KIVI Security avond

IT & OT security
De RWS aanpak

Jeroen Gaiser, MSc BSc CISSP

Rijkswaterstaat

TLP: Green (voor deelnemers aan de sessie, niet verder verspreiden)

@Whoami

LinkedIn
(trust me)

Who am I?

- IT (side)jobs sinds 1995
- Begonnen met techniek/(applicatie)beheer, nu focus op beleid/governance
- Security focus sinds 2010
- Werkzaam bij RWS sinds 2014
  - Lead Architect Cybersecurity
  - Coordinating advisor Cybersecurity

Wat is een Cyber Physical System?
ook wel: Operational Technology (OT)

"Cyber-Physical Systems (CPS) are integrations of computation and physical processes."

E. A. Lee, "Cyber Physical Systems: Design Challenges," 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), vol. 00, no. , pp. 363-369, 2008. doi:10.1109/ISORC.2008.25

Voor deze presentatie:
Systemen die een digitale actie (Vb. uit software) omzetten in een actie in de fysieke wereld en vice versa.

IT vs OT

- Gemeenschappelijk doel: zorgen voor correcte en betrouwbare werking
- IT incident: dienst onbereikbaar
- OT incident: mens/omgeving in gevaar
- Overzicht belangrijkste verschillen

	IT	OT/ICS
Performance	Consistent response High throughput of data Delay and jitter are OK	Real-time Response is time-critical Response is deterministic Modest throughput Delay/jitter unacceptable
Availability	Reboot acceptable Small availability issues are OK DoS not critical to business Ops	Always available demand Redundancy is commonplace DoS has significant impact
Security Architecture	Protect IT assets (data in transit/rest) Controls are found everywhere Pentest tools are used	Protect the edge Not many controls at processing level (PLC) Pentesting will break stuff (e.g. portscan)
Users	Everybody	Engineers (user & admin roles)
Risk management	Data CIA Delay of business operations	Human safety first Regulatory compliance, environment impact, equipment damage
Security tooling	LOTS of IT security testing solutions for IT	Tools must be tested before use to ensure no impact on operations/performance
System Operation	Software/systems intended for use with common OS Upgrading/patching is straightforward (and automated)	Different proprietary systems and OS are combined No security capabilities Software changes very complex
Resources	Systems specs can support additional tasks like security controls	Systems designed for (very) specific tasks with no room for additional tasks
Communications	Proprietary and common protocols (slide 17!) Various media used (e.g. serial/Ethernet) Networking requires specific resources and become complex	Standard communication protocols Wired & Wireless Standard networking principles
Change management	Changes are 'going concern' Automation common & increasing	Changes must be thoroughly tested Outages must be planned months beforehand Lack of support on e.g. OS is common
Support	Multiple service providers	Single vendor
Component lifetime	3-5 years	15-20 years
Access to components	Good accessibility	Locations can be isolated and require effort to reach (buoy at sea)

Digitalisering van objecten importeert IT risico's

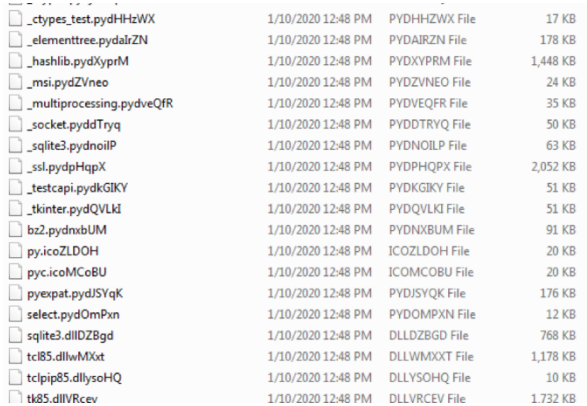
- Digitization of assets has great efficiency & effectivity benefits
- IT components/libraries find their way into OT
- Distinction (tech) between IT & OT is fading (a bit)
- Example: EKANS ransomware

