Oslo

From zero to hero

– en reise i sikkerhetskultur for Oslo Origo

Image by Clker-Free-Vector-Images from Pixabay

Oslo

… men et forsøk på dele erfaringer og tanker om

seire, nederlag og drømmer om reisen til god sikkerhetskultur i Oslo Origo

av

Ingvild Nilsson (EY)
Rune Schumann (Origo, Oslo kommune)

Oslo

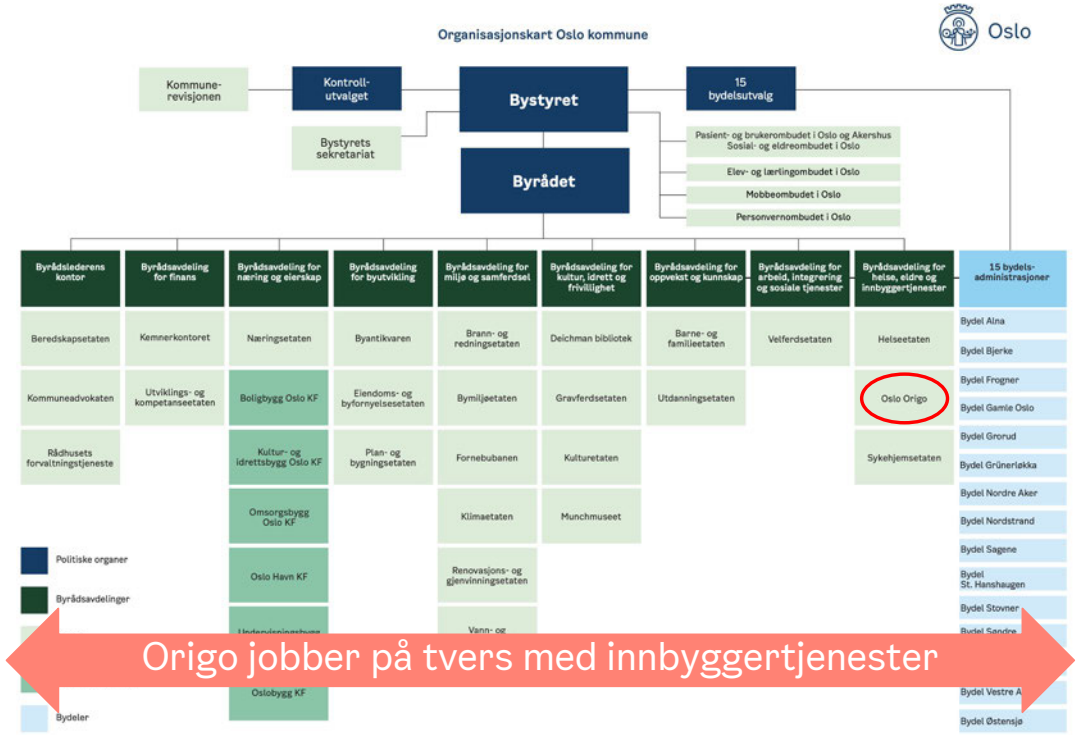
Felles visjon for den digitale transformasjonen i Oslo kommune

Vi forstår innbyggerne våre og løser deres behov ...

... uavhengig av offentlig sektors organisering

Oslo

Skalaen til Oslo kommune er (mildt sagt) stor



Hvordan forener man

9 byrådsavdelinger

~30 virksomheter

15 bydeler

52 000 ansatte

for å møte behovene til

700 000+ innbyggere

Oslo

Oslo Origo – kommunens interne kompetansemiljø for digital transformasjon

135 fast ansatte

5 produkt-områder

12 tverrfaglig e team

Oslo

Cybersikkerhetskultur destillert

God cybersikkerhetskultur er vesentlig for å ta frem trygge digitale tjenester for både innbyggere og ansatte

Et kjennetegn er at cybersikkerhet er et naturlig tema i *hele* organisasjonen – som toppledelse, personalledere, utviklere, arkitekter, teamledere mfl.

Image by Pete Linforth from Pixabay

Det var en gang ...

