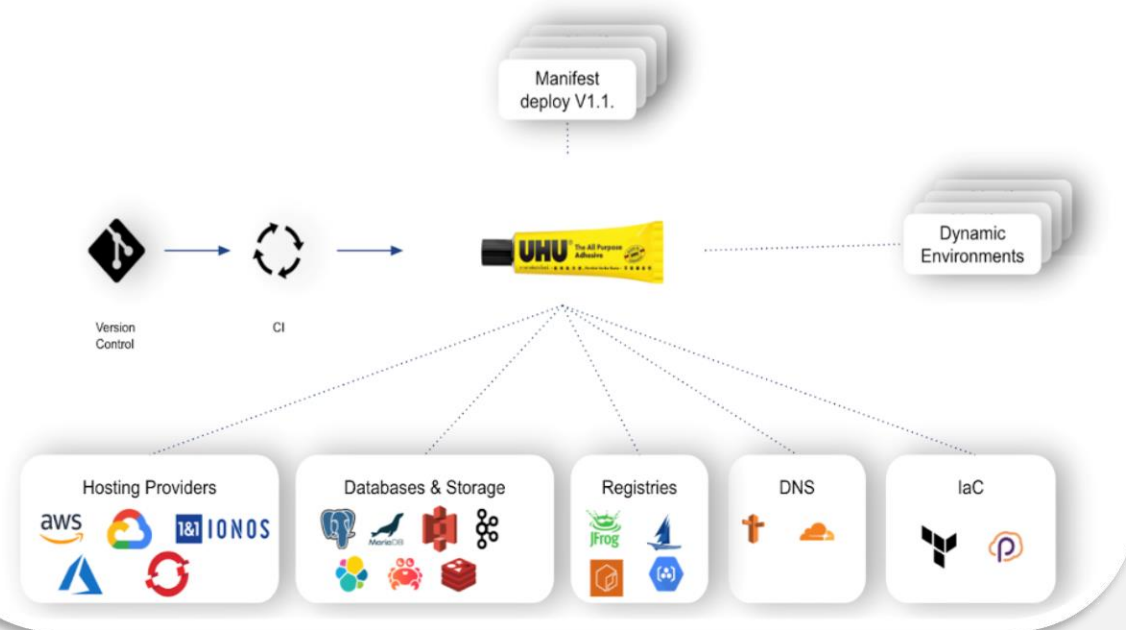


IDP is a set of tools and services that support software development providing all developers needs .

They centralize and streamline various aspects of the development lifecycle.

IDP aims to improve developer experience and productivity.

Glue for Gold



which provides all development requirements

What is an Internal Development Portal (IDP)?



Relationship Between Platform Engineering and IDP

Platform engineering focuses on building and maintaining shared infrastructure.

Platform engineering creates the foundation on which IDPs operate.

IDP provides tools and services for software development through unified platforms.

