NIS2 in practice
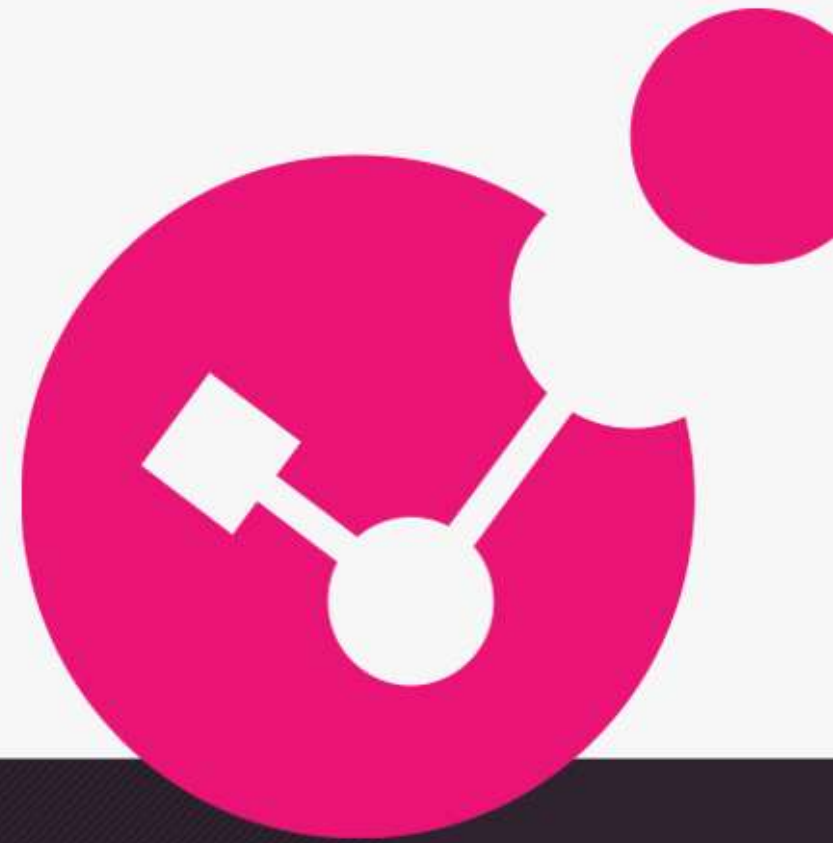## An overview

ITSA 2023

Marco Eggerling, LL.M | Chief Information Security Officer EMEA

October 2023

YOU DESERVE THE BEST SECURITY

October 18th 2024
NIS2 will come into full force

<u>Enforced</u> collaboration among Member States

Establishment of a regulatory <u>controls</u> framework

<u>Mandatory</u> reporting mechanism towards ENISA

CHECK POINT

The Mechanics

EU Security Network

- Improve cross-border cooperation and create national CSIRTS
- Requirement for National Competent Authorities (NCAs)
- Assign single point of contact (SPOC) for cyber security monitoring

Incident Reporting

Applicable organizations must implement a range of risk management measures both technical and operational and must comply with timely NIS2 incident reporting protocol

Penalty
$10m or 2% ATO

Cooperation Groups

- Facilitate collaboration around cybersecurity w/ ENISA
- Focus on planning, steering, and reposting on NIS implementation
- CSIRTS <-> SPOCs report every 18 months at minimum

Member State Strategy

Required to implement a national cybersecurity strategy and framework defining security goals, risk matrix, establish 1+ NCA for monitoring and enforce collaboration among SPOCs

CHECK POINT

In-scope risk vectors

A CISOs point of view

NIS2 elevates the role of CISOs

Interlock of CISO and DPO intensifies

Enforces compliance with updated security and incident notification obligations

Brings Business and IT closer together

Need to adapt our security strategies and practices to align with the NIS2 regulations

Strengthens bonding with national security agencies

Maintain close interlock and exchange with NCA(s) across company's geography

Automatically increases GDPR compliance

Ensure proper incident reporting within the mandated 72-hour timeframe

CHECK POINT

"Appropriate and proportionate technical, operational and organizational measures[...]"

Art. 21, Cybersecurity risk-management measures

How do you meet the requirements?