én sikkerhetsfyr
som dro til Oslo Origo for å gjøre det sikkert

Oslo

Alene om jobben

- Størrelse, Oslo Origo: 95 stk. med stort og smått
- Ansvar: cybersikkerhet + personvern
- Personvern: «fake it till you make it»

Hybris: «dette går fint! 👍✊👌»

Image by Elias from Pixabay

Oslo


NOT!
Oslo
Image by Jenny Friedrichs from Pixabay

Noe måtte gjøres
Mark I

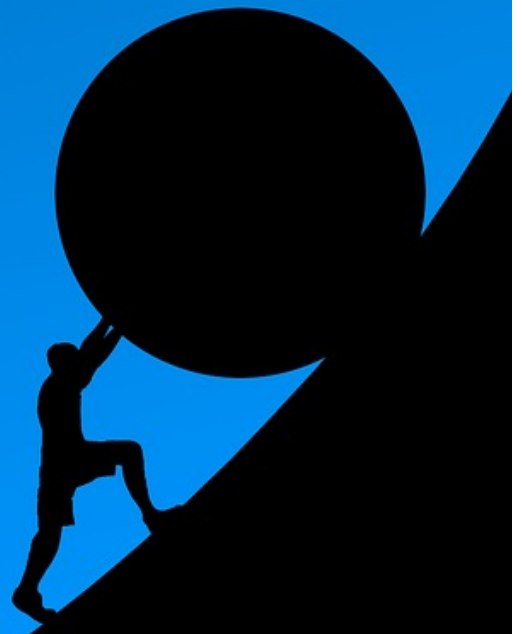


Image by Elias from Pixabay

Oslo

Sikkerhetsansvarlig

- Én per team
- Formål: styrke kapasitet på cybersikkerhet i team
- Funksjon: cyberseckompetanse og å kunne «sette foten ned»

Image by Alexa from Pixabay


YOU
CANNOT
PASS!
Blei kanskje litt mye Møllers
tran i første forsøk, gitt 😬
Image: New Line Cinema

Oslo

Fungerte ikke

Initiativet døde på rot

Oslo

Hvorfor?

- Ingen klar forankring i ledergruppe og teamledelse
- Ikke avsatt tid → «best effort»
- Dårlig oppfølging (fra meg 😬)
- Ikke kontinuitet i møter eller kompetansebygging
- Det fantes entusiasme, men ikke rom for å utøve den

Hele greia var i praksis et slags politikonsept

Noe måtte gjøres
Mark II

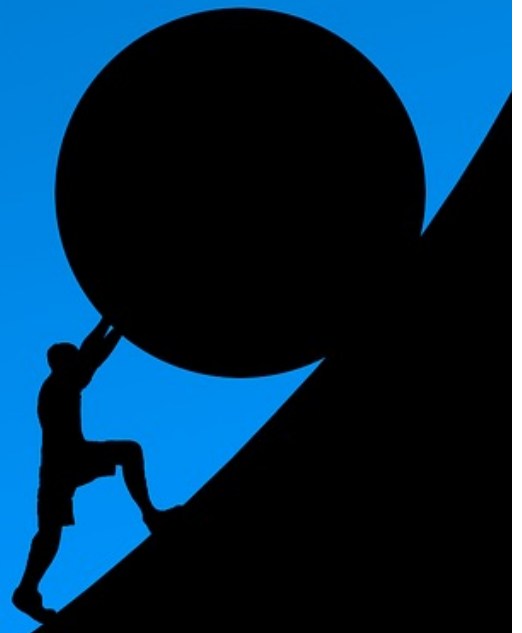


Image by Elias from Pixabay

Oslo

Hovedfokus på **to** områder

Regelmessig sikkerhetstesting av de digitale produktene våre

Øke cybersec.bevisstheten og -kultur i produktoperasjonen

Formål med sikkerhetstesting

1. Sikre de digitale produktene
2. Holde regelmessige sikkerhetstester
3. Bygge kompetanse på sikkerhetstesting i teamene
4. Sikkerhetstestere med kontinuitet for å bygge forståelse for domene og teknologistack
5. Være tett på teamene
6. Over tid gå fra sikkerhetstesting til mer rådgiving og «revisjon»

Anskaffelsen

Image by Burhan Khawaja from Pixabay

Hvorfor

- Manglet kompetanse
- «Nye øyne»
- Tett på
- Ha solid ryggdekning kompetansemessig

Det var en gang ...

en pentester
som dro til Oslo Origo for å gjøre det sikkert

Formålet er å gjøre sikkerhetstesting

ufarlig, gøy og ettertraktet!

