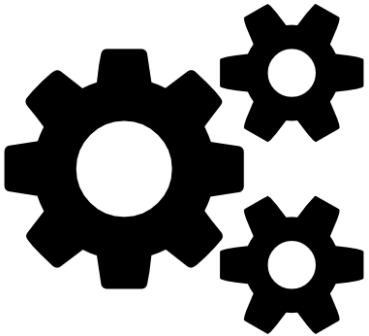
Modern delivery & cyber for enterprise IT

Long version presentation

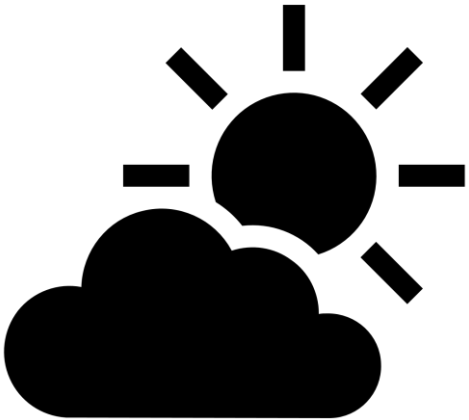


Pini Cohen

stki.info

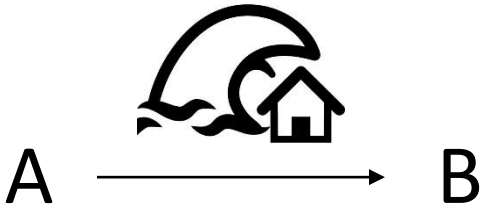
What is happening in delivery & cyber?

But after the tsunami we expect stable weather



Mainstream platform for enterprise IT

- How most new applications are built and operate



From A to B

- **Monolithic** web applications based on Rest developed in **water fall** based on relational dbms distributed and configured with automation tools (puppet, chef, ansible) run on **virtualized environment** (compute) and traditional storage and network secured with 30 (or so) tools
- **Microservices**, **stateless**, agile built, devops Rest /GrapQL web applications built on **nosql** or sql dbms and containers operated with container orchestrators based **APaaS** on top of private/public cloud or directly on commodity servers with virtualization enabled by SDN, SDS secured with software defined perimeter architecture and **HW based security**

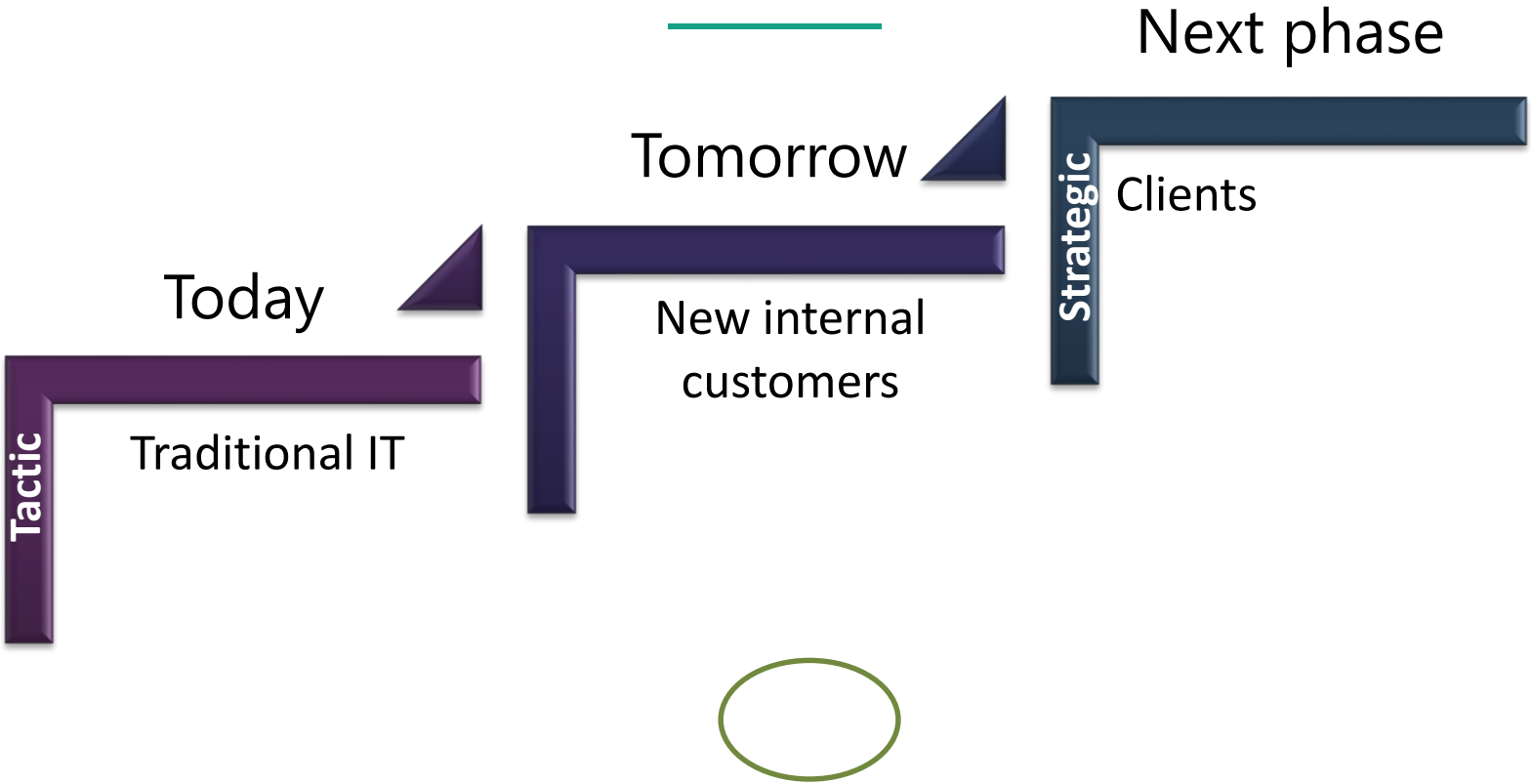
TL;DR

Too Long; Didn't Read

stki.info

Now let’s go step by step

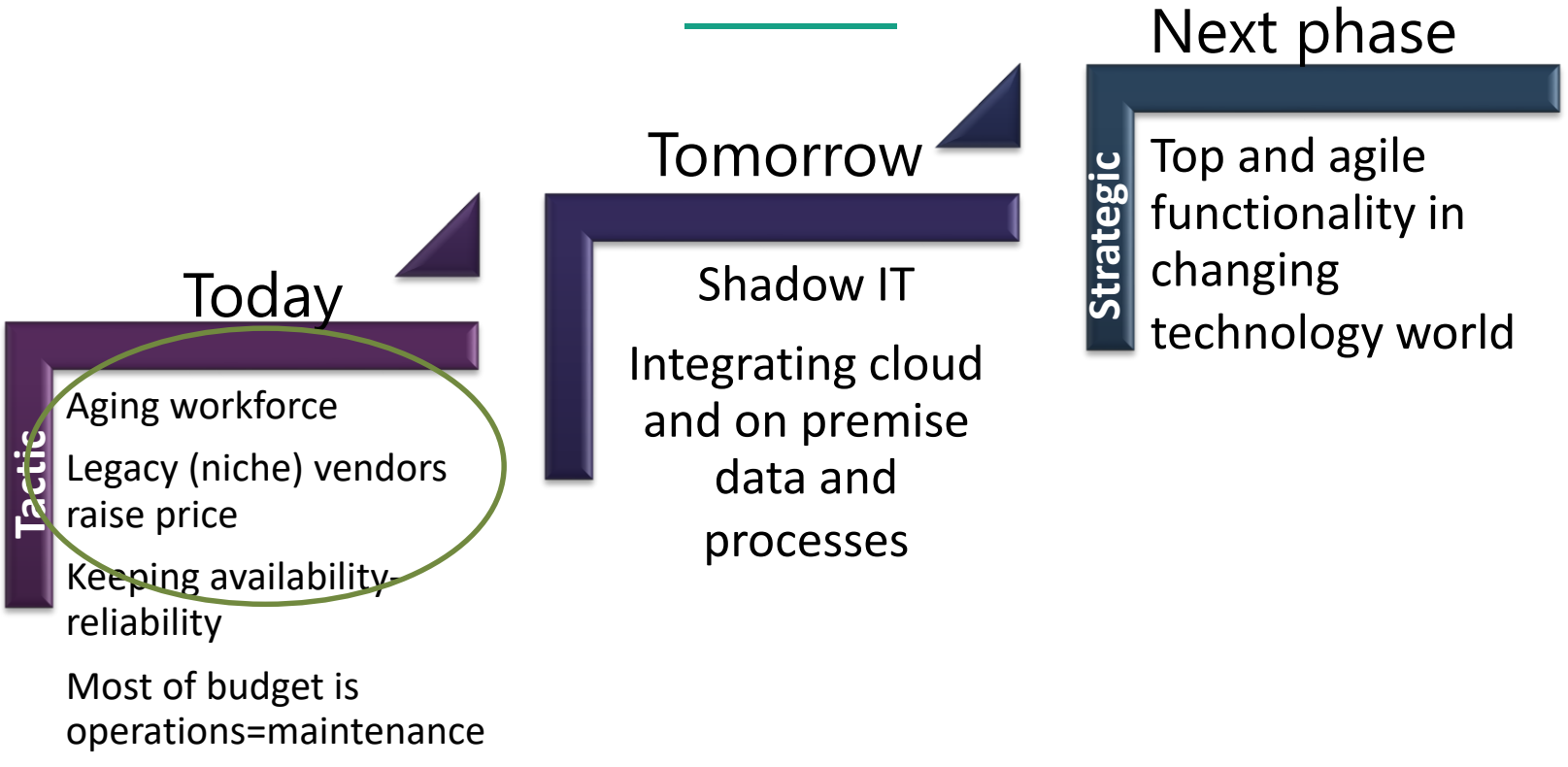
Enterprise IT different fronts



Let’s start

Basic theme

Basic challenges



Before we conclude: what about our legacy?

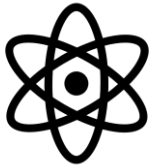
STKI on Legacy platforms

- Last longer than anyone expected
- The slope to oblivion:
  - New technology arrives. It looks immature but gain momentum.
  - Legacy vendors raise prices
  - Shortage in new\young personnel
  - Less support to 3rd parties (example – security 3rd parties)
  - Important functionality\standards missing
  - Availability \ performance -unresolved issues

stki.info

STKI on Legacy platforms: when do I stop?