Platform Engineering = The discipline, the team IDP = the tools

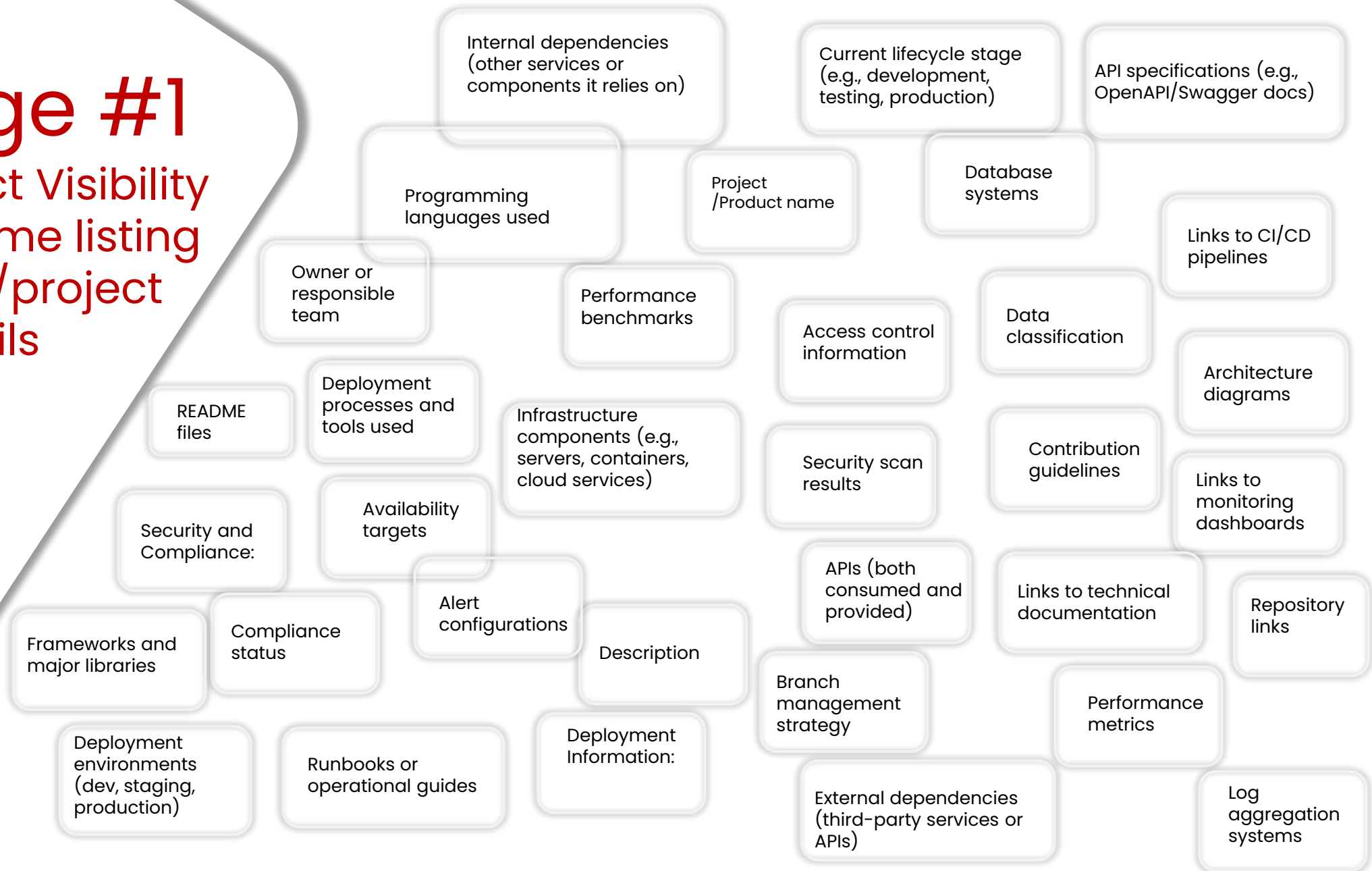


what do I do with IDP (Internal Development Portal) ?



IDP Usage #1

Product/project Visibility
- create real time listing
of the product/project
technical details
(**catalog**)
teams



IDP Usage #2

Empower developers with **self-service capabilities**, enabling them to perform tasks previously requiring assistance from other teams

Identity and Access Management (IAM)

Document Management

Data services that handle data warehousing, data pipelines, data lakes BI tools that are part of the application

Continuous Integration and Continuous Delivery (CI/CD) pipelines automate the software development lifecycle (SDLC)

API Management

Monitoring and Alerting

Infrastructure as Code (IaC) automate infrastructure provisioning, configuration, and management

