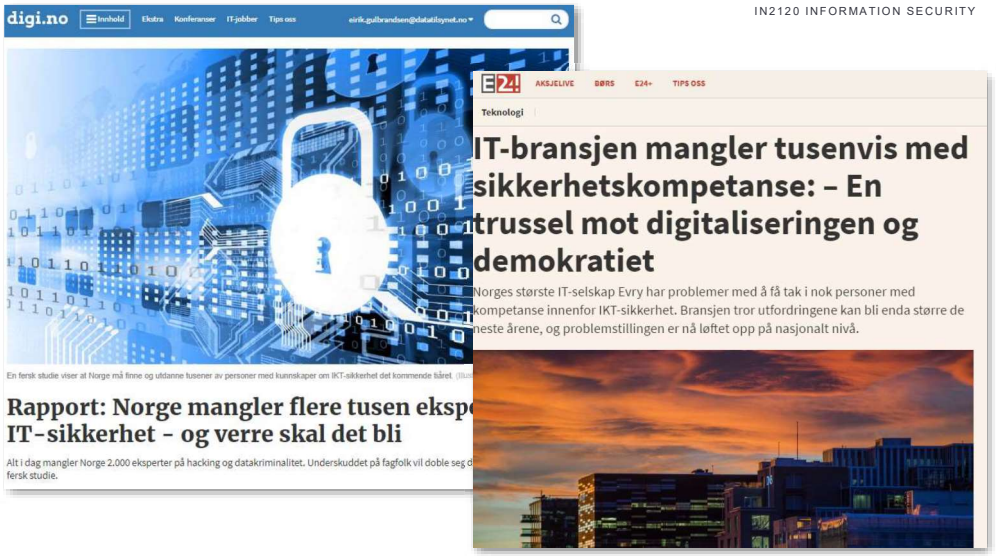
IN2120 Information Security

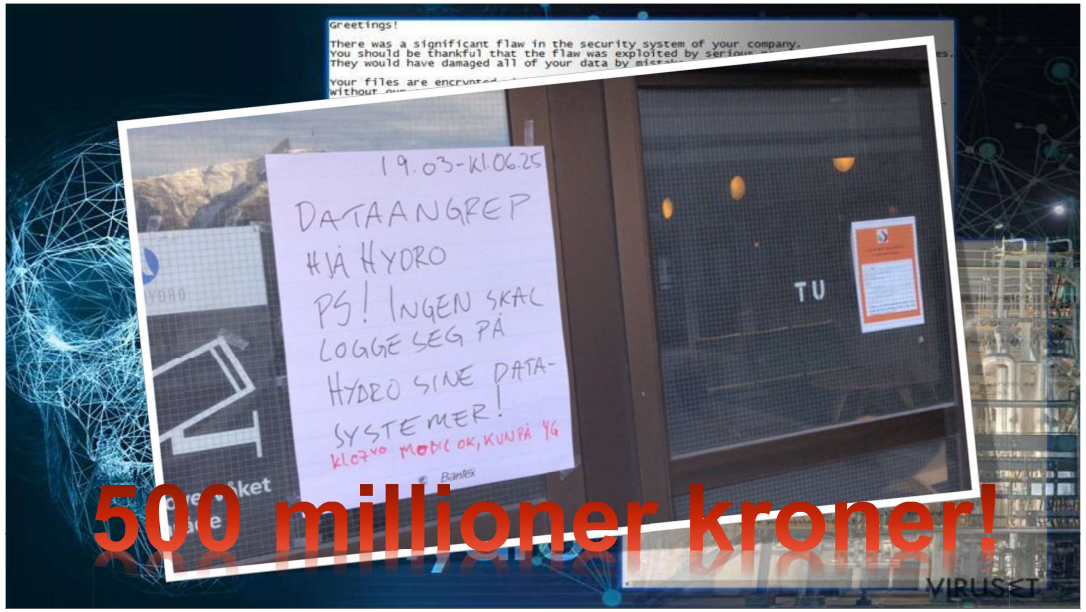
Universitetet i Oslo - Institutt for Informatikk

Høst 2019

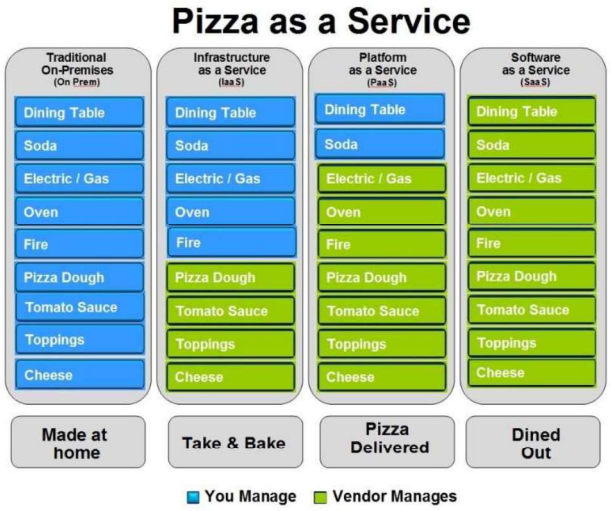
Eirik Gulbrandsen
Cloud Security Alliance Norway / Datatilsynet

DevSecOps/
Sikkerhet i skyen

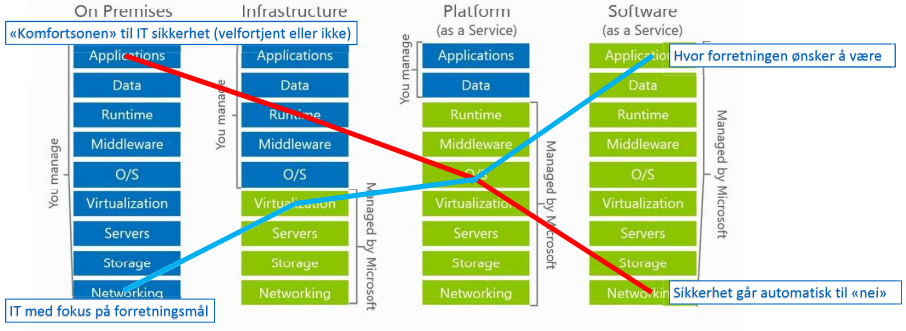




500 millioner kroner!

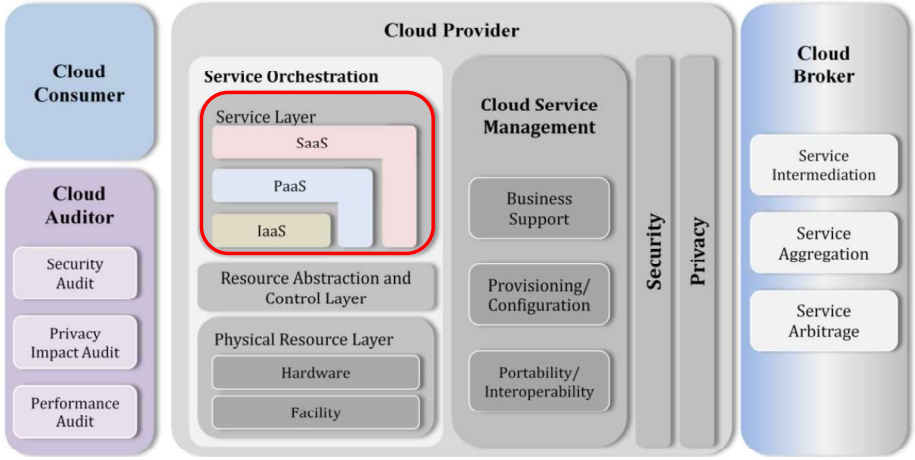


Cloud Models (delt ansvar – inkl sikkerhet)



- SAAS = Office 365
- PAAS = Azure Web Services
- IAAS = Windows Server (VM)
- On Premises = Exchange Server

NIST Cloud Computing Reference Architecture



«Skya» @ Norge

5.
«Too big to fail» –
Utenlandske selskaper
bærer norske
samfunnsfunksjoner

Sikkerhet og skytjenester

NOU 2015:13 D… sikkert

«Tjenesteutsetting av IKT-tjenester til profesjonelle aktører **kan gi bedre sikkerhet** og **mer stabile og tilgjengelige tjenester**. Tilgang til ekspertkompetanse og verktøy mai ikke selv besitter kan bedres, kostnader kan bli lavere og mer forutsigbare og det kan i større grad bidra til bedre fokus på virksomhetens kjerneaktivitet. Samtidig må virksomheter være **bevisst hvilken risiko** en tjenesteutsetting medfører. Tilsvarende eller