Agenda



DC and infrastructure

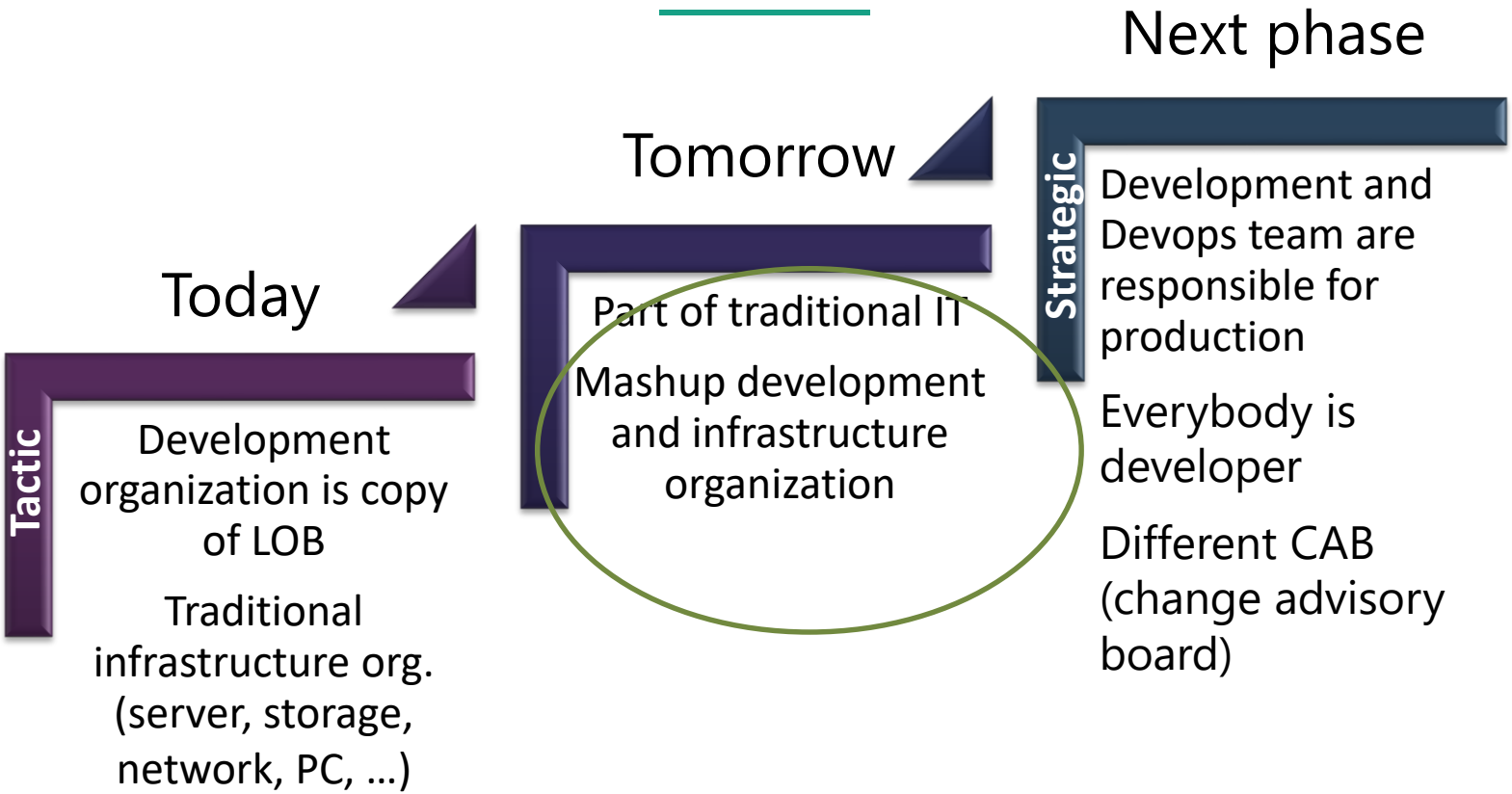
organization, processes and skills

middleware

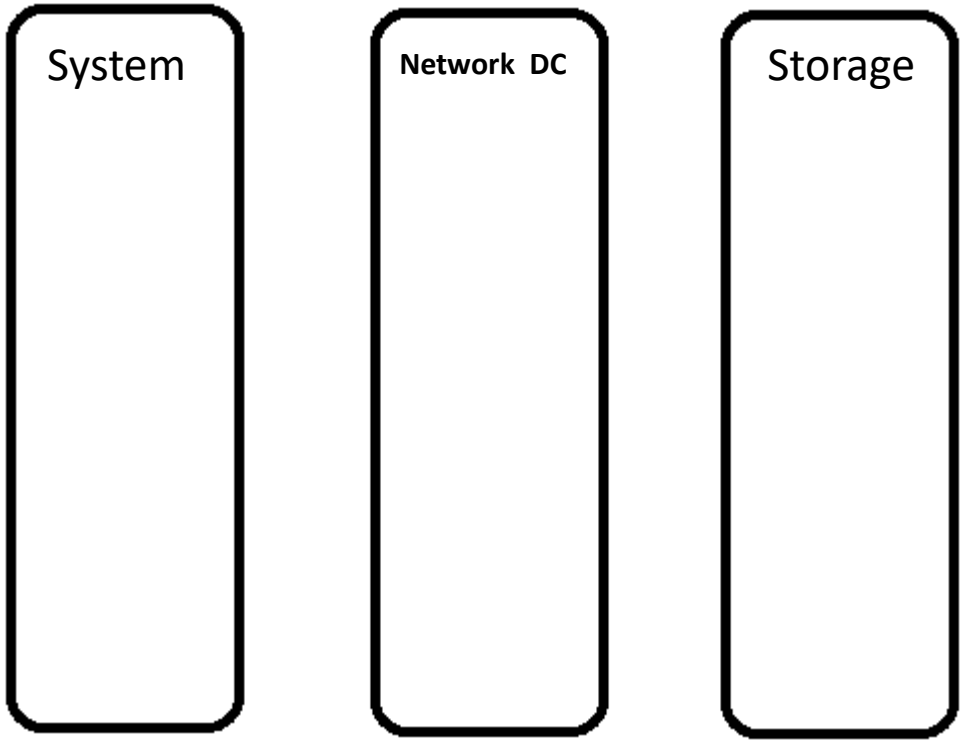
cyber security

development and architecture

Staffing, organization, skills, operations

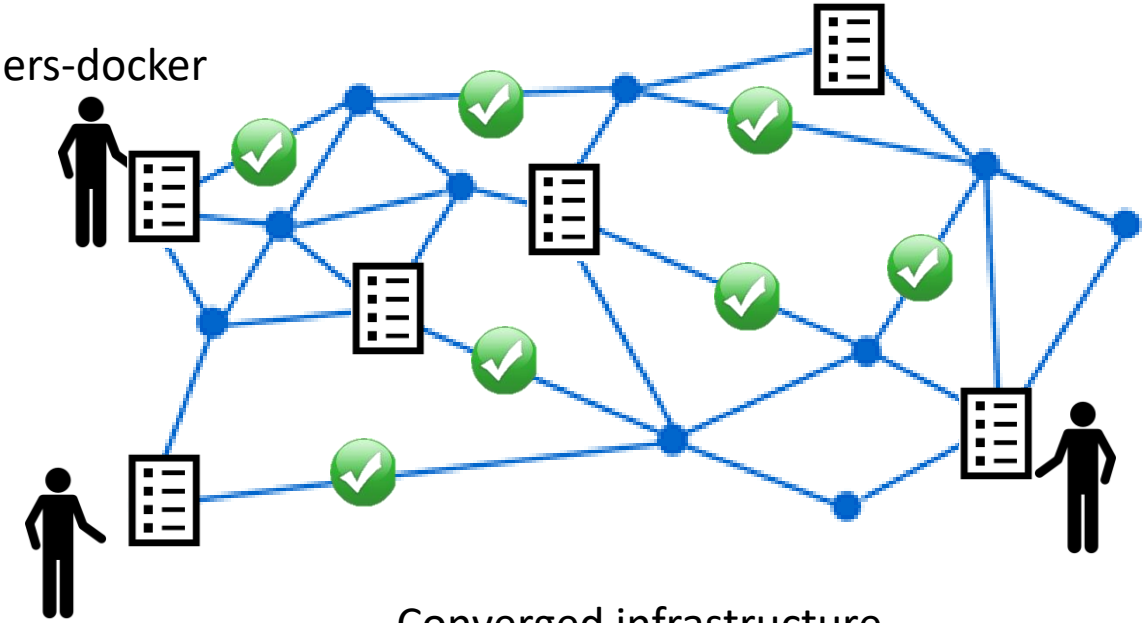


Traditional infra. organization



What we need for new organization at operations\infrastructure?

Containers-docker



Private cloud

Devops

Hyper-converged infrastructure

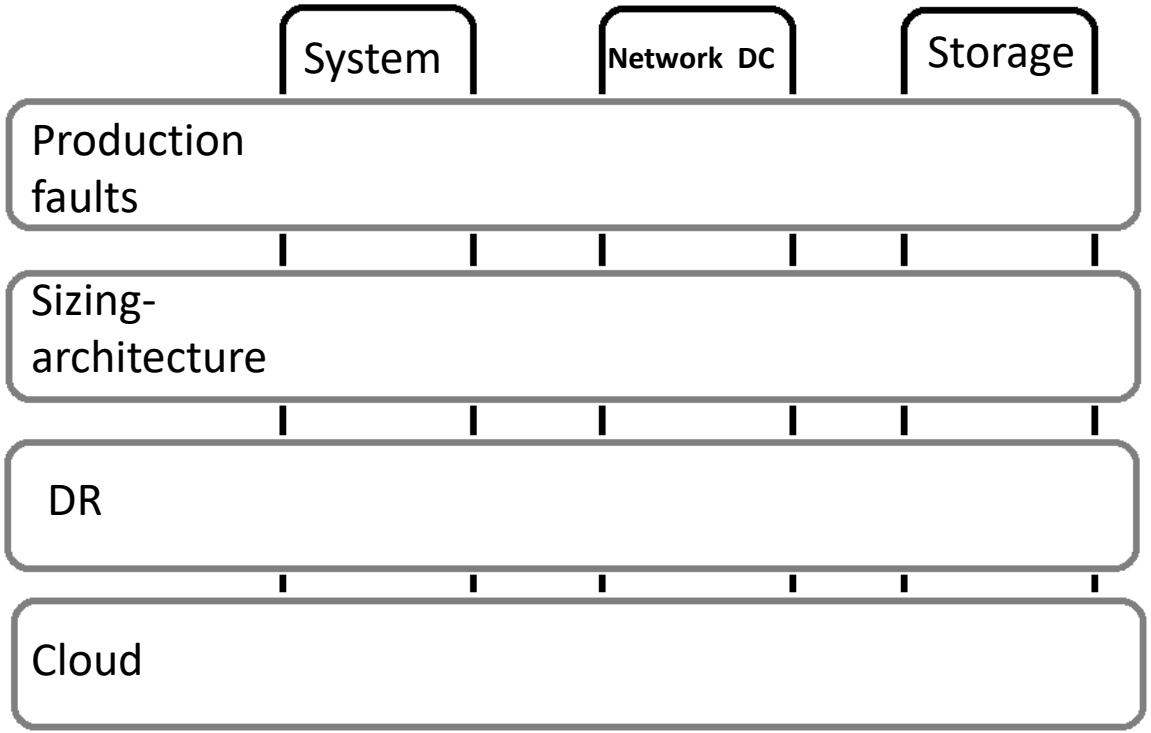
Converged infrastructure

Public\hybrid cloud

stki.info

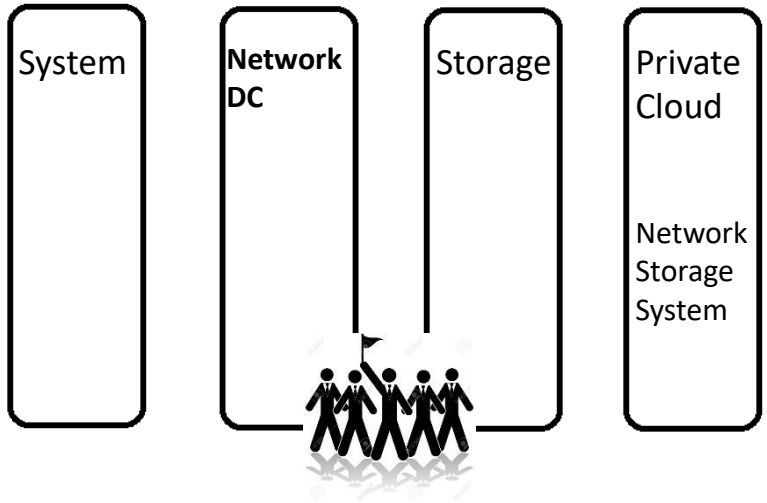
The best way – one team!!

Recommended mashup (product) organization



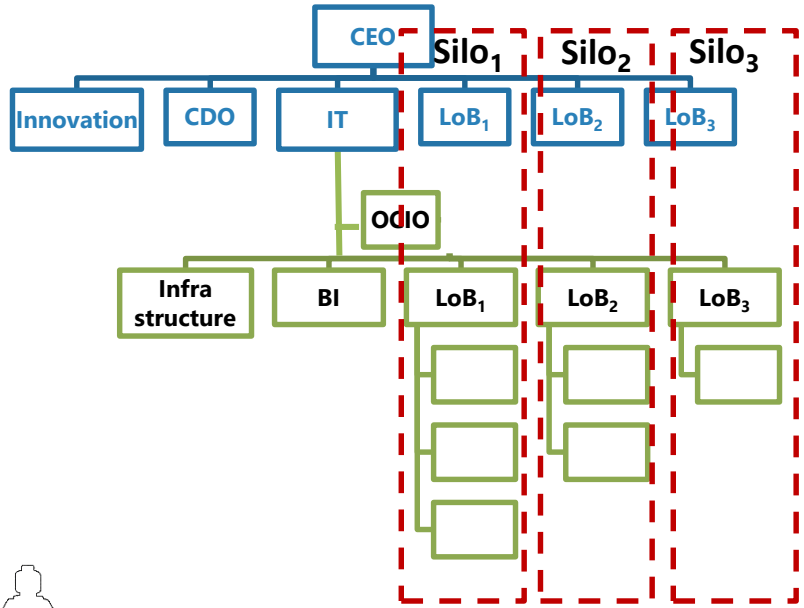
Also possible (short term)

- One team (for converged, cloud, etc.) , with skills differentiated, into the same department
- Also have security people integrated

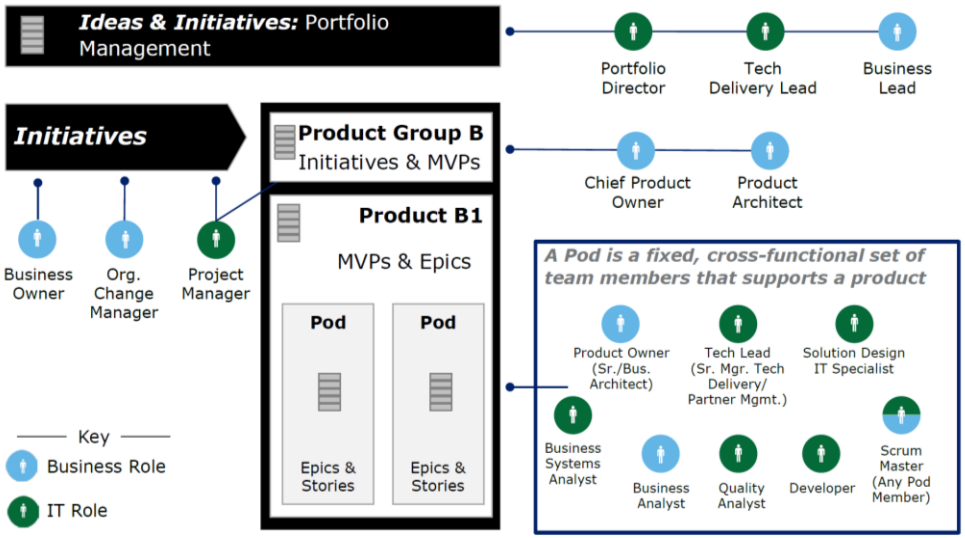


Development organization: break the functional silos. Use agile\lean

Sequential project phases with **different skill** groups



Multi skilled, **result** oriented teams



Source: Deloitte

Delivery skills and staffing

- Everybody (infrastructure, delivery) is a software developer (scripts)
    - implementing SDLC (source control, versioning, testing, agile, etc.)
- Delivery staffing might decline by 25%
    - Storage will decline more
    - System\server will decline less
    - Fragmented IT will experience less decline in staffing

Devops vs. CAB (change advisory board)

Head of operations\infrastructure responsibility:

Availability of IT

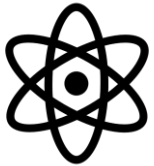
Change management (CAB)

What about Devops?

“Let them Devops” but approve the process (not specific change):

- Which tests are needed before prod?
- Which types of change don’t need CAB? (most of changes…)

Agenda



DC and infrastructure

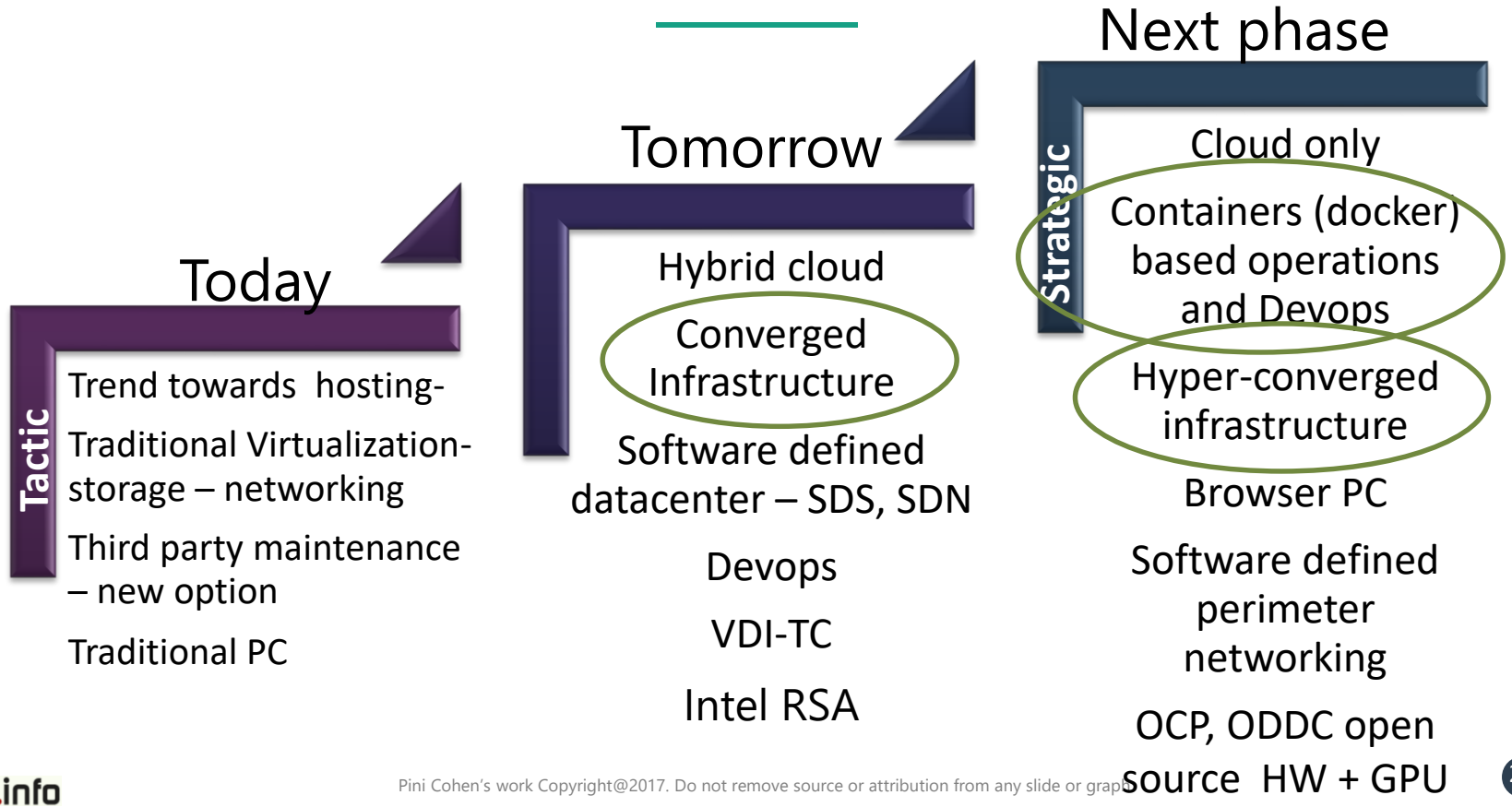
organization, processes and skills

middleware

cyber security

development and architecture

DC-Infrastructure layers



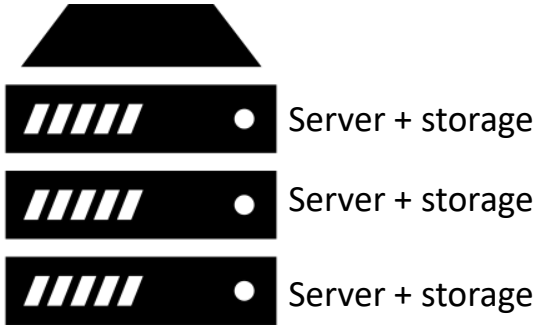
Converged infrastructure proven benefits