Security and Compliance

FinOps Tags

Developer Experience (DX) documentation, and training resources



IDP Usage #3

Create a **productivity dashboard** of the developer and team

Deployment Frequency: How often the team deploys code to production

Lead Time for Changes: Time from code commit to deployment in production

Mean Time to Recovery (MTTR): Average time to resolve production issues

Change Failure Rate: Percentage of deployments causing failures in production

Code Complexity: Measure of how complicated the codebase is

Code Coverage: Percentage of code covered by automated tests

Pull Request (PR) Cycle Time: Time from PR creation to merge

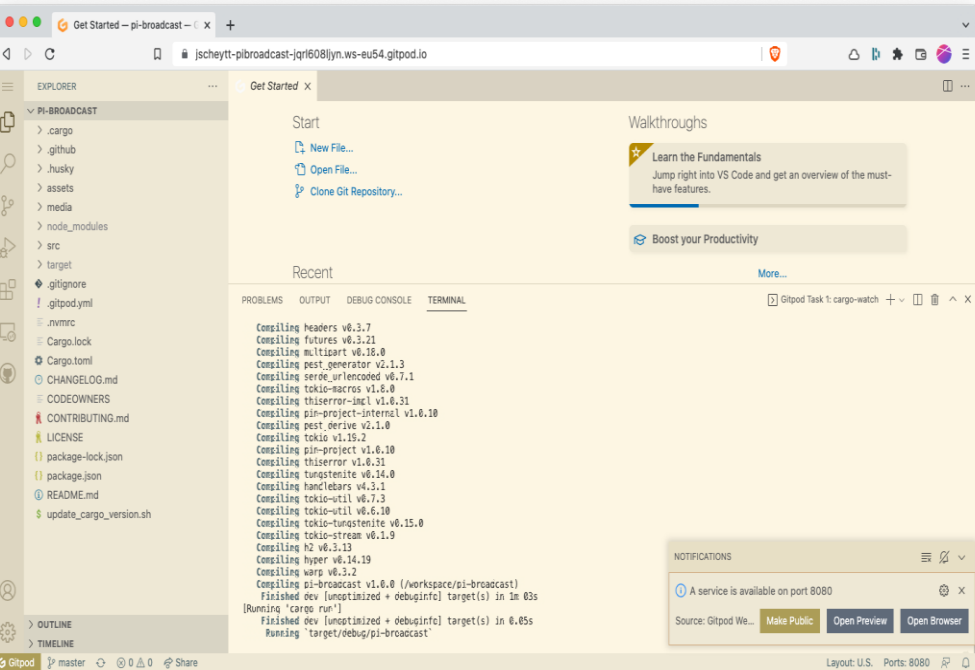
Bug Fix Rate: Speed at which reported bugs are resolved

Feature Delivery Rate: Number of new features delivered in a given time period

Team Velocity: Amount of work completed in a sprint or given time period



ICE: Integrated Cloud Environment



ICE provides cloud-based development tools and resources.

It allows for collaboration and access from any location.

ICE offers integrated deployment pipelines and scalability.

It simplifies management and enhances team productivity.

ICE supports continuous integration and continuous deployment (CI/CD).

ICE's has some integration with Visual Studio



ICE

(Integrated Cloud Environment)



Traditional IDE

Accessible from any device with internet

Accessibility

Installed on local machine

Built-in real-time collaboration

Collaboration

Limited, often requires tools

Automatic updates

Updates

Manual updates usually required

Limited or no offline capabilities

Offline usage

Full functionality offline

Often subscription-based

Cost model

One-time purchase or free





GenAI code
assistance
tools are a
major thing
in DevEx



Code assistant tools in israeli enterprises :

vs



All* believe that code assistant tools will be standard in the future

*most of development managers

None* see real productivity gain ("from 100% capacity to 120% capacity")



Without digital trust, we
can't do anything.



The Protector



Disinformation Security

Disinformation is a growing threat to enterprise security, as it can be used to **spread false information** that can damage a company's reputation and bottom line. It's related to **cyber intelligence** domain

Enterprises must take a proactive approach to disinformation monitoring, detection, and response to mitigate risks.

Effective disinformation security requires collaboration between different teams within an enterprise, including IT, legal, and communications.



Disinformation security protection tools

Cyabra

Offers AI-driven real-time alerts, analysis, and insights to combat disinformation and protect corporate reputation.

cyabra.com

Blackbird.AI

Identifies and protects against narrative attacks created by misinformation and disinformation.

blackbird.ai

Red Points

Helps find, track, and remove counterfeit listings and sellers from the web, focusing on IP protection.

redpoints.com

Reality Defender

Detects deepfakes and manipulated media.

realitydefender.com



Cloud Security

Additionally, organizations adapt their organizational security environment to the public cloud and continue to implement solutions to protect and hedge risks from organizational supply chain partners.



The different cloud security tools categories:

CSPM

Cloud Security Posture Management

Continuously monitors and manages cloud infrastructure security by identifying misconfigurations, compliance risks, and security gaps .

SSPM

SaaS Security Posture Management

Focuses on securing SaaS applications by managing configurations, user access, and data sharing settings across multiple cloud-based software services .

ASPM

Application Security Posture Management

Provides visibility, detection, correlation, prioritization, and remediation of security vulnerabilities across the entire software development lifecycle .

