Datadrivet bygger på tillit – och tillit kräver säkerhet

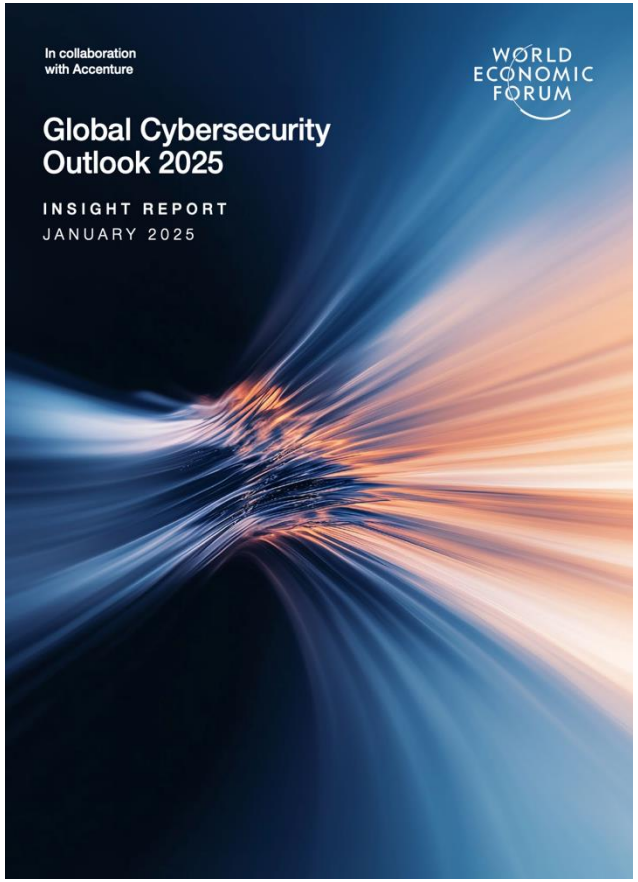
Fyra kritiska förmågor för en trygg och motståndskraftig datadriven kommun

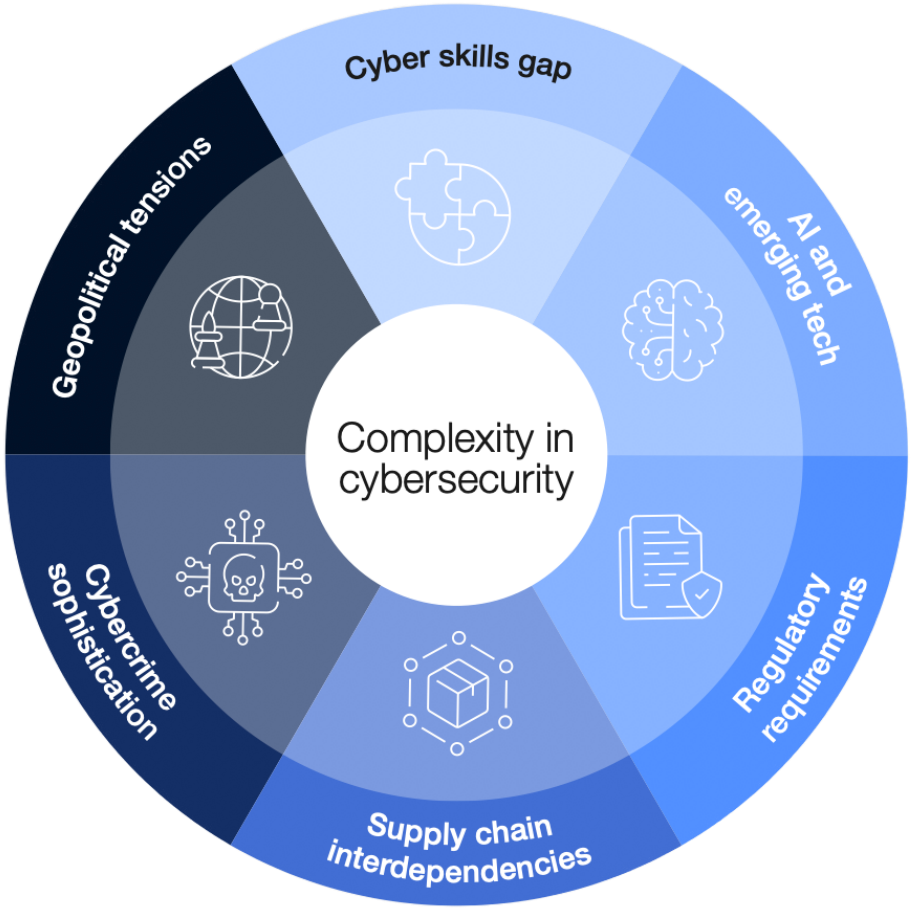
13:50-14:20 ˚ 17/11 ˚ 2025

I en tid där kommuner samlar, delar och analyserar mer data än någonsin behöver cyberhygienen vara lika självklar som renhållningen. I det här passet får du konkreta insikter om de fyra förmågor som skiljer en sårbar organisation från en robust, säker och datadriven kommun.
Göran Walles (Cybersecurity CTO, NetNordic)