- Time to market from (many) months to weeks
  - Especially in integration and acceptance testing
- Easier maintenance and updates
  - Traditionally firmware update is done when error happens
  - Traditionally upgrade of one component leads to other upgrades

Big servers + big storage + network

Hyper-converged Infrastructure

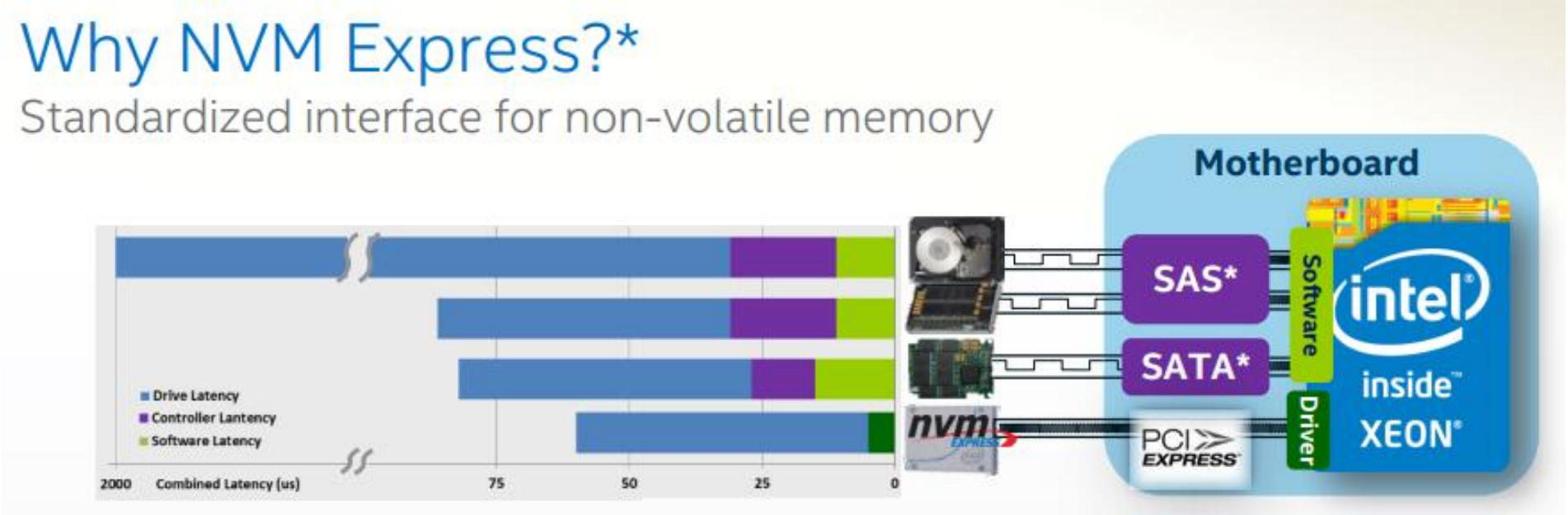
- Currently best fit for branches, SME, specific projects
- Performance and flexibility lags traditional infrastructure
- 40G DC networks will push Hyper-converged to main stream usage
- Network is part of hyper-converged vendor offering or part of client's DC



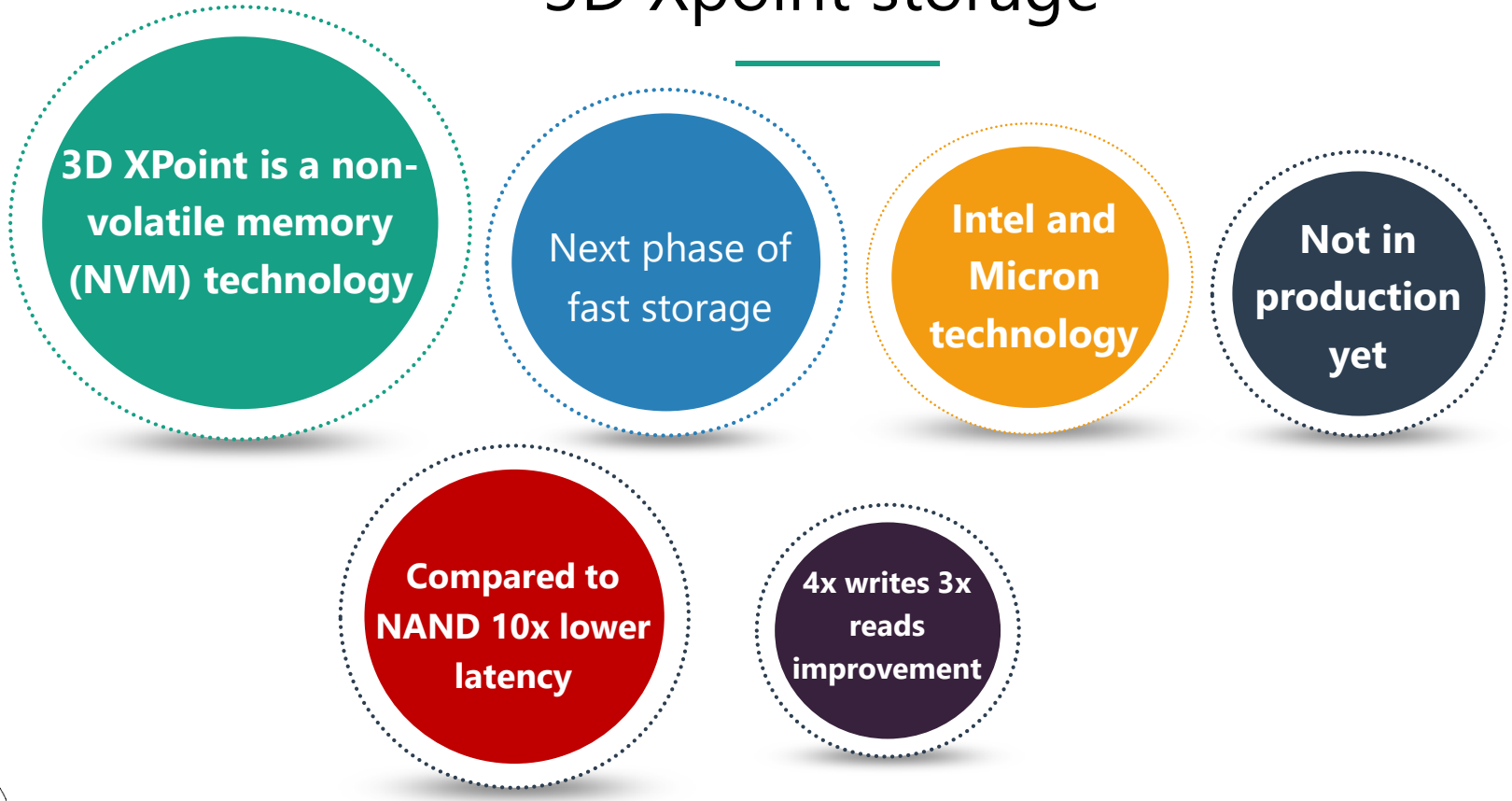
Storage as separate entity is evolving

- Flash is standard
- Active-Active is matured
- Organizations should explore object storage as part of their software defined storage journey

NVME based storage: no more SCSI



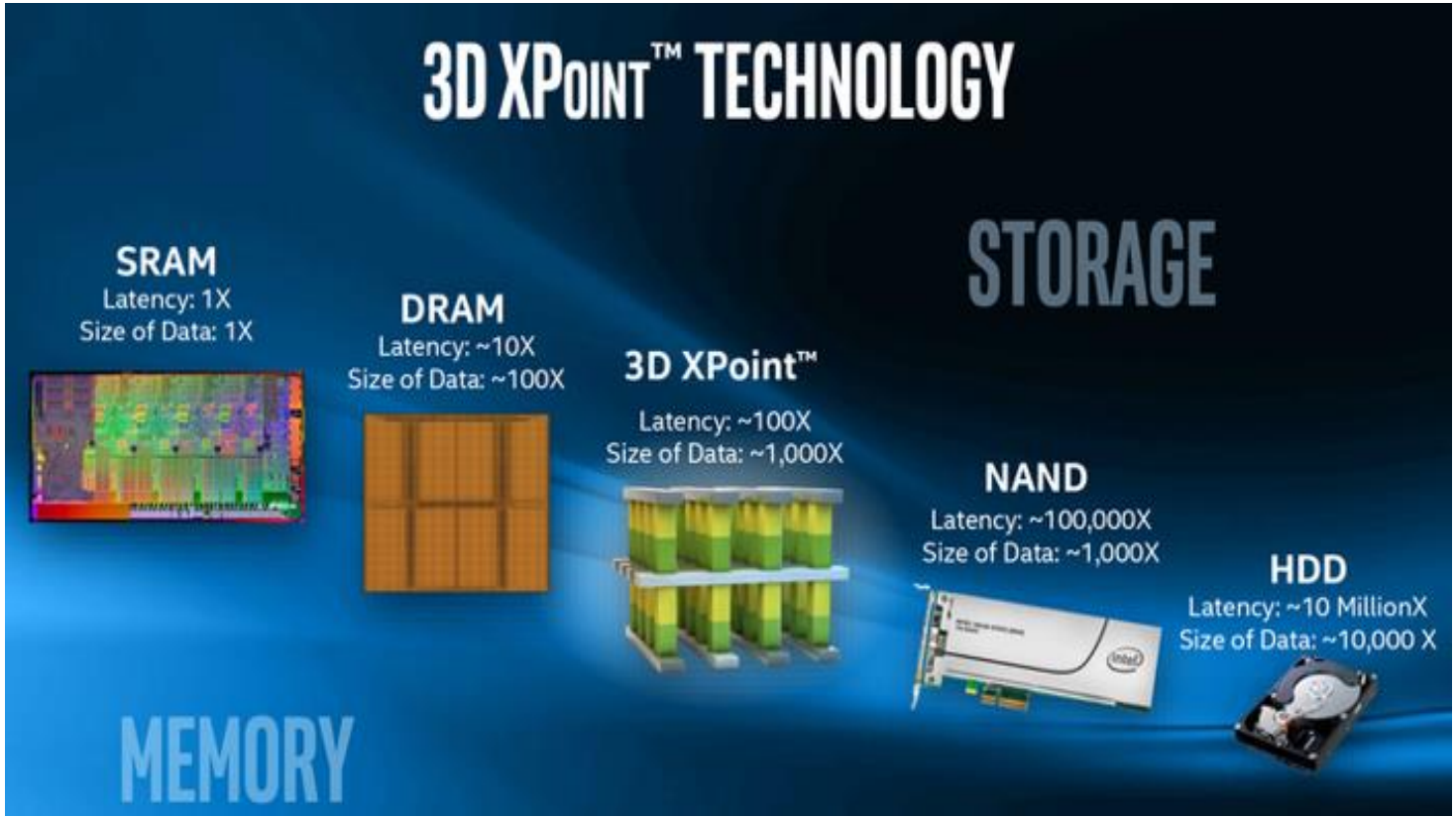
3D Xpoint storage



High

Speed

Low

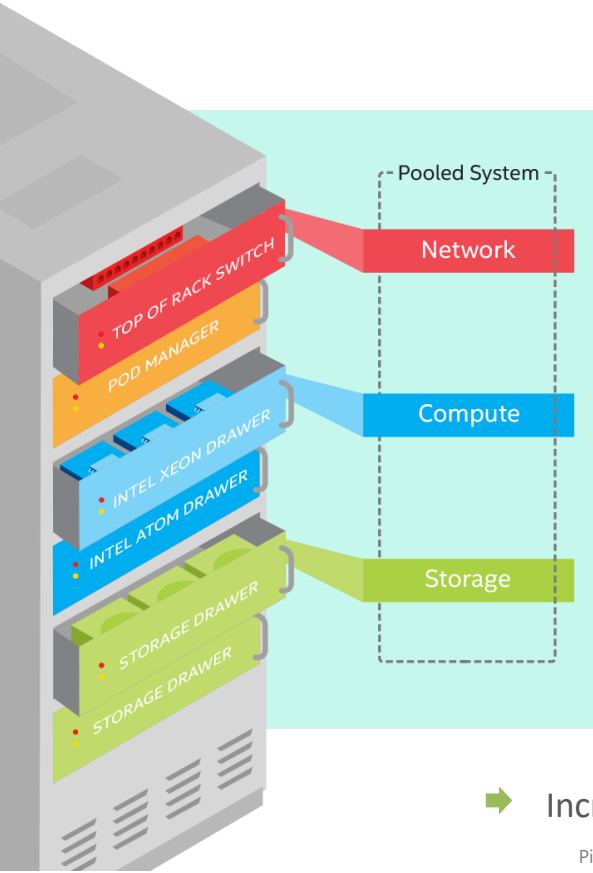


High ⟵ **cost** ⟶ Low

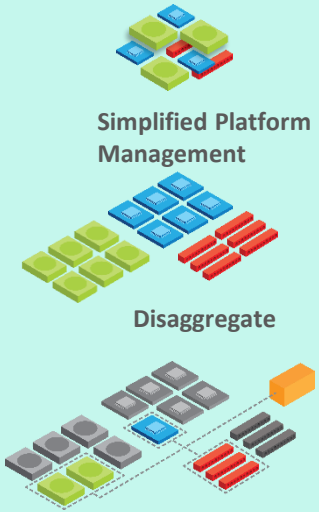
Source: Kaminario

Intel® Rack Scale Architecture (RSA)

ERICSSON



- Logical architecture for efficiently building and managing Cloud-Scale Infrastructure
- Provides the simplest path to a Software Defined Datacenter

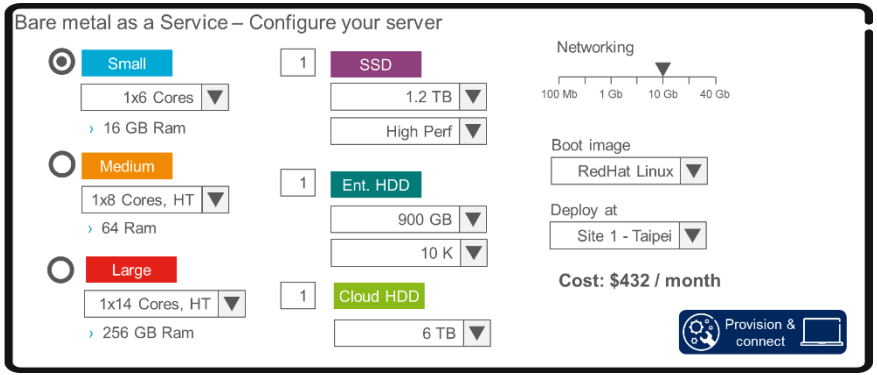


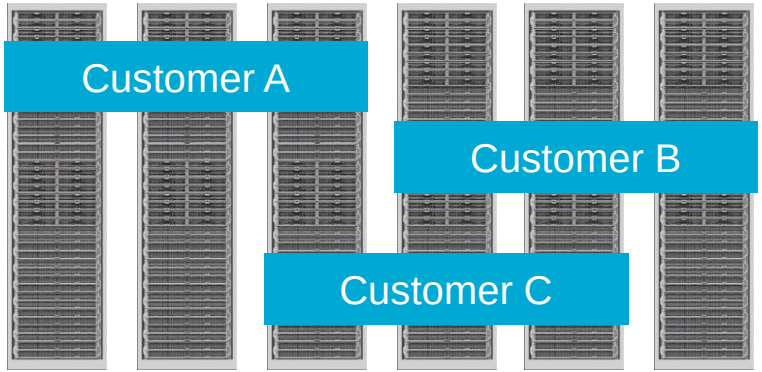
Compute, Network & Storage

➡ Increase performance per TCO$ & accelerate cloud adoption

Bare-Metal as a Service

- Next phase of Cloud Computing
- Leverage RSA and hardware orchestration to fully customize servers
- Move both legacy & performance critical workloads to the Cloud
- Cloud economics for Bare-Metal infrastructure
- Consolidate internal IT





