



176*

* 124



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Implementing NIS2 as a national and sectoral CSIRT

Bouke van Laethem

3RD Conference – 2024-04-24

NCSC



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

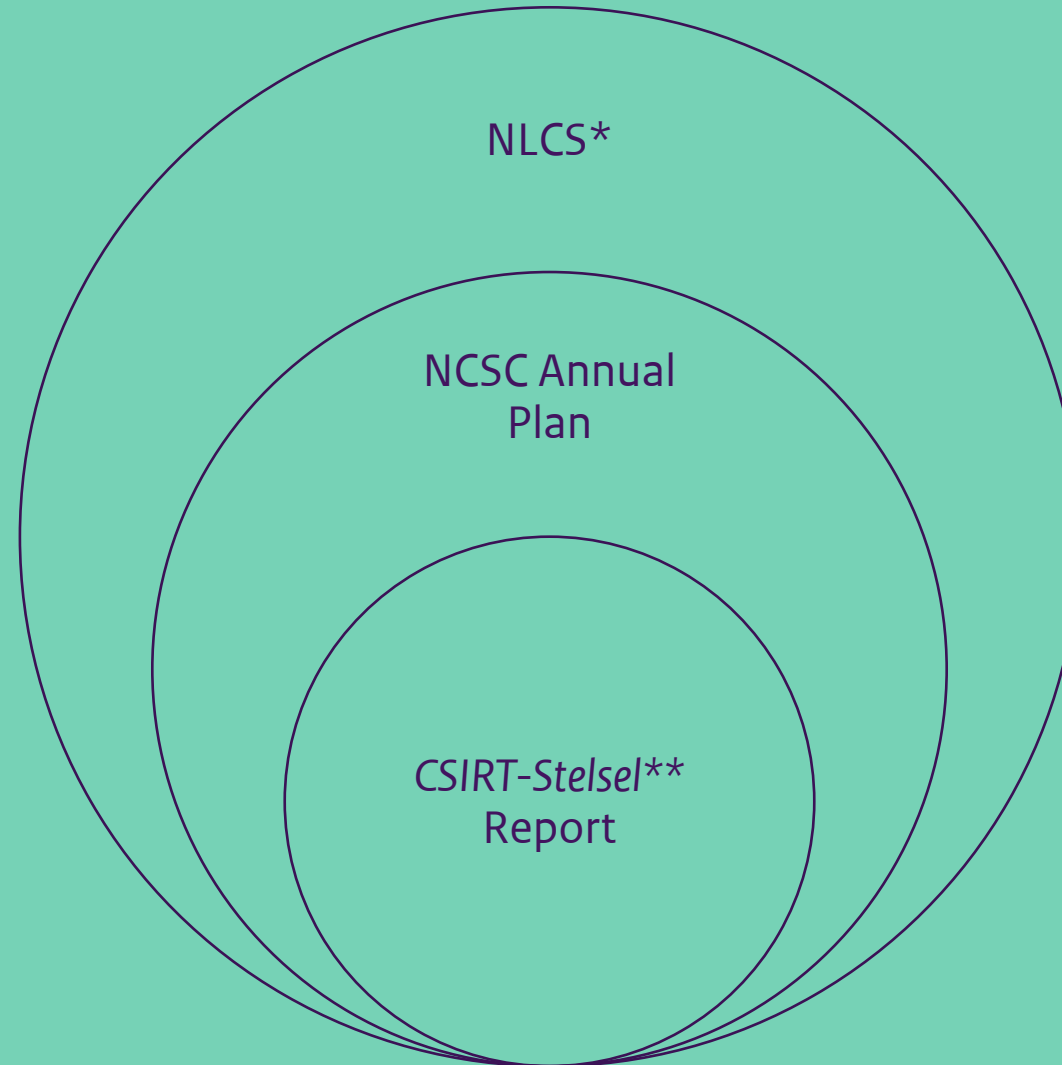
Bouke van Laethem

*Senior Projectlead National and Sectoral
CSIRT – NCSC-NL*

"Turning incidents into actionable intelligence"



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid



* Dutch Cybersecurity Strategy 2022-2028

** CSIRT System



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

National | Sectoral

The Dutch way of doing CSIRT(s)



Sectoral CSIRT*

National CSIRT

Monitoring

Analysis

Notifications

Incident Management

Coordination

11.3.a

CSIRTs: **SHALL** monitor and analyse, and assist entities with monitoring

11.3.e

CSIRTs: **SHALL** provide proactive vulnerability scanning on request of entities

11.3.add.1

CSIRTs: **MAY** carry out proactive scanning of publicly accessible entities' systems

11.3.a

CSIRTs: **SHALL** monitor and analyse, and assist entities with monitoring

11.3.d

CSIRTs: **SHALL** collect data and provide dynamic analysis and situational intel

11.3.b

CSIRTs: **SHALL** provide warnings and alerts to entities, authorities, etc.

