Cyber is een informatie- en kennisoorlog

Samenwerking van bedrijfsketens met een Kennisintensieve Overheid bij het verhogen van de cyberweerbaarheid van de maatschappij.

Drs. Ir. Aernout Reijmer,
Senior Director ASML
CISO Circle of Trust
Semi CyberSecurity Consortium
Cyclotron Program Governance

ASML

De trends gaan de verkeerde kant op voor security

Aantal ransomware incidenten verdrievoudigd in 2031 (tov 2023)

Geopolitieke spanning en dreiging neemt toe

Toenemende digitalisering maatschappij, alles is connected

Aantal nieuwe IT kwetsbaarheden: 80+ per dag en stijgende. Onbeheersbaar voor kleine partijen

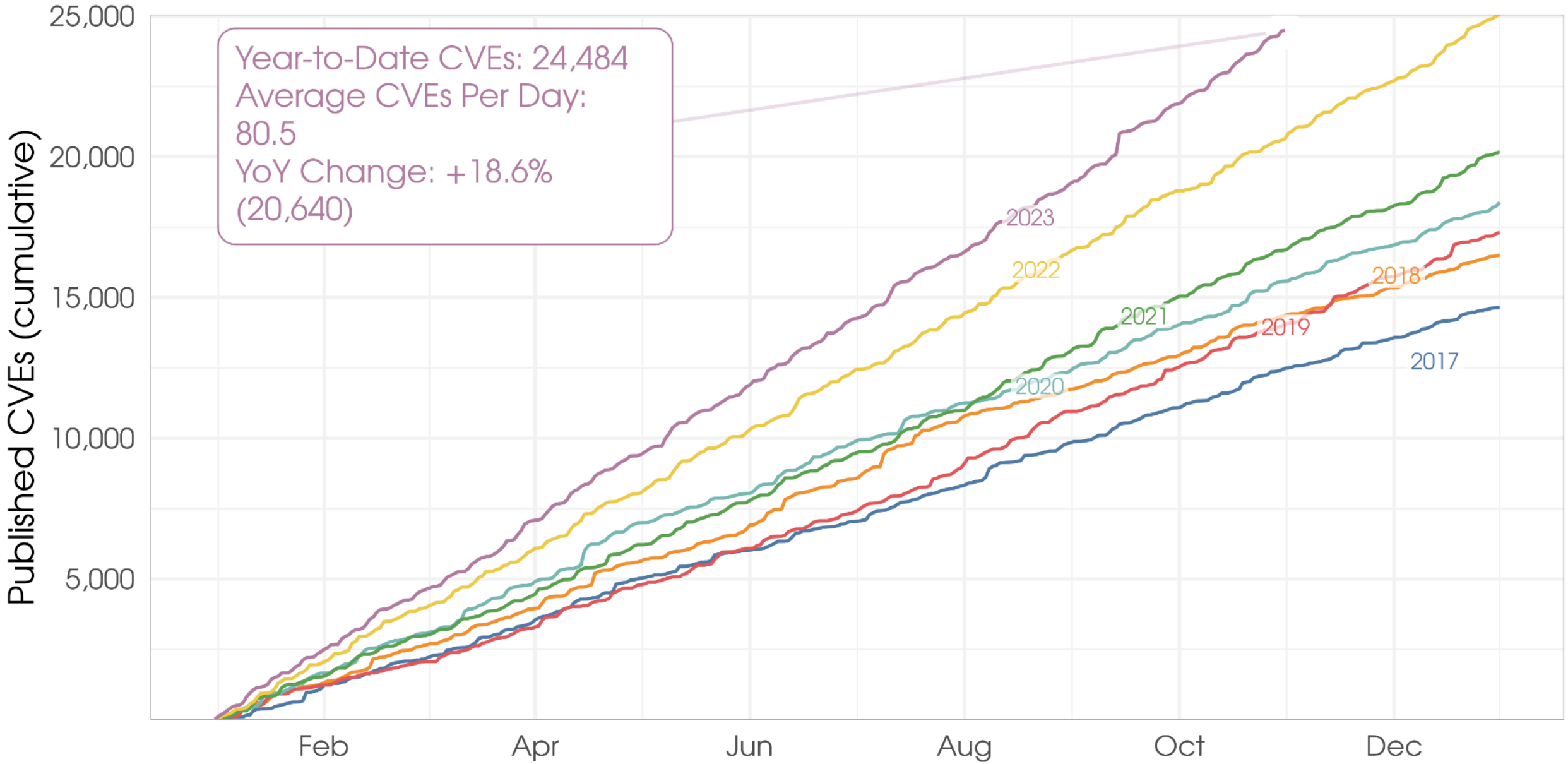
Disruptieve technologieen

Cloud, GenAi en Post Quantum Computing

Enorm tekort aan Cyber experts; en het tekort wordt groter!

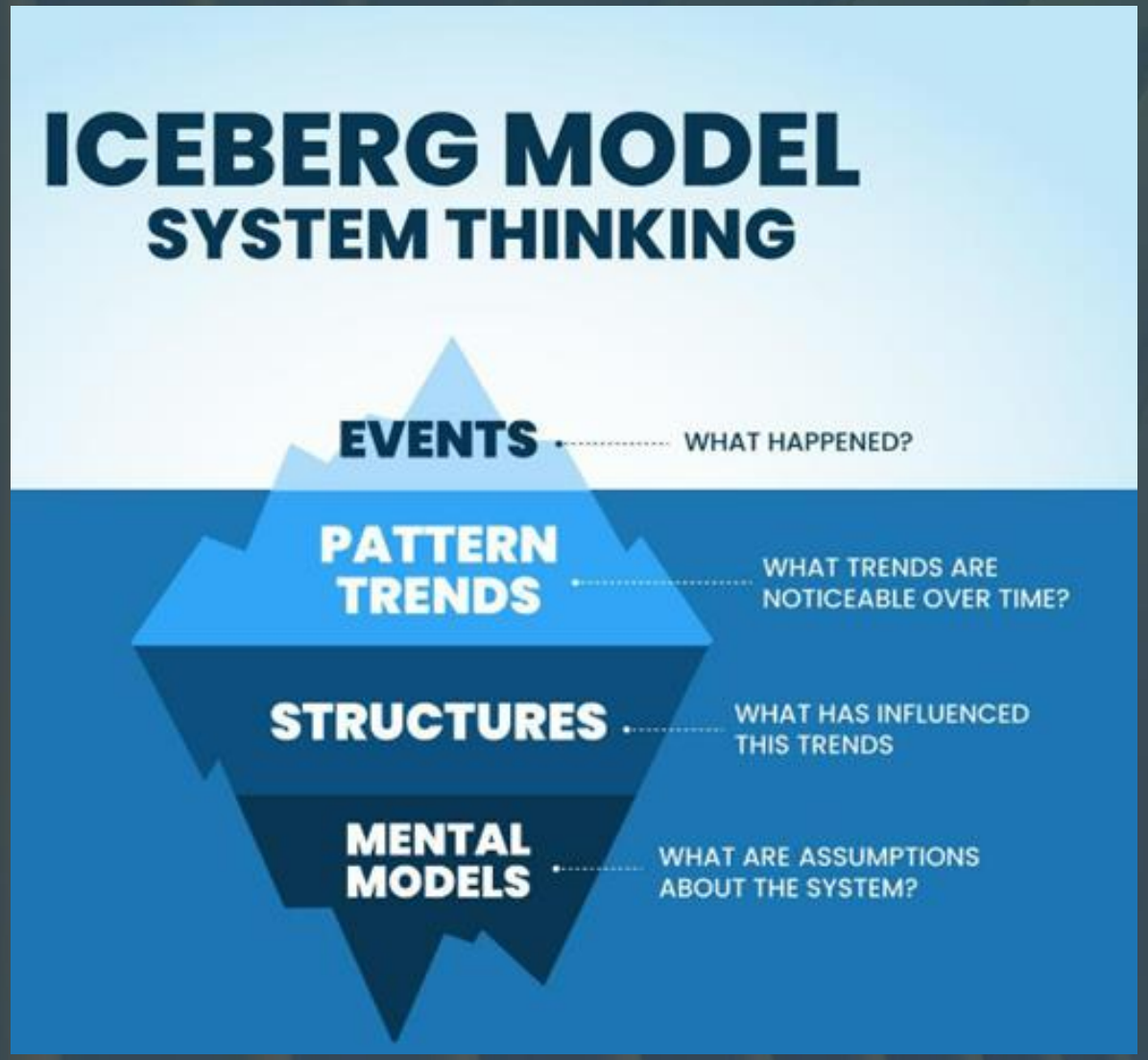
Year-to-date CVE publications (MITRE CVE List)