Göran Walles
CTO Cybersecurity
NetNordic Sverige

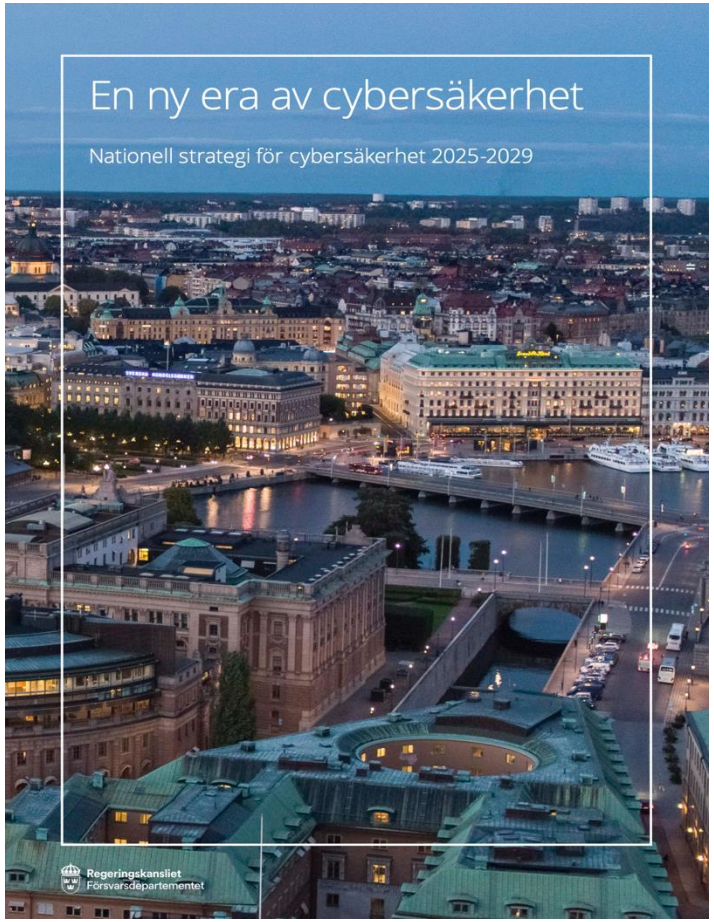
Komplexiteten inom Cybersäkerhet





https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Nationell strategi för cybersäkerhet 2025-2029



