Get ready for the AI attack bot

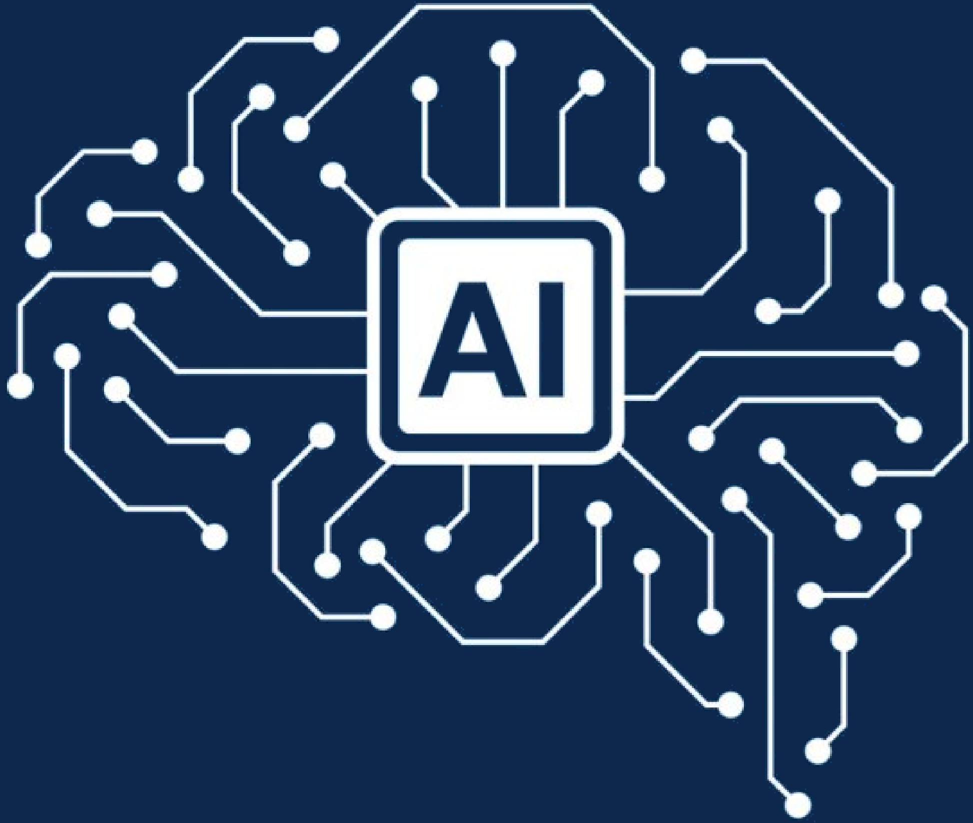
When looking back is not enough anymore

Richard de Vries
Operational Security Manager @ Tata Steel Europe
Blogger @ https://tales-from-a-security-professional.com/
September 22, 2022

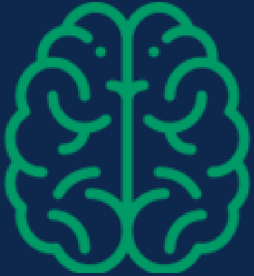
Share experience. Build resilience.

Share experience. Build resilience.

What *is* Artificial Intelligence exactly?