Lines showing the daily cumulative count of published CVEs on MITRE's CVE List, https://cve.mitre.org/cve/



Source: https://first.org/epss/data_stats, 2023-10-31

De trends gaan de verkeerde kant op voor security



1. Ransomware. De kosten van cybercrime zijn hoog
2. Diefstal van Intellectueel Eigendom
3. Wet- en regelving NIS 2 / CRA
4. Digitalisering en Cloud gaat door; PQC komt er aan
5. Toename in cyber incidenten
6. Aantal kwetsbaarheden neemt toe
7. 1000en werknemers per jaar nodig; vs slechts 100en uit de schoolbanken
8. Wie is verantwoordelijk voor security; juridisch kader
9. Wie kan wat doen op het gebied van cyber security?
10. Hoeveel willen we betalen voor Cyber Security?
11. Wat is de rol van de overheid en het bedrijfsleven?
12. Groot helpt Klein; maar hoe vaak?

‘Als we blijven doen wat we altijd deden, dan krijgen we wat we altijd kregen’


Kortom, als we niets veranderen, hebben we een groot probleem

Naar een kennisintensieve overheid: Gebruik en dessimineer de bestaande cyber kennis en inzichten in het bedrijfsleven

- Cyber Weerbericht / Alarm rondom kwetsbaarheden
- Cyber Threat Intel rondom dreigingen
- Centrale bibliotheek met Best Practices en Handelings Perspectief, hoe kom je ‘in control’

Vraag: Minder versplintering, sterkere regie/agenda, coordinatie en executiekracht door de overheid.

Faciliteer, stimuleer en organiseer kennisdeling via Public Private Partnerships

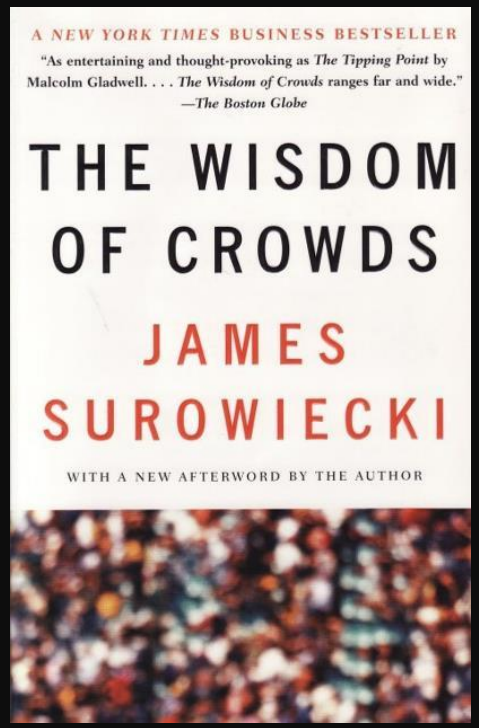
- Overwin perverse incentive van inwendige focus
- Groot helpt Klein
- Versterk sectorale/regionale cyber weerbaarheid organisaties.
- Oefen met elkaar: weet elkaar vooraf te vinden; wordt samen beter in crisesbeheersing.