CWPP

Cloud Workload Protection Platform

Secures cloud workloads, such as virtual machines, containers, and serverless functions, by providing threat protection, compliance, and vulnerability management .

DSPM

Data Security Posture Management

Focuses on discovering, classifying, and protecting sensitive data across cloud environments, ensuring proper data handling and compliance .

CIEM

Cloud Infrastructure Entitlement Management

Manages and secures **identities** , dna ,sthgir ssecca snoissimrep duolc sсорca ot smroftalp eht ecrofne tsael fo elpicnirp .egelivirp

CASB

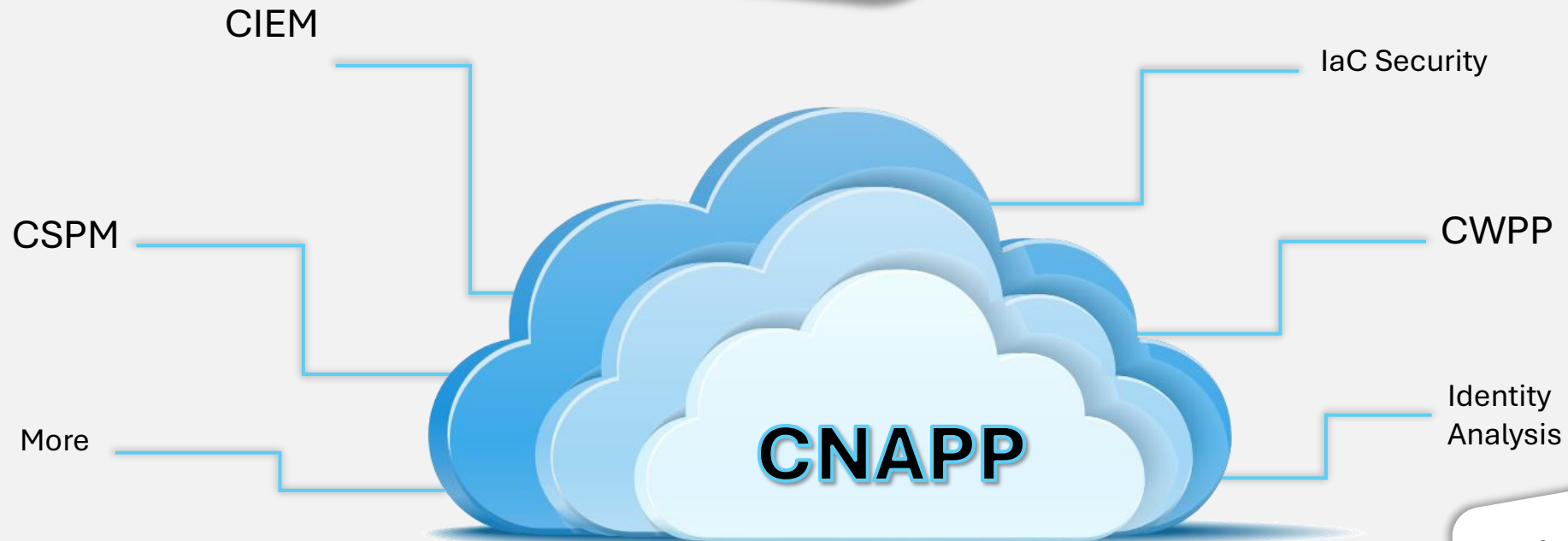
Cloud Access Security Broker

Securing and monitoring cloud service usage across an organization such as mass downloads by an internal user or unusual access patterns



The different cloud security tools categories:

Provides comprehensive protection for applications running in cloud environments



CNAPP Cloud Native Application Security

The pivot of the cloud security



Cloud security platforms provide a unified environment, simplifying management.

Best of breed solutions offer specialized tools with potentially higher functionality.

Platforms may compromise on functionality but are easier to manage.

Best of breed solutions can struggle with data integration and user experience.

Choosing the right approach depends on company size, security maturity, and IT staff skills.

Debate in Cloud Security: Best of Breed vs. Platforms



What is SASE (SSE)?

Secure Access Service Edge (SASE) is a network architecture.