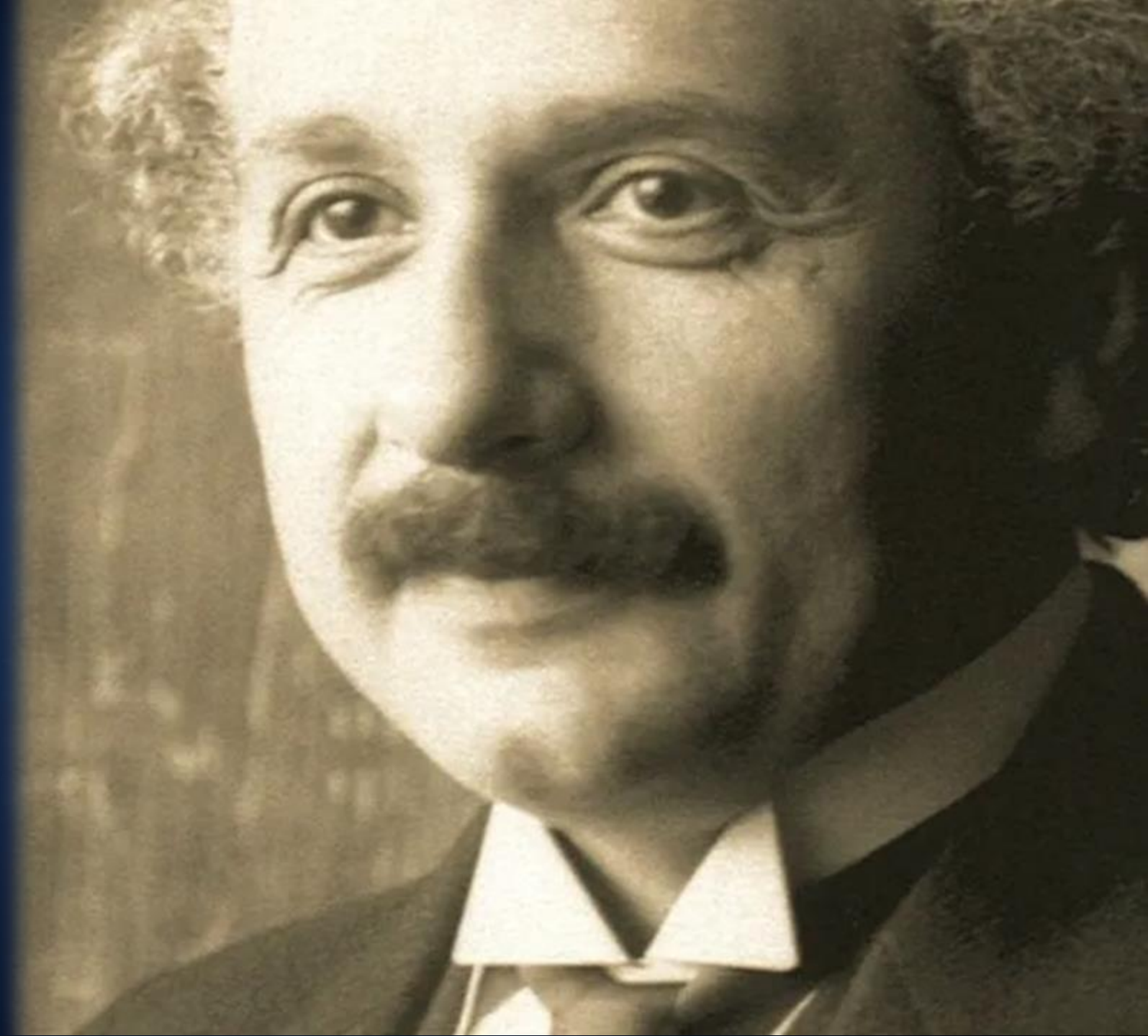
Kommuner är hårt ansatta


Datakvalité
IaaS
PaaS
SaaS
XaaS
Digital Service
Digital Först
OT
Data Fabric
PUBLIC CLOUD
CASB
Platformization
Informationsförsörjning
OT SÄKERHET
PRIVATE CLOUD
HYBRID CLOUD
Automation Journey
Shift Left / Shift Everywhere
HCI
PAM
ISO27001
CTI
IAM
Data Mesh
NIS2
ISO27002
Digital Mindfulness
EDR
DLP
IEC62443
DORA
COMPLIANCE
XDR
Quantum-safe Security
NDR
SASE
RISK
GOVERNANCE
PQC
DATA LAKE
AUTOMATION
Observability
BCP
Lag (2018:1174)
AI Governance
ZERO TRUST
CTEM
ML
AI
BCM
Digital Twin Security
AI-Ops
AI SÄKERHET
Red Team
ZTNA
IAC
LLM
K8s
MDR
Blue Team
NIST
Sec-Ops
Purple Team
CIS18
SIEM
Cloud-Ops
SOAR
OT
DDoS
IOC
SOC
MFA
Chat Control / CSAR
BAS
MLOps
DevSecOps
DATA LAKE
BEC
DRP
GRC
IRP