Zorg voor meer cyberexperts door meer budget voor onderwijs

- Meer programma’s moeten kunnen starten
- Samen met Universiteiten/ HBO / MBO.
- Stageplekken, job rotation met overheid
- Naast master studenten ook praktische scholing
- Bedrijfsleven en overheid kunnen gezamenlijk een aantrekkelijk carierre pad aanbieden

Groepswijsheid is het fundament van onze Collectieve verdediging.

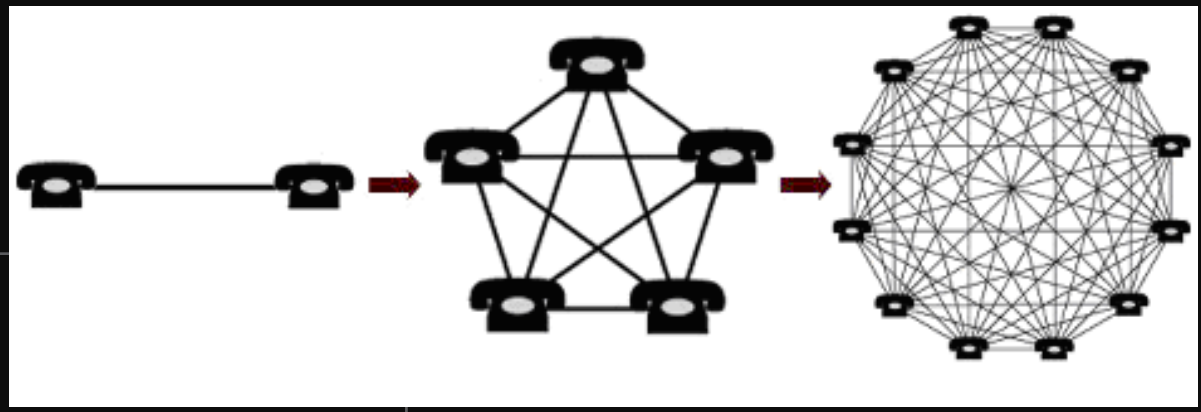
Met de Overheid als een autoriteit richting de expertise die in het bedrijfsleven aanwezig is en tot groot nut kan zijn.



Metcalfe’s Law

‘De waarde van een network neemt exponentieel toe ten opzichte van het aantal nieuwe nodes in het netwerk’

(cyber criminals doen dit sinds de start van het internet)

