Yet another story on information sharing...

- NATO Malware Information Sharing Platform
- Panel discussion Threat information sharing: Strategies and threat Scenario’s
- George Mason University Barriers and pathways to improving effectiveness of cybersecurity Information Sharing Among Public and Private Sectors
- ...
Case study on improving shared situational awareness by focusing on community building

✓ Situational Awareness as is
✓ Why we saw cause for action
✓ The NDN initiative
✓ Steps in community building
National Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Expertise & Advice
Monitoring & Response
Insight
Perspective for Action
Enhancing Crisis management

Police
AIVD
NFI
Regulators
ISP’s
Academia
Defence
NCC
ISAC’s
Vendors
National partners
Critical Infrastructure
**NCSC-NL situational awareness**

<table>
<thead>
<tr>
<th>Tactical</th>
<th>Operational</th>
<th>Daily</th>
<th>Yearly</th>
</tr>
</thead>
</table>
| • News analysis  
  • *Daily weather report* | • Advisories | | |
| • Tactical analysis  
  • Monthly monitor  
  • Guidelines  
  • Factsheets  
  • White papers  
  • Media analysis  
  • Policy briefings | • Malware analysis  
  • End of week  
  • Ad hoc  
  • *Observables and context* | | |
| • One conference  
  • Trend report  
  • End of year | • One conference | | |
2012 Dorifel

August 8th
• We receive first calls
• Requests for advice
• Municipality of Weert
• Malware sample
• Indicators sharing
• Actionability
2012 Dorifel

August 9th
• New reported infections
• Notice and Takedowns
• ‘Release me of a botnet’

August 10th
• Total of 30 public and private organizations
• Scaled down
• Clean up still ongoing
2012 Dorifel Evaluation

Shortcomings

• No early warning
• No access to the networks
• No use of standards
• No feedback on indicators
• No community driven approach
• And thus ...no actual shared situational awareness
2015: National Detection Network
NDN offers

1. An IDS for government organisations
2. Threat intel data not (yet) widely available
3. Targeted at NL, high impact, high likelihood
4. Platform for private sectors in critical infrastructure
5. Use of standards and open source
6. Based on voluntary sharing with NCSC-NL
7. Available to all of our constituency
10 Steps in community building

1. Legal and policy assurances
2. Explore the territory
3. Communication
4. Start the collaboration
5. Decision making
6. Business Case
7. Controls
8. Results
9. Information Process
10. Evaluate and adjust
Steps in community building

1. Legal and policy assurances
2. Explore the territory
3. Communication
4. Start the collaboration
5. Decision making
6. Business Case
7. Controls
8. Results
9. Information Process
10. Evaluate and adjust
Step 1. Policy and legal

1. Embed activities in NCSS
2. Create political commitment
3. Organise broad support
4. Inform employee council
5. New policies will be developed
6. Check your legal base

www.overheid.nl
Step 2. Exploring the territory

- Information
- Trust level
- Volume
- Sharing model
- Benefit
- Authority
- Exchange base
- Size
- Length
- Connectedness
- Diversity
- ...

<table>
<thead>
<tr>
<th>Step 2. Exploring the territory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>information</strong></td>
</tr>
<tr>
<td><strong>trust level</strong></td>
</tr>
<tr>
<td><strong>volume</strong></td>
</tr>
<tr>
<td><strong>sharing model</strong></td>
</tr>
<tr>
<td><strong>benefit</strong></td>
</tr>
<tr>
<td><strong>authority</strong></td>
</tr>
<tr>
<td><strong>exchange base</strong></td>
</tr>
<tr>
<td><strong>size</strong></td>
</tr>
<tr>
<td><strong>length</strong></td>
</tr>
<tr>
<td><strong>connectedness</strong></td>
</tr>
<tr>
<td><strong>diversity</strong></td>
</tr>
</tbody>
</table>
Step 3. Communications