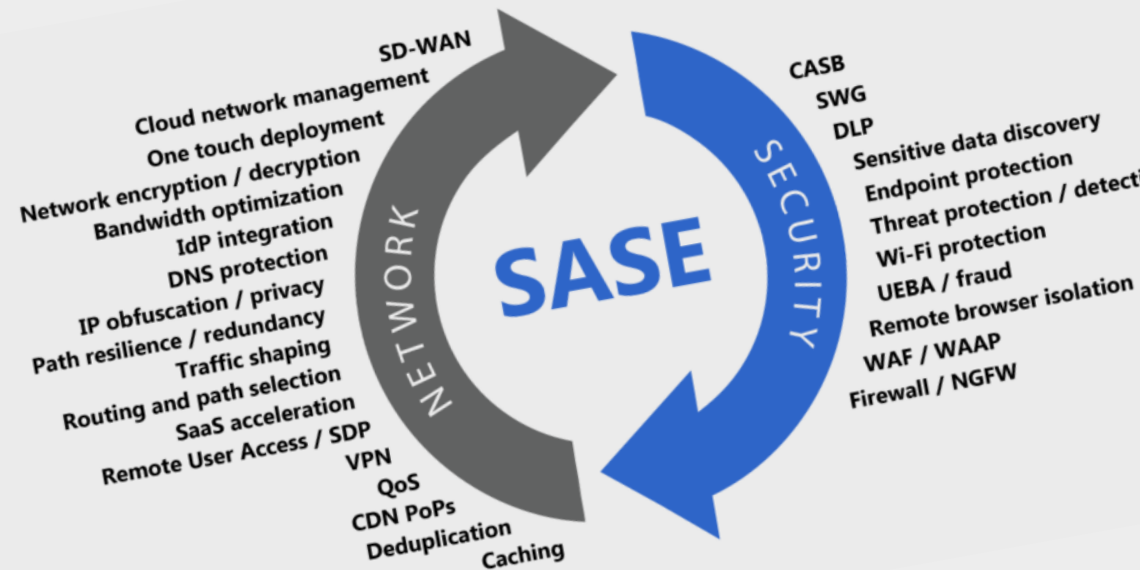
SSE – Secure Service Edge

It combines network security functions and WAN capabilities.

SASE integrates these functions into a single cloud-based service.

SASE benefits:

- ❑ Enhanced security through integrated solutions.
- ❑ Improved network performance and reduced latency.
- ❑ Simplified management with a unified platform.
- ❑ Greater scalability and flexibility for growing businesses



HIGH PERFORMERS

Mainframe Market Pulse survey | A commissioned study conducted by Forrester Consulting on behalf of Deloitte

Mainframe talent drain

Our recent survey shows mainframes are here to stay.

Will IT organizations have the talent they need to deliver on hybrid strategies?

Think mainframes are on their way out? Think again. Deloitte's 2020 Mainframe Market Pulse survey tells an alternative story. Business and IT leaders show plenty of interest in mainframes—especially in upgrading legacy environments as the foundation for hybrid strategies in data and transaction-heavy industries.

But the workforce with the skills to support mainframe systems is aging out—and the pipeline of new talent with the skills to fill those roles is diminishing. How are businesses addressing this talent gap to support hybrid strategies as they move into the future?

Here's what 261 business and IT leaders revealed about the talent gap and how they're attempting to mitigate it. These survey insights offer a window into their thinking, and can be useful in guiding your talent, investment, and IT strategies.

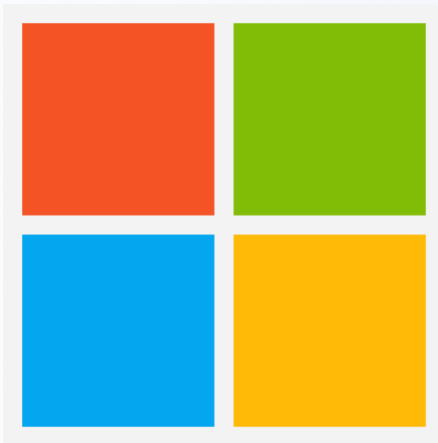
Skill gap in
traditional
DC
technologies



Skill set slow-down

Rising reliance on mainframes





How can I get
MCSE certification?

YOU DON'T

UPDATE: March 26, 2020.
All remaining exams associated with Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Solutions Expert (MCSE) will retire on January 31, 2021





The Operator

I make everything work, only better



Site Reliability Engineering (SRE)

SRE uses a data-driven, engineering-focused and automation approach to managing and improving system reliability.

