National Cyber Security Centre
Ministry of Justice and Security

Template Ambering form

Templates ISAC

March 2020

The information shared during the agenda item referred to as the ‘Indepth Sharing TLP:RED’ may only be used by the ISAC participants present. Level 2 of the capability ‘Information structure and information management’ recommends to record information from the ‘Indepth Sharing TLP:RED’ according to a fixed method. The recommendation is to disseminate this information further so that other internal and external parties can also benefit from it, it will have to be assigned AMBER status. The Template Ambering form on ncsc.nl can be used to this end. On the basis of this form, the ISAC participants can inform their own organization. These forms can also be used to share information with other ISACs.

TLP: Amber

Number of incident *(#)*:

Date of report *(date of ISAC meeting)*:

Name of the person / organisation
sharing an incident:

Date of incident:

Incident information

Motive:

(potential) actor:

Means

- Malware / exploit kit / 0-day,
  RAT, spear phishing, etc:
- CVE:
- Non-digital:
- Tactics:
- Specific / generic incident:
- Relation to other incident(s):
- Other :

What target / who affected:

Detection:

Mitigation:

Duration:

Impact:

Entities to be notified

Other ISACs:

Cybersecurity community (e.g. THTC, AIVD, NCSC):

Within sector:

Lessons learned

Technical:

Communication (internal / external):

Procedure(s):

Other:

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Maart 2020

Aan deze informatie kunnen geen rechten worden ontleend.