Doelgroep omgeving

Deskundigen

Belanghebbenden

Vitale Sectoren

Overheid

NDN - NCSC

National Police

CIP

SSC-ICT

Rijks SOC

ISP

Nuclear ISAC

Multi-nationals ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

doelgroep omgeving

Deskundigen

Belanghebbenden

Vitale Sectoren

Overheid

NDN - NCSC

National Police

CIP

SSC-ICT

Rijks SOC

ISP

Nuclear ISAC

Multi-nationals ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer

RIJKS ISAC

VNO/NCW

Privacy related

Liaisons

EU-Fin. ISAC

Energie ISAC

MSP ISAC

Zorg ISAC

Computer
Steps in community building

1. Legal and policy assurances
2. Explore the territory
3. Communication
4. Start the collaboration
5. Decision making
6. Business Case
7. Controls
8. Results
9. Information Process
10. Evaluate and adjust

Prior
Start
Obstacle
Loop
Step 4. Collaboration process

- Invite
- First insight
- Share and reflect
- Negotiate
- Scoping
- Execute
- Evaluate

- Individual interests and ambitions
- Understand consequences
- Pace and direction
- Master plan
- Results, products
- Exits, new entries

Leren samenwerken tussen organisaties, alianties netwerken ketens partnerships, Kaats, Pheij, 2013
<table>
<thead>
<tr>
<th>Stages</th>
<th>Period</th>
<th>Activities</th>
</tr>
</thead>
</table>
| 1 Invite        | May-Nov ’13  | - Representative organizations  
|                 |              | - Delegates                                                                 |
| 2 First insight | Dec ’13      | - Round table sessions  
|                 |              | - Introductions  
|                 |              | - Proposition: benefits, challenges                                         |
| 3 Share and reflect | Feb ’14    | - Interests made explicit  
|                 |              | - Implicit a group was made                                                 |
| 4 Negotiate     | Mar, Jun ’14 | - Agenda  
|                 |              | - Roles, responsibilities                                                   |
| 5 Scoping       | Jun-Nov ’14  | - Process, organization, information, infrastructure, legal, policy, communication |
| 6 Execute       | Dec ’14      | - Start pilot: infrastructure, sharing                                       |
| 7 Evaluate      | Jun-Sep ’15  | - Roadmap, growth scenario, sharing                                        |
Step 5. Decision making

**Stakeholders**
- 150 corporate organizations
- 20 public organizations
- 3 founding partners
- ? Managed service providers

**Structure**
- 1 steering group, 2-monthly
- Senior management
- Sounding board
- Round table

**Topics**
- Project and pilots
- Policy, legal and politics
- Finance and resources
- Communication

**Results**
- Consensus
- Political support
- Stakeholder collaboration
- Autonomy untouched
- Missing: MSSP, researchers, interest groups, ...

www.rcc.int
Steps in community building

1. Legal and policy assurances
2. Explore the territory
3. Communication
4. Start the collaboration
5. Decision making
6. Business Case
7. Controls
8. Results
9. Information Process
10. Evaluate and adjust
Step 6. Costs and benefits

<table>
<thead>
<tr>
<th>Short term</th>
<th>Long term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs</td>
<td>Benefits</td>
</tr>
</tbody>
</table>
## Step 6. Costs and benefits

<table>
<thead>
<tr>
<th>Short term Costs</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Reputation through Corporate Soc Resp</td>
<td>- Higher security level</td>
</tr>
<tr>
<td>- Compliancy</td>
<td>- Efficient processes</td>
</tr>
<tr>
<td>- Collaboration</td>
<td>- NL digitally (more) safe</td>
</tr>
</tbody>
</table>

**Long term Benefits**
Step 6. Costs and benefits

<table>
<thead>
<tr>
<th>Short term</th>
<th>Long term</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Labour (legal, policy, techs, ..)</td>
<td>- Infrastructure / maturity.</td>
</tr>
<tr>
<td>- Tooling (IDS, MISP, SIEM)</td>
<td>- IDS appliance</td>
</tr>
<tr>
<td>- Service management</td>
<td>- Commercial feeds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Higher security level</td>
</tr>
<tr>
<td>- Efficient processes</td>
</tr>
<tr>
<td>- NL digitally (more) safe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Reputation through Corporate Soc Resp</td>
</tr>
<tr>
<td>- Compliancy</td>
</tr>
<tr>
<td>- Collaboration</td>
</tr>
</tbody>
</table>
Step 7. Information controls