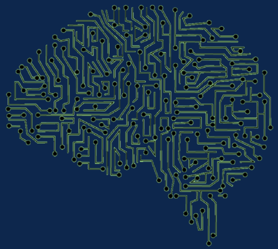
3 stages of Artificial Intelligence



Artificial narrow intelligence

Machine learning

Specializes in one area and solves one problem



Artificial general intelligence

Machine Intelligence

Refers to a computer that is as smart as a human across the board

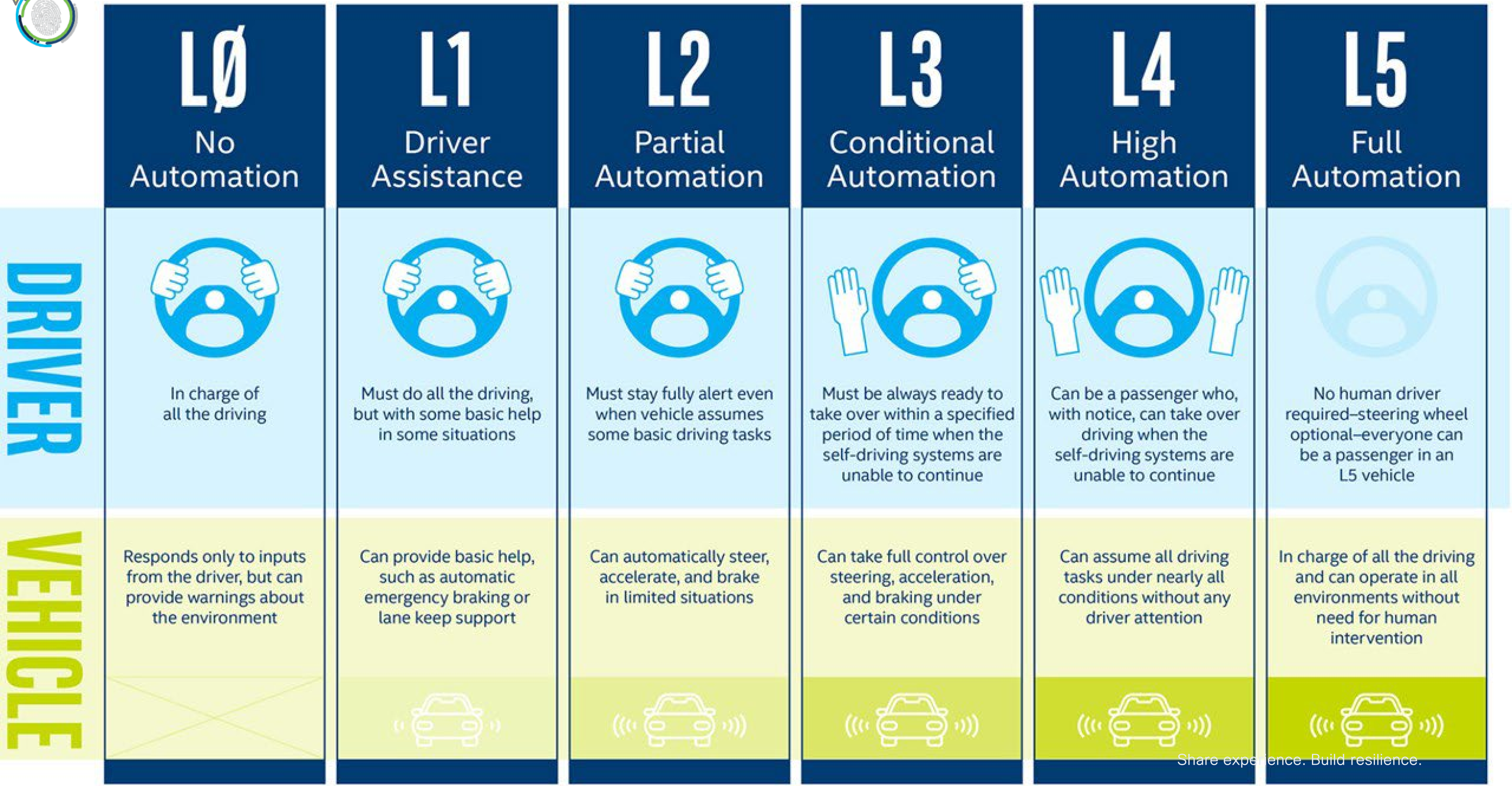
Artificial super intelligence

Machine consciousness

An intellect that is much smarter than the best human brains in practically every field.

Let’s talk about some of the *security risks* of Artificial Intelligence.

