

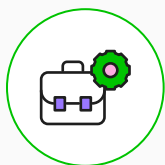
Strengthening Your Cybersecurity and Risk Reduction

A Vulnerability Management Journey

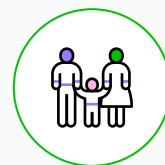
Who Am I

Etienne Kuijkhoven

Director BLUEteam (SOC, CERT and Abuse)



11 years working with KPN, 6 at KPN



Worked with Qualys since 2014



Lives near Amsterdam
in the Netherlands



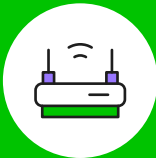
A real family man, a daughter and a son
and recently became grandfather

KPN at a Glance.



12 m Mobile subscribers

- Consumer 4,4 m
- Business 2,2 m
- Wholesale 5,4 m



4.3 m Broadband customers

- Consumer 2,8 m
- Business 389 k
- Wholesale 1,1 m

5,2 mln

KPN Fiber Connections

By the end of **2026**, **80%** households will have access to fiber from KPN.



Since 2011, we've been using **100% green electricity** and we've been **completely climate neutral** since **2015**.

€1,2 bn

Investments Yearly Capex

9.771 fte

Employees



Umlaut

KPN best mobile network 2024



Ecovadis

Platinum CSR rating 2024



SBI

KPN most sustainable telecombrand 2024 (NL)





Complexity of the KPN Organisation and Infrastructure

Siloed business units

- ✓ 1,600 Support groups/ Technical teams

Segmented infrastructure

Different network layers (layer 2, 3, hybrid)

On-Premises and Cloud (Azure and AWS)

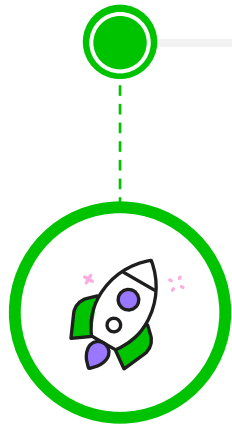
280,000 assets

- ✓ 40,000 servers
- ✓ 240,000 network devices

400,000 IP addresses

2012

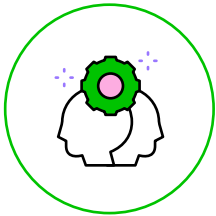
Shit hits the fan!!!!



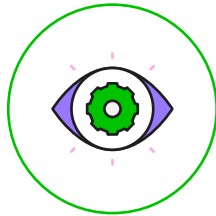
Strengthening Our Cybersecurity and Risk Reduction!!!

The early days

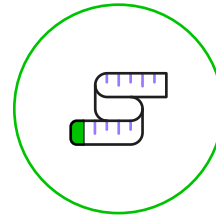
2012



No Vulnerability
Management



No insights



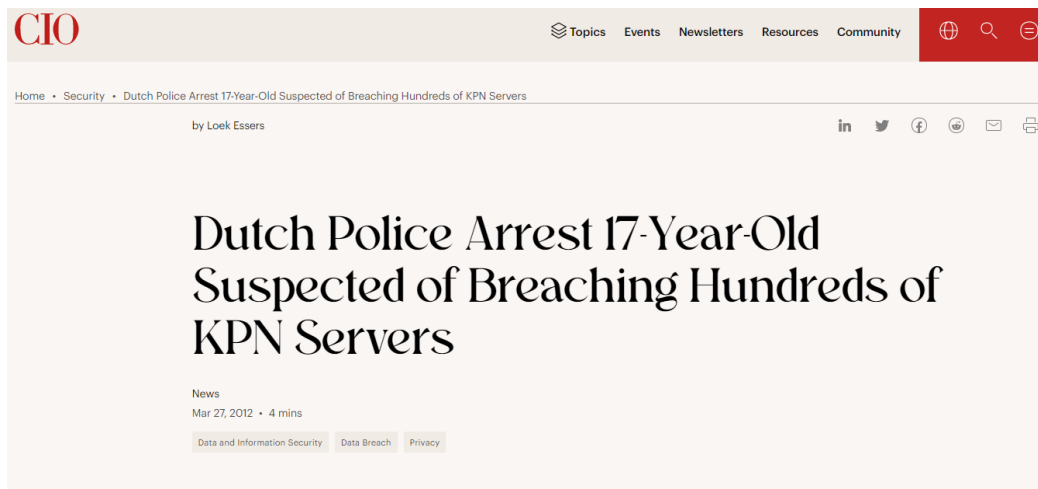
No measurement



No clue
about risks

You Have Been HACKED!!!!