Software defined perimeter

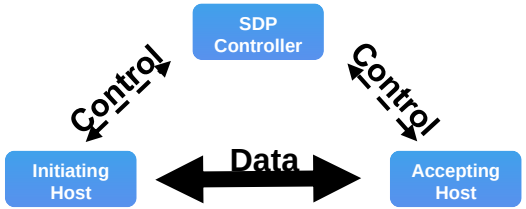
Connectivity based on a need-to-know model

identity is verified before access to application is granted

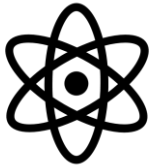
Black Cloud: deny all SDN application

Replace the "NAC" concept

"tighten the belt"



Agenda



DC and infrastructure

organization, processes and skills

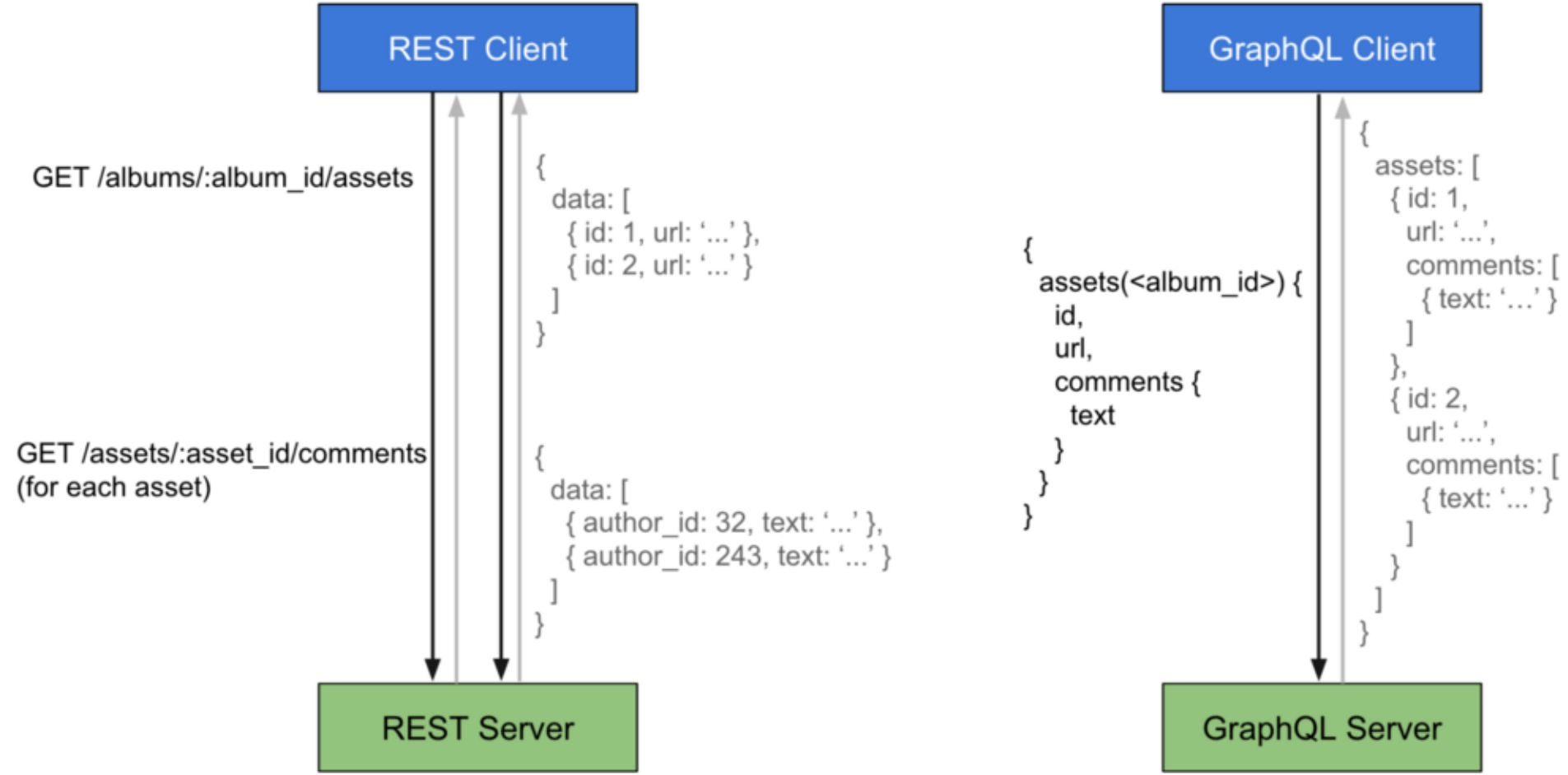
middleware

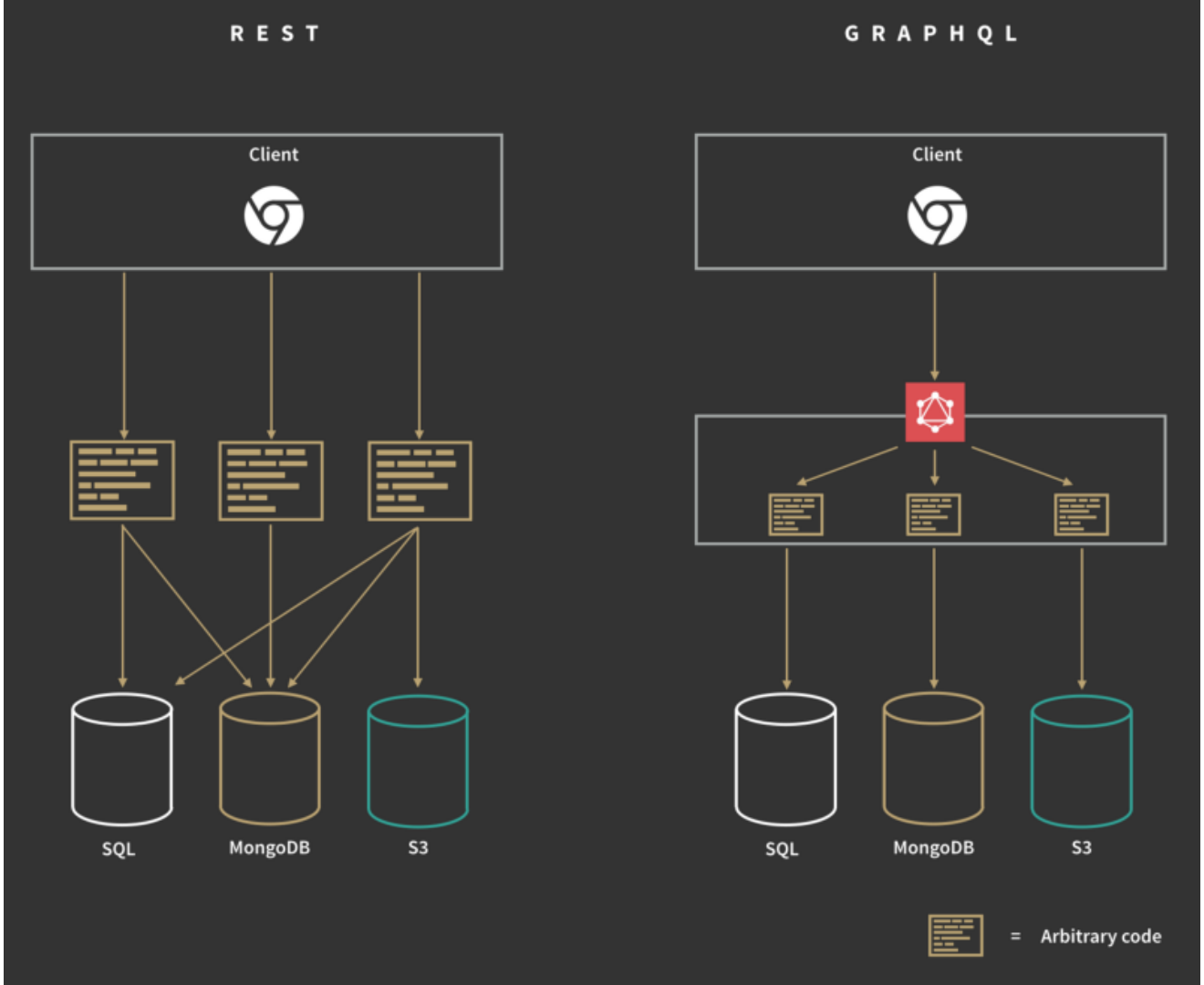
cyber security

development and architecture

Facebook's graphQL

- The client says to the server:

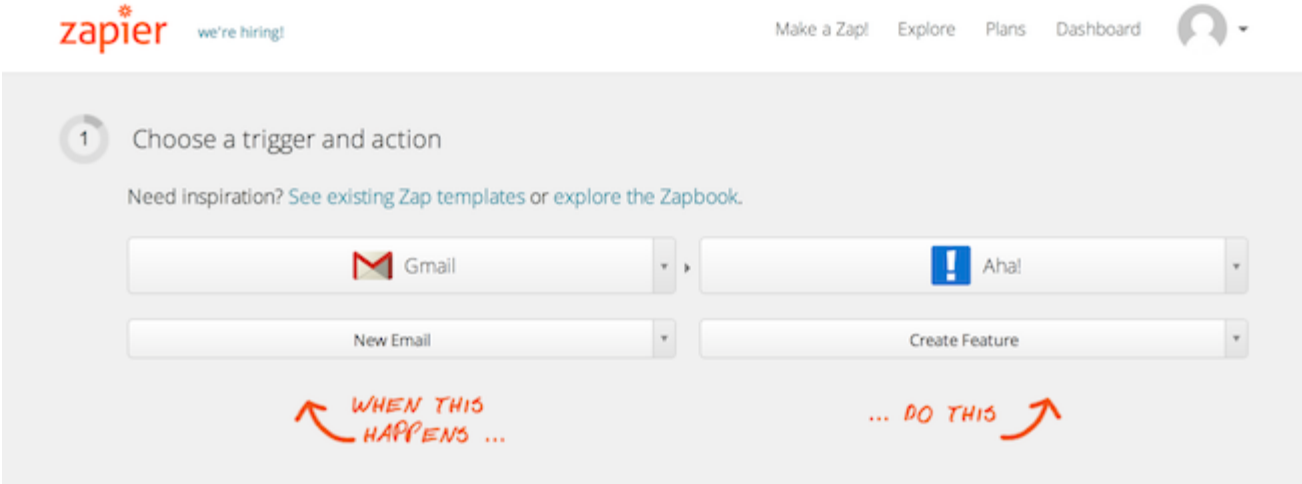



REST
GRAPHQL
Client
Client
SQL
MongoDB
S3
SQL
MongoDB
S3
= Arbitrary code

Cloud integration alternatives:

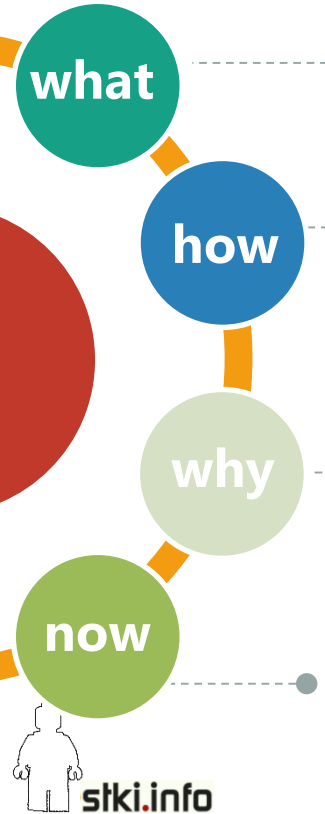
- Write code that access the API
- Reach the API via ESB + adaptor

zapier



stki.info

API mashup enablers



Swagger, Raml
Standards for API documentations

Common documentation specification
language for describing API's . Provides all the information necessary to describe RESTful or other APIs.

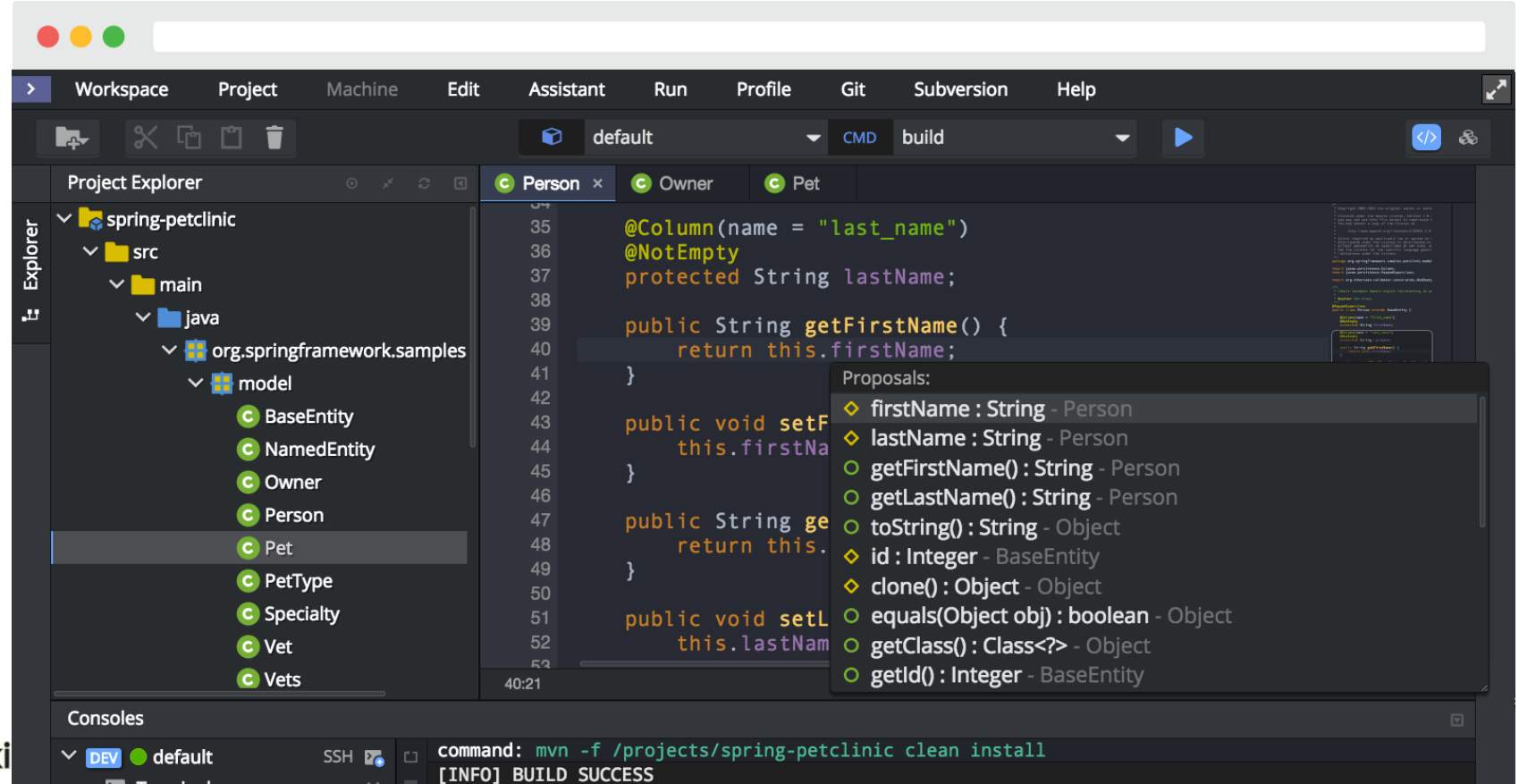
API economy
API economy is emerging as innovative force in growing companies