STOP

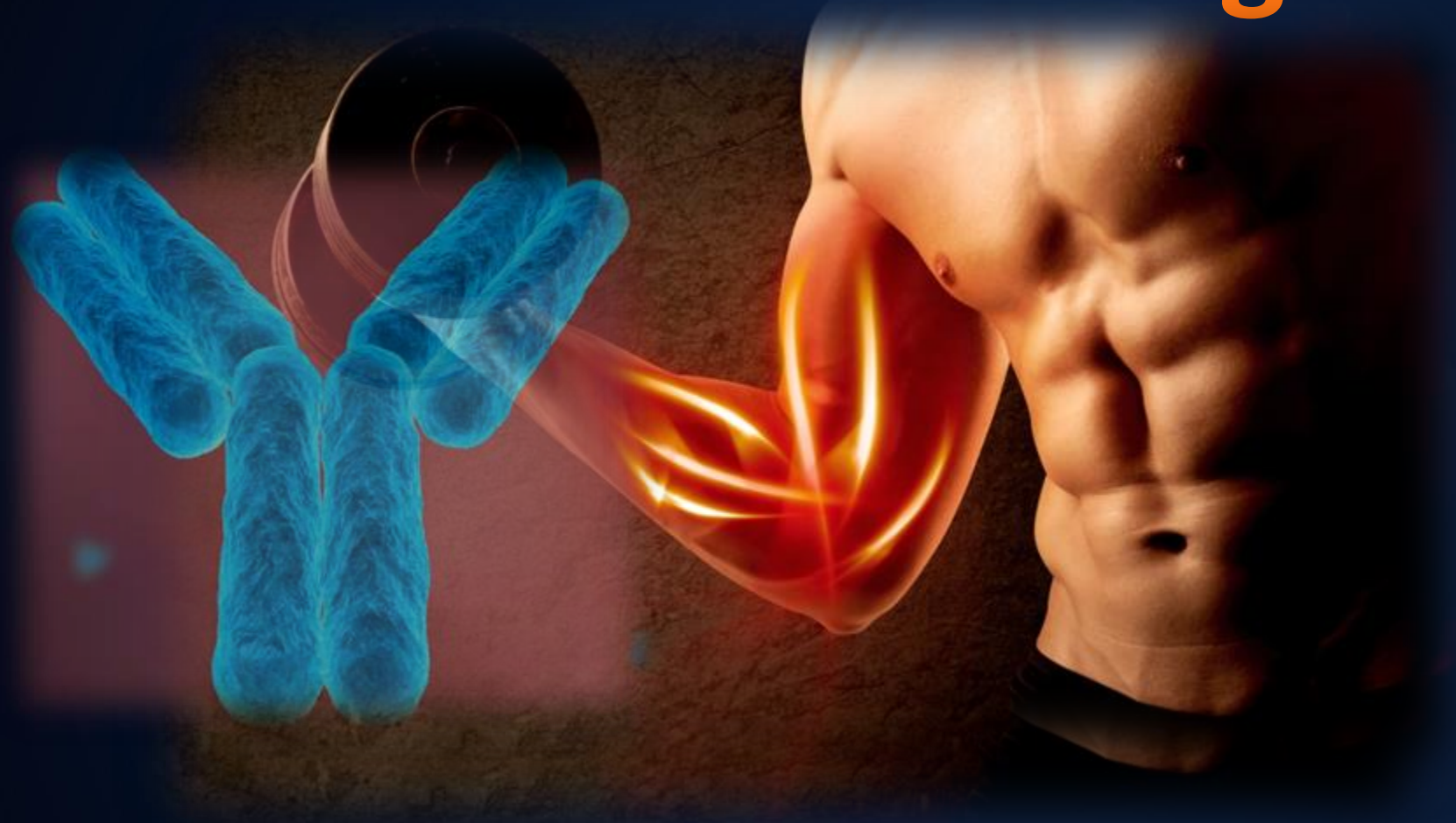

~~digital, hybrid och fysisk~~
Rörliga hot och möjligheter

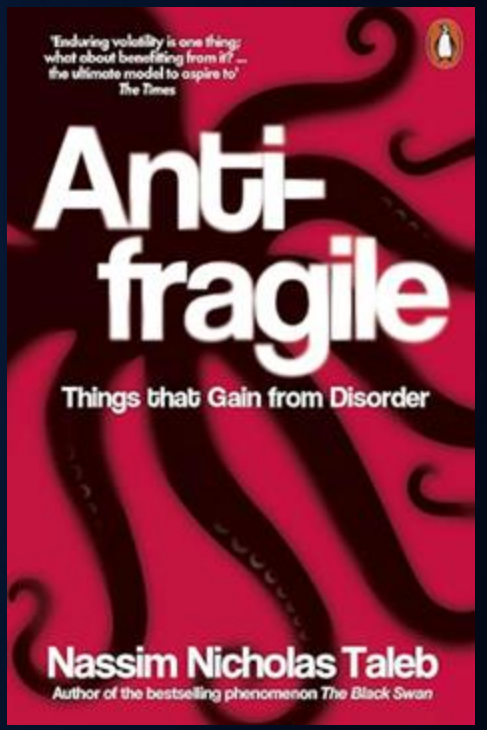
Galenskap är att göra samma sak om och om igen och förvänta sig ett annorlunda resultat