'Zo'n jonge KPN-hacker, daar sta je wel even van te kijken'

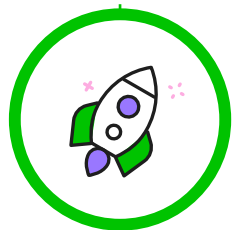
INTERVIEW De Nationale Recherche trekt alle registers open wanneer begin februari blijkt dat KPN wordt bedreigd door een hacker. Het spoor loopt van Rusland via Zuid-Korea naar Australië. Rechercheurs vliegen de hele wereld over. Uiteindelijk vinden ze de verdachte op een bijzondere plek. Een interview met Wilbert Paulissen, hoofd van de Nationale Recherche.

Elsbeth Stoker, Wil Thijssen 7 april 2012, 21:51

THIS IS YOUR WAKE UP CALL

2012

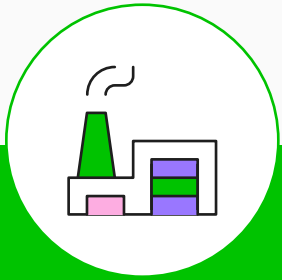
Shit hits the fan!!!!



2013-2015

Scan factory

Vulnerability Management in the Early Days

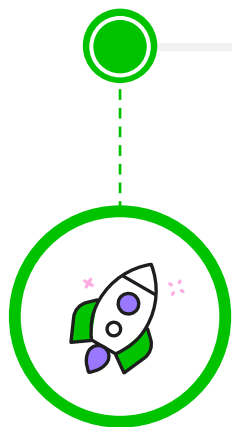


The "Scan Factory"

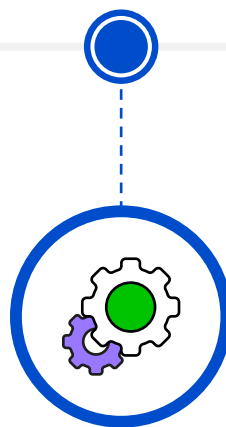


2012

Shit hits the fan!!!!



 **Qualys.**
2015-2020
Qualys Implemented



2013-2015

Scan factory

Qualys Initial Environment



Private Cloud Platform (PCP)



250+ network scanners













4 external scanners



Unauthenticated scanning

QualysGuard scanner implementation options

01	Scanner type	 Virtual	 Physical			
02	Number of scanners	 ≥ 1 scanner per security zone				
03	Connectivity model	 Layer -2 (switched)	 Layer -3 (routed)	 Layer -2/3 (hybrid)		
04	Management network	 DCI (VRF 1910)	 GMN	 IPSB	 TPA	