Oslo


Heldigvis er grunnlaget for etablering
av **ufarlig, gøy og ettertraktet**
sikkerhetstesting i Origo bra!
Image by Adrian Campfield from Pixabay

1: Unngå byråkratiske og administrative mareritt

1: Unngå byråkratiske og administrative mareritt

Forberedelser og oppstartsmøte

Velfungerende plattformteam ordner med eventuelle tilganger

Fullmakt, taushetserklæring osv. ordnes én gang


Image by PublicDomainPictures from Pixabay
2: Engasjere utviklerteam i testen

2: Engasjere utviklerteam i testen

- Lage en **samarbeidsmodell** som passer det enkelte team
- **Åpen kommunikasjon** mellom testere og team
- Sitte **fysisk** sammen

3: Blame game og pekelek

Funn og observasjoner fra sikkerhetstesting brukes ikke til uthenging av utviklere

Det er kult at det ble oppdaget og vi lærer av det!


Forhåpentligvis vil nå jungeltelegrafen
spille oss gode blant utviklerteamene


“Produktet vårt har aldri blitt **pentestet** før, når har dere tid?”
“Skulle gjerne **sparret** litt om Log4Shell, kan noen fra infosec bistå?”
“Vi (tror vi) har remediert funnene fra forrige test, kan vi ha en **retest** også?”
“Vi har implementert ny funksjonalitet, vi skulle gjerne hatt et sett med nye øyne til å **vurdere** det?”
Forhåpentligvis vil nå jungeltelegrafen spille oss gode blant utviklerteamene

Øke cybersec.bevisstheten og -kultur i produktoperasjonen

- At tidligere forsøk har feilet økte jo ikke akkurat selvtilliten 😬
- Sikkerhetstestingen hjalp oss et stykke på vei
- … men, vi savnet en «misjonær» i teamet
- Vi så behovet for en slags sikkerhetsansvarlig 2.0

Image by Pete Linforth from Pixabay

Vi så lyset!

Julian

Jan-Kåre

- JavaZone 2021
- Presentasjon av NAVs Security Champion-konsept
- Knallidé!
- Fikk treffe ildsjelene i NAV som delte sine erfaringer

