Privacy Policy

INTERnet Abuse Detection System (INTERADS)

Date
23 November 2015

Classification
Public

Author
SIDN Labs

Page
1/2

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Title of application/study	INTERnet Abuse Detection System (INTERADS)
Policy start date	23 November 2015
Purpose of application/study	The purpose of INTERADS is to analyse data from the ENTRADA platform and to classify it using (as yet undeveloped) algorithms, with a view to, for example, detecting botnets, phishing, IP spoofing and other forms of internet-abuse. The project is also intended to ascertain what other parties would find the ENTRADA data useful, alongside the Abuse Information Exchange, and would therefore like to interface with the system. All project activities are ultimately aimed at continuous improvement of the internet and its security and trustworthiness.
Personal data	For the purpose described above, we require the following data from the ENTRADA platform: • IP addresses • DNS query data Times and frequencies of domains visited
Legitimate basis	Reasonable interest
Filters	Published documents are anonymised.
Retention	Data is to be retained for the duration of the study. Upon conclusion of the study, the data will be deleted from the local discs and the Windesheim Community.

Access

The data is saved on Windesheim's servers and on the project team members' laptops. Physical access to Windesheim's servers is restricted accordingly. Only Windesheim's system administrators have physical access to the servers. Access to the data via the internet is requires a user name, a password and the assignment of appropriate rights.

The following people have access to the data:

- The Manager of SIDN Labs
- The SIDN Labs staff member with responsibility for student supervision
- A multidisciplinary team of students at Windesheim University of Applied Sciences

Publication/sharing

The data will be shared with one party outside SIDN, namely a multidisciplinary team (of students) at Windesheim University of Applied Sciences, who are carrying out the project.

SIDN and Windesheim University of Applied Sciences will enter into a contract, which will include provisions regulating data disclosure and associated conditions.

Type

Research and development

Other security measures

Project team members' laptops:

- Each project team member will require at least a user name and password to log in.
- Each project team member will use a form of encryption (e.g. VeraCrypt, BitLocker full disk or folder encryption) when saving project data made available to them.

Windesheim Community:

- The Windesheim Community uses SSL (communities.windesheim.nl).
- Private community open only to project team members, the Manager of SIDN Labs and the SIDN Labs staff member with responsibility for supervising project team members.