Nasjonal strategi for bruk av skytenester

Målet er at dette skal gi:

- meir kostnadseffektiv IKT
- auka merksemd på kjerneverksemda
- auka fleksibilitet
- **betre tryggleik gjennom meir profesjonalisert og standardisert IKT**
- lågare terskel for innovasjon og nyetablering
- redusert klimaavtrykk frå IKT-drift

Sikkerhetsfaglige anbefalinger ved tjenesteutsetting, NSM 2018

Sikkerhet kan også være en driver for tjenesteutsetting, særlig med fremveksten av skytjenester fra store, anerkjente IT-selskaper. Gitt at virksomheten har vurdert risiko og gjennomført tiltak for å bøte på risiko, vil tilgangen til store, profesjonelle sikkerhetsmiljø hos driftsleverandøren erfaringsmessig gi **bedre sikkerhet**, fordi **kompetansen er større, sikringstiltakene er flere,** og tjenester og løsninger i bruk er oppdatert til siste versjoner

Meld.St. 38 IKT-sikkerhet – Et felles ansvar

Selv om utkontraktering og bruk av skytjenester kan bidra til økt teknisk IKT-sikkerhet, **fritas ikke virksomheten for IKT-sikkerhetsansvaret og -arbeidet.**

Hva er "skya"?
...og hva er Dev(Sec)Ops?

Hint; IT-automasjon → *økt forretningshastighet*

"Functions"

"Cloud Thinking"

CISSP;
Cloud Computing

The use of shared ~~remote~~ computing ~~devices~~ for the purpose of providing ~~improved~~ efficiencies, performance, reliability, scalability and security.

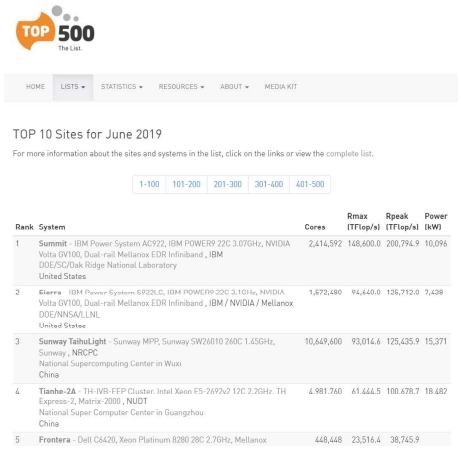
"Shift and Lift"

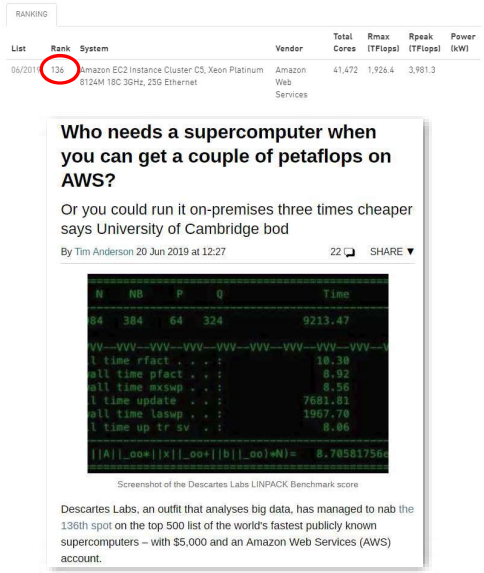

Equinor inngår partnerskap med Microsoft om skytjenester fra norske datasentre

20. juni 2018 09:00 CEST

Samarbeidet ... setter Equinor i stand til å utforme og fremskynde utviklingen av hensiktsmessige IT-tjenester for energibransjen, og sikre en raskere overgang til skytjenester. ***Å kunne utnytte skyen er en forutsetning for industriens digitale framtid.*** *Sikker, pålitelig og kostnadseffektiv drift er en forutsetning for Equinors bruk av skytjenester.*

– Den raske teknologiutviklingen skaper nye muligheter, og samarbeidet muliggjør vår digitale reise for levere sikrere og mer effektiv drift. Equinors ambisjon er å bli en digital leder innen vår industri, og et skydatasenter i Norge vil forenkle og fremskynde Equinors bruk av skyen, sier Equinors IT-direktør (CIO) Åshild Hanne Larsen.





“Only in the Cloud”

- Big Data
- Kunstig Intelligens
- Integrasjon/samhandling
- Innebygget sikkerhet (DevSecOps)
- Automatiske oppgraderinger
- Kvantekryptografi
- *Osv osv…*

Hva er “skya”?
…forretningsdefinisjonen

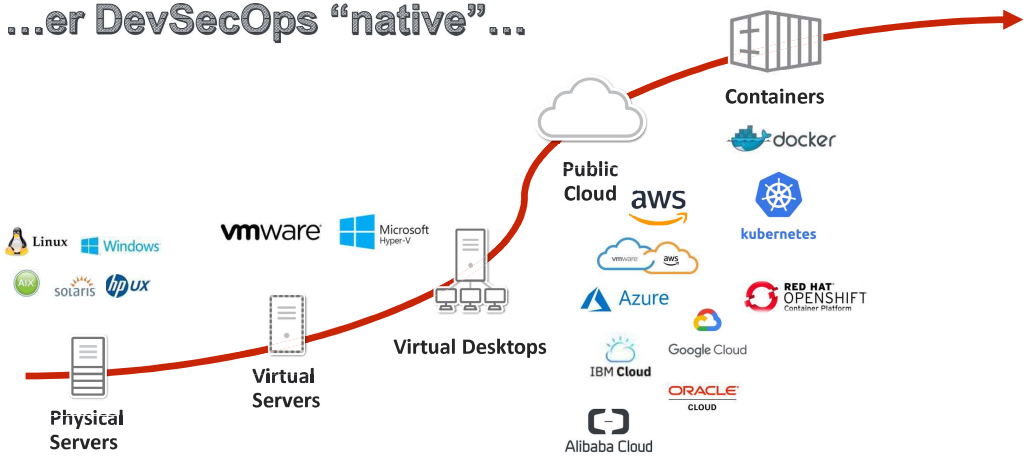
Supply Chain Management!

HVORFOR LOGISTIKKLEDELSE - SUPPLY CHAIN MANAGEMENT?

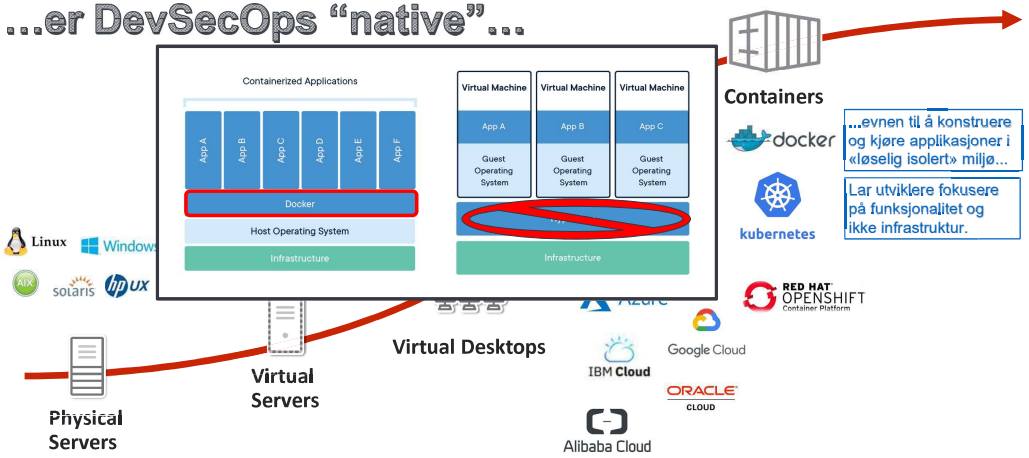
Fordypningen skal gi deg dyptgående, ledelsesorientert kunnskap og forståelse om utvikling og ledelse av forsyningskjeder og om bedriftsintern logistikk. Videre vil du lære de fysiske og administrative prosesser som er knyttet til det å anskaffe, håndtere, lagre, planlegge produksjon, transportere og levere ~~varer~~ **skytjenester** på en måte som oppfyller kundenes servicekrav på en kostnadseffektiv måte. Du vil forståelse for hvordan forskjellige logistikkløsninger påvirker miljøet og hvilke etiske utfordringer man kan møte på i innkjøpsarbeidet.