EKANS

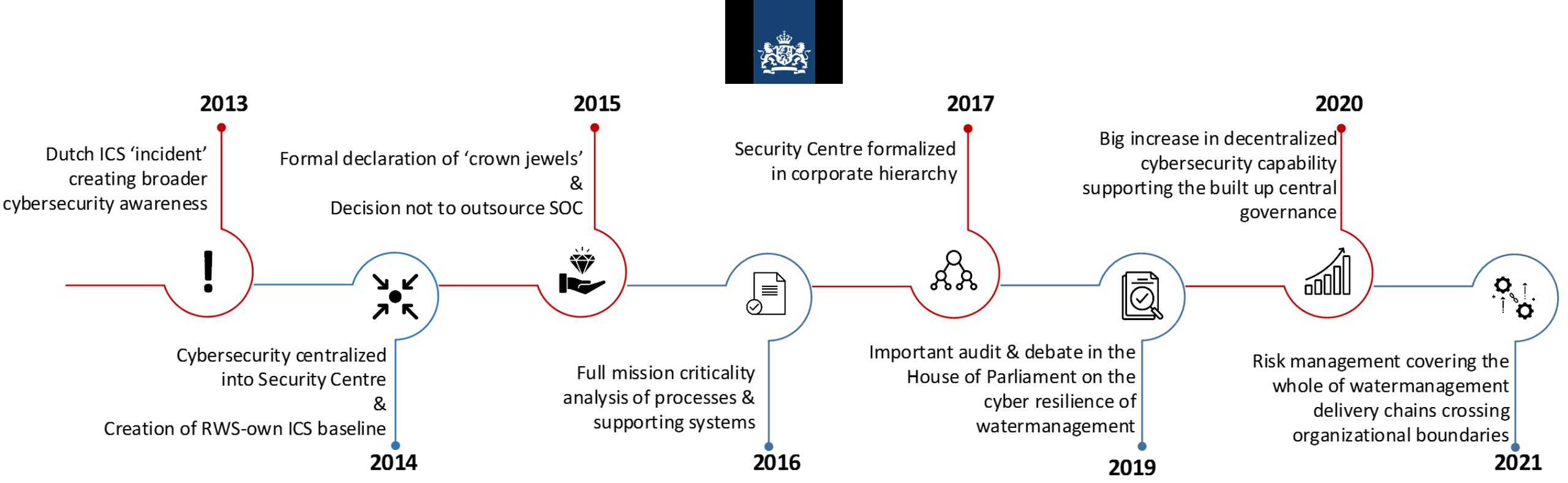
"With a limited set of ICS-specific malware in existence, EKANS, though primitive, represents an evolution in adversaries targeting control system environments."

Dragos

- Kills specific ICS processes
  - GE's Proficy data historian
  - Honeywell's HMIWeb application
  - ThingWorx Industrial Connectivity Suite.
- User can access system
  - Less disruptive than LockerGoga (Norsk Hydro)
  - Focus on enterprise network compromize instead of self-propagation
  - Financial incentive or APT? What does the 'less disruptive' approach signify?