SRE is a response to the challenges of running and maintaining complex systems at scale.

SRE is a discipline that focuses on the reliability and maintainability of large-scale systems.



Understanding Error Budgets

Teams use error budgets to prioritize tasks and allocate resources.

When an error budget is depleted, the primary focus shifts from developing new features to improving system reliability

Error budgets help balance innovation and reliability.

Application owners are (also) responsible for its availability





Infrastructure organization challenge

As part of adapting to technological changes, the organization understands that the existing organizational structure is no longer suitable and needs to be changed to fit the cloud era.



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)



System

Cyber

Storage

Networking

DBA

Monitoring



Cloud effort is done in (percent)



Source: STKI



STKI Staffing Ratio Research

In Enterprises IT
Infrastructure – Cyber – Operations

STKI.INFO Copyright©2024 STKI Do not remove source or attribution from any slide, graph or portion of graph

1



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



System

משרתים



Cyber

משרתים



Storage

משרתים



Networking

משרתים



Cloud

אדונים



What do we do?



Design the overall cloud and DC architecture

Define technical requirements

SA is multi cloud (all clouds +DC)

Make decisions on which cloud/DC
deploy new product, project or
service

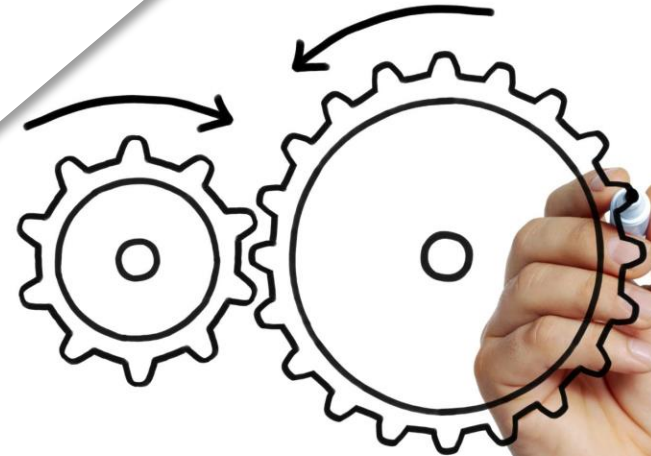
Step 1 –
Build Solution
Architect (SA)
team



Subject Matter Expert (SME)

Specialized Knowledge: SMEs possess in-depth knowledge of specific cloud technologies, services, or domains that goes beyond the general expertise of a solution architect or cloud engineer