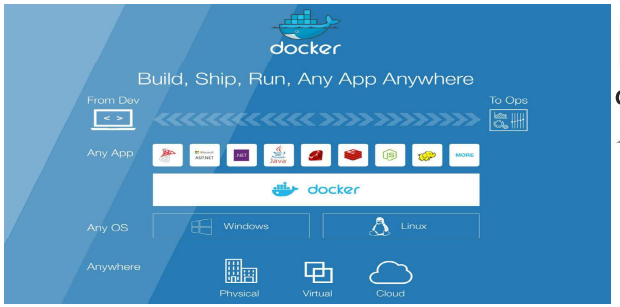
Hva er skya?
...den tekniske definisjonen
...and beyond...

Fremtiden for skytjenester...
...er DevSecOps "native"...



Fremtiden for skytjenester...
...er DevSecOps "native"...





Containers

docker

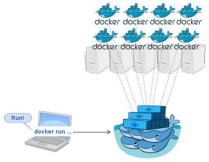
...evnen til å konstruere og kjøre applikasjoner i «løselig isolert» miljø...

kubernetes

Lar utviklere fokusere på funksjonalitet og ikke infrastruktur.

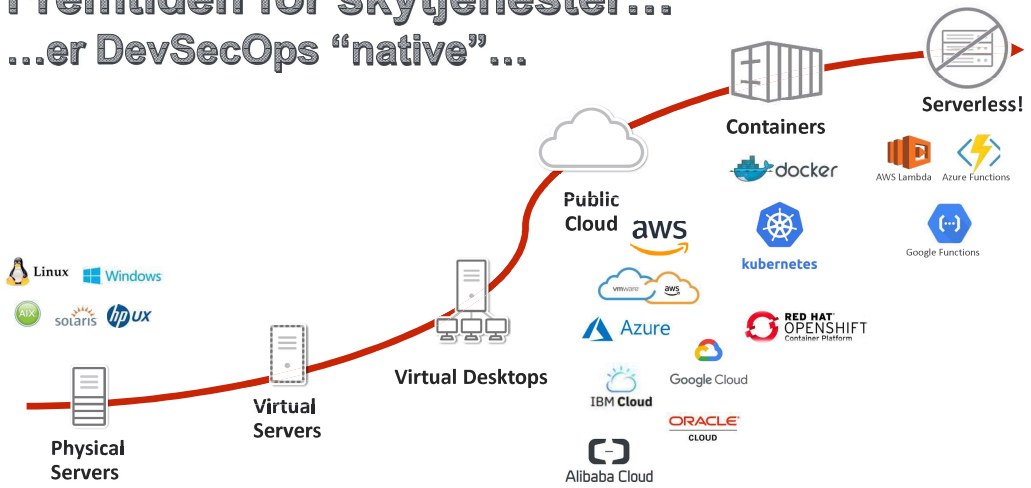
RED HAT OPENSHIFT Container Platform

Available Container Security Features, Requirements and Defaults			
Security Feature	LXC 2.0	Docker 1.11	CoreOS Rkt 1.3
User Namespaces	Default	Optional	Experimental
Root Capability Dropping	Weak Defaults	Strong Defaults	Weak Defaults
Procfs and Sysfs Limits	Default	Default	Weak Defaults
Cgroup Defaults	Default	Default	Weak Defaults
Seccomp Filtering	Weak Defaults	Strong Defaults	Optional
Custom Seccomp Filters	Optional	Optional	Optional
Bridge Networking	Default	Default	Default
Hypervisor Isolation	Coming Soon	Coming Soon	Optional
MAC: AppArmor	Strong Defaults	Strong Defaults	Not Possible
MAC: SELinux	Optional	Optional	Optional
No New Privileges	Not Possible	Optional	Not Possible
Container Image Signing	Default	Strong Defaults	Default
Root Interaction Optional	True	False	Mostly False



Vmware/VShpere
Hyper-V
XenServer Orchestra
Windows
Linux Native
AWS EKS
Google GKE
Microsoft Azure

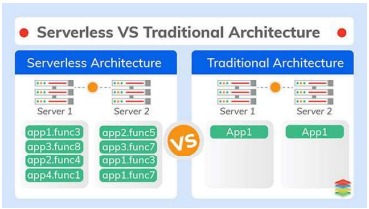
Fremtiden for skytjenester...
...er DevSecOps "native"...

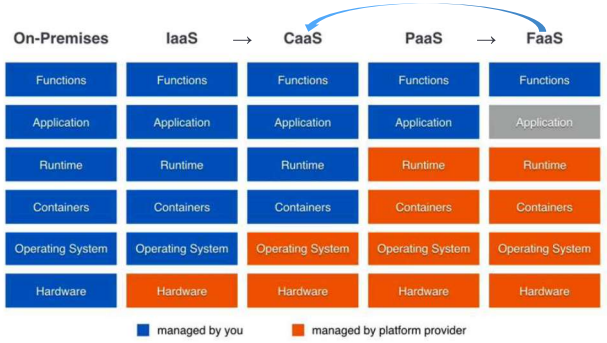


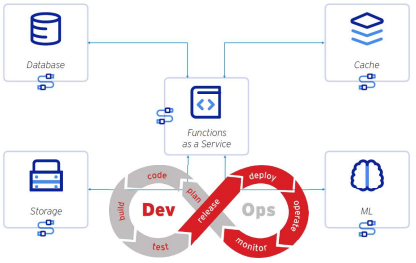
Event Publishers

Event Handlers

I en serverless verden tenker du ikke på containers mer, du skriver bare kode







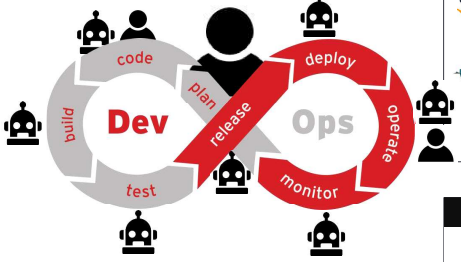
AUTOMASJON AV PRODUKSJONSPROSESSER = HASTIGHET!

Pipeline Management & Deployment

GitHub
Jenkins
ANSIBLE
CHEF
puppet
SALTSTACK
kubernetes
PowerShell
AWS OpsWorks

IT Service Management

slack
Jira Software
now
Amazon SNS



Environments

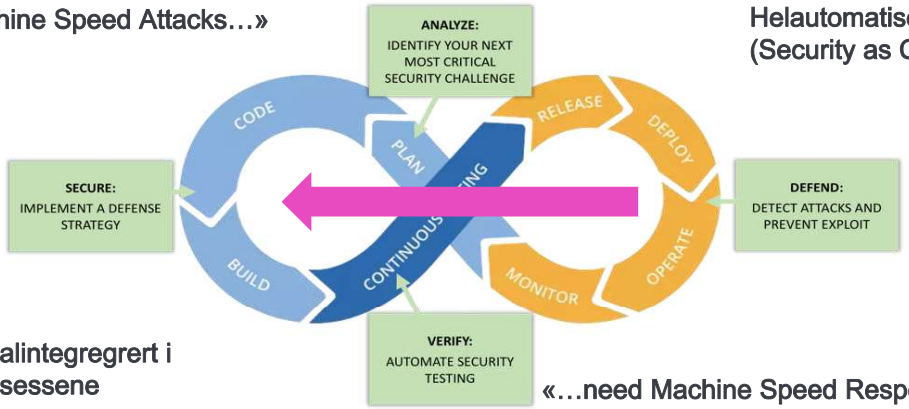
aws
Azure
Google Cloud
docker
RED HAT OPENSHIFT
vmware