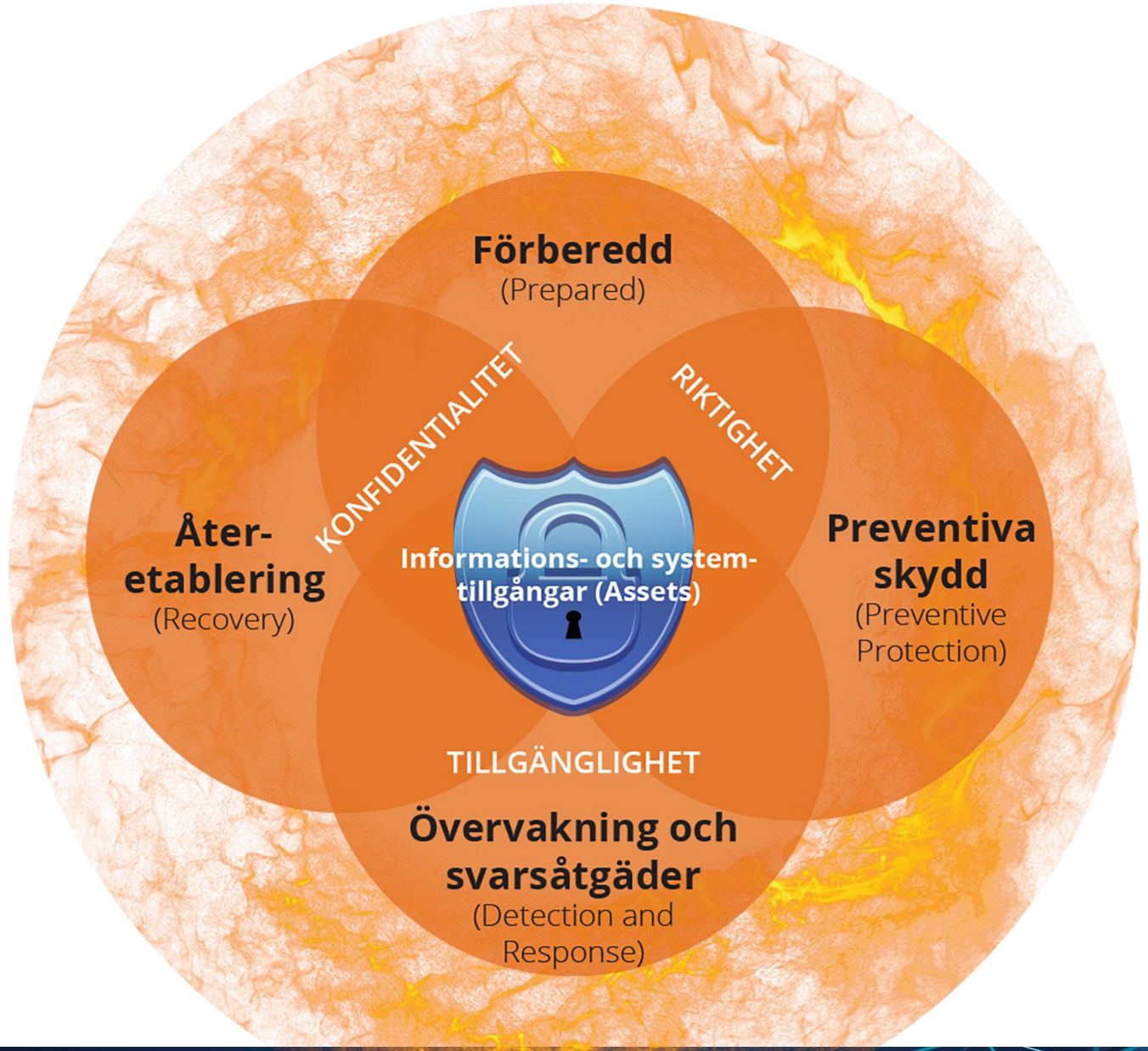

Förändring och nya vägar

Antifragil





Påfrestningar bryter inte det *antifragila*: de gör det starkare.
Exempel: kroppens immunförsvar, muskler, evolution och ekosystem.


Förberedd
(Prepared)
KONFIDENTIALITET
RIKTIGHET
Åter-
etablering
(Recovery)
Informations- och system-
tillgångar (Assets)
Preventiva
skydd
(Preventive
Protection)
TILLGÄNGLIGHET
Övervakning och
svarsåtgäder
(Detection and
Response)

DaaS =

Data (ex. Personuppgifter)
Applications (ex. Mjukvara)
Services (ex. Användarkatalog / AD)
Assets (ex. IoT)

~~Säkra på "insidan"~~

Se inspelning

For Security & Risk Professionals

September 14, 2010 | Updated: September 17, 2010

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security

by John Kindervag
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model.