Share experience. Build resilience

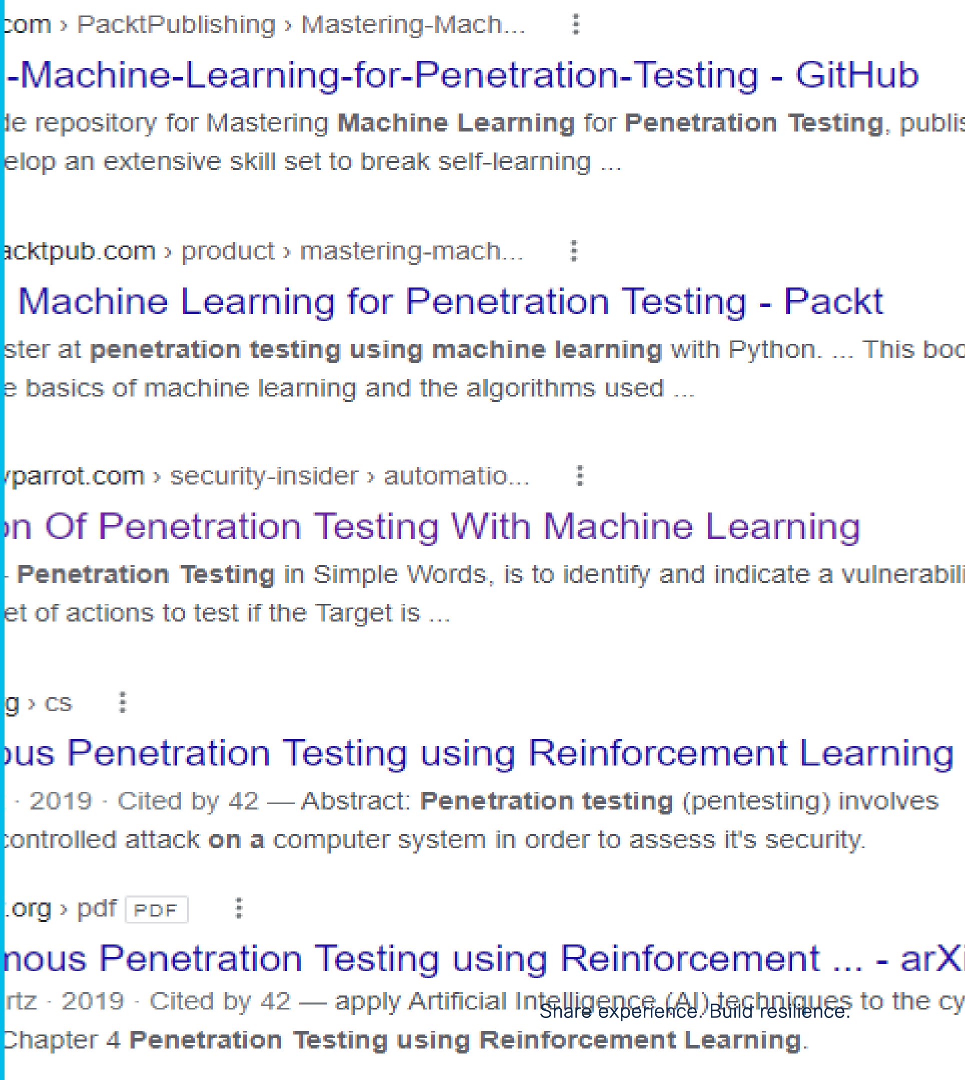


	LØ No Automation	L1 Driver Assistance	L2 Partial Automation	L3 Conditional Automation	L4 High Automation	L5 Full Automation
DRIVER	In charge of all the driving	Must do all the driving, but with some basic help in some situations	Must stay fully alert even when vehicle assumes some basic driving tasks	Must be always ready to take over within a specified period of time when the self-driving systems are unable to continue	Can be a passenger who, with notice, can take over driving when the self-driving systems are unable to continue	No human driver required–steering wheel optional–everyone can be a passenger in an L5 vehicle
VEHICLE	Responds only to inputs from the driver, but can provide warnings about the environment	Can provide basic help, such as automatic emergency braking or lane keep support	Can automatically steer, accelerate, and brake in limited situations	Can take full control over steering, acceleration, and braking under certain conditions	Can assume all driving tasks under nearly all conditions without any driver attention	In charge of all the driving and can operate in all environments without need for human intervention

Tesla AI hickup.