NIS2 emphasizes:

- Focus on improving overall security posture
- European and international standards
- Level of security systems appropriate to the risks posed

More specific guidelines will be released as we approach actual date of enforcement

"By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%"
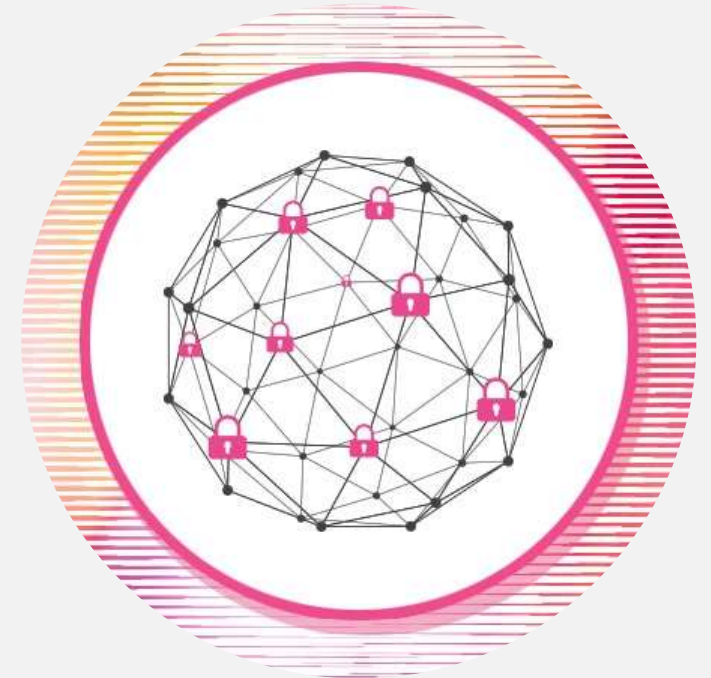
- Gartner

Cybersecurity Mesh Architecture
i.e. CSMA et al.

Few combined platform offerings will significantly improve security programs

- **Reduce** unnecessary **complexity** by choosing interconnected controls

- **Avoid point solutions,** as piece-meal leads to best-of-breed mess

- Prefer **prevention-first** over monitor-first approaches

- Focus on **interoperability** for investment protection reasons

Important: InfoSec is a trust game, so choose your partners wisely.
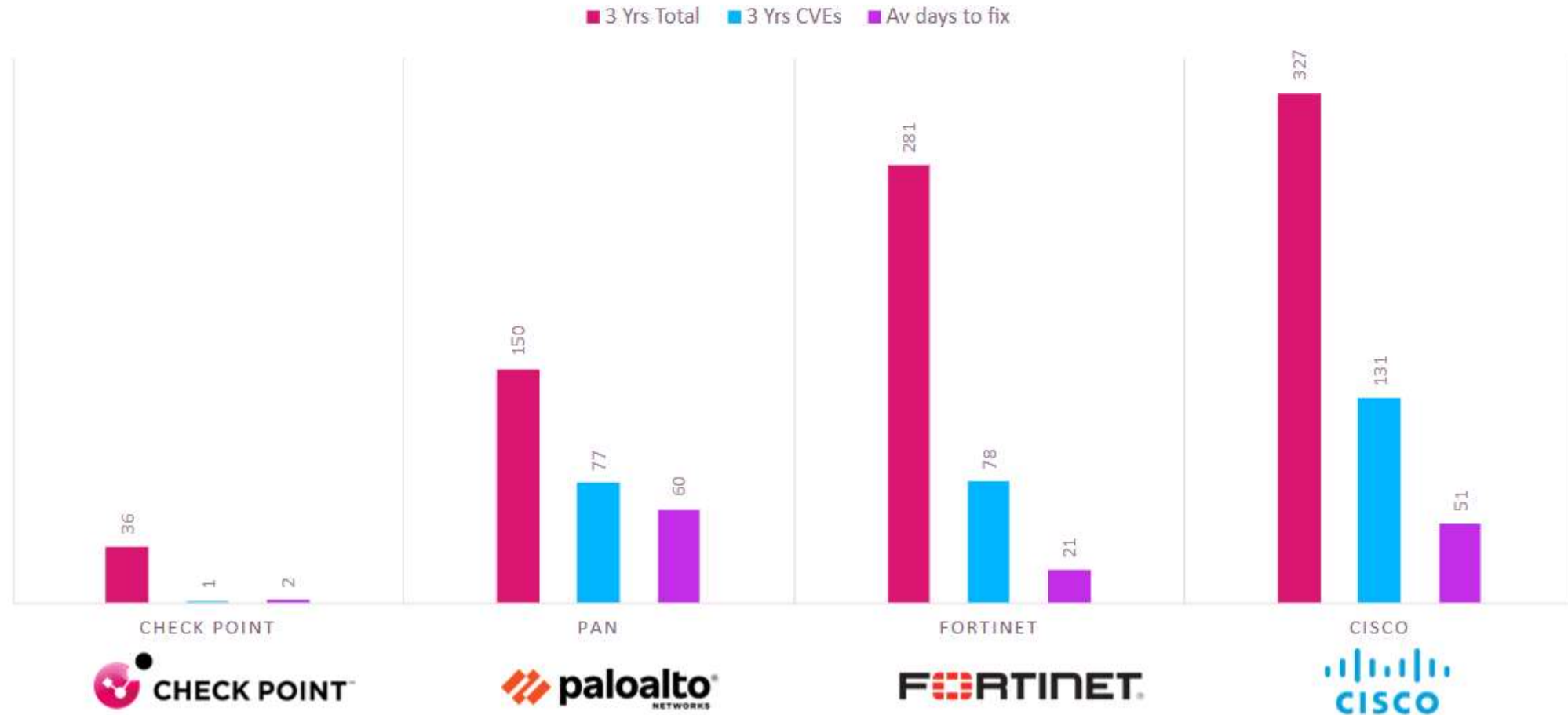
Trust is a life vest
Would you trust one with lots of holes?