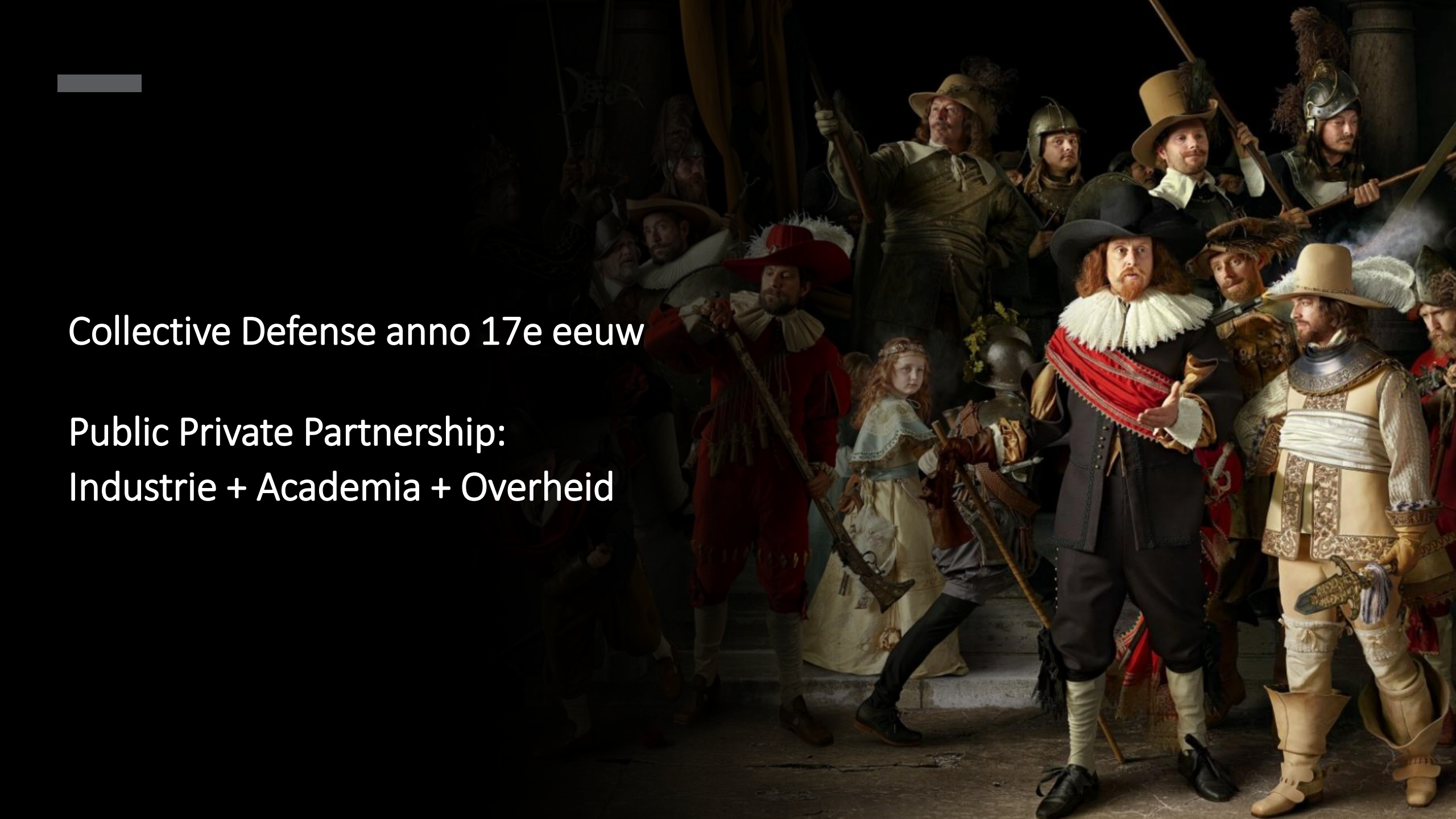


Verbindt:

Het bouwen, verenigen en efficient maken van kennisnetwerken heeft grote voordelen; Als ook het offline brengen van criminele netwerken.

Collective Defense anno 17e eeuw

Public Private Partnership:
Industrie + Academia + Overheid



Collective Defense anno 2024
Public Private Partnership: Industrie + Academia + Overheid