Monitoring Tools

New Relic.
AWS CloudTrail
AWS Config

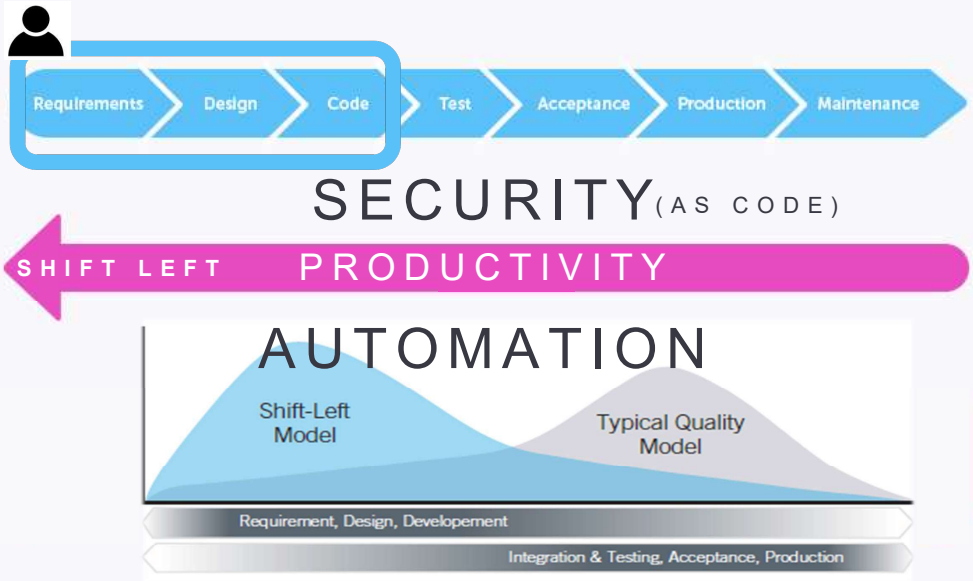
«Machine Speed Attacks…»

Helautomatisert (Security as Code)



Totalintegregrert i prosessene

«…need Machine Speed Response»



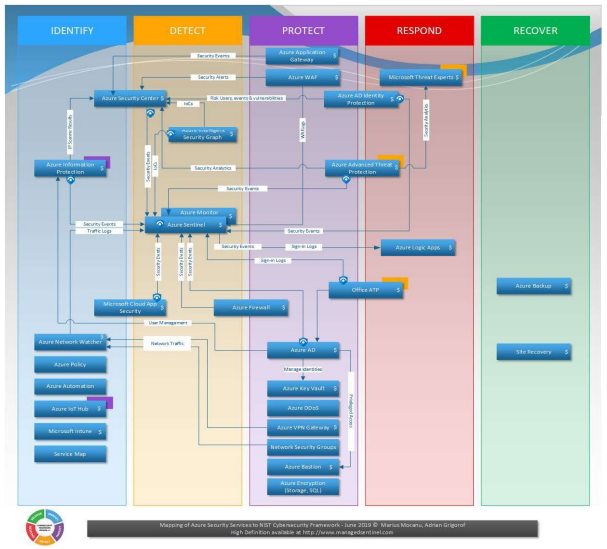
Skyleverandørene tilbyr omfattende sikkerhetstjenester innebygget i skya

(det er opp til deg å ~~vite om~~ ~~forstå~~ bruke og betale for dem…)

IN2120 INFORMATION SECURITY

Mapping of On-Premises Security Controls vs Major Cloud Providers Version 4.5 May 2019 © Adrian Grigorof, Marius Mocanu
High Definition available at http://www.managedsentinel.com

MAPPING OF ON-PREMISES SECURITY CONTROLS VS MAJOR CLOUD PROVIDERS



Microsoft 365 E3		
	Office 365 E3	EMS E3
Windows 10 Enterprise E3 Per User	Office Pro Plus for O365 SharePoint Online Plan 2 Exchange Online Plan 2 Skype for Business Online Plan 2 Yammer Office Online (Web Apps) OneDrive	Microsoft Intune Azure Active Directory Premium Plan 1 Azure Information Protection Premium Plan 1 Microsoft Identity Manager CAL Advanced Threat Analytics Windows Server CAL equivalency
Microsoft 365 E5		
Contains everything in Microsoft 365 E3 and adds:		
	Office 365 E5 Additive Features	EMS E5 Additive Features
Windows Defender ATP	Threat Intelligence Advanced Threat Protection Advanced Security Management Advanced Compliance (Advanced eDiscovery, Customer Lockbox, Advanced Data Governance) Audio Conferencing Phone System Power BI Pro MyAnalytics	Cloud App Security Azure Active Directory Premium Plan 2 Azure Information Protection Premium Plan 2

AZURE SECURITY STACK VS. NIST CYBERSECURITY FRAMEWORK

Om fem år er hele NAV i skyen

Personvern, informasjonssikkerhet og IT-sikkerhet

- Sky er sikkert
  - De store skyleverandørene har betydelig kapasitet og kompetanse innen IT-sikkerhet
  - Skyleverandørene leverer omfattende sikkerhetsfunksjonalitet og har omfattende sikkerhetsovervåkning
- NAV må ha tilstrekkelig kompetanse og ta i bruk skytjenester kontrollert
  - Kompleksiteten øker og det er stadig nye trusler
  - NAV må forstå (og dokumentere) hvordan sikkerheten ivaretas hos våre skyleverandører, hvordan egenutviklede løsninger kan leveres med nødvendig sikkerhet og hvordan den totale sikkerheten ivaretas
  - Kompetanse og kapasitet hos både fag og IT til å gjøre vurdering av personvern, informasjonssikkerhet og IT-sikkerhet er en kritisk forutsetning

Bestillerkompetanse!

Virksomhets-kompetanse	Sikkerhets-kompetanse	Integrasjons-kompetanse	Kompetanse om anskaffelser	Juridisk kompetanse
- For å kunne definere behov og stille nødvendige krav.	*- For å kunne vurdere risiko og stille riktige sikkerhetskrav. Dette gjelder alle områder av sikkerhet dvs. fysisk, personell- og informasjonssikkerhet.*	*- For å kunne forstå hvordan tjenestene kan integreres i virksomheten på best mulig måte.*	*- Slik at anskaffelsen kan gjennomføres på en måte som støtter virksomhetens forretningsmessige og funksjonelle behov på best måte.*	*- Slik at virksomhetens juridiske krav og behov ivaretas og at kontrakten kan oppfylles i produksjonen.*
Grunnleggende IKT-kompetanse er en forutsetning for kvalitet i kompetanseområdene over.				

CSA cloud security alliance®

Fremme av god praksis for å sikre skytjenester, og gi opplæring i bruk av skytjenester for å sikre alle andre former for databehandling.