Privacy controls (public IDS)
  • Raw data only locally
  • No IoC’s on personal identifiable information
  • IP addresses hashed and salted
  • Retention time <30 days
  • Hits after 30 minute delay
  • White box solution
  • No remote management
Step 7. Information controls

Privacy controls in process and organization
• Describe the working process
• Protocols in place that describe how to handle
• Perform a privacy impact assessment
• Processes are externally audited
• Keep checking on compliance with legislation and policies
• Only screened personnel handle data
Step 7. Information controls

Sharing controls (private sector)

*Public access and access from supervising authorities to government information*

- Describe the working process
- Retention times on IoC’s, sightings,...
- Policy statement, law amendment

*TLP Amber, confidential or secret*

- MSSP’s, international branches
- Research e.g. Blooming filter
- Transparency in processing, (NDA’s)
Step 8. Results

- Span, location, availability
- Bandwidth, performance
- Skill level
- Contextual information
- (Too) high expectations
- Remote access
- New friends

- MISP Forum
- MISP community driven
- MISP STIX
- MISP groups
- Government syndrom
- Data retention
- New friends

Various pics via www.google.com
Step 9. Collect & share

- Collect
- Analyse
- Enrich
- Share
- Report
Step 9. Collect & share

- Collect
- Analyse
- Enrich
- Report
- Share

- Levels of sharing
- IoC’s received
- Follow up
Step 9. Collect & share

- Collect
- Analyse
- Share
- Enrich

- Levels of sharing
- IoC’s received
- Follow up

- Sightings
- Statistics
- Comments
Step 9. Collect & share

- Anonimization
- Few results

- Sightings
- Statistics
- Comments

- Levels of sharing
- IoC’s received
- Follow up
Step 9. Collect & share

- Collect
  - Volume
  - Contextual information
  - Workprocess

- Analyse
  - Levels of sharing
  - IoC’s received
  - Follow up

- Share
  - Sightings
  - Statistics
  - Comments

- Enrich
  - Anonimization
  - Few results

- Report
Step 9. Collect & share

- Collect
  - Volume
  - Contextual inf.
  - Workprocess

- Analyse
  - Too strict
  - Active collaboration
  - Repository missing

- Enrich
  - Anonimization
  - Few results

- Share
  - Levels of sharing
  - IoC’s received
  - Follow up

- Report
  - Sightings
  - Statistics
  - Comments
Steps in community building

1. Legal and policy assurances
2. Explore the territory
3. Communication
4. Start the collaboration
5. Decision making
6. Business Case
7. Controls
8. Start a pilot
9. Information Process
10. Evaluate and adjust
10. Continuous improvement
To conclude

Preparations
• Results
• Involvement

Collaboration
• Takes endurance
• Very intensive
• Trust issues reduced

http://www.tortoiseknowsbest.com/john-bachar-%E2%80%93-a-true-slow-hero/
To conclude

Obstacles
- Controls: transparency sources/ncsc/private
- Process: make a good inventory
- ROI: first insights, hard to put $/€/¥/£ to it
- Results: start small, make it work

Improvement
- Other practices, tooling, disciplines, industries
This presentation is based on our own experiences as well as others:

- Electrotechnik und informationstechnik, Cyber security information exchange to gain insight into the effects, 2015
- NCSC, Ahead of the threat, enhancing cyber intelligence communities, 2015
- Microsoft, a framework for cyber security information sharing and risk reduction, 2015
- Nist, Guide to Cyber Threat Information Sharing, 2014
- MISP, main developers Belgian Defence and Nato
  - [https://github.com/MISP/MISP](https://github.com/MISP/MISP)