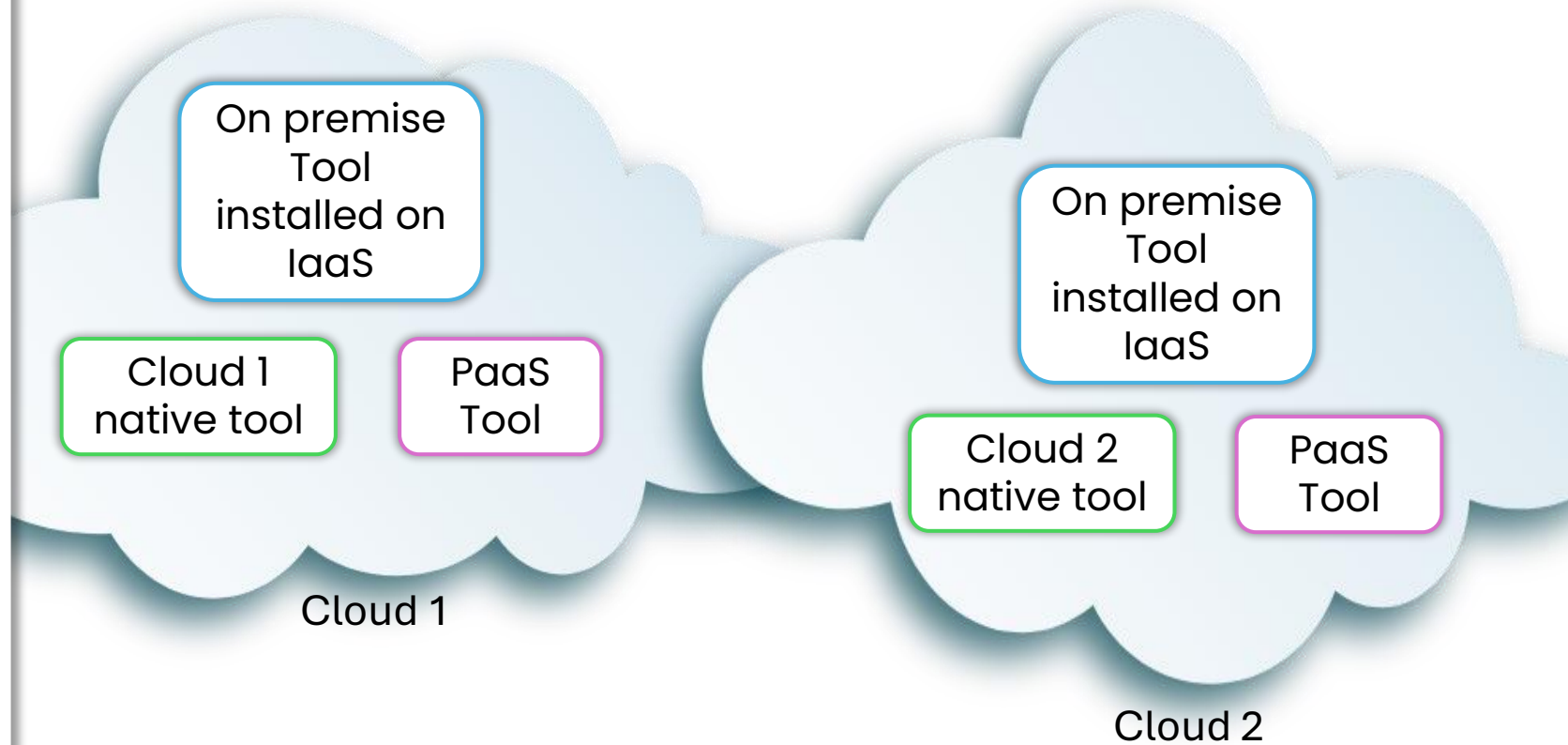
SME examples: per cloud / DC, per vendor, per domain (e.g. regulation)



Step 2 – for each domain

Decide between single and multi team in each technology domain

“Multi Cloud” here means “Clouds + DC”



On premise Tool

PaaS Tool replacing the on premise tool



Step 2 –

Decide between single and multi team in each technology domain

Single Cloud/DC team – the team will be responsible, hands on, for its technology domain in its own cloud/DC

- ❑ Might be faster, cost efficient, integrated better and easier with specific cloud functionality

Multi Cloud/DC team – the team will be responsible, hands on, for its technology domain across DC and clouds

- ❑ The complete picture
- ❑ Processes that involve several clouds/DC

Typical single cloud/DC team – System (VM's), Storage

Typical multi cloud/DC team – Identity



Step 2 – for each domain

Decide between single and multi team in each technology domain

Decide if the team is single or multi cloud/DC

Then the teams decides whether to use single or multi cloud/dc tools

Multi cloud/DC team might decide to use different tools for each cloud/DC

The Multi cloud/DC team can change its mind –start with different tools for each cloud/DC (fast + cost efficient results) and later move to single tools