Image by Pete Linforth from Pixabay

(noen) erfaringer

- FRIVILLIG, IKKE TVANG -

- FÅ TIL ET COMMUNITY -

- MÅ VÆRE NOEN ILDSJELER SOM HOLDER FYR PÅ BÅLET -

- HA REGELMESSIGE MEETUPS MED INTERESSANT INNHOLD -

- DEDIKERT TID TIL Å PRAKTISERE ROLLEN -

- KULT MED MERCH -

Tid for egenrefleksjon

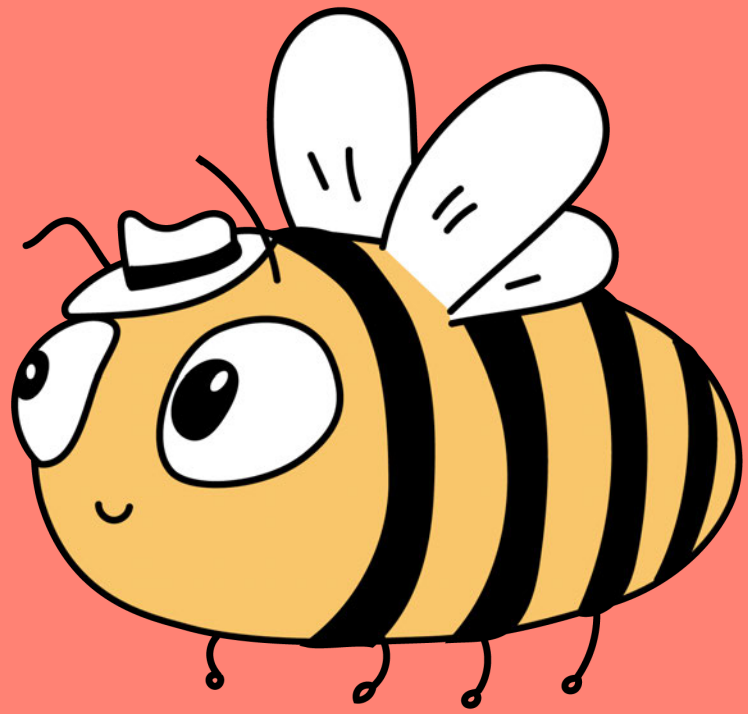
Image by Peter Hüller from Pixabay

Oslo

“Sikkerhetsansvarlig 2.0”

Security Champion

- Skal ikke være ansvarlig for sikkerheten i teamene
- Målsetting om å være teamets sikkerhetssamvittighet



Security Champion

Pre-launch

Legge en plan

- Nov ✓ Informere ledergruppen
- Des ✓ Erfaringsutveksling NAV
- Jan ✓ Informere POL-PL-TL*
- Feb ✓ Intervju “sikkerhetansvarlig”
- Mar ✓ Opprette Task Force
- Apr ✓ Utrede (2 møter)
- Mai ✓ Beslutningsgrunnlag klart
- Jun ✓ Beslutning i ledergruppe

Image by David Mark from Pixabay

Oslo


Security Champion
mer «Guru»-style
Image by u_7jp9rawlmt from Pixabay

Security Champion – august 2022

Launch

«bredde først, dybde så ...»