Upgrade to tools that support standard API documentations such as Raml or Swagger

Swagger definition

a specification for defining the interface of a REST web service

Using API's in IDE's



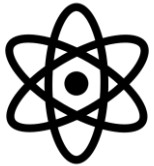
Swagger basic example

- For basic function http://host/greetings/hello/world that returns 'Hello world‘, basic swagger will be:

```
{  "swaggerVersion": "1.2",  "apis": [   {
     "path": "http://localhost:8000/listings/greetings",
     "description": "Generating greetings in our application."
   } ] }
```

More at: https://github.com/OAI/OpenAPI-Specification/wiki/Hello-World-Sample

Agenda



DC and infrastructure

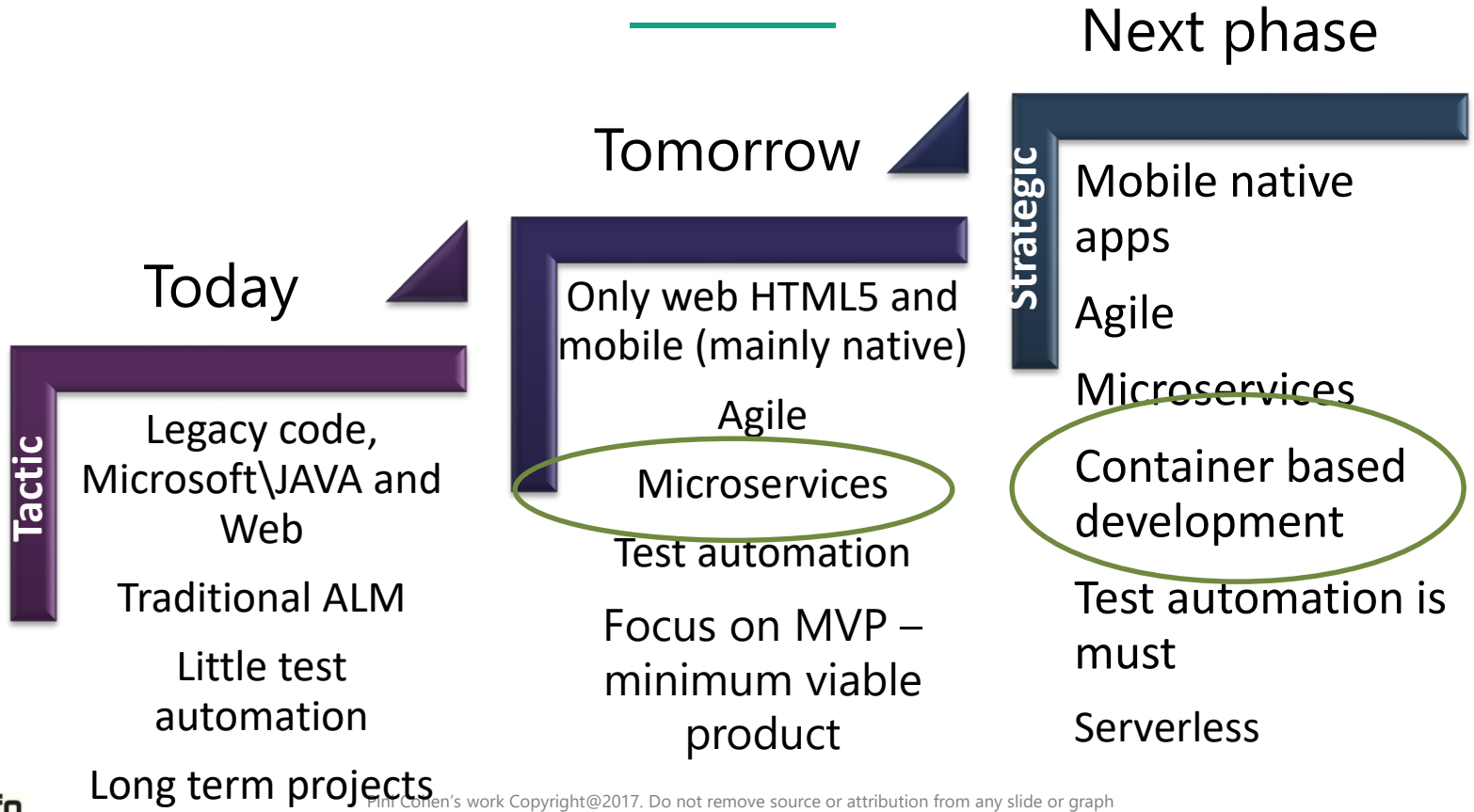
organization, processes and skills

middleware

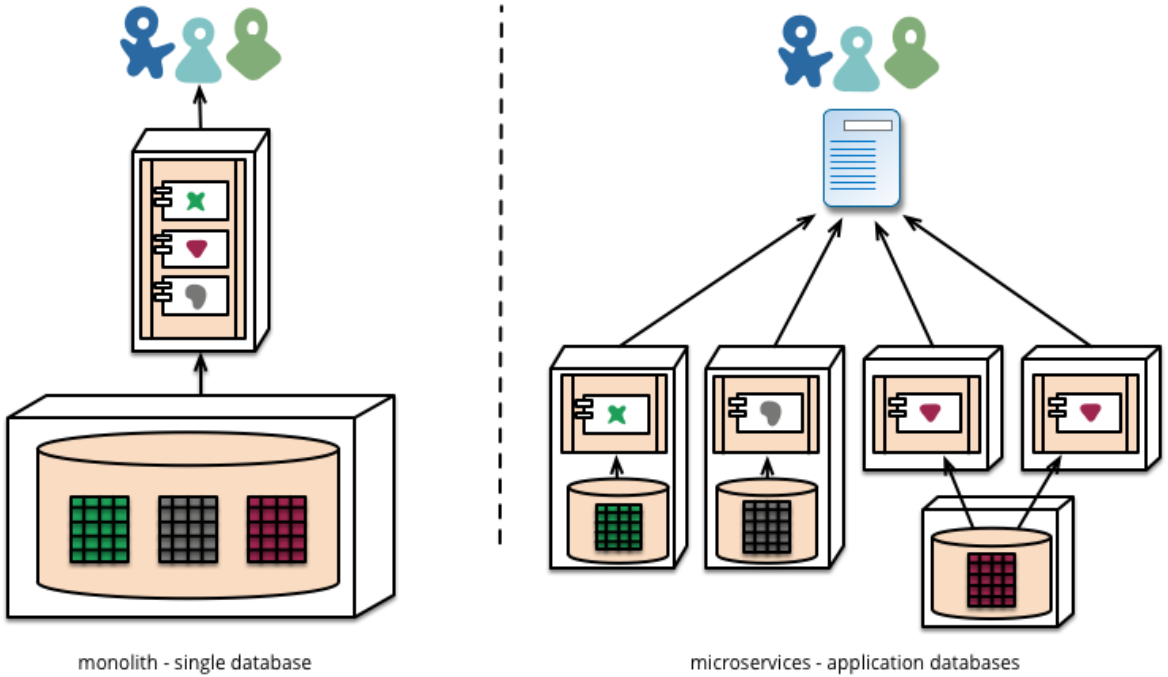
cyber security

development and architecture

Development and architecture

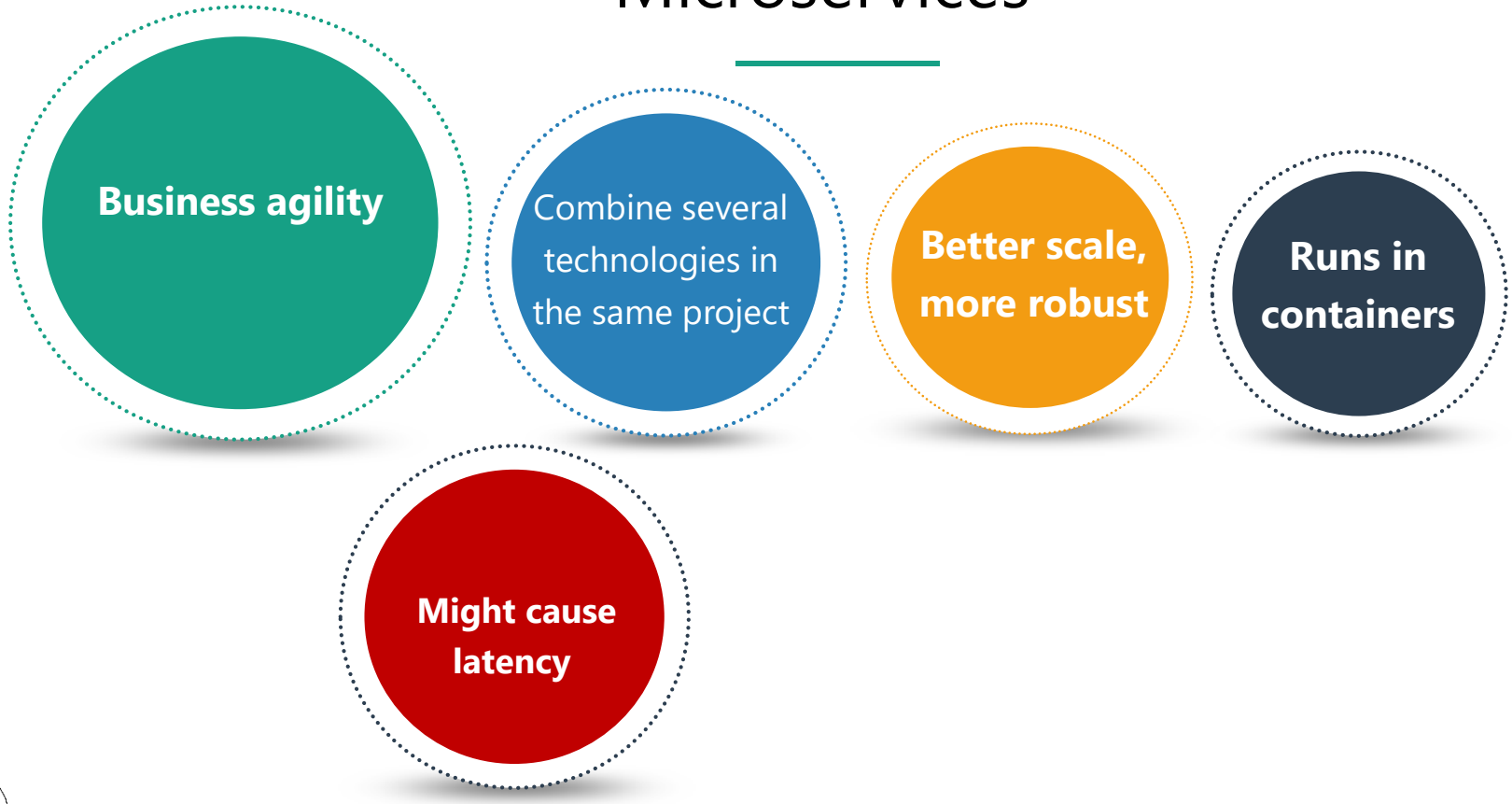


Microservices architecture



Source: http://martinfowler.com/

Microservices

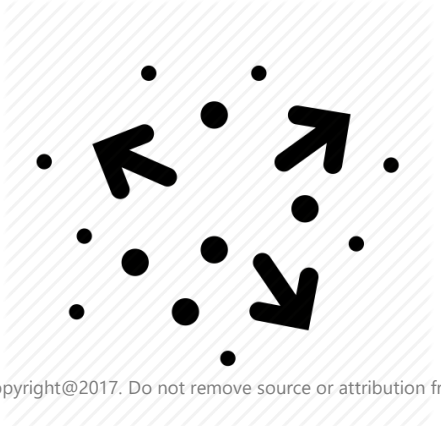


Stateless development

- When app falls – you simply start it
- Intermediate state (data) should be stored in persistent area (DB, disk)
- Application should run “as is” in dev-test-prod-cloud

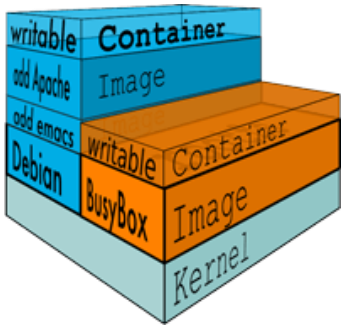
Development languages

- Client (web) in javascript with angular, react, meteor, amber or redux (and more…) frameworks
- Server in .net, java, nodejs, python, php, ruby, go, or scala (and more…) languages
- Client to server (to infra) in Rest/GraphQL communication

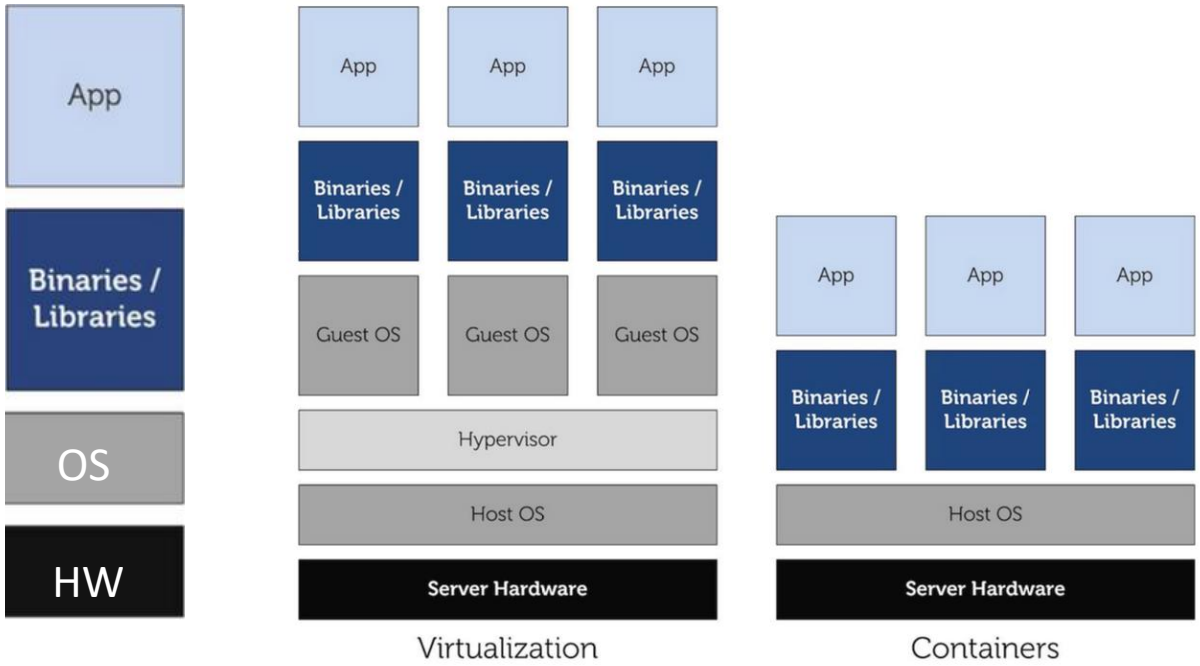


What are Linux Containers ?