Different teams (Single Cloud/DC team) using the same tool is also an option

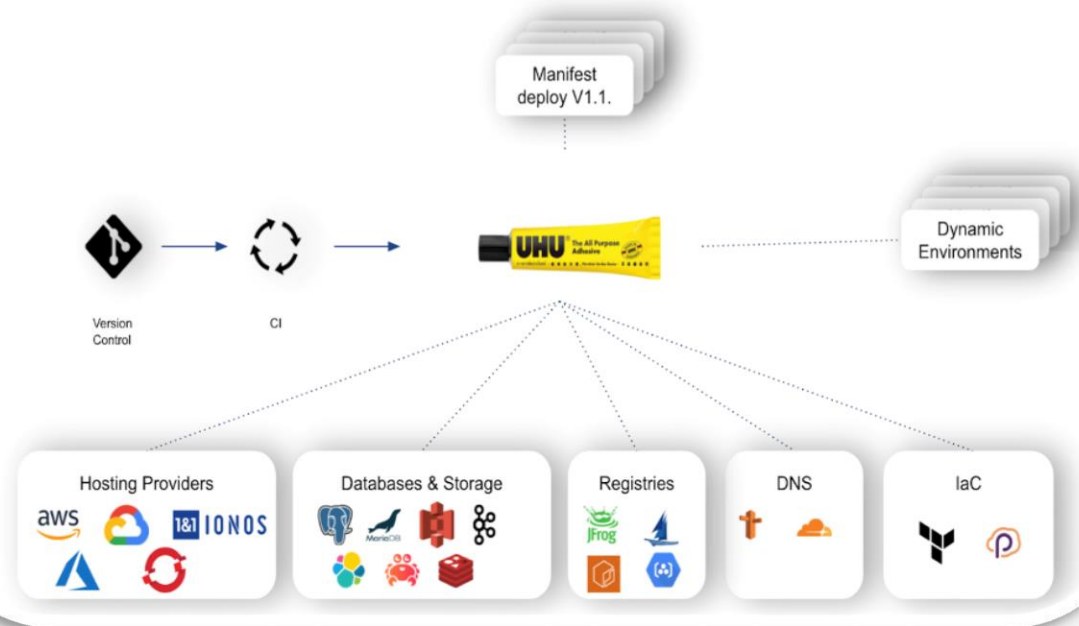


Step 3 –

Platform Engendering (IDP) team

Platform Engineering team (IDP) is multi cloud team (i.e. deals also with DC)

Glue for Gold



Single cloud/DC teams – hands on

Multi cloud/DC teams – hands on

Solution Architects (SA)– that see the complete technical picture all clouds/DC. Coordinate the day-to-day work of all teams.

Platform Engineering (IDP) team – enable DevEx (automation) for all technology domains

SME – subject matter experts (in some groups)

New organization structure will consist of



New Infr. Org.



Networking SME DC Networking SME cloud1

Solution Architects



Platform Engineering (IDP) team



Observability (monitoring)



DR – multi cloud



DBA – multi cloud



Cloud1 – core



Cloud2 – core



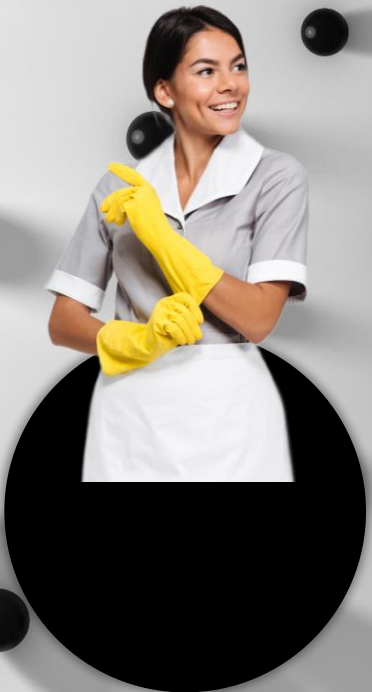
DC – core

Core = compute, storage, network security

This is a suggestion



All organizations
should address the
master slaves
conflict
High performance
organizations
already did





Cross measurement metrics

Error Budgets

Web Assembly

CNAPP (Cloud Native Application Protection Platform)

Open Telemetry

Cloud Native

Dora Metrics

Summary of Recommendations

Application Instrumentation

IDP (Internal Development Portal)

GENAI usage in Infrastructure, Operations and Cyber

DC Infra Skill Gap

ICE (Integrated Cloud Environments)

New Infrastructure Organization

SASE (Secure Access Service Edge)

Availability Manager

SRE (Site Reliability Engineering)





"Every IT professional must undergo reskilling and upskilling to stay relevant and competitive in the rapidly evolving technology landscape"

Reut Shefer-Bar
VP and Senior Analyst



Thank you Inbal Raanan!!





אלי שרעבי
ELI SHARABI
(51)

ז"ל
YOSSI SHARABI
(53)

BRING
HIM

HOME NOW!

HOSTAGES AND MISSING
FAMILIES FORUM

BRING
HIM

HOME NOW!

HOSTAGES AND MISSING
FAMILIES FORUM

הדור שלינו
עשוי ניצח
BRING THEM
HOME-NOW!





Thank
You!

Pini Cohen

pini@stki.info

<https://www.linkedin.com/in/pinicohen/>