Share experience. Build resilience.

Machine Learning assisted Penetration testing is becoming a thing.



:om › PacktPublishing › Mastering-Mach...

-Machine-Learning-for-Penetration-Testing - GitHub

de repository for Mastering **Machine Learning** for **Penetration Testing**, publis

elop an extensive skill set to break self-learning ...

acktpub.com › product › mastering-mach...

Machine Learning for Penetration Testing - Packt

ster at **penetration testing using machine learning** with Python. ... This boo

e basics of machine learning and the algorithms used ...

'parrot.com › security-insider › automatio...

on Of Penetration Testing With Machine Learning

- **Penetration Testing** in Simple Words, is to identify and indicate a vulnerabili

et of actions to test if the Target is ...

g › cs

ous Penetration Testing using Reinforcement Learning

· 2019 · Cited by 42 — Abstract: **Penetration testing** (pentesting) involves

controlled attack **on a** computer system in order to assess it's security.

.org › pdf PDF

nous Penetration Testing using Reinforcement ... - arX

rtz · 2019 · Cited by 42 — apply Artificial Intelligence (AI) techniques to the cy

Chapter 4 **Penetration Testing using Reinforcement Learning**.

But what if our adversaries are starting to *adopt* these techniques as well?

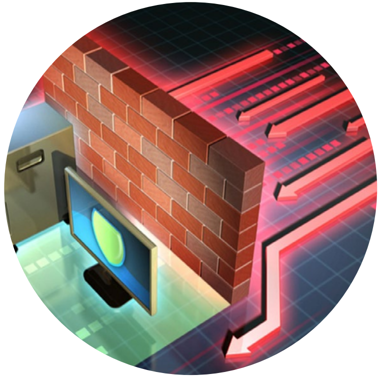
Therefore, the question is:

What can you do to protect an IT/OT environment against an Artificial Intelligence attack bot?

Let's talk about the *attack surface*.

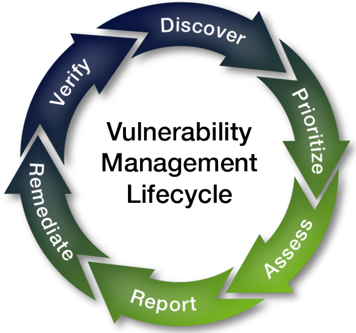
Share experience. Build resilience.

Some of the measurements you should implement to reduce the attack surface.