Done

QualysGuard
Private Cloud Platform

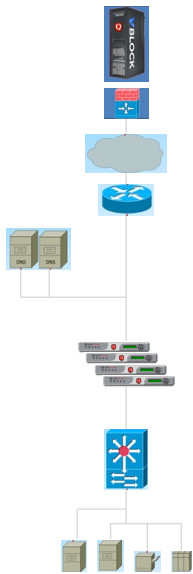
Scanner management network

Domain Name System

Scanner appliances

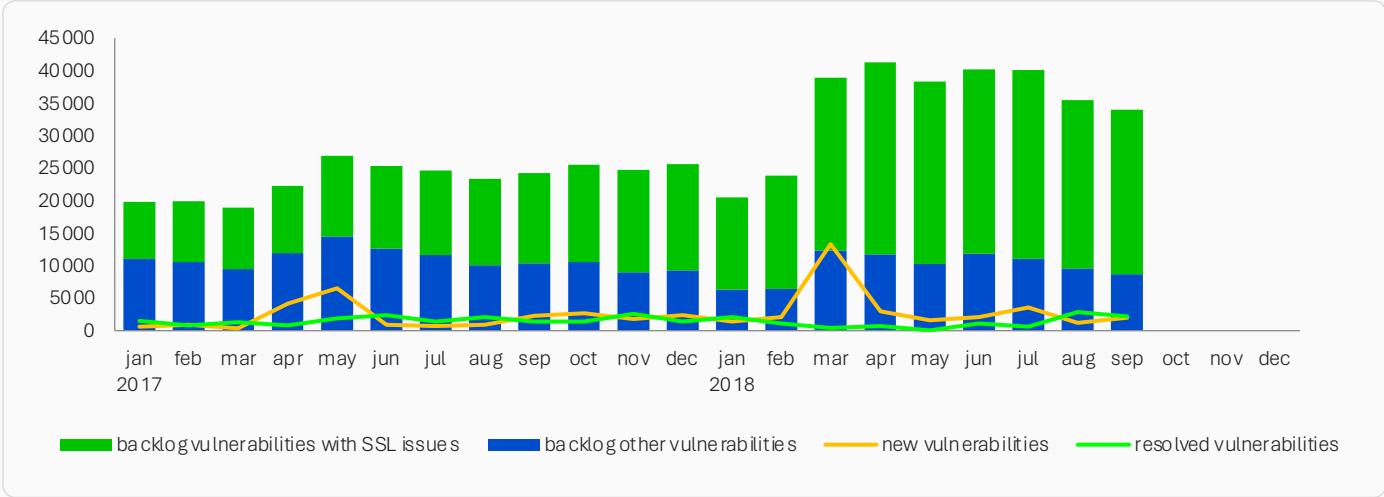
Scanner to-target network
connectivity

Target networks and hosts



TruRisk Insight Using Qualys' Central Environment

- To provide more insight to the technical teams, SRT is evolve to become a VM portal for technical teams
- How are we going to prioritize?
 - Prio table introduction
- Are there unknown assets?
 - CMDB challenge
 - “Ghost” scanning

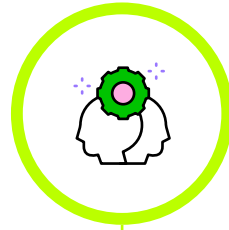


SRT priority	Action →	Mail Spoc's	2 weeks	1 month	2 months	6 months	Best effort
Scanner ↓	Zone ↓	Prio 1	Prio 2	Prio 3	Prio 4	Prio 5	Prio 6
External	Black red	Critical	Hi		Medium		Low
External	Other (illegal)	Critical	Should not happen, report to CERT/SOC, log as P1				
Internal	Black red blue		Critical	Hi	Medium		Low
Internal	Orange			Critical	Hi	Me-lo	Low
Internal	Green				Critical	Hi	Med-Low

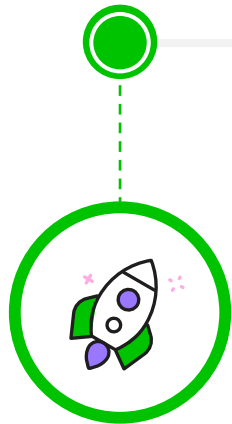
CVSS Scores
Critical 9.0-10
High 7.0-8.9
Medium 4.0-6.9
Low 0.1-3.9
Informational 0.0

2012

Shit hits the fan!!!!