Zero Trust = Eliminera tillit som säkerhetsprincip

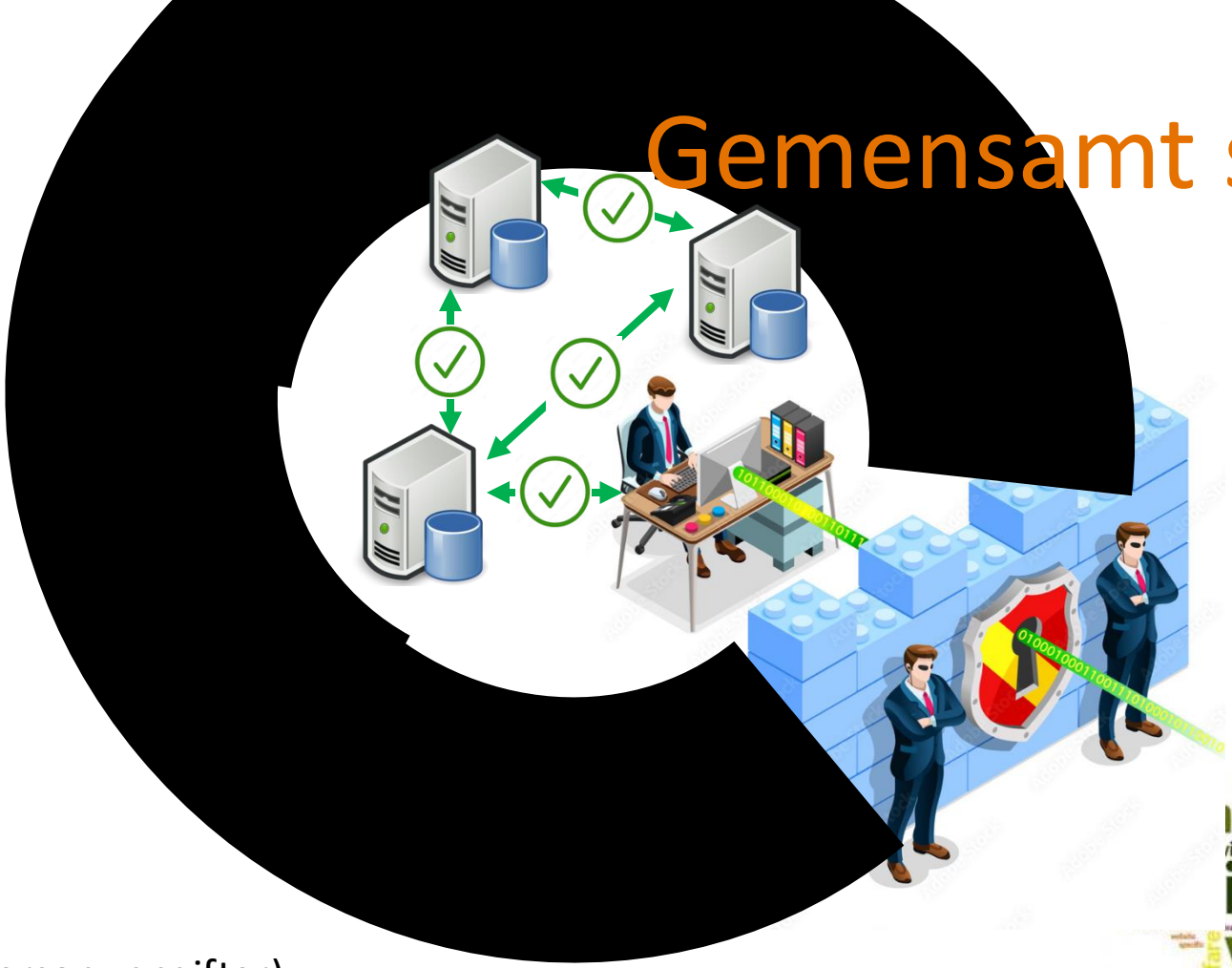
ZERO TRUST
"Nolltillit"

En strategi utformad för att stoppa dataintrång och förhindra andra cyberattacker från att lyckas, genom att eliminera tillit från digitala system.

Missförstånd

- Zero Trust handlar bara om identitet
  - → Fel: det handlar om hela ekosystemet
- Zero Trust betyder att göra systemet ”trusted”
  - → Fel: Zero Trust betyder nolltillit som utgångspunkt
- Det finns färdiga Zero Trust-produkter
  - → Fel: det är en strategi och arkitektur
- Zero Trust är för komplicerat
  - → Fel: det kan (bör) implementeras steg för steg

Gemensamt skydd mot Internet



DaaS =

Data (ex. Personuppgifter)
Applications (ex. Mjukvara)
Services (ex. Användarkatalog / AD)
Assets (ex. IoT)

Ringmursprincipen slopad

DaaS =

Data (ex. Personuppgifter)
Applications (ex. Mjukvara)
Services (ex. Användarkatalog / AD)
Assets (ex. IoT)

Varje system skyddat/övervakat

DaaS =

Data (ex. Personuppgifter)
Applications (ex. Mjukvara)
Services (ex. Användarkatalog / AD)
Assets (ex. IoT)

Segmentering = tillåt endast legitim trafik

DaaS =

Data (ex. Personuppgifter)
Applications (ex. Mjukvara)
Services (ex. Användarkatalog / AD)
Assets (ex. IoT)