- **Linux Containers** (LXC) is an operating-system-level virtualization method for running multiple **isolated Linux systems** (**containers**) on a single control host (LXC host).

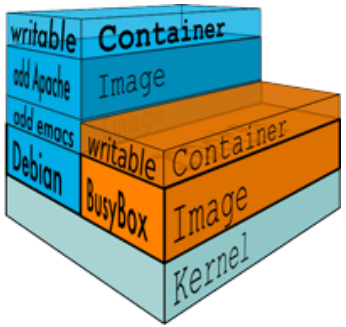


Virtual Machine Vs. Containers



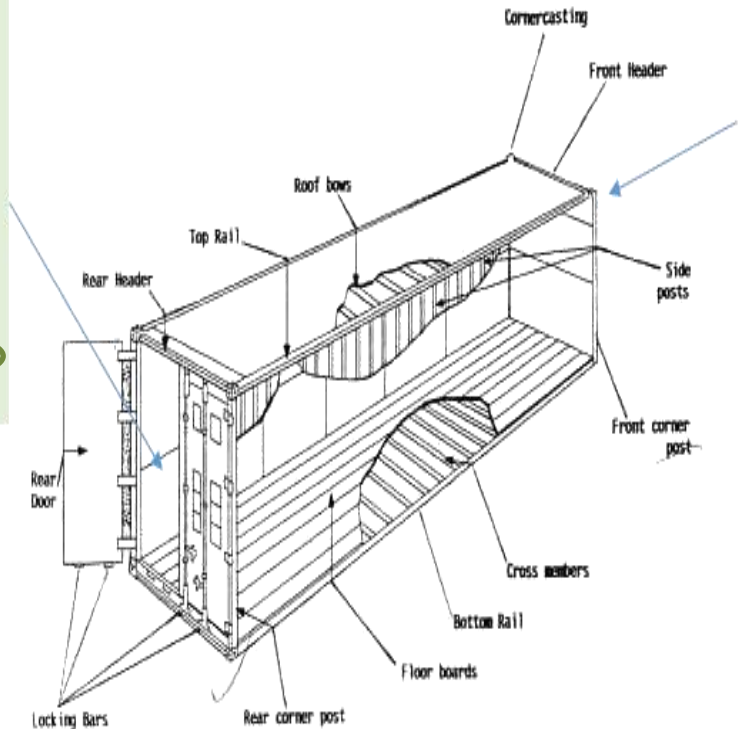
What is Docker ?

- **Docker** is an open-source project that automates the deployment of applications inside software **containers**, by providing an additional layer of abstraction and automation of operating-system-level virtualization on **Linux**. (Wikipedia)



Why it Works: Separation of Concerns……

- Dan the Developer
  - Worries about what's "inside" the container
    - His code
    - His Libraries
    - His Package Manager
    - His Apps
    - His Data
  - All Linux servers look the same



Major components of the container:

- Oscar the Ops Guy
  - Worries about what's "outside" the container
    - Logging
    - Remote access
    - Monitoring
    - Network config
  - All containers start, stop, copy, attach, migrate, etc. the same way

Source: files.meetup.com/11185112/**Docker**-Meetup-jan-2015-Final.ppt

Containers basics

- **Image**: ready to use, read only container file
- **Container**: specific image that is running (with “docker run” command). Able to run several containers based on the same image

stki.info

docker run

which image to run

other parameters (which program to run o
the image, etc.)

Which containers are running?

- docker ps

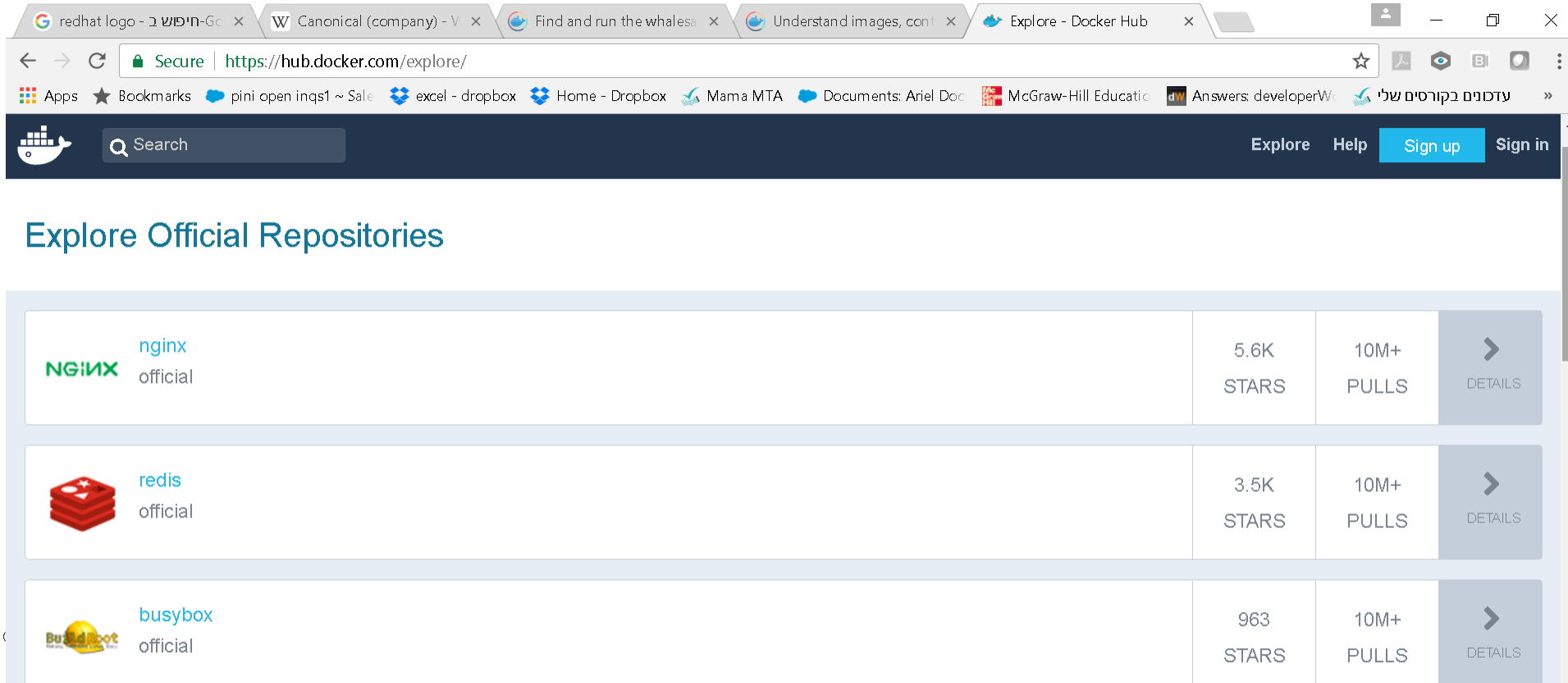
```
C:\Users\pini>docker run  nginx

C:\Users\pini>docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS               NAMES
be3d878a7e7a        nginx               "nginx -g 'daemon ..."   16 seconds ago      Up 15 seconds       80/tcp, 443/tcp     quizzical_ritchie
1109aa4b3886        nginx               "nginx -g 'daemon ..."   2 minutes ago       Up 2 minutes        80/tcp, 443/tcp     compassionate_hoover

C:\Users\pini>
```

stki.info

Docker Hub


redhat logo - חיפוש ב-Go
Canonical (company) - W
Find and run the whales
Understand images, cont
Explore - Docker Hub
Secure | https://hub.docker.com/explore/
Apps
Bookmarks
pini open inqs1 ~ Sale
excel - dropbox
Home - Dropbox
Mama MTA
Documents: Ariel Doc
McGraw-Hill Educatio
Answers: developerW
עדכונים בקורסים שלי
Search
Explore
Help
Sign up
Sign in
Explore Official Repositories
nginx
official
5.6K STARS
10M+ PULLS
DETAILS
redis
official
3.5K STARS
10M+ PULLS
DETAILS
busybox
official
963 STARS
10M+ PULLS
DETAILS

Pulling down the image

```
C:\Users\pini>docker run -d -p 80:80 --name webserver nginx
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
5040bd298390: Downloading [=======>                                           ] 7.339 MB/51.36 MB
31123d939af1: Downloading [==================>                                ] 7.239 MB/20.24 MB
23f1bdd267a9: Download complete
```

stki.info

Defining new image

- Defining new image with “dockerfile

- **FROM** docker/whalesay:latest
- **RUN** apt-get -y update && apt-get install -y fortunes
- **CMD** /usr/games/fortune -a | cowsay

APT-GET is linux installation utility
CMD – which program to run

stki.info

Creating new image based on dockerfile

- C:\Users\pini\docker2>docker build -t docker-demo-stki-2 .

```
C:\Users\pini\docker2>docker build -t  docker-demo-stki-2 .
Sending build context to Docker daemon 2.048 kB
Step 1/4 : FROM docker/whalesay:latest
 ---> 6b362a9f73eb
Step 2/4 : RUN apt-get install -y fortunes
 ---> Using cache
 ---> 905887f5c5ec
Step 3/4 : RUN apt-get install -y vsftpd
 ---> Running in 7859f3dffa68
Reading package lists...
Building dependency tree...
Reading state information...
The following extra packages will be installed:
  libwrap0 tcpd
The following NEW packages will be installed:
  libwrap0 tcpd vsftpd
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 181 kB of archives.
After this operation, 599 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu/ trusty/main libwrap0 amd64 7.6.q-25 [46.2 kB]
```

List of docker images

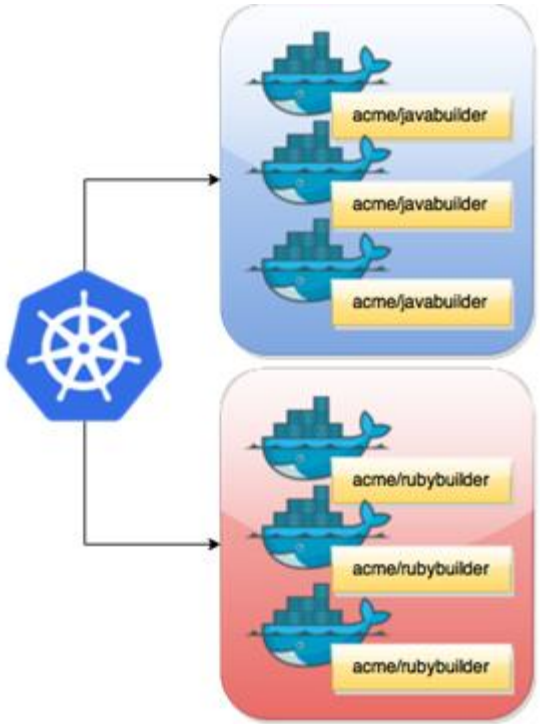
docker-demo-stki-2

```
C:\Users\pini\docker2>docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
docker-demo-stki-2  latest              07f588df1561        2 minutes ago       259 MB
docker-demo-stki    latest              cbfa30ee4721        4 weeks ago         254 MB
pini_image          latest              cbfa30ee4721        4 weeks ago         254 MB
docker-pini         latest              762357029855        4 weeks ago         277 MB
nginx               latest              db079554b4d2        5 weeks ago         182 MB
hello-world         latest              48b5124b2768        2 months ago        1.84 kB
docker/whalesay     latest              6b362a9f73eb        22 months ago       247 MB

C:\Users\pini\docker2>
```

stki.info

Container schedulers and orchestration



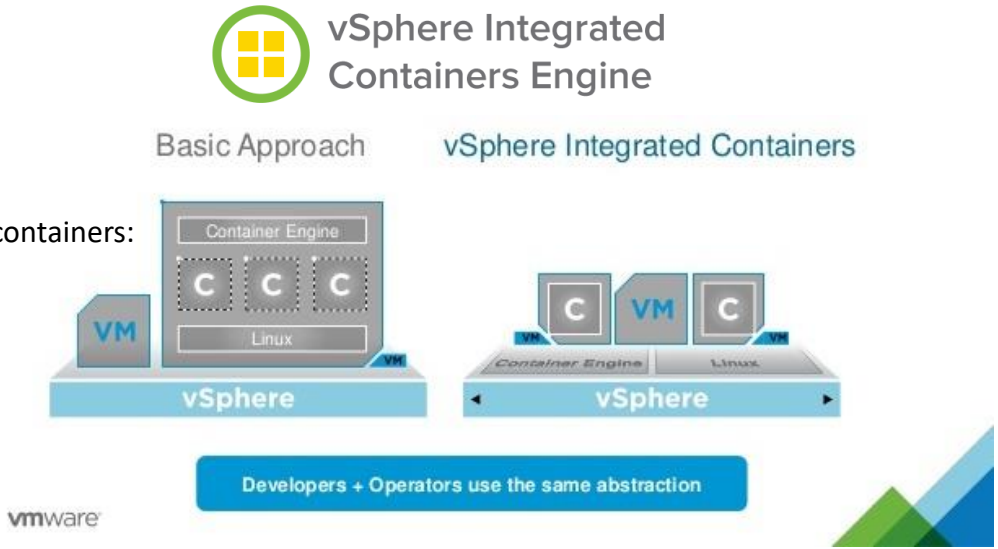
About containers

- Containers bundle your app code, dependencies, configuration in a unit, *abstracting your app from infrastructure*
- Operations: easier to deploy across dev, test, and prod environments. Less errors
- Developers: faster, independent development.
- Better scale up\down (time to provision 10th of second)
- Perfect fit for microservices and Devops
- Standard way for ISV to distribute their SW
- Broad adoption by ISV, cloud, and infrastructure
- New procurement model server→CPU→Core→container

stki.info

The floor is shaking

VMWARE and containers



docker & vmware

PHOTON OS™

VIC : each container runs in its own micro vm (dedicated kernel) using memory clone technology named vmfork that spin the micro vm fast and efficiently

Microsoft and containers

Scott Guthrie

https://blogs.msdn.microsoft.com/wsl/2016/04/22/windows-subsystem-for-linux-overview/

Microsoft | Developer

Search

Sign in

Windows Subsystem for Linux

The underlying technology enabling the Windows Subsystem for Linux

Windows Subsystem for Linux Overview

Follow Us

Rate this article

Jack Hammons April 22, 2016

Share 1

91

Archives

ZDNet

CXO HARDWARE MICROSOFT STORAGE INNOVATION HARDWARE APPLE MORE NEWSLETTERS ALL

MUST READ CAREER PROSPECTS IN TECHNOLOGY: HOW FAR CAN YOU REALLY GO?

Microsoft and Canonical partner to bring Ubuntu to Windows 10

You'll soon be able to run Ubuntu on Windows 10.

Windows Subsystem for Linux (WSL) is a compatibility layer for running Linux binary executables ….**natively on Windows 10** …. WSL provides a Linux-compatible kernel interface developed by Microsoft (containing no Linux kernel code)

Duck Test

Do you know this Linux machine?

Mainstream platform for enterprise IT

- Web - Rest/GrapQL
- Microservices
- Stateless
- Agile & lean

- Devops and infrastructure as code
- SQL or noSQL
- Container (Docker)
- Operated by container schedulers (kubernetes, etc.)