11.3.c

CSIRTs: **SHALL** respond to incidents and provide assistance to entities

11.3.d

CSIRTs: **SHALL** collect data and provide dynamic analysis and situational intel

11.3.f

CSIRTs: **SHALL** participate in CSIRTs network and provide assistance

11.3.g

CSIRT: **SHALL** coordinate vulnerability disclosure (CVD) under Article 12.1

(SPOC)

11.3.h

CSIRTs: **SHALL** contribute to deployment secure information-sharing tools

11.4

CSIRTs: **SHALL** cooperate with private sector

11.5.a

CSIRTs: **SHALL** promote common incident-handling practices, schemes and taxonomies

11.5.b

CSIRTs: **SHALL** promote common crisis management practices, schemes and taxonomies

11.5.c

CSIRTs: **SHALL** promote common CVD practices, schemes and taxonomies



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

n/sCSIRT Mission

- **Intelligence Driven Incident Management**
- **Impose Cost and Increase Resilience**
- **Stimulate and Support Self-Reliance**



Mission areas

Actively and effectively contribute to cyber resilience of (inter)national entities through “*Digital First, Human led, Entity Centric, Tech Enabled, CTI Driven*” CSIRT services:

- **Analysis (CTI, situational awareness, etc.)**
- **Monitoring (including detection)**
- **Threat, incident and vulnerability notification**
- **Incident response and coordination, operational coordination**
- **Collaboration and cooperation**

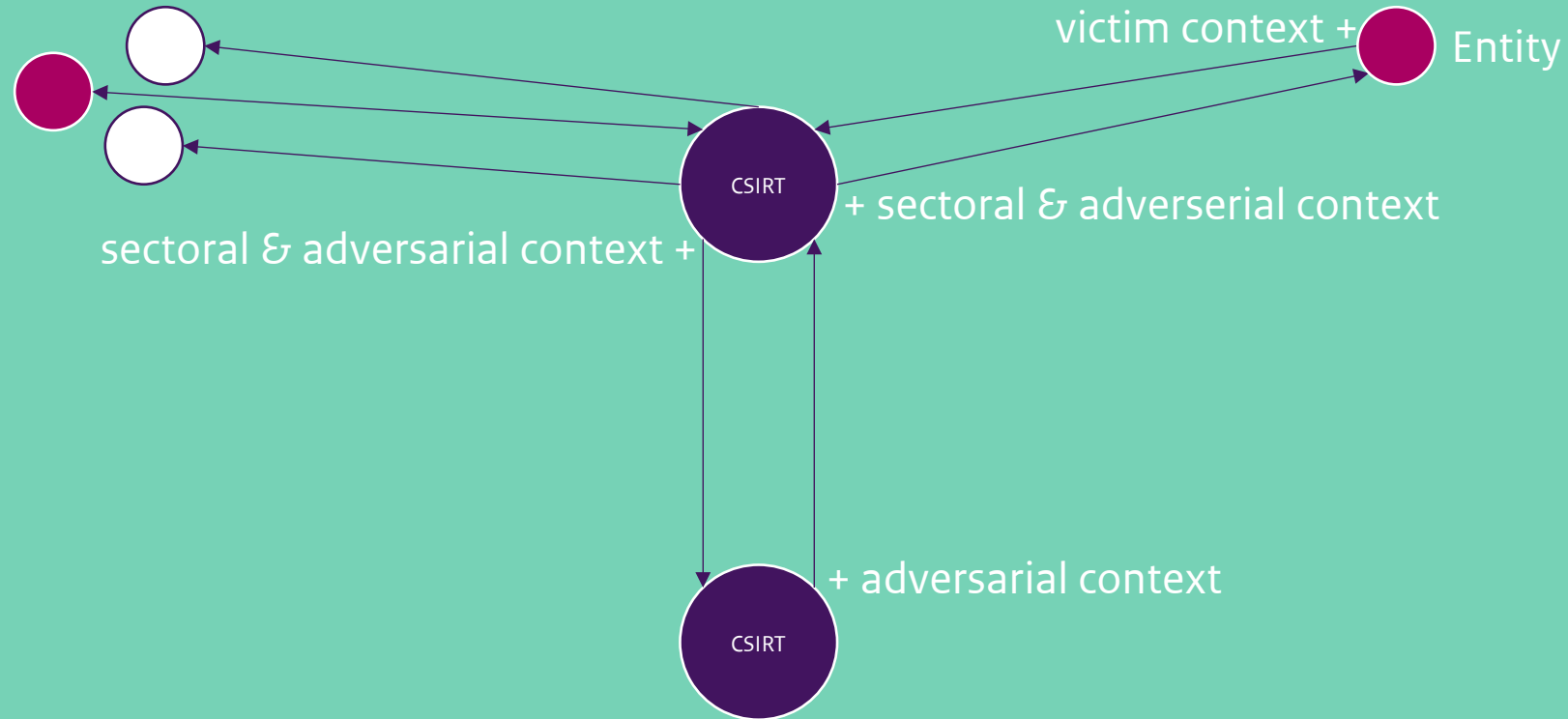


Principles

- **Proactive role in collaboration**
- **Co-creation and sharing of Data, Information, Knowledge and Expertise**
- **Leading by example (expertise & best practices)**
- **Manage, operate and share resources**
- **Measurable impact & results**



Enrich, Support and Share





Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Sectoral CSIRTs in action

A scenario



Company: DuckSends
Sector: Financial
CISO: Nessie Woo



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