Förstå Zero Trust något djupare: 5 stegen

Antifragil

Data
Applications
Assets
Services

Define the protect surface

Map the transaction flows

Architect a Zero Trust Environment

Create Zero Trust policy

Monitor and maintain

Skräddarsydd

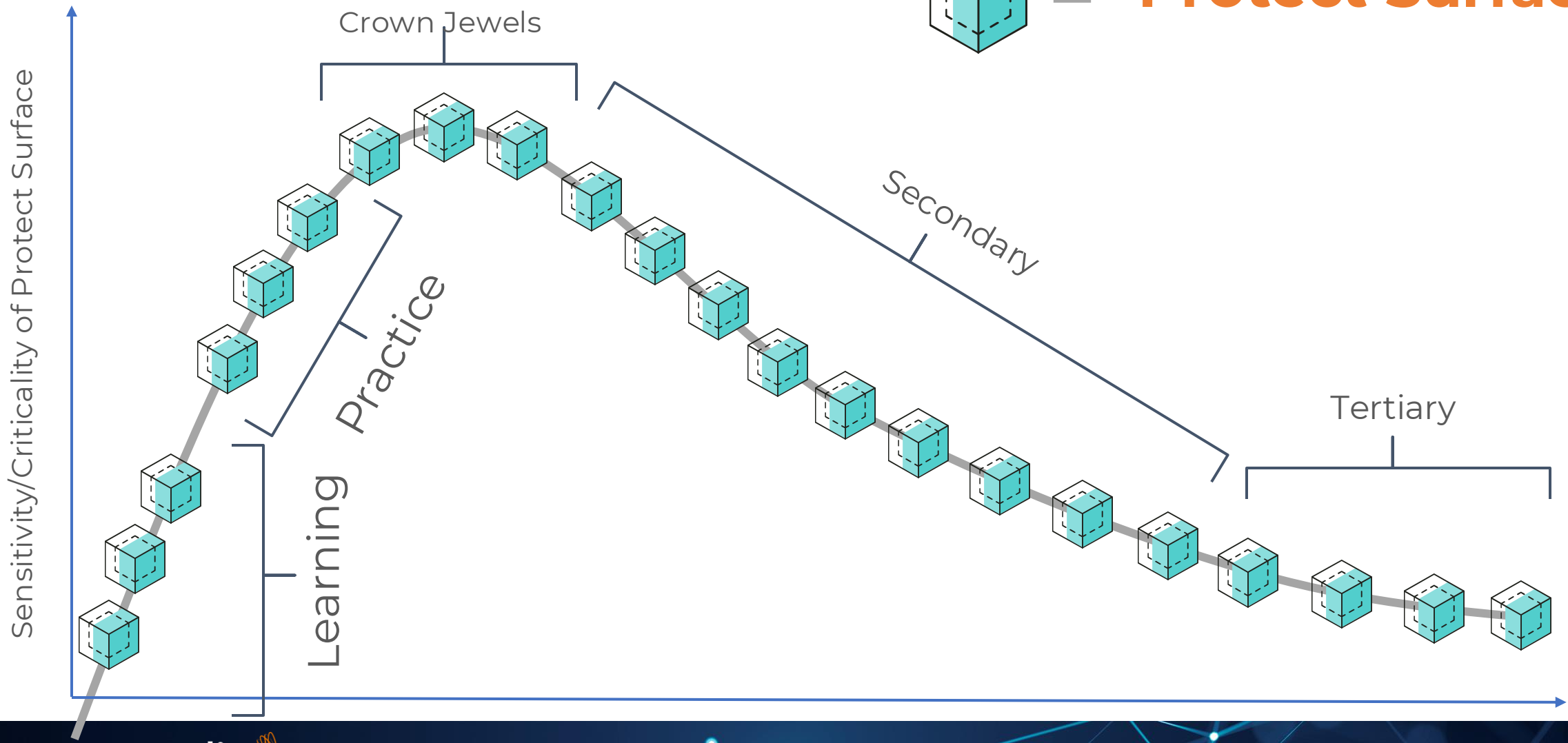
Kipling-metoden för att skriva policys

Who	What	When	Where	Why	How
Resource Validation	**Application Validation**	**Time Limitations**	**Location**	**Environment**	**Flow Validation**
Ex -Identity Attributes	Application Name	Ex -Working Hours	Workload Location	Protect Surface	Workload Metadata
Ex -Workload Name	Ex -AD	Ex -Anytime	Ex -New York	DAAS Element	
Ex -OT Asset Name	Ex –AD_Port, Protocol Range		Ex -Azure	Ex -Test Environment	
Ex -Endpoint Name	Ex –AD Process ID		Ex -Remote	Ex -SCADA	

IF Who = AD_Admins, What = AD_App_Validation, When = Anytime, Where = Domain Controller (On Prem or Cloud), Why = Protect Surface Tag, How = AD_Meta, THEN Allow.