www.cloudsecurityalliance.no

90,000+
INDIVIDUAL MEMBERS

75+
CHAPTERS

300+
CORPORATE MEMBERS

19
ACTIVE WORKING GROUPS

Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

IN2120 INFORMATION SECURITY

CSA
OUR COMMUNITY

2009
CSA FOUNDED

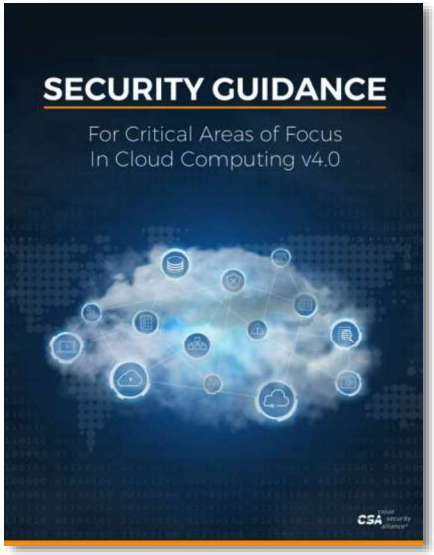
SEATTLE/BELLINGHAM, WA //
AMERICAS HEADQUARTERS

BERLIN //
EMEA HEADQUARTERS

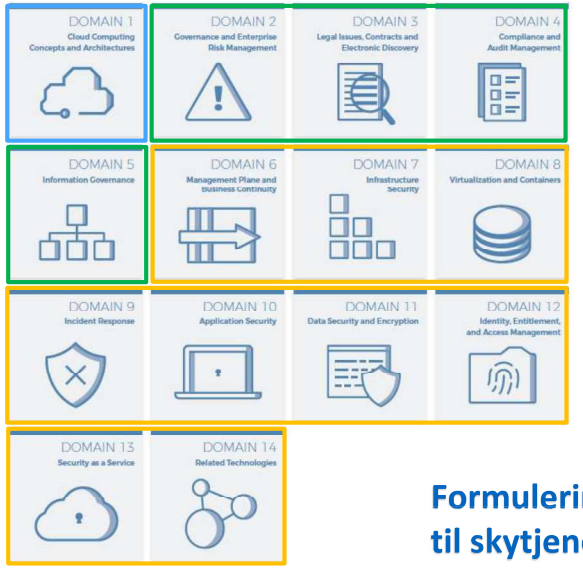
SINGAPORE //
ASIA PACIFIC
HEADQUARTERS

www.cloudsecurityalliance.no/linkedin

En praktisk veiledning for å spesifisere sikkerhetskrav til skytjenester



https://cloudsecurityalliance.org/download/security-guidance-v4/



Del I: Generelt

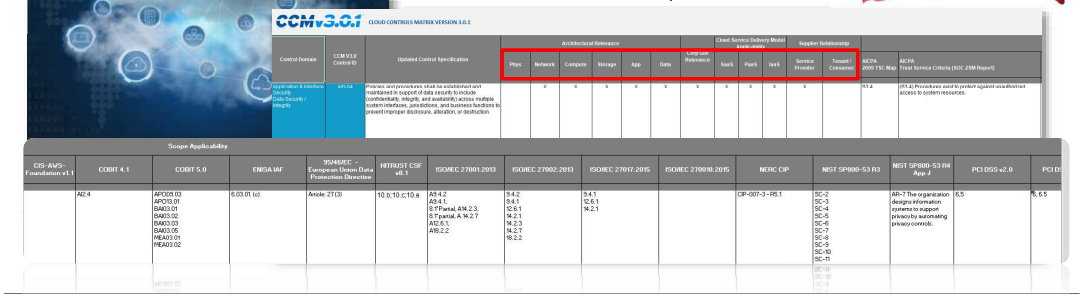
Del II: Styring

Del III: Drift

Formulering av sikkerhetskrav til skytjenester

CCM
Cloud Controls Matrix

133 kontrollkrav (14 kontrollområder)



CCM Cloud Controls Matrix

16 kontrollområder

AIS Application & Interface Security	DSI Data Security & Information Lifecycle Management	[illegible]an Resources	MOS Mobile Security
AAC Audit Assurance & Compliance	DCS Datacenter Security	IAM Identity & Access [illegible]Management	SEF Security Incident Management, E-Discovery, & Cloud Forensics
BCR Business Continuity Management & Operational Resilience	EKM Encryption & Key Management	In[illegible]e & Virtualiza[illegible]n Security	STA Supply Chain Management, Transparency, and Accountability
CCC Change Control & Configuration Management	GRM Governance and Risk Management	IPY Interoperability & Portability	TVM Threat and Vulnerability Management

CCM Cloud Controls Matrix

DSI
Data Security & Information Lifecycle Management

7 spørsmål

Control specification	
DSI-01	Classification
DSI-02	Data Inventory / Flows
DSI-03	E-commerce Transactions
DSI-04	Handling / Labeling / Security Policy
DSI-05	Nonproduction Data
DSI-06	Ownership / Stewardship
DSI-07	Secure Disposal

CCM Cloud Controls Matrix

DSI-01
Classification

Kontrollspørsmål (CAIQ)	
DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?
DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?

Microsoft Azure

amazon web services

Google Cloud Platform

Microsoft Azure

https://cloudsecurityalliance.org/star

Cloud Services by Microsoft

Microsoft Azure

STAR Self-Assessment — **Submitted:** March 30th, 2012

Consensus Assessments Initiative Questionnaire v3.0.1 — Download

Supporting Asset #1

Deprecated

STAR Attestation — **Submitted:** October 1st, 2016

STAR Attestation v1 — Download

STAR Certification — **Submitted:** March 30th, 2012

STAR Certification v1 — Download

Kontrollspørsmål (CAIQ)	
DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?
DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?

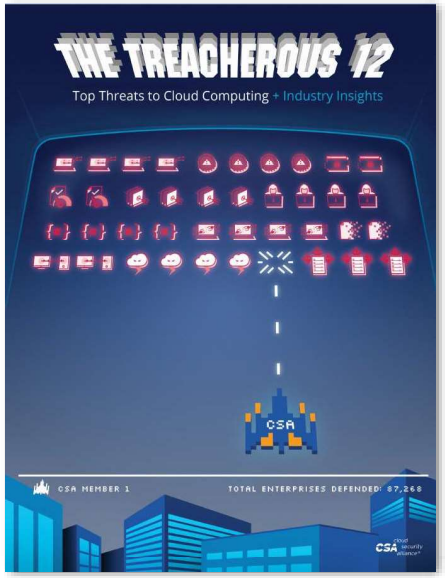
DSI-01.5: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location / geography of storage of a tenant's data in advance?*	Y			Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area or region for redundancy, but it will not be replicated outside of it unless specifically configured so by the customer.

Cloud Control Matrix (CCM) Oppsummert…

- Er ikke et rammeverk for å gjennomføre risikovurdering
  - → kan dokumentere sikkerhetskrav i et standardisert format
- Er ikke en metode for å identifisere alle dine sikkerhetskrav
  - → kunnskap, begreper og konsepter for å identifisere kravene
- CCM er metode for å raskt, strukturert og på en forutsigbar måte (for begge parter) sikkerhetsevaluere ulike skytjenester og besvarer risikovurderingen i kontekst spesifikt av skytjenester ved å dokumentere om det er akseptabelt for din virksomhet å flytte den spesifikke informasjonen, applikasjonen og/eller prosessen til en bestemt (del av en) skytjeneste.

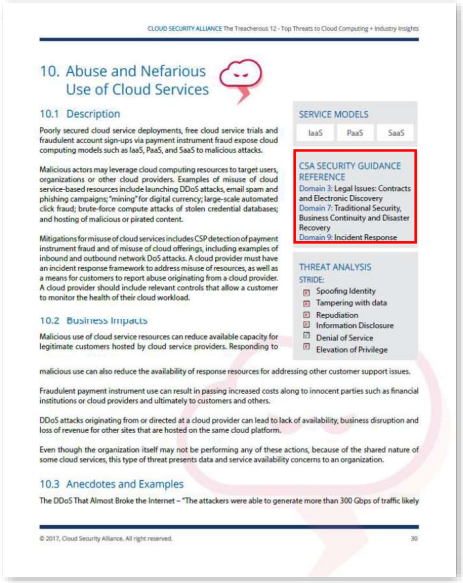
Cloud Security Alliance produserer fortløpende en rekke rapporter og veiledninger

(det er opp til deg å ~~vite om~~ bruke dem – de er gratis!…)



cloud security alliance®

1. Data Breaches
2. Insufficient Identity, Credential and Access mgt
3. Insecure Interfaces and APIs
4. System Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities



CLOUD SECURITY ALLIANCE The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights

10. Abuse and Nefarious Use of Cloud Services

10.1 Description

Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

Malicious actors may leverage cloud computing resources to target users, organizations or other cloud providers. Examples of misuse of cloud service-based resources include launching DDoS attacks, email spam and phishing campaigns; "mining" for digital currency; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting of malicious or pirated content.

Mitigations for misuse of cloud services includes CSP detection of payment instrument fraud and of misuse of cloud offerings, including examples of inbound and outbound network DoS attacks. A cloud provider must have an incident response framework to address misuse of resources, as well as a means for customers to report abuse originating from a cloud provider. A cloud provider should include relevant controls that allow a customer to monitor the health of their cloud workload.

SERVICE MODELS

IaaS | PaaS | SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 3: Legal Issues: Contracts and Electronic Discovery
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 9: Incident Response

THREAT ANALYSIS

STRIDE:

- Spoofing Identity
- Tampering with data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

10.2 Business Impacts

Malicious use of cloud service resources can reduce available capacity for legitimate customers hosted by cloud service providers. Responding to malicious use can also reduce the availability of response resources for addressing other customer support issues.

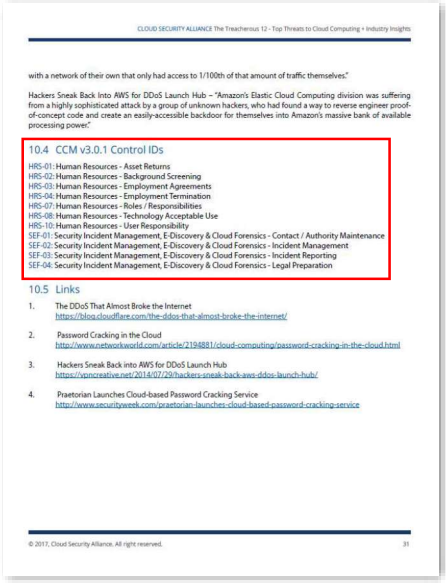
Fraudulent payment instrument use can result in passing increased costs along to innocent parties such as financial institutions or cloud providers and ultimately to customers and others.