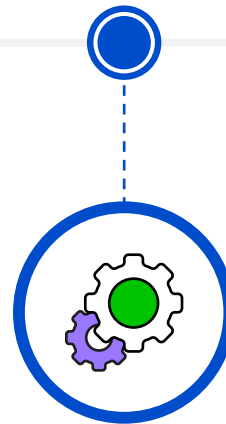


 Qualys.
2015-2020
Qualys Implemented



2013-2015

Scan factory



2021-2024

Evolution of Vulnerability
Management based on
Security Strategy

What Makes a Winning Security Team

The security team is not limited to CISO, it is the entire organization

01

Doing It Together

Opening up CISO to the rest of the organization to define a strategy and what we will do together.

02

Changing The Mindset

Creating a culture of shared responsibility for security and transparency on vulnerabilities.

03

Adding New Skills

Adding new talent to the CISO team with the skills to change the mindset in the organization.

04

Creating A Clear Vision

Having a clearly defined vision and goals that resonate within the organization.

Qualys Environment Evolution



Three environments (On-Premise, Azure and AWS) to manage regarding Vulnerability Management so the SCP is introduced



From Unauthenticated to Authenticated scanning



22.000 agents installed, need to grow to 40.000
(No workstations of employees)

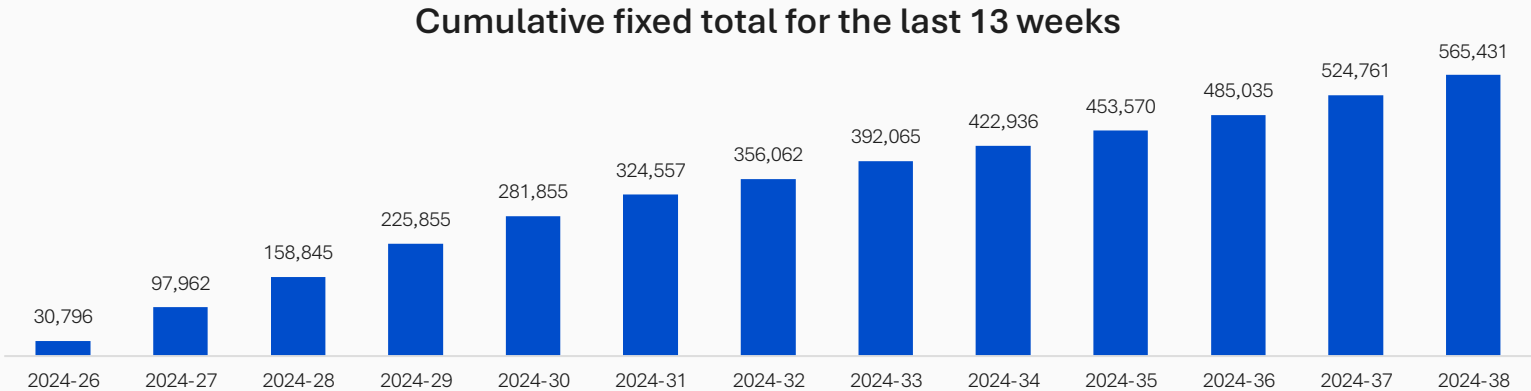
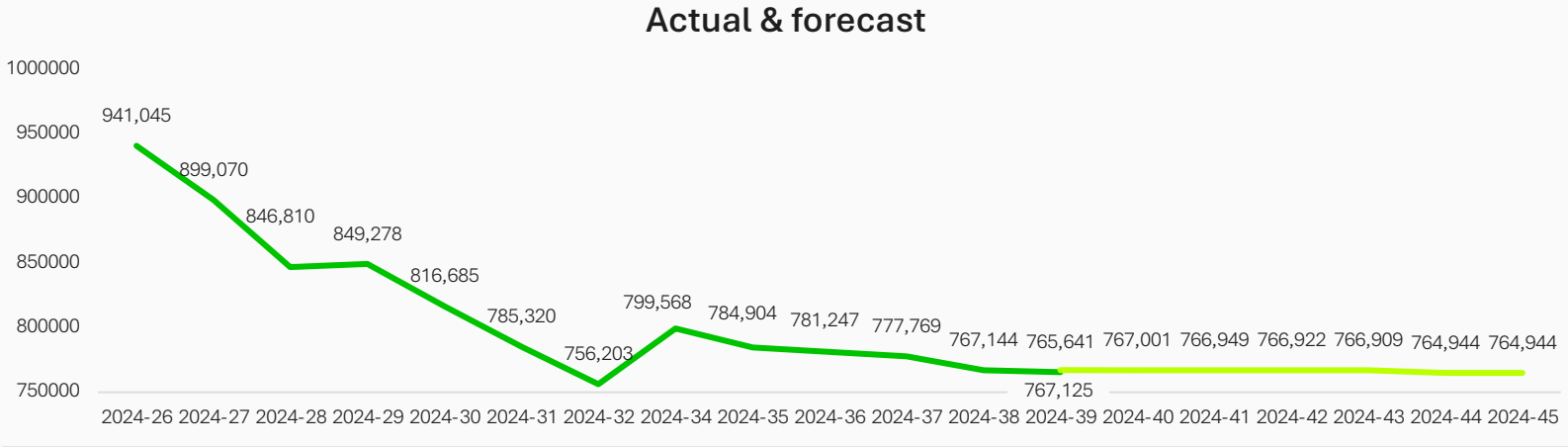
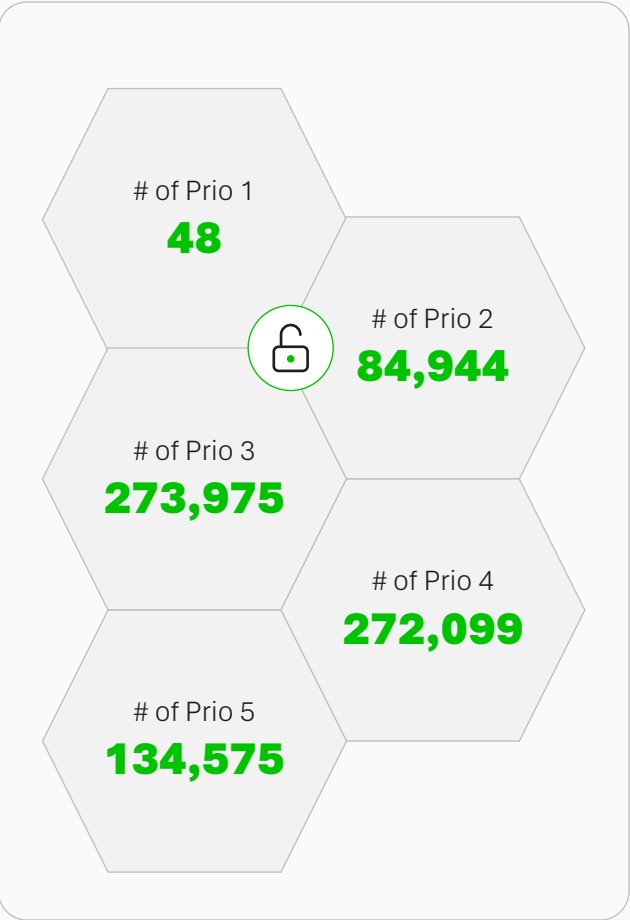