Inlärningskurvan

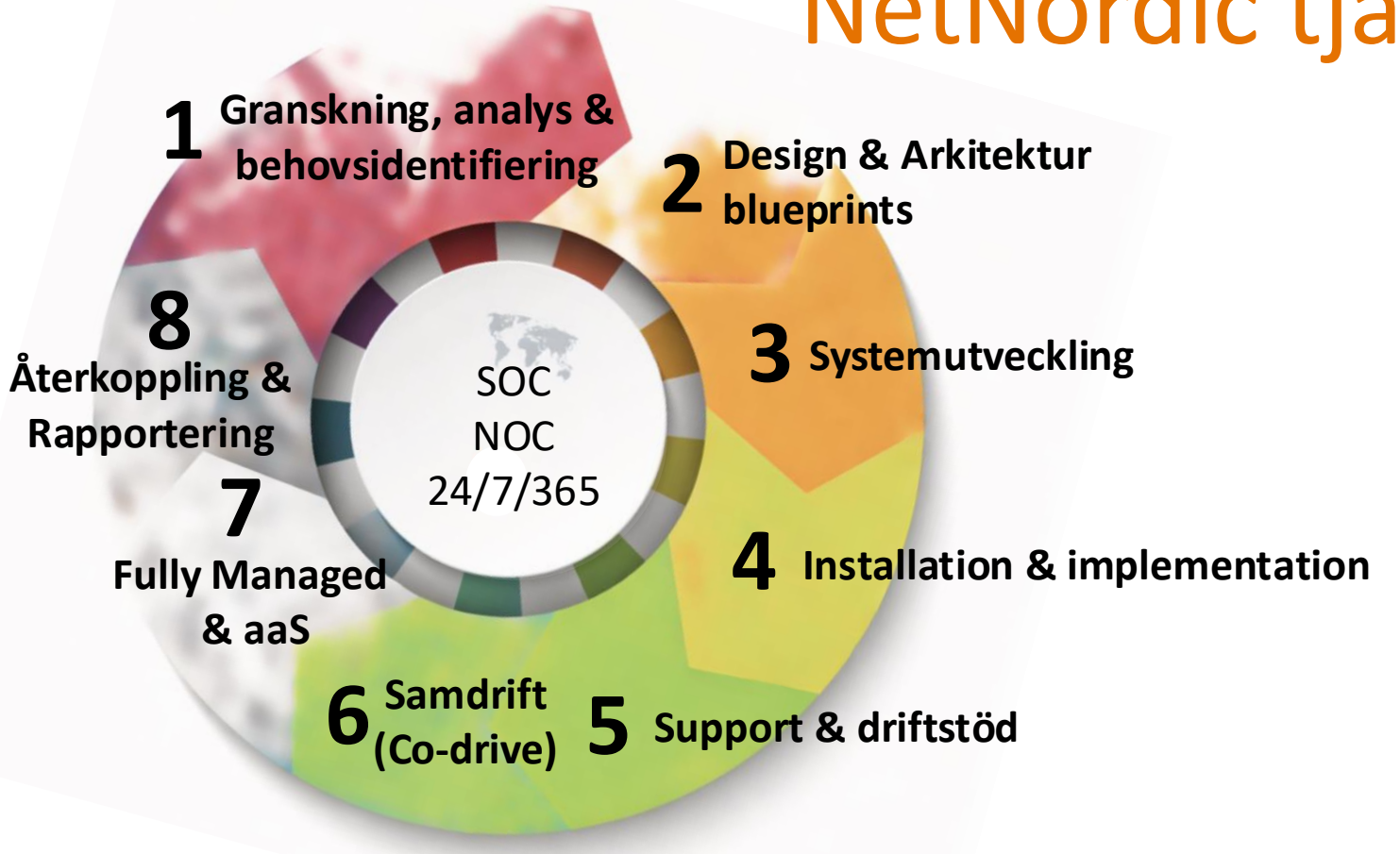
= **Protect Surface**



Mognadsmodell

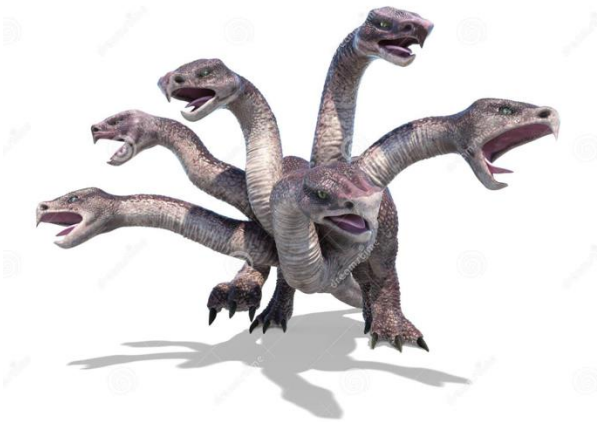
DAAS Element / Protect Surface	Initial	Repeatable	Defined	Managed	Optimized
1. Define your Protect Surface	1	2	3	4	5
2. Map the Transaction Flows	1	2	3	4	5
3. Architect a Zero Trust Environment	1	2	3	4	5
4. Create Zero Trust Policy	1	2	3	4	5
5. Monitor and Maintain the Network	1	2	3	4	5

NetNordic tjänsteleveranser



Vi erbjuder expertstöd där det passar.

Summering



- Cyberförsvar baseras på **fyra** kritiska förmågor:
  - Förberedd
  - Preventiva skydd/kontroller
  - Säkerhetsövervakning
  - Backup

  (Människor, processer och teknologi)

  Zero Trust (Nolltillit) är en säkerhetsmodell utifrån principen att varken system eller användare ska utgå ifrån tillit, utan nolltillit med kontinuerlig kontroll.

  - Effektiv
  - Implementeras “System för System” i motsats till “alla på en gång”
  - Antifragile (sv. Anti-bräcklig)
- Zero Trust byggs steg för steg, sällan i big-bang för en befintlig miljö