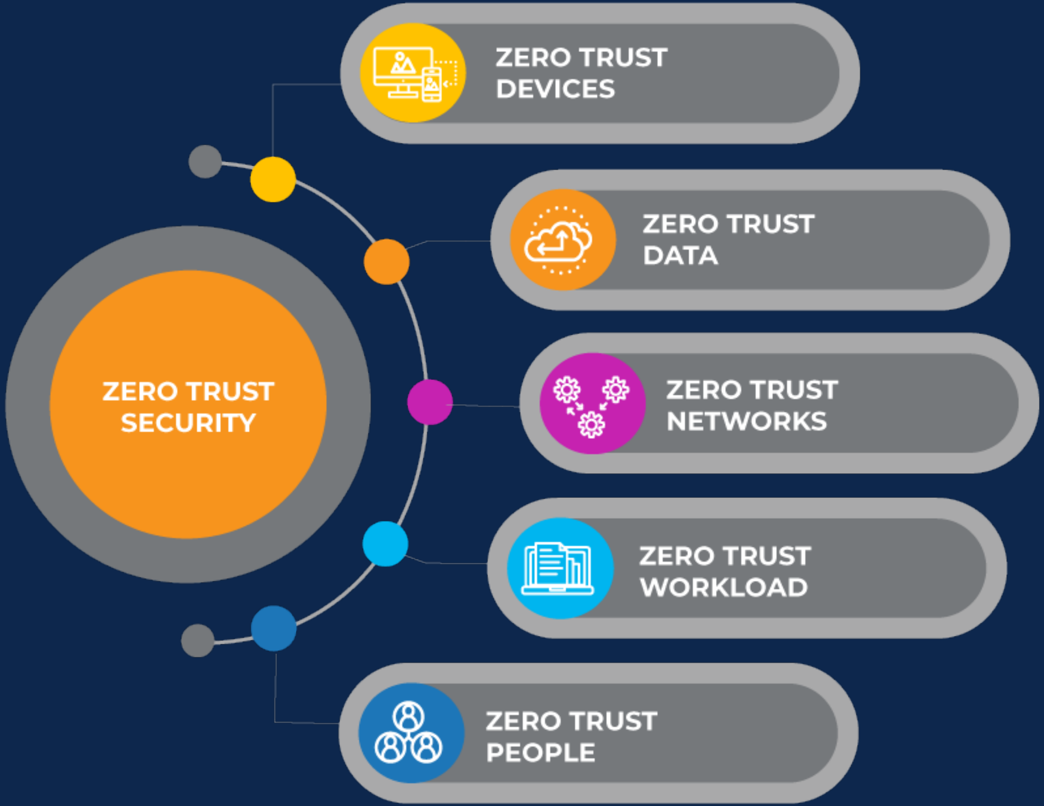
Implement Host-based firewall

Implement In- *and* outbound firewall rules



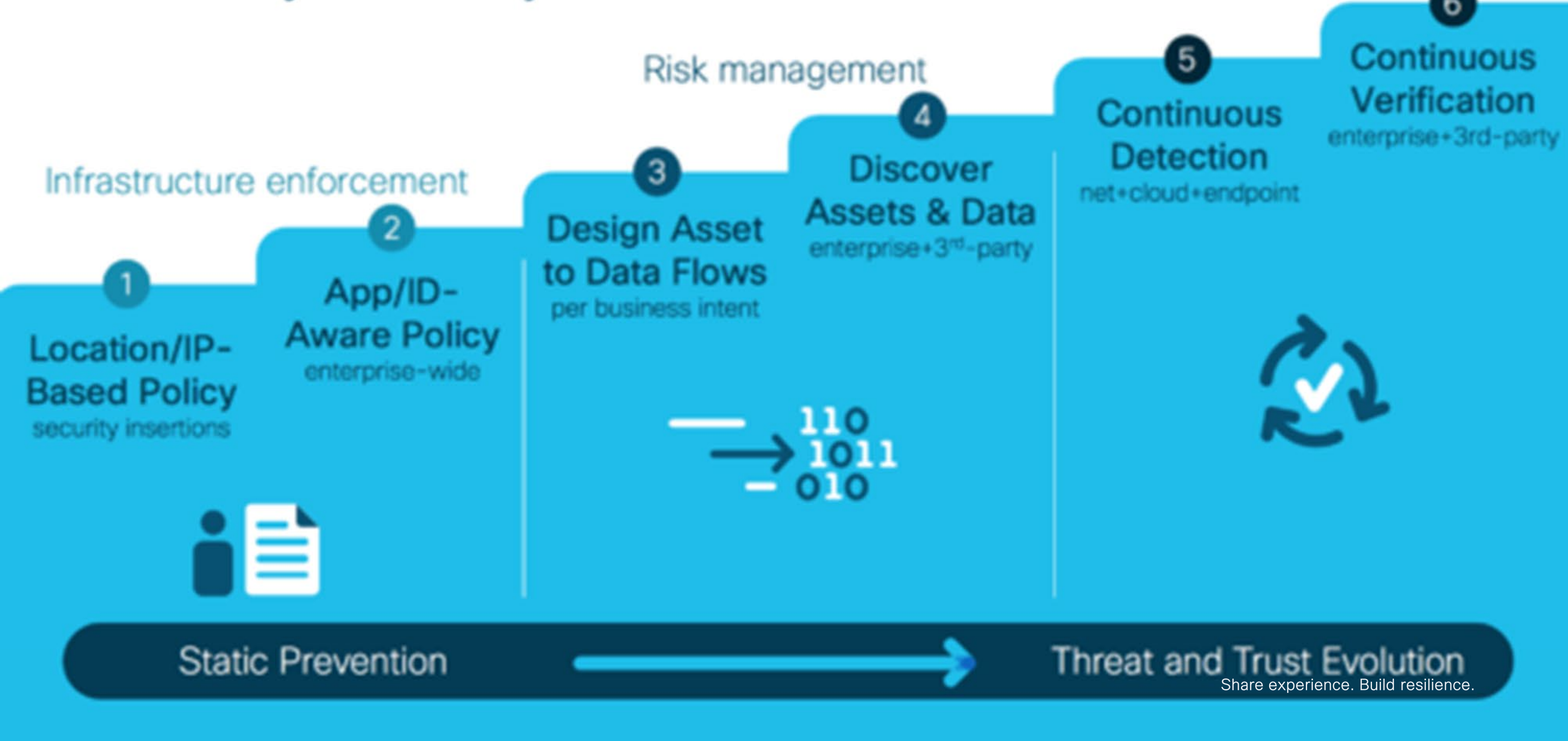
Vulnerability management program

Let’s talk about *architecture.*



Share experience. Build resilience.

Security Maturity Model



Dynamic context

Risk management

Infrastructure enforcement

1 Location/IP-Based Policy
security insertions

2 App/ID-Aware Policy
enterprise-wide

3 Design Asset to Data Flows