Cyberaanvallen op vitale infrastructuur

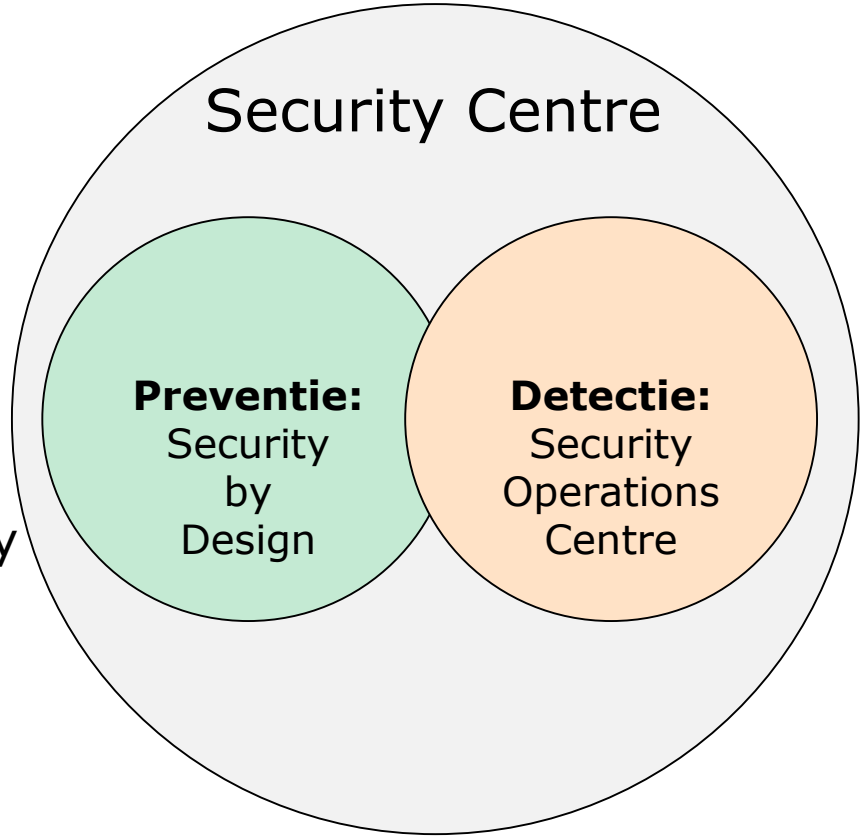

2013
Dutch ICS ‘incident’ creating broader cybersecurity awareness
2014
Cybersecurity centralized into Security Centre
&
Creation of RWS-own ICS baseline
2015
Formal declaration of ‘crown jewels’
&
Decision not to outsource SOC
2016
Full mission criticality analysis of processes & supporting systems
2017
Security Centre formalized in corporate hierarchy
2019
Important audit & debate in the House of Parliament on the cyber resilience of watermanagement
2020
Big increase in decentralized cybersecurity capability supporting the built up central governance
2021
Risk management covering the whole of watermanagement delivery chains crossing organizational boundaries

De RWS aanpak

- IT en OT holistisch aanpakken en niet in silo’s
- Multi disciplinair security team
- Cybersecurity inbedden in bestaande voortbrengingsprocessen
- Samenwerking tussen security experts en engineers is essentieel!
- Governance cybersecurity omvat alle digitale risico’s