DDoS attacks originating from or directed at a cloud provider can lead to lack of availability, business disruption and loss of revenue for other sites that are hosted on the same cloud platform.

Even though the organization itself may not be performing any of these actions, because of the shared nature of some cloud services, this type of threat presents data and service availability concerns to an organization.

10.3 Anecdotes and Examples

The DDoS That Almost Broke the Internet – "The attackers were able to generate more than 300 Gbps of traffic likely



with a network of their own that only had access to 1/100th of that amount of traffic themselves."

Hackers Sneak Back Into AWS for DDoS Launch Hub – "Amazon's Elastic Cloud Computing division was suffering from a highly sophisticated attack by a group of unknown hackers, who had found a way to reverse engineer proof-of-concept code and create an easily-accessible backdoor for themselves into Amazon's massive bank of available processing power."

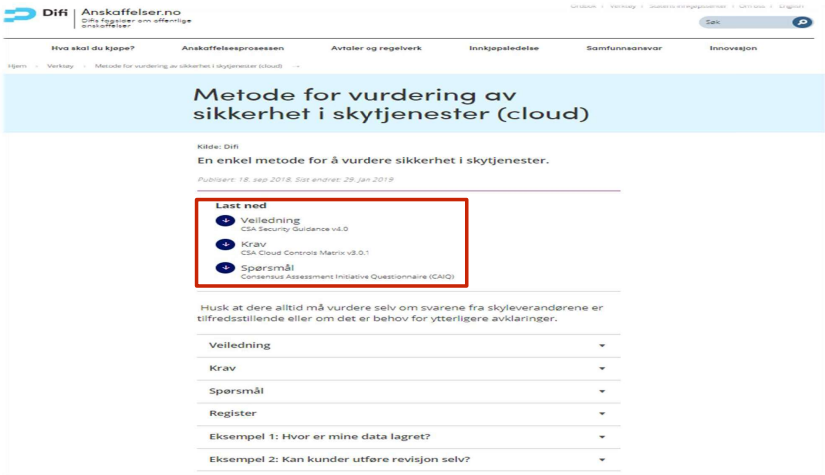
10.4 CCM v3.0.1 Control IDs

HRS-01: Human Resources - Asset Returns
HRS-02: Human Resources - Background Screening
HRS-03: Human Resources - Employment Agreements
HRS-04: Human Resources - Employment Termination
HRS-07: Human Resources - Roles / Responsibilities
HRS-08: Human Resources - Technology Acceptable Use
HRS-10: Human Resources - User Responsibility
SEF-01: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance
SEF-02: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management
SEF-03: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting
SEF-04: Security Incident Management, E-Discovery & Cloud Forensics - Legal Preparation

10.5 Links

1. The DDoS That Almost Broke the Internet
   https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/
2. Password Cracking in the Cloud
   http://www.networkworld.com/article/2194881/cloud-computing/password-cracking-in-the-cloud.html
3. Hackers Sneak Back into AWS for DDoS Launch Hub
   https://vpncreative.net/2014/07/29/hackers-sneak-back-aws-ddos-launch-hub/
4. Praetorian Launches Cloud-based Password Cracking Service
   http://www.securityweek.com/praetorian-launches-cloud-based-password-cracking-service

www.anskaffelser.no/verktoy/veiledere/metode-vurdering-av-sikkerhet-i-skytjenester-cloud



Difi | Anskaffelser.no

Hva skal du kjøpe? | Anskaffelsesprosessen | Avtaler og regelverk | Innkjøpsledelse | Samfunnsansvar | Innovasjon

Hjem › Verktøy › Metode for vurdering av sikkerhet i skytjenester (cloud)

Metode for vurdering av sikkerhet i skytjenester (cloud)

Kilde: Difi

En enkel metode for å vurdere sikkerhet i skytjenester.

Publisert: 18. sep 2018. Sist endret: 29. jan 2019

Last ned

- Veiledning
  CSA Security Guidance v4.0
- Krav
  CSA Cloud Controls Matrix v3.0.1
- Spørsmål
  Consensus Assessment Initiative Questionnaire (CAIQ)

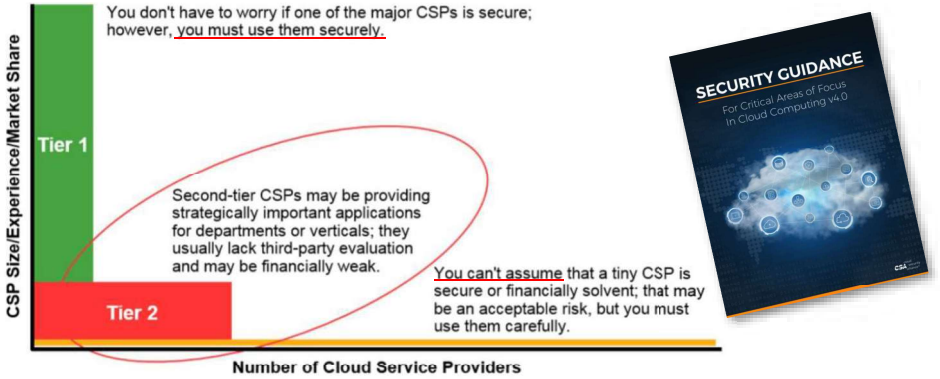
Husk at dere alltid må vurdere selv om svarene fra skyleverandørene er tilfredsstillende eller om det er behov for ytterligere avklaringer.

- Veiledning
- Krav
- Spørsmål
- Register
- Eksempel 1: Hvor er mine data lagret?
- Eksempel 2: Kan kunder utføre revisjon selv?

Hvordan bruke Skytjenester "riktig" og sikkert

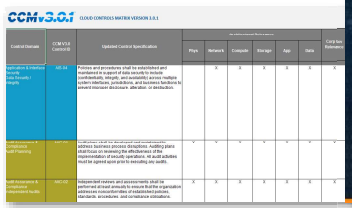
Leverandører og sikkerhet

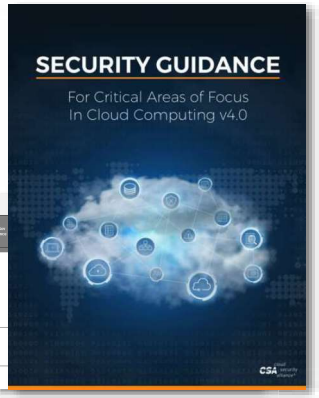
ISO 27001 | ISO 27018 | ISO 27017 | ISO 22301 | ISO 9001 | SOC 1 Type 2 | SOC 2 Type 2 | SOC 3 | CSA STAR Self-Assessment | CSA STAR Certification | CSA STAR Attestation



"Basics"

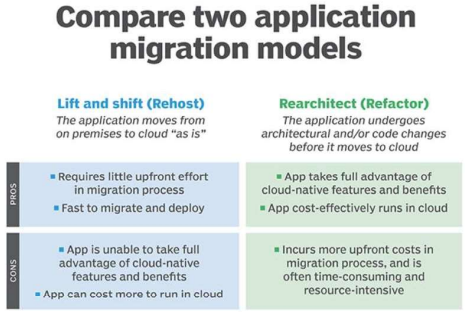
- ❑ Tilgangsstyring (brukerkatalog, prosesser)
- ❑ Konfigurasjonstyring (DevSecOps)
- ❑ Applikasjonssikkerhet (OWASP, HTTP, API)
- ❑ Synlighet (logging, hybrid)
- ❑ Sikkerhetskopiering/katastrofehåndtering