CRITICAL VULNERABILTIES AND DAYS TO FIX

■ 3 Yrs Total   ■ 3 Yrs CVEs   ■ Av days to fix

Check Point: The LEADING Global Cyber Security Company

GLOBAL LEADER
100,000+ CUSTOMERS,
88+ COUNTRIES, 6,200+ PARTNERS

CUTTING-EDGE TECHNOLOGIES
OVER 30 YEARS OF EXPERTISE,
INDUSTRY'S MOST VISIONARY PLAYER

INNOVATION LEADERSHIP
HIGHEST NUMBER OF AI REAL-TIME
PREVENTION TECHNIQUES

6,000+
EMPLOYEES WORLDWIDE,
TOP TALENT

TRADED ON NASDAQ
1996 I CHKP

WORLD'S BEST EMPLOYER
BY FORBES,
#1 CYBER SECURITY VENDOR

TRUSTED BY

FORTUNE 500 COMPANIES
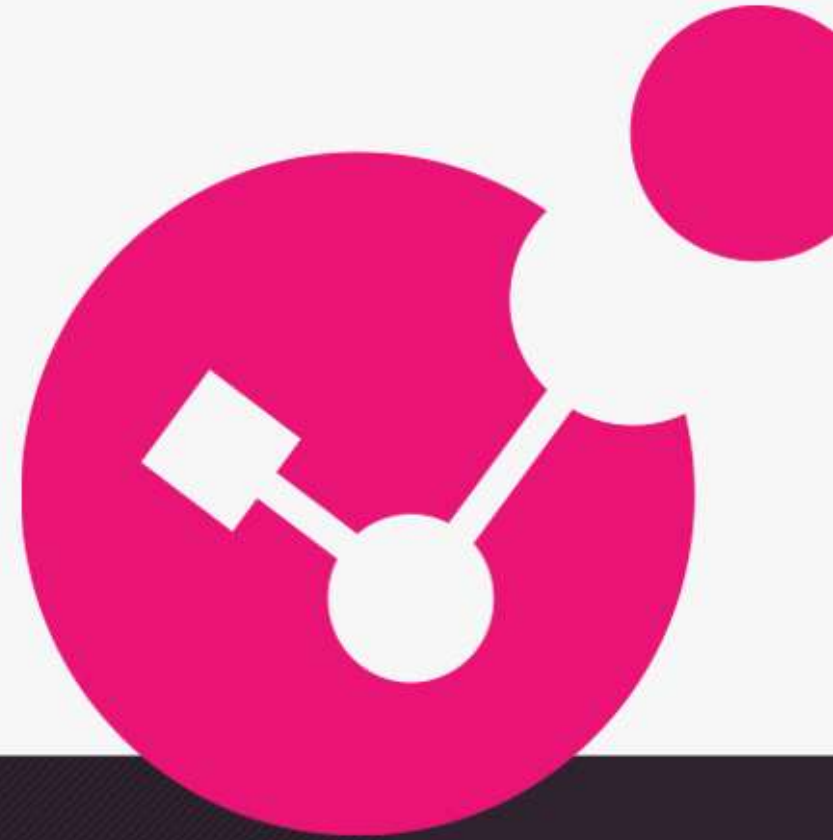
CONCLUSION

- Familiarize with NIS2 requirements and understand implications on your business

- Review CSMA suggestions to improve your security program

- Put your trust in those who deserve it

- Focus on prevention-first protection

- Get in touch with my colleagues for a deeper technical dialogue: Booth 322, Hall 6

Feel free to reach out, and thanks for your interest.

marco.eggerling@checkpoint.com

linkedin.com/in/eggerling