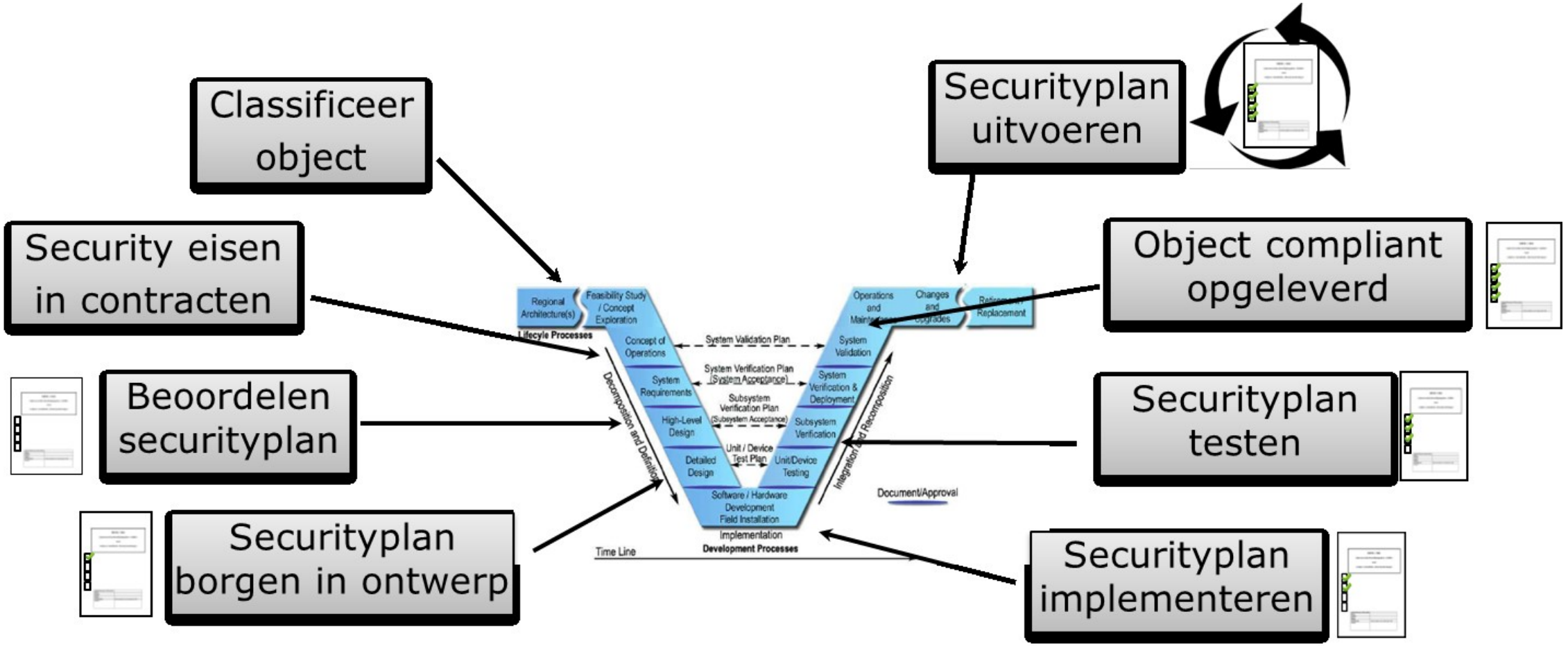
Organisatie: Preventie & detectie

- Zo vroeg mogelijk in een bouwtraject security eisen meegeven
- Zowel bij IT als Industriële Automatisering (objecten)
- Voor IT: BIO
- Voor IA: CSIR (Cybersecurity Implementatie Richtlijn Objecten)
- Advies bij ontwerp, bouw en beheer

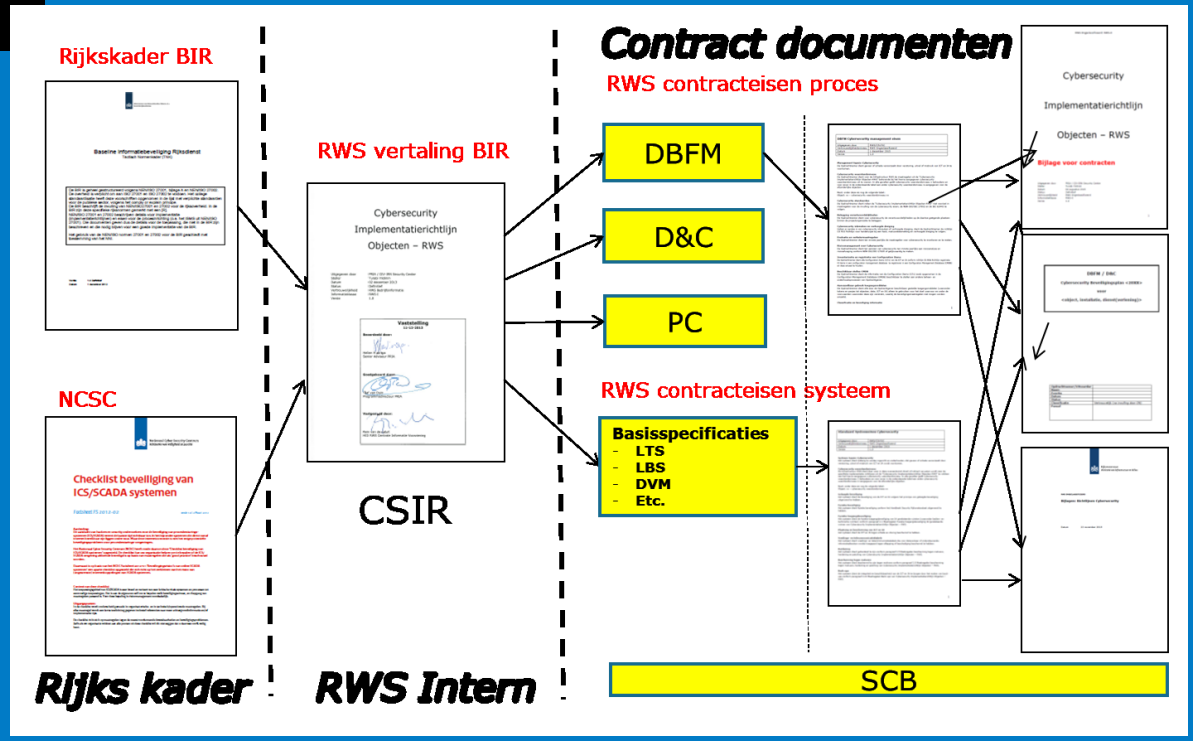


- Monitoring van IT en OT infrastructuur oa de RWS netwerken
- Monitoring van objecten is aparte uitdaging
- Analyseren ca 34,5 miljard (!) events per week
- Threat intelligence
- Forensics
- Pentesting
- Expert bij een incident of CERT

Security in OT lifecycle



CSIR: Cybersecurity Implementatierichtlijn Objecten RWS



BOX	Weerstands niveau
A	4
B	3
C	2
D	1
E	

Vragen?