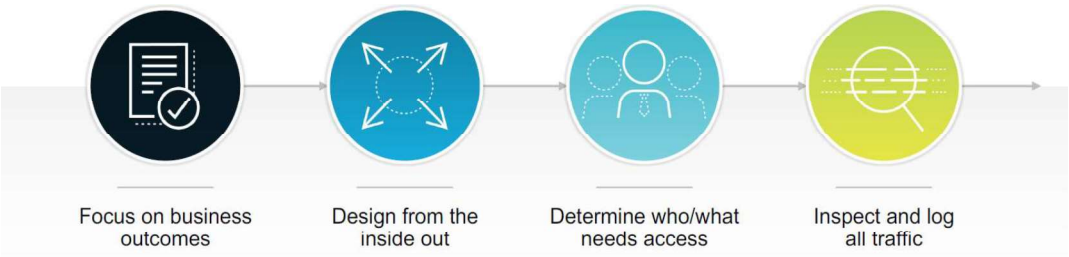
www.anskaffelser.no/verktoy/veiledere/metode-vurdering-av-sikkerhet-i-skytjenester-cloud
www.cloudsecurityalliance.no

Lift and Shift vs Refactoring

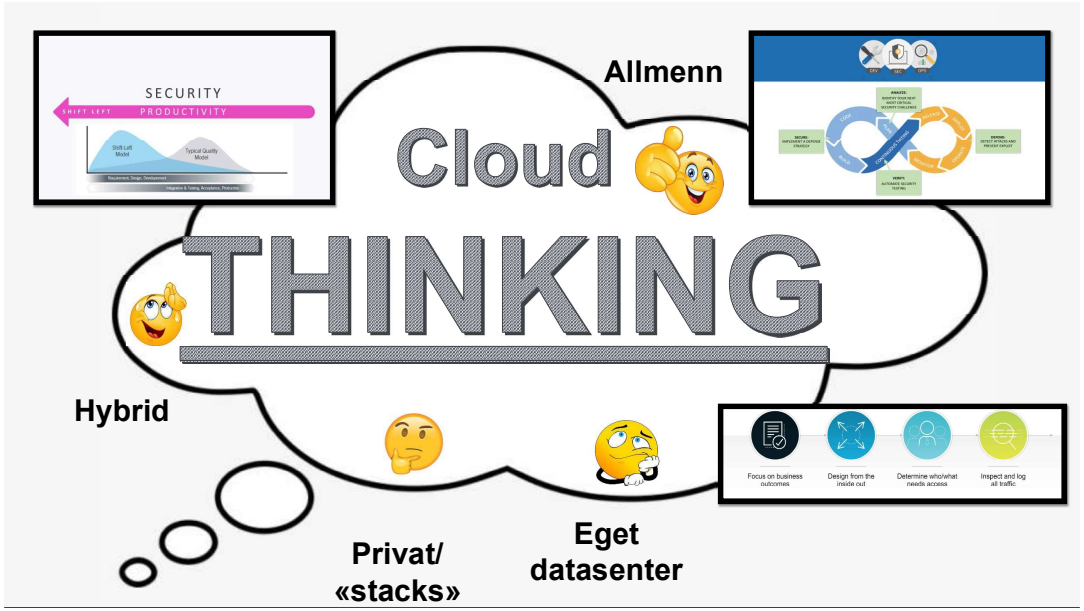


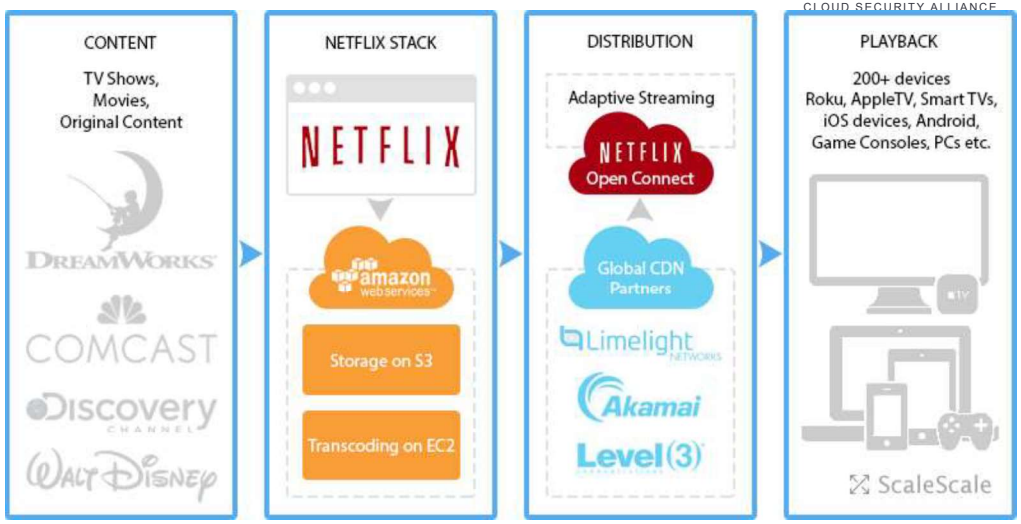
whatis.techtarget.com/definition/lift-and-shift

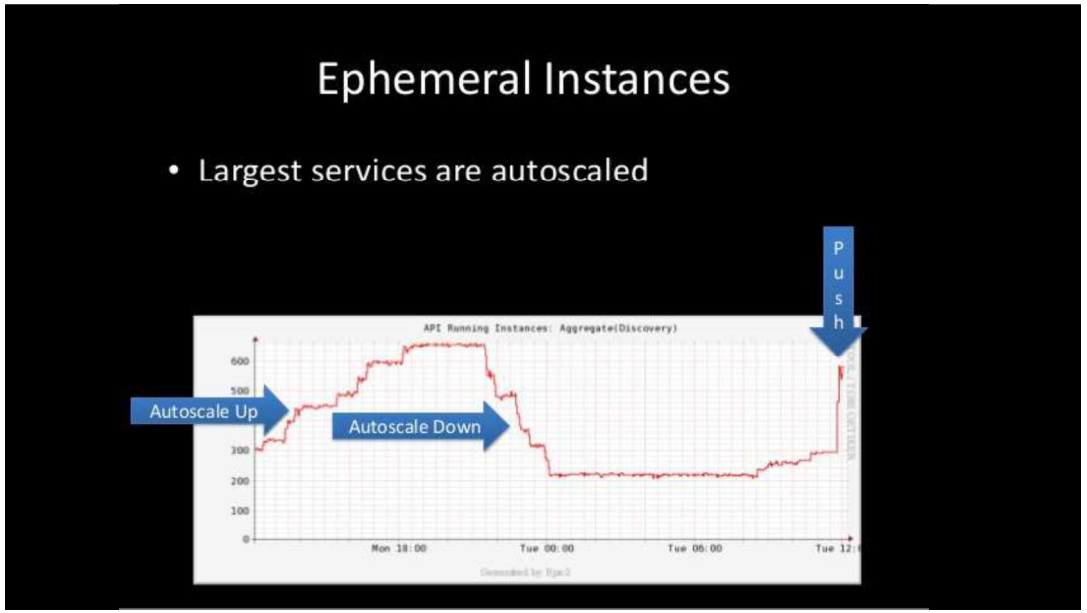
#ZeroTRUST



PrivJIT







DevSecOps

ShiftLEFT

Refactoring

ZEROTrust

IT og sikkerhetsautomasjon = Økt forretningshastighet

IaaS/PaaS/Caas/Faas/Saas/ "Serverless": Alle arkitekturene og teknologiene kan/må sameksistere

Må.Ha.Skystrategi !

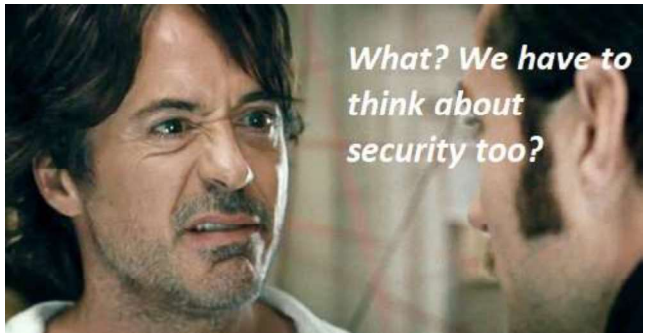
- *Begynn med forretningsbehov eller visjon – går deretter tilbake i modellene*
- *«Sky først → SaaS først" - er det mulig?*
- *Vurdèr deretter andre modeller inkl «egen kjeller» (if it work, don't fix it…)*
- *Ikke "Lift and Shift", såfremt du ikke vet nøyaktig hvorfor*
- *Re-factor, gjerne til SaaS-tjenester, modeller kan/må kombineres*

"På hvilken måte gjør dette oss til en bedre organisasjon"?