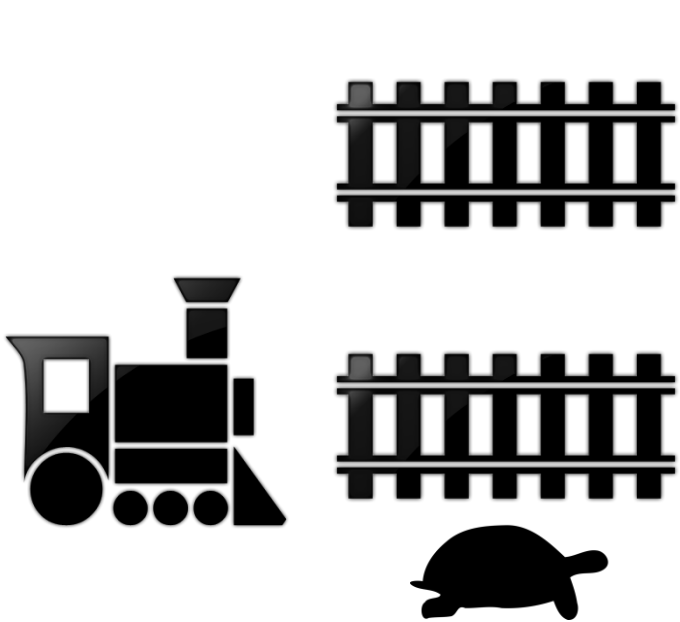
B$ questions about mainstream:

- Will 

run on bare metal or on cloud computing platform (Openstack, VMWARE-VRA, etc.)?

Kubernetes (containers) enables cloud interoperability

The Openstack train



Telecos
Service providers
Huge enterprise IT

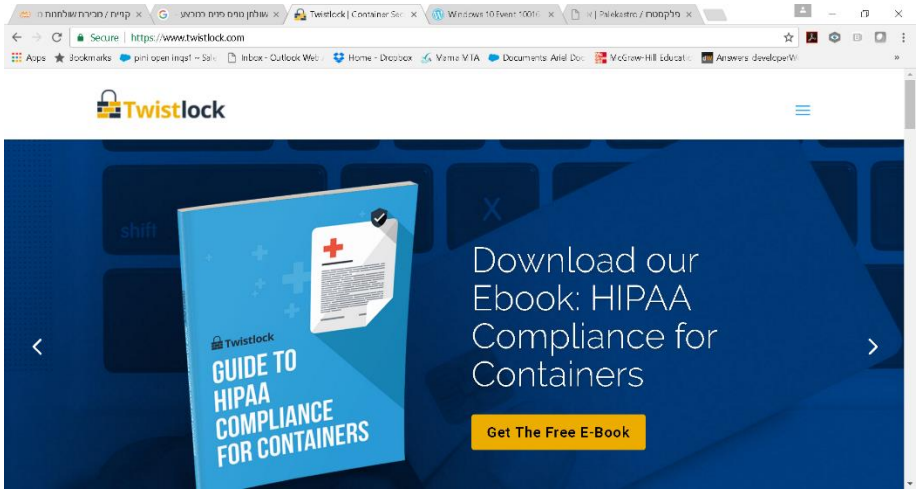
Israeli enterprise IT

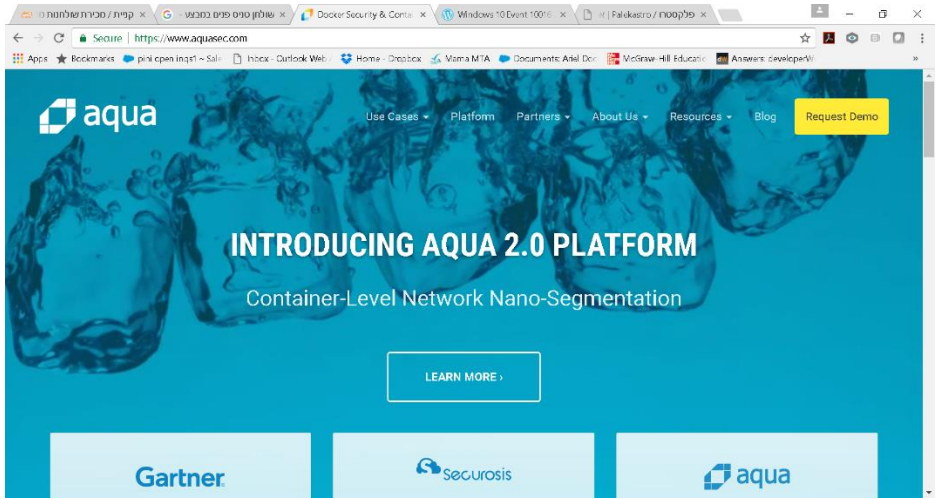
B$ questions about mainstream:

- Will 

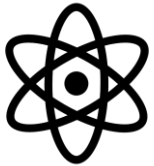
run and be configured natively or delivered via APaaS/XPaaS (Openshift, Cloud-Foundry, Bluemix, etc.)?

Containers security





Agenda



DC and infrastructure

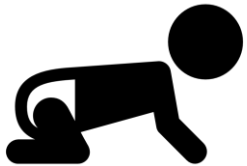
organization, processes and skills

middleware

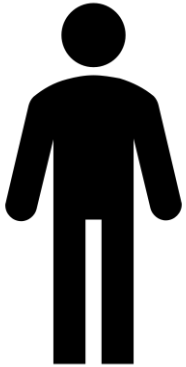
cyber security

development and architecture

Cyber security vs. Information Security



Information Security



Cyber security

Cyber security vs. Information Security

And the winner is: Cyber security

Cyber, internal politics, organization and roles

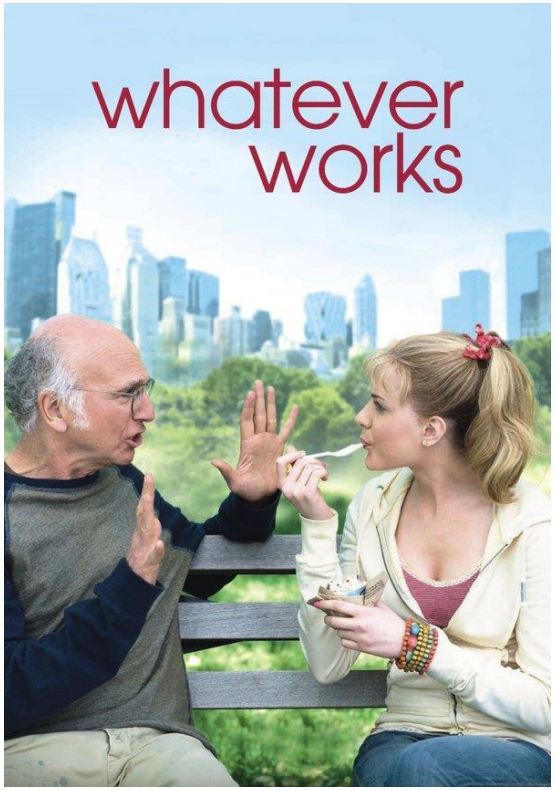
Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

נייר עמדה: מבנה ארגוני וקבלת החלטות בתחום סייבר בארגוני Enterprise IT

סיכום מנהלים:

- בתחום הסייבר יש להבחין בין **"גורם מבקר"**, **"גורם מנחה"** ו**"גורם מתפעל"** (אחראי סייבר).
- הגורם האחראי לטיפול ותפעול נושא הסייבר בארגון הוא ה-CIO (**"הגורם המתפעל"**). **לא ניתן להפריד בין תפעול ה- IT הכללי לבין תפעול נושא הסייבר**.
- לעיתים, יאציל ה- CIO סמכות (ואחריות) לטיפול ותפעול נושא הסייבר למנהל התפעול-תשתיות.

STKI on cyber organization:



Cyber organization principals

- Dedicated cyber operations team
- Dedicated cyber guidance team
- Dedicated cyber control team

Cyber organization and roles

- Dedicated cyber operations team
  - Security analysts that take action
    - Deepest cyber knowledge but also multidisciplinary (T-people)
    - Responsible for the SIEM-SOC rules
    - Practical guidance for the rest of IT (development, infra, PC, network, etc.)
    - **Tight link to operations (part of operations = part of CAB)**
    - Outsourcing the security analysts is not trivial
  - Cyber operations team (FW, EPP, patches, DBMS, development)
  - Permission team

Cyber organization and roles

- Dedicated cyber guidance team
  - "Head above water"
  - Regulations
  - Risk management methodology
  - Business priorities

Cyber organization and roles

- Dedicated cyber control team
  - Independent of operations and guidance

Conflicts in cyber

- No Objectives + No Measurement = conflicts !!

נייר עמדה: מדידה בתחום סייבר

סיכום מנהלים:

- על הנהלות ארגונים (ורגולטורים) להנחות את הארגונים לבצע מדידה בתחום סייבר.
- המדידה תתבצע ברמה ארגונית, מחלקתית, פרוייקטלית ואישית.
- ספציפית, יש למדוד את מנהלי התפעול\תשתיות מבחינת סייבר כפי שהם נמדדים כיום מבחינת תפעולית (זמינות, ביצועים וכד'). מדידה זו תסייע להוריד את הקונפליקט בין תחום התפעול לתחום הסיבר.
- יש לשים דגש על דיווח ומדידה של החרגות תוך ציון ההסבר לשיקול הדעת שגרם להחרגה.

Add cyber metrics to operations

דרכי מדידה

להלן תיאור של דרכי מדידת סייבר בקרב ארגוני enterprise :

1. קיום כלי אבטחת מידע \ סייבר בהתאם ל- BEST PRACTICE . בהמשך התייחסות ליוזמה של מטה הסייבר בתחום זה.
2. עמידה ביעדים שנקבעו בארגון. בתחום זה ניתן לציין מדדים תפעוליים\טכנולוגיים בהקשר לתפעול מערכות הסייבר שמותקנות והתהליכים שהוגדרו. לדוגמה "מספר מחשבי ה- PC אשר אינם מחוברים לרשת ואשר לא קיבלו עדכון של אבטחת מידע יותר משלושה ימים הנו 5". " 90% מה- patches הקריטיים בשרתים יעודכנו תוך חודש" . "מה אחוז מהתוכניות שעבר סריקת קוד ללא ממצאים" (appscan checkmarks וכד'). "זמינות ה- FW היא מעל 99% " וכד'.
3. עמידה בתוכנית העבודה בתחום סייבר (גם היא סוג של יעד).
4. כמות ארועי אבטחת מידע שהתרחשו בארגון בתקופה מסויימת (כולל התקפות שנחסמו, חדירות ללא פגיעה וכד').
5. תוצאות מבדקי אבטחת מידע טכנולוגים. כאן יש להגדיר מדדים לגוף הבודק (עמידה בכמות המבדקים, עמידה בזמן המוקצה למבדקים). יש להגדיר מדדים לגוף הנבדק – כמות הממצאים, חומרתם[2] ותוך כמה זמן טופלו (לפי חשיבות הממצע) . מדד נפרד בתחום זהוא הוא תמונת המצב הארגונית בהקשר ל- awareness.
6. ביצוע סימולציה של מתקפה בארגון (יבשה או רטובה – כולל קוד שמשתילים בארגון) ובחינת אופן התנהלות הארגון.
7. תוצאת מבדקי אבטחת מידע שאינה טכנולוגים בעיקרם – לדוגמה משאירים disk on key

Israel National Cyber Authority standardization act (in process)

מדינת ישראל
משרד ראש הממשלה
הרשות הלאומית להגנת הסייבר

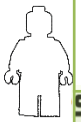
	A	B	F	G	H	I	J	K	L	M
1				לא רלוונטי	לא קיים	הטמעה טכנולוגית (התקנת המוצר)	הטמעה לוגית הגדרות עפ"י	פריסה בארגון (אחוז פריסה	מבדקי חדירה והגדרות פרטניות	תחזוקה שוטפת
17	רשת									
18		IPS / IDS	האם קיימת מערכת לזיהוי / חסימת מתקפות בארגון?							
19		NAC	האם קיימת מערכת בקרת גישה לרשת?							
20		Segmentaion	האם קיימת הפרדת רשתות בארגון ?							
21		AntiVirus	האם מוטמעת מערכת אנטי וירוס בארגון?							
22		VA Scanning	האם מבוצעות סריקות ברשת לאיתור חולשות אבטחת מידע?							
23	שרתים									
24		OS Hardening (Disable Admin etc)	האם קיימת מערכת להקשחת מערכת הפעלה ?							
25		OS updates (Patch Management)	האם קיימת מערכת לביצוע עדכונים (טלאים) ?							
26		VM Machine protection	האם קיימת מערכת להגנה על מכונות וירטואליות?							
27		Anti Virus / Anti Malware	האם מותקנת מערכת אנטי וירוס על גבי השרתים ?							
28		Cyber protection	האם קיימת מערכת לזיהוי מתקפות סייבר על שרתים ?							
29	תחנות קצה									
30		Anti Virus / Anti Malware	האם קיימת מערכת לזיהוי מתקפות סייבר על שרתים ?							
31		End Point Security	האם קיימת מערכת להגנה על התקני קצה ?							
32		OS updates (Patch Management)	האם קיימת מערכת לביצוע עדכונים (טלאים) ?							
33		Device Control	האם קיימת מערכת לניהול רכיבי קצה (DOC, CDROM ובד')							

ראשי | תוכנית הגנה IT | תוכנית הגנה ICS | תוכנית הגנה אוש

רמת אבטחה	טכנולוגיות הגנה / בקרות	קריטיות מימוש רמת אבטחה (3-1) - 1 נמוך	קריטיות בקרות (3-1) - 1 נמוך	שכלול	מוצרים לדוגמא	הטמעה לוגית הגדרות עפ"י הגדרות יצרן	הטמעה טכנולוגית (התקנת המוצר)	פריסה בארגון (אחוד הפריסה בכלל הארגון)	מבדקי חדירה והגדרות פרטניות מותאמות לארגון - אוטומיזציה	תחזוקה שוטפת	רמת בשלות	אחוז מימוש מצב הארגון (ממוצע)	אחוז בשלות יחסי	אחוז מימוש מצב הארגון (קריטיות בקרה)	שלבי הטמעה (סדרי עדיפות להטמעה בארגון)					
						0%	30%	70%	90%	100%					שלב 1	שלב 2	שלב 3	שלב 4	שלב 5
תוכנית-הגנה-IT																				
כלי ניהול שליטה וניטור	1.1	1		100%								73%		75%						
	1.11	SIEM		20%	3					1	HP Arcsight		100%		20.0%					
	1.12	הגדרת Log במערכת		20%	3			1					70%		14.0%					
	1.13	System Change Management		20%	3				1		Tufin, algosec		90%		18.0%					
	1.14	DLP - דלף מידע		13%	2						Websense, Se	1	0%		0.0%					
	1.15	מערכת לזיהוי אנומליות		7%	1				1		lightcyber		90%		6.0%					
	1.16	ניהול גיבויי מערכות אבטחת מידע		13%	2				1		BACKBOX		90%		12.0%					
	1.17	תקקור סייבר		7%	1			1			Wirex		70%		4.7%					
הגנה חיצונית	1.2	3		100%								73%		76%						
	1.21	Firewall		21%	3						CheckPoint, Pa	1	60%		12.9%					
	1.22	Anti Spam / Email Protection		14%	2						Fortinet	1	60%		8.6%					
	1.23	Web filtering		21%	3				1		Websense		90%		19.3%					
	1.24	SSL VPN		14%	2						Juniper	1	60%		8.6%					
	1.25	WAF		21%	3					1	F5, Imperva		100%		21.4%					
	1.26	SandBox		7%	1			1			FireEye		70%		5.0%					
רשת	1.3	2		100%								48%		47%						
	1.31	IPS / IDS		15%	2						PaloAlto	1	0%		0.0%					
	1.32	NAC		8%	1			1					70%		5.4%					