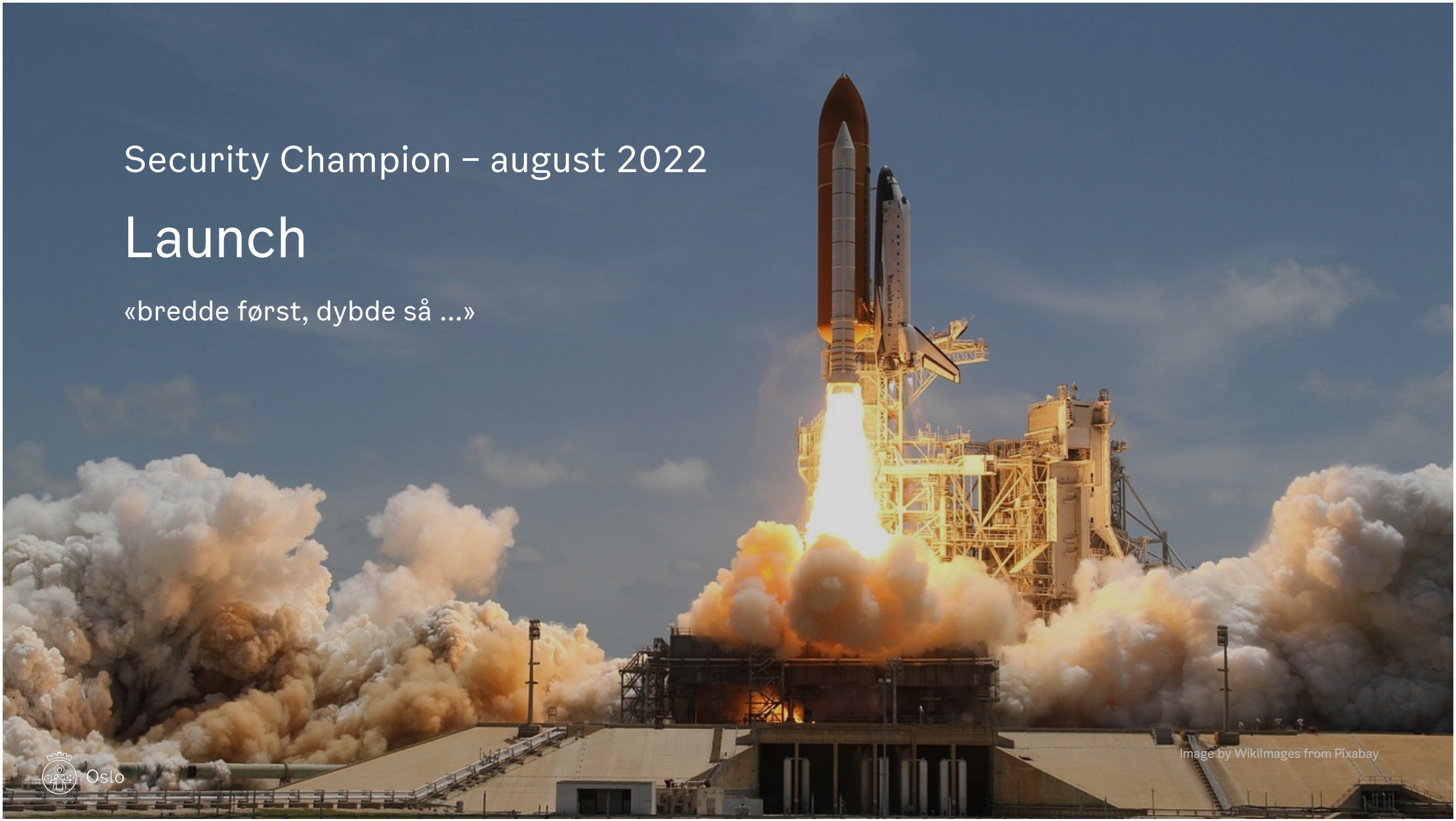


Image by WikiImages from Pixabay

Oslo

Noen refleksjoner rundt arbeid med pentesting og Origos modell for DevOps

Image by Demetros from Pixabay

Noen refleksjoner rundt arbeid med pentesting og Origos modell for DevOps

- rfc/0007-devops-i-origo: Definisjon av DevOps i Origo
- Utvikling av DevOps i Origo og ansvarsfordeling
- Varierende kunnskapsnivå og overskudd til å forholde seg til både sky- og appsikkerhet

Image by Demetros from Pixabay

Pentest og ansvarsfordeling med DevOps

- Risikoeier
- Ansvarlig for utbedre svakhet
- Ansvarlig for å finne løsning for utbedring