Container sensors



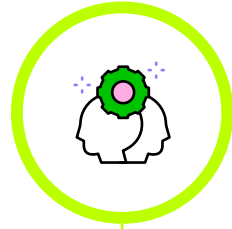
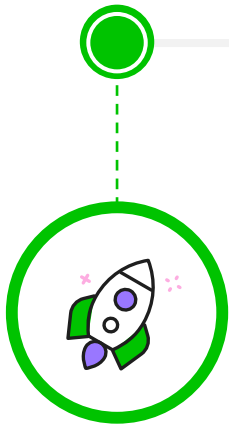
Hardening of assets via Qualys agent, Compliance module

More Reporting and Measurement Possibilities



2012

Shit hits the fan!!!!



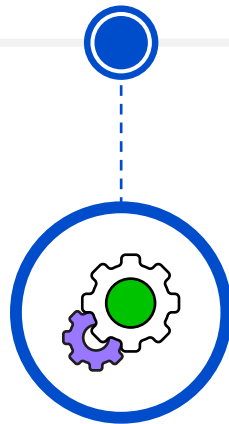
2013-2015

Scan factory



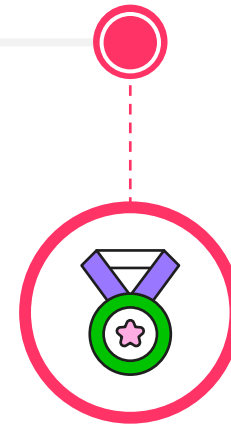
2015-2020

Qualys Implemented



2021-2024

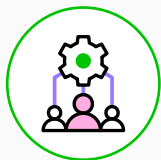
Evolution of Vulnerability
Management based on
Security Strategy



2025-xxxx

Future

Future (Short and Middle Term)



Embed QDS and TruRisk in the Vulnerability Management process



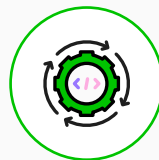
Custom Assessment and Remediation (CAR) for incident Response



Web Application Scanning (WAS) use for pre-scanning assets before submitting to the KPN REDteam



Vault implementation started for authenticated scanning with network scanners



"Automatic" Patch Management

Action →	1 week	2 weeks	1 month	2 months	6 months	Best effort
Scanner ↓	Prio 1	Prio 2	Prio 3	Prio 4	Prio 5	Prio 6
In-/external, all zones	Critical	High	Medium	Low		Info

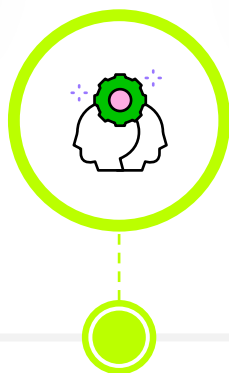
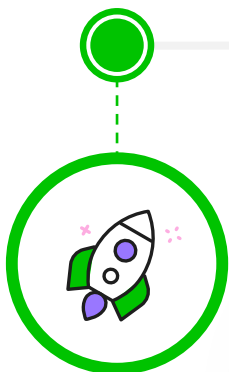
CVSS Scores	QDS Scores
Critical 9.0-10	Critical 90-100
High 7.0-8.9	High 70-89
Medium 4.0-6.9	Medium 40-69
Low 0.1-3.9	Low 0-39
Informational 0.0	Informational 0.0

No scanners

No MTTD
No MTTR

2012

Shit hits the fan!!!!



2013-2015

Scan factory

Manual scanning

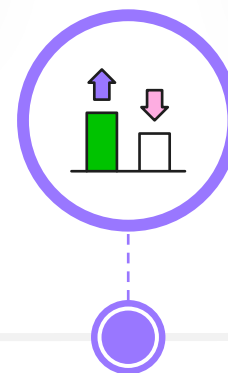
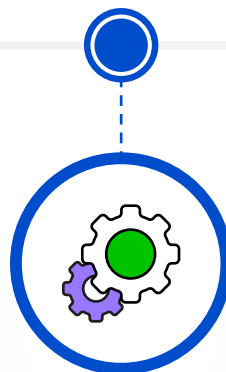
MTTD = Months
MTTR = Years

Network scanners

MTTD = 1 Month – 1 week
MTTR = 1 Year

2015 - 2020

Qualys Implemented



2021

Network scanners, Qualys agents, Container sensors

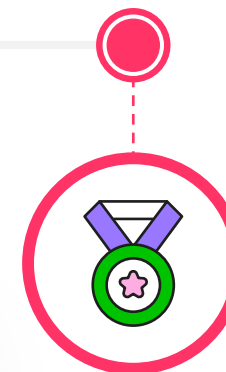
MTTD = 4 hours
MTTR become in control

Network scanners, Qualys agents, Container sensors, Passive scanners

MTTD = 4 hours
MTTR is in control

2025-xxxx

Future





Together, within the organization and with Qualys, from numbers to real TruRisk and remediation on time!!!!