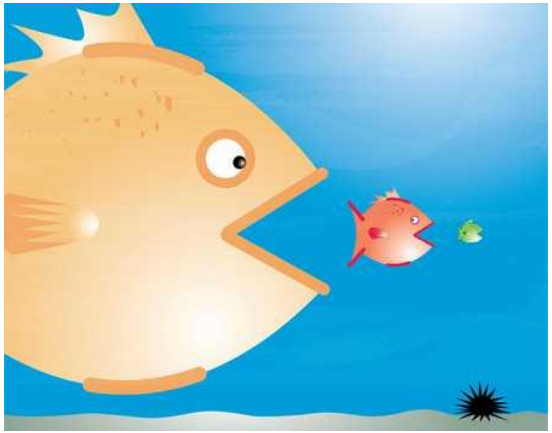
Too many cyber tools …

EDR endpoint detection & response	Code scanning tools	Authentication	Bio Authentication	CASB (cloud access)
Data Classification	Data Masking	Database Security	DDOS	Deception Honeypot
DLP	Email Security (email gateway)	Encryption	Endpoint Security	Firewall
Fraud Prevention	Incident Response	IPS	MDM MAM - mobile device management	PAM – Privileged access management
Network Access - NAC	Secure Email Gateway	Web security - Secure Web Gateway	SIEM	Web Application Firewall



Cyber security personnel

Conclusion – something needs to change



Market consolidation

Game changer technology

The nightmare: zero day attack

- Attack exploiting undisclosed computer-software vulnerability

Categorization of cyber (zero day?) defense approaches

Anomaly detection (prod and sandbox, network-endpoint, application-business level)

Pattern of malicious activity (basic example – user entry but much too fast)

Format changing (הלבנה, secured browsing)

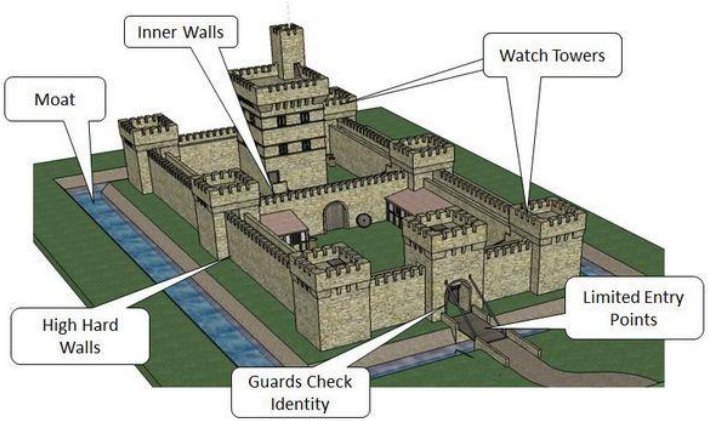
Honeypots \ Deception

HW security (Intel's SGX, ARM's trusted zone CPU)

Technology "tricks" (morphisec, IBM's ROP solution)

Moving Target Defense

- Moving-target (MT) techniques seek to randomize system components (IEEE)
- Tricks + Deception

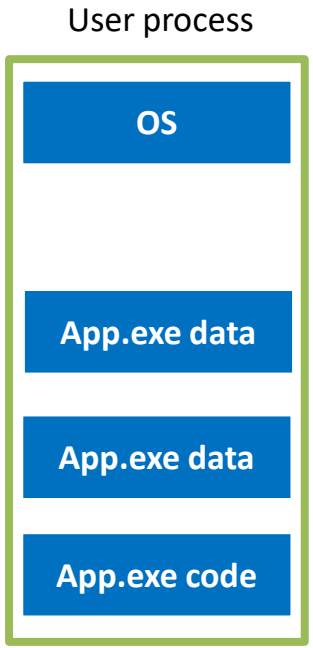


Moving Target Defense

- What is moving (changing)?
  - Memory addresses, Heap structure
  - User names \ credentials
  - Physical location
  - Code Obfuscation - change the exec file
- How fast?
  - Every time the program runs
  - While the program is running
- Detection level

Intel Software Guard Extension (SGX)

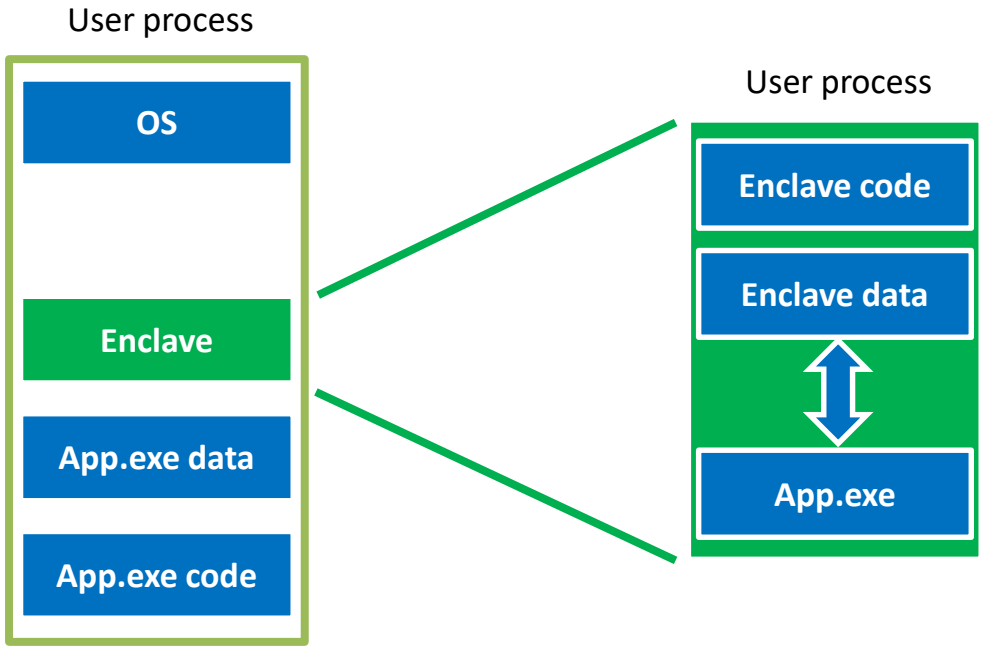
Current architecture:



F.Schuster et al. “VC3: trustworthy data analytics in the cloud using SGX,” 36th IEEE Symposium on Security & Privacy,

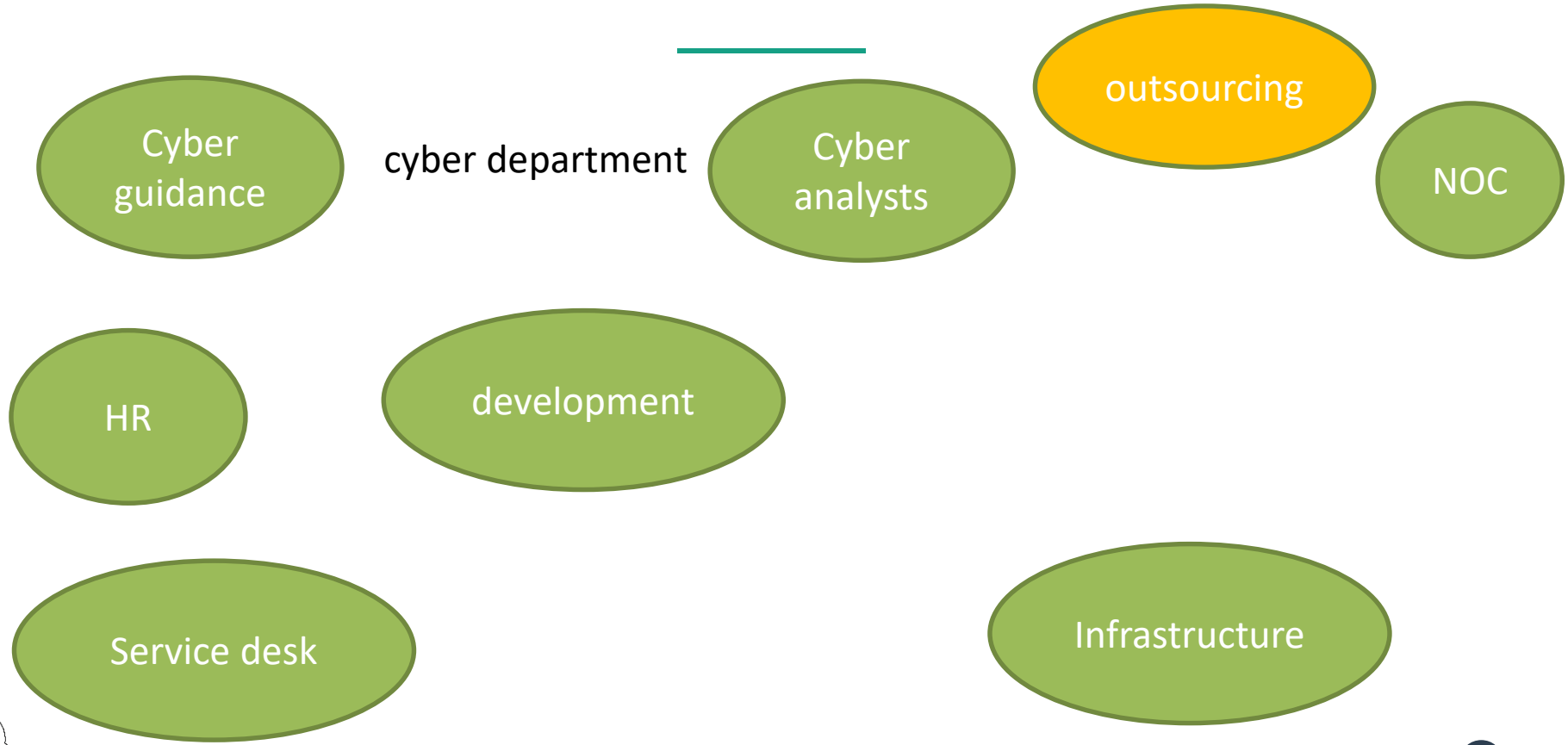
Intel Software Guard Extension (SGX)

- **ENCLAVE?**
- Hardware-based protection
- User level execution
- E-init (compare measurements of enclave)



F.Schuster et al. "VC3: trustworthy data analytics in the cloud using SGX," 36th IEEE Symposium on Security & Privacy

FTE ratios are not trivial – cyber roles map



Cyber roles map

outsourcing

Regulations
Top management
cyber risk management
high level policy

Cyber guidance

practical policy
(development, suppliers, identity)

Cyber analysts

analyst - response team, define siem rules
בקרים

NOC

awareness

cyber tools: FW, dlp, encryption, DBMS FW, EPP (AV), deception

HR

development

cyber related tools: patch management, networking, hardening, privileged account management, email security, data masking, authentication

permission (operations - not policy)

Service desk

Infrastructure

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

stki.info

2017

Cyber personnel: operational/guidance

- Number of operational cyber personnel divided to cyber guidance personnel for **non regulated** orgs (regulations is less 50% of cyber budget):

Per FTE	# operational / # guidance
25 percentile	1.58
Median	2.00
75 percentile	2.75

Source: STKI

stki.info

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

stki.info

2017

Cyber personnel - guidance

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

Per FTE	# employees / # cyber guidance
25 percentile	338
Median	410
75 percentile	1095

Source: STKI

Insurance agents (not employees) are not counted but still get service

stki.info

Cyber personnel – first level SOC

- Options for **first level** SOC operations mode:
  - In sourcing : 1-2 FTE at work hours, 1 FTE at night. Total is about 6-9 FTE
  - In sourcing: 1-2 FTE at work hours, at night - part of NOC. Total is about 3-4 FTE
  - Outsourcing mode - 0 FTE.

Source: STKI

Cyber personnel – cyber analysts

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

Per FTE	# employees / # cyber analysts
25 percentile	600
Median	667
75 percentile	1000

Source: STKI

- Regulated organizations will have minimum 2 cyber analysts (part of SOC or guidance). External response team might be used when needed.

Insurance agents (not employees) are not counted but still get service

2017

Cyber personnel - operations

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

Per FTE	# employees / # cyber operations
25 percentile	217
Median	285
75 percentile	500

Source: STKI

- Example for cyber operations activities: FW, network security, email security, DBMS firewall, encryption, authentication, security patches, hardening, etc.
- In many cases part of infrastructure technology teams (networking, sytem, PC, etc).

stki.info

2017

Cyber personnel – permissions team

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

Per FTE	# employees / # permissions team
25 percentile	465
Median	600
75 percentile	667

Source: STKI

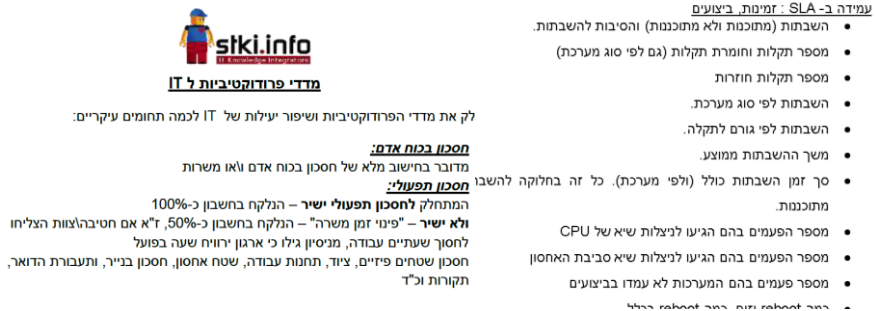
- Permissions team might be part of service desk, security guidance or security operations

Insurance agents (not employees) are not counted but still get service

Before we conclude - some questions

- Do you give enough priority to “the new mainstream” ?

- How do you measure my progress? What do you measure (example: Devop metrics)? What are your KPI’s?



stki.info

מדדי פרודוקטיביות ל IT

לק את מדדי הפרודוקטיביות ושיפור יעילות של IT לכמה תחומים עיקריים:

חסכון בכוח אדם:

מדובר בחישוב מלא של חסכון בכוח אדם ו\או משרות

חסכון תפעולי:

המתחלק **לחסכון תפעולי ישיר** – הנלקח בחשבון כ-100%

ולא ישיר – "פינוי זמן משרה" – הנלקח בחשבון כ-50%, ז"א אם חטיבה\צוות הצליחו לחסוך שעתיים עבודה, מניסיון גילו כי ארגון ירוויח שעה בפועל

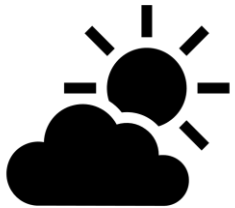
חסכון שטחים פיזיים, ציוד, תחנות עבודה, שטח אחסון, חסכון בנייר, ותעבורת הדואר, תקורות וכ"ד

עמידה ב- SLA : זמינות, ביצועים

- השבתות (מתוכנות ולא מתוכננות) והסיבות להשבתות.
- מספר תקלות וחומרת תקלות (גם לפי סוג מערכת)
- מספר תקלות חוזרות
- השבתות לפי סוג מערכת.
- השבתות לפי גורם לתקלה.
- משך ההשבתות ממוצע.
- סך זמן השבתות כולל (ולפי מערכת). כל זה בחלוקה להשבו
מתוכננות.
- מספר הפעמים בהם הגיעו לניצלות שיא של CPU
- מספר הפעמים בהם הגיעו לניצלות שיא סביבת האחסון
- מספר פעמים בהם המערכות לא עמדו בביצועים

Summary- Let's ride the tsunami wave!

But focus on where you want to go!!



That’s it.

Thank you!