per business intent

4 Discover Assets & Data
enterprise+3rd-party

5 Continuous Detection
net+cloud+endpoint

6 Continuous Verification
enterprise+3rd-party

Static Prevention → Threat and Trust Evolution

Response should be the
key element in your defensive strategy.

Share experience. Build resilience.

Cyber Threat INTELLIGENCE

Share experience. Build resilience.

Cyber Threat Hunting

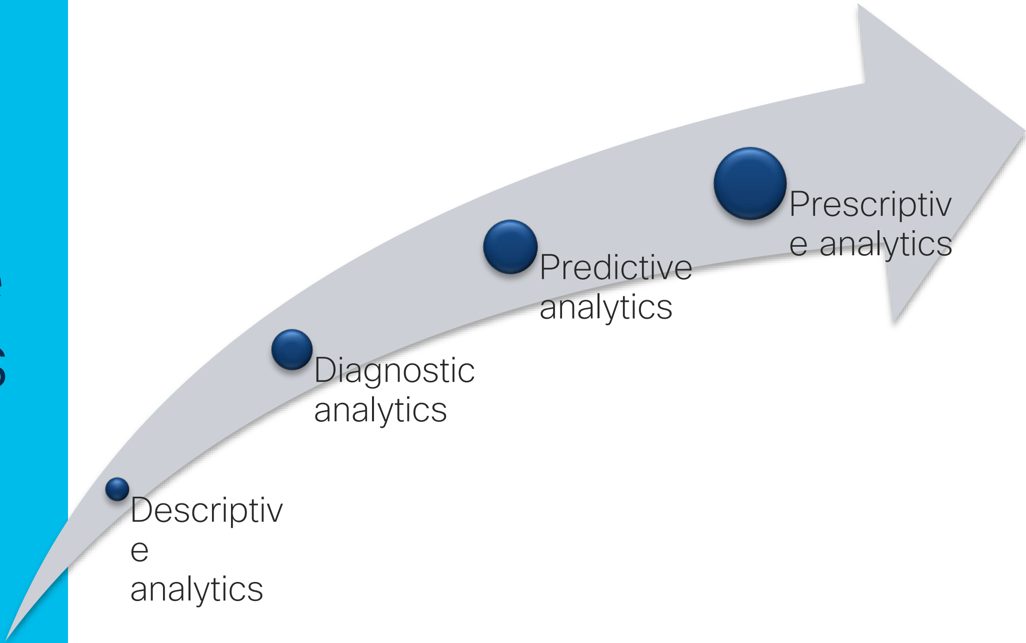
Share experience. Build resilience.