Bruk re-factoring mot SaaS-tjenester som hovedstrategi
Skytjenester kan styres etter prinsipper om forsyningstjenester (SCM)
Sikkerhet må automatiseres (ShiftLeft) og integreres i prosessløpet; DevSecOps)
Velg/utfordre leverandører med 3dje part sertifiseringer (CSA/CCM, SOC-2, ISO27K)
ZeroTrust og JIT-filosofier reduserer angrepsflate og risiko

DU har ALLTID ansvar for:

- *Egen risikovurdering*
- *Operere ihht lover og regler*
- *Kontroll på egen data (inkl personvern)*
- *Tilgangsstyring/brukeradministrasjon*
- *Konfigurasjon av tjenester (S3 buckets…)*
- *Typisk tiltak ved bruk av skytjenester; ekstra fokus på endepunktsikkerhet*
- *Hvis du ikke har en skystrategi vil du tape forretnings-handlerom og -hastighet på både kort og spesielt lang sikt (bare spør Equinor…)*
- *Det finnes tjenester i markedet som tilbyr "buyback" av egen datasenterhardware + lisensadministrasjon via portal*

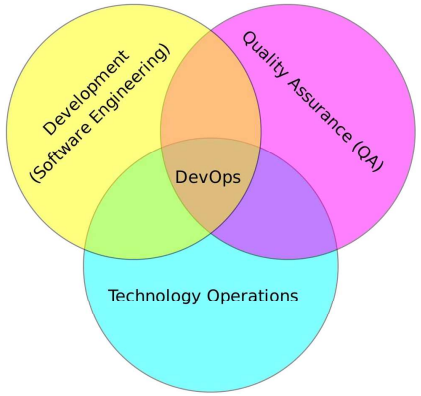


"THE PURPOSE AND INTENT OF DEVSECOPS, IS TO BUILD ON THE MINDSET THAT 'EVERYONE IS RESPONSIBLE FOR SECURITY' WITH THE GOAL OF SAFELY DISTRIBUTING SECURITY DECISIONS AT SPEED AND SCALE TO THOSE WHO HOLD THE HIGHEST LEVEL OF CONTEXT WITHOUT SACRIFICING THE SAFETY REQUIRED."

- SHANNON LIETZ

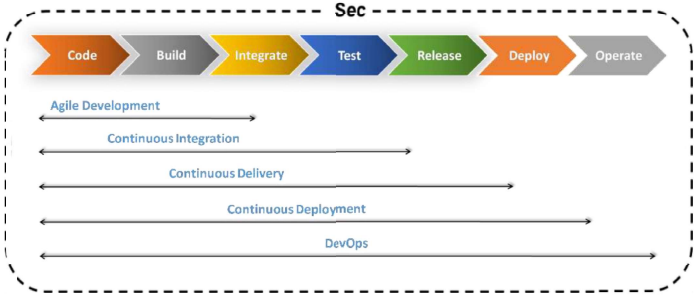
Applikasjonssikkerhet

DevOps Ven Diagram



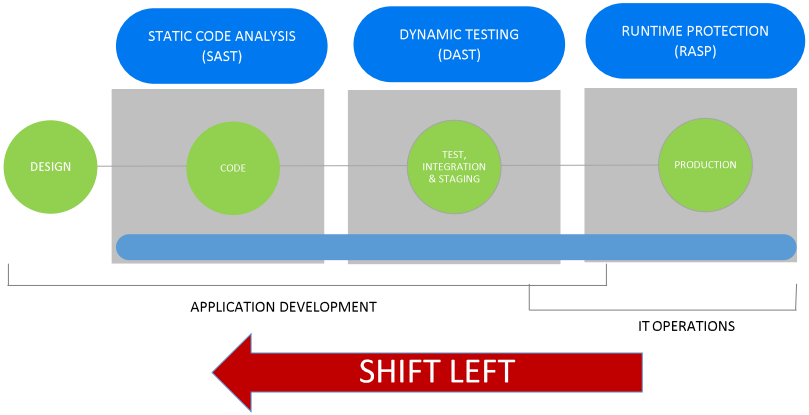
The intersection of 3 Key domains

DEVSECOPS

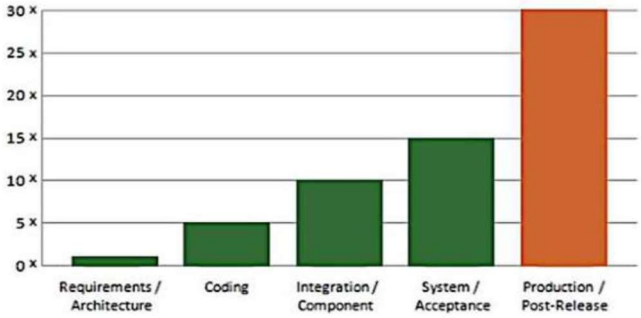


DEVSECOPS

SECURITY SHIFTING TO THE LEFT



By The Numbers



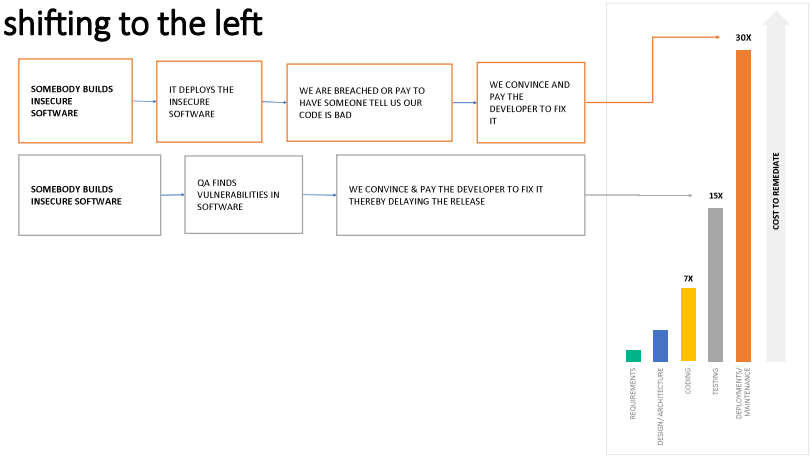
- High performers - 30X frequent deployments and doing so 200X faster
- High Performers - 60X more successful & fix problems 168X faster
- High Performers - 2X more likely to exceed profit, market share, and productivity goals & have a 50% higher market cap growth over 3 years

Time and Cost to Fix

www.securityinnovationeurope.com/the-business-case-for-security-in-the-software-development-lifecycle-sdlc

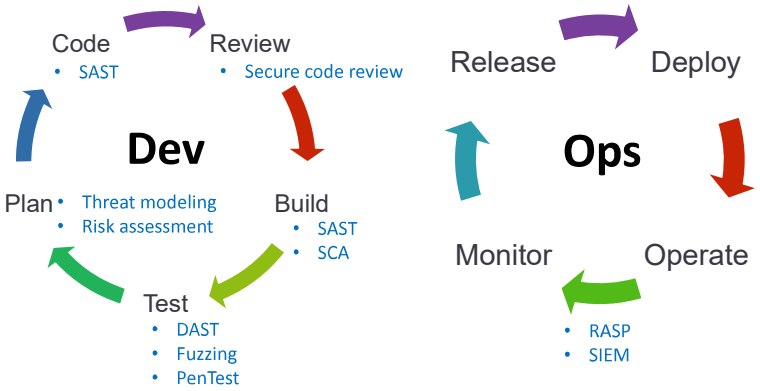
DEVSECOPS

Security shifting to the left



DEVSECOPS

Integrating security in DevOps



DEVSECOPS

TECHNICAL BENEFITS:

- CONTINUOUS SOFTWARE DELIVERY
- LESS COMPLEX PROBLEMS TO FIX
- FASTER RESOLUTION OF ISSUES WHEN THEY ARISE
- SECURE ENVIRONMENT

BUSINESS BENEFITS:

- FASTER DELIVERY OF FEATURES
- MORE STABLE OPERATING ENVIRONMENTS
- MORE TIME AVAILABLE TO ADD VALUE (RATHER THAN WASTE IT WITH FIXES/MAINTENANCE)
- NO BREACHES / BETTER IMAGE