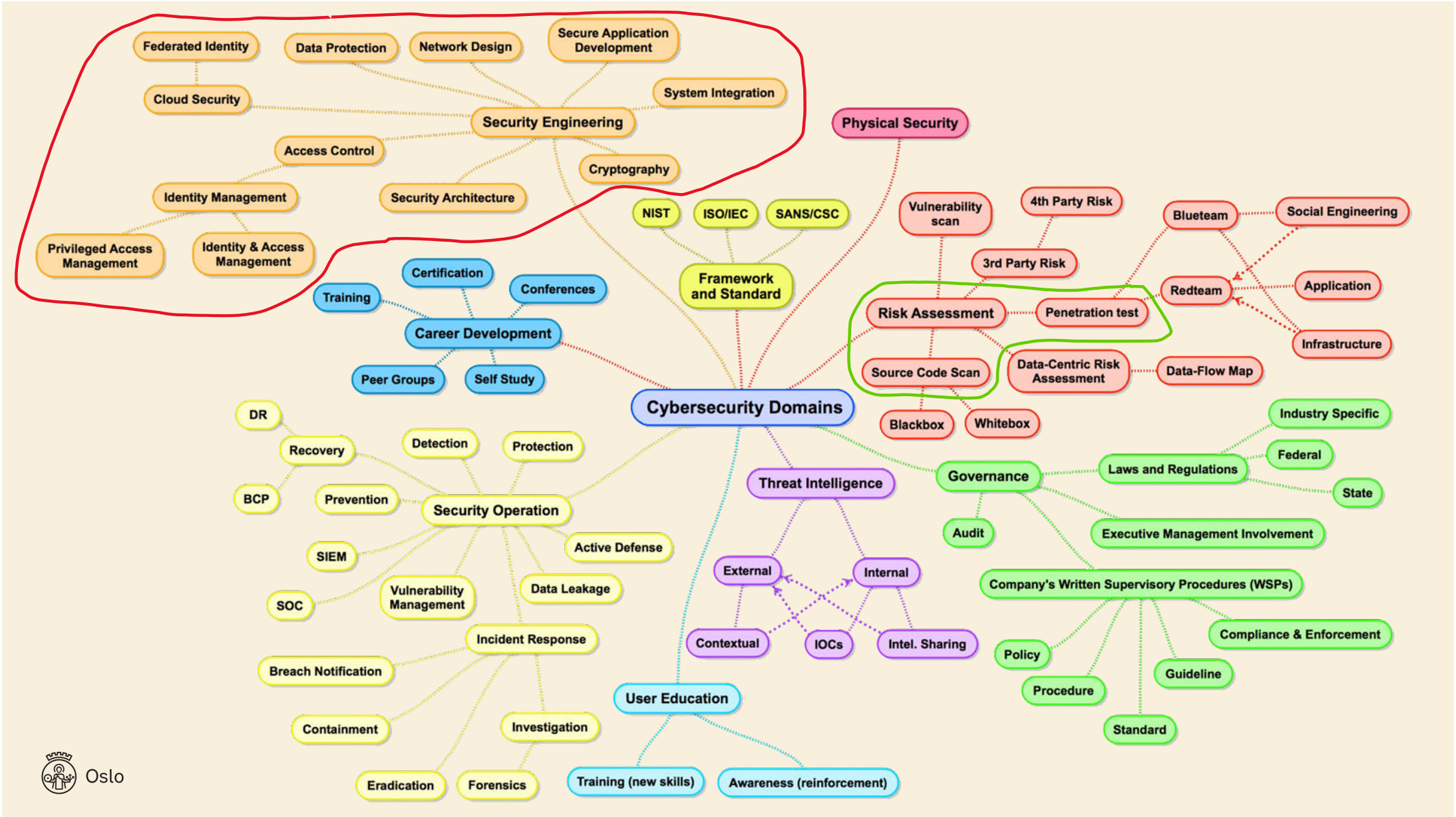
Utviklerne må forholde seg til mer enn bare applikasjonssikkerhet

... på godt og vondt!

Cybersikkerhetsdomener

Hvordan bredde ut cybersikkerhetskompetansen?

Oslo


Federated Identity
Data Protection
Network Design
Secure Application Development
Cloud Security
System Integration
Security Engineering
Access Control
Cryptography
Identity Management
Security Architecture
Privileged Access Management
Identity & Access Management
Physical Security
NIST
ISO/IEC
SANS/CSC
Framework and Standard
Certification
Training
Conferences
Career Development
Peer Groups
Self Study
Vulnerability scan
4th Party Risk
3rd Party Risk
Risk Assessment
Penetration test
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Cybersecurity Domains
DR
Recovery
BCP
Detection
Protection
Prevention
Security Operation
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Procedure
Guideline
Standard
Oslo

Hvor er vi i dag?

- Hva skal vi fortsette med?
- Hva skal vi slutte med?
- Hva skal vi jobbe med for å få til?

Image by Gordon Johnson from Pixabay

Oslo

NTNU

DEVELOPED AT THE NORWEGIAN CYBER RANGE

NITO

C.S. TECHNOPOLY

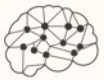
OUR MISSION

Making cyber security strategy interesting and fun

- NTNU is building a serious game community
- Devoted to providing society with a deeper understanding of cyber security

A role-playing and scenario game where to win, you will need to learn:

Threat Intelligence



Cybersecurity investments

Security value chain

Systems thinking & Socio-technical transitions

SIKKERHETS FESTIVALEN

28.08 - 30.08 2023

REGISTER HERE

WHEN: WEDNESDAY, 30.AUGUST, kl. 9-12

WHERE: FESTSALEN, KULTURHUSET BANKEN, LILLEHAMMER