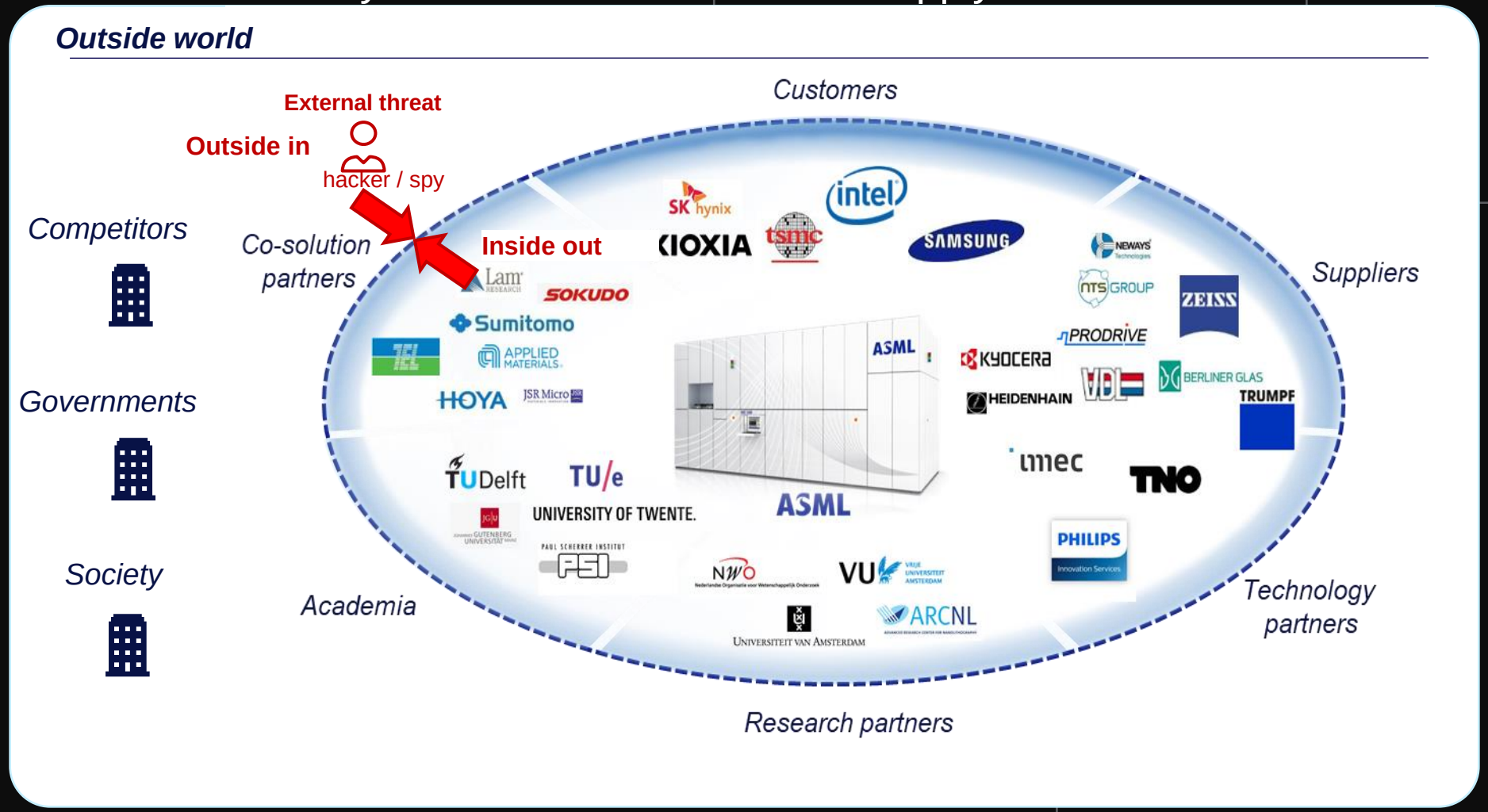
image created by ChatGPT depicting Rembrandt's 'The Night Watch' and the theme of cybersecurity

Source: Edwin Franse, CISO Van Oord)

ASML collaborates with partners in an eco-system

80%+ of components in the Litho machines are made by our suppliers / partners

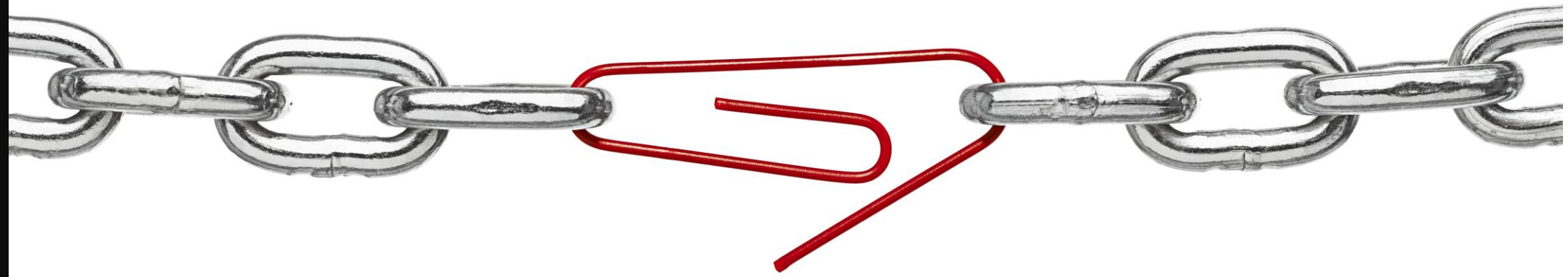
Rapid increase of security incidents observed in the supply chain