Adopt the *smart SOC* concept.

Share experience. Build resilience.

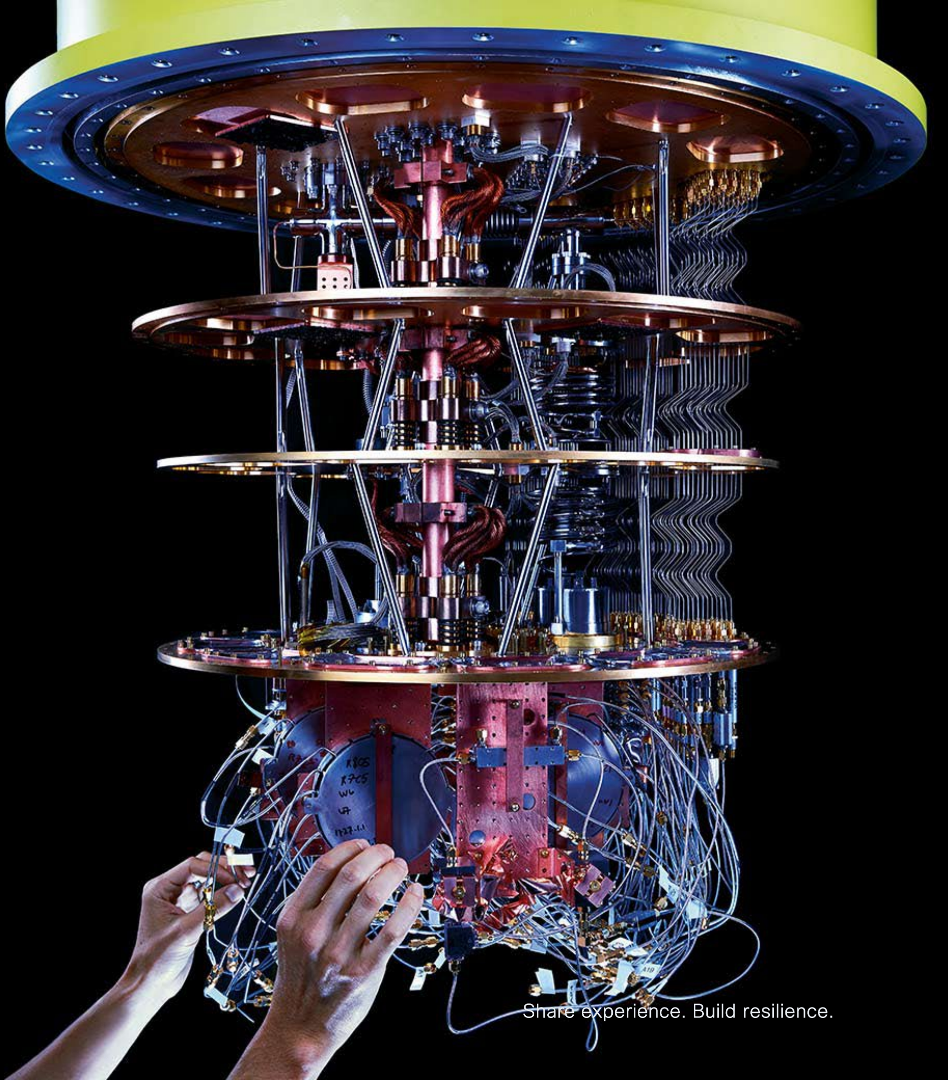
With the adoption of Zero Trust Architecture, you can build an *early warning detection system.*

Evolve from descriptive to prescriptive analytics



Share experience. Build resilience.