'OEM' Companies innovating and producing in eco-systems need to lead on protecting information and infrastructure beyond the corporate boundary, as the attack surface is extended to the perimeter of the full ecosystem.

The Global Ecosystem

We are all connected



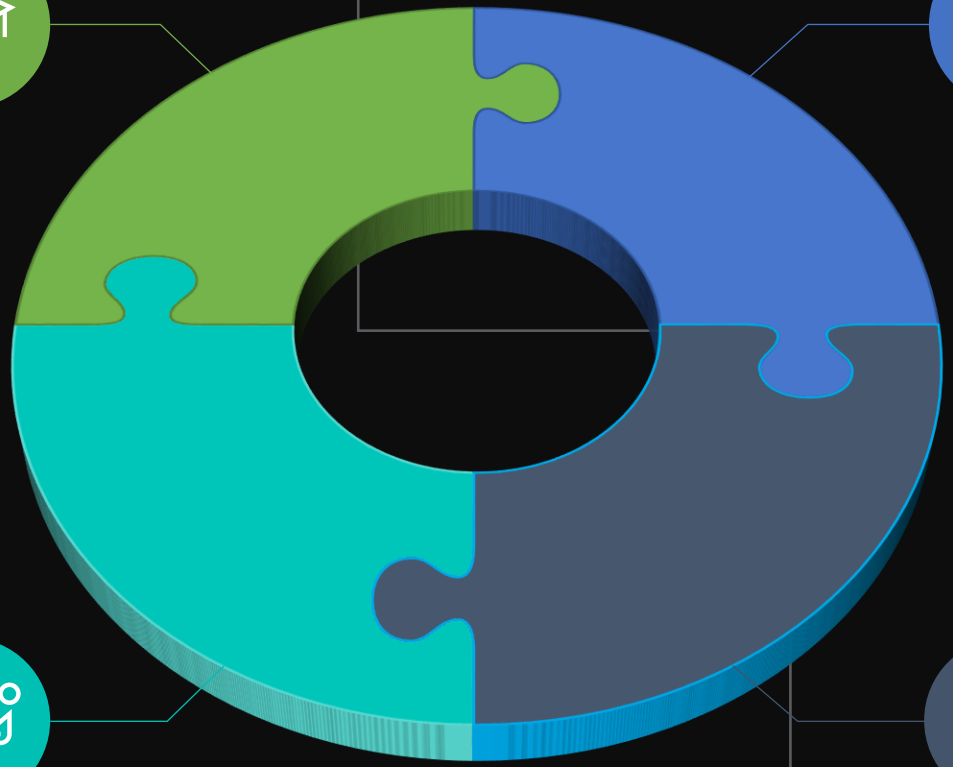
Learn from each other, don’t compete on Cybersecurity
We’re in this cyber arms race together

Don’t reinvent the wheel → Learn from each other!

Security Circles of Trust

Drive the security maturity in the ecosystem – for our partners and for us

Organizing Masterclasses



Work on Knowledge Products and standards, i.e. a standardized Cyber Rating tool for Industry CYRA on Supplier Security

Sharing knowledge, and best practices

Exchange Cyber Threat Intel, and align on Vulnerability Assessments for communication to the broader ecosystem.