There is still *time* left to act. But less then you think.



Share experience. Build resilience.

Ask me anything

Share experience. Build resilience.

SECCON-NL 2022

Share experience. Build resilience

Time					
09:00 - 10:00	Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)				
	Main stage (Zilversmederij 300 seats)	Breakout room 1 (Penningzaal 80 seats)	Breakout room 2 (Depot 80 seats)	Breakout room 3 (Stempelkamer 60 seats)	Breakout room 4 (Schatkamer 30 seats)
10:00 - 10:15	Break - switch to main stream				
10:15 - 10:45	Threat Intell	Threat Intel	Post Quantum Security	Threat Intel	AI
	Threat Intel update from Talos - Martin Lee (Talos Threat intelligence organization)	No More Leaks Project - Felix Nijpels (Dutch Police)	The Impact of Quantum on security - a general outlook - Sam Samuel (Cisco)	Threat managemen at the Dutch Railway - Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)	Get ready for the AI attack bot - Richard de Vries (Tata Steel)
10:45 - 11:00	Break - switch to main stream				
11:00 - 11:30	Detection and Response	SOAR	Post Quantum Security	Detection and Response	Detection and Response / AI
	Day in life at the Dutch Tax Office SOC - Karl Lovink (Belastingdienst)	Stay Ahead of the Game: Automate your Threat Hunting Workflows - Christopher van der Made (Cisco)	Quantum hurdles: an optimistic view of post-quantum security - Sander Dorigo (Fox Crypto)	What Cyber can learn from Biology? - Koen Hokke (KPN)	Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use - Julik Keijer (Northwave)
11:30 - 11:45	Break - switch to main stream				
11:45 - 12:15	Detection and Response	Detection and Response	DevSecOps/ Detection and Response	DevSecOps	
	Compliancy vs security. Pentesting is dead - Edwin van Andel (ZeroCopter)	Incident Response without compromise. How to prepare for the worst day of your career with dice! - Wouter Hindriks (Avit)	Threat Modelling: it's not just for developers - Timothy Wadhwa-Brown (Cisco)	Changed responsibilities in modern software development environments - Martin Knobloch (Microfocus)	How to break a data center? Fred Streefland (Secior)
12:15 - 13:00	LUNCH				
13:00 - 13:45	Panel Discussion with Liesbeth Holterman (host CVNL) Koen Sandbrink (NCSC), Jochem Smit (Northwave), Oscar Koeroo (Min Ezk), Jan Heijdra (Cisco)				
13:45 - 14:00	Break - switch to main stream				
14:00 - 14:30	Threat intel / Detection and Response	Threat Intel	Detection and Response	DevSecOps	
	CERT in Ukraine exeperience sharing by Andrii Bezverkhyi (SOCPrime)	This is why you will fail: Most successful attack scenarios and their defenses - Tijme Gommers (Northwave)	Risk-based Auth & ZTA - Frank Michaud (Cisco)	Creating clarity and unity in security standards and guidelines - OpenCRE.org - Rob van der Veer (Software Improvement Group)	(Placeholder) WICCA Breakout (with Wendy joining)
14:30 - 14:45	Break - switch to main stream				
14:45 - 15:15	Detection and Response	Detection and Response	Detection and Response	Threat Intel	Detection and Response / AI
	Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences - David Warburton (F5)	Security Maturity: from XDR to SIEM - Gilles van Heijst (Orange Cyber Defense)	Improving Business Security by implementing Security.txt - Julius Offers (Digital Trust Center)	Tackling the challenge of translating threat intelligence into actual action - Raymond Bierens (Connect2Trust)	Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy.- Christian van der Woude (Dcypher)
15:15 - 16:00	Closing Keynote - Wendy Nather				