

Application for Incident Response Teams

<http://www.uvt.nl/infolab/airt>
airt-dev@uvt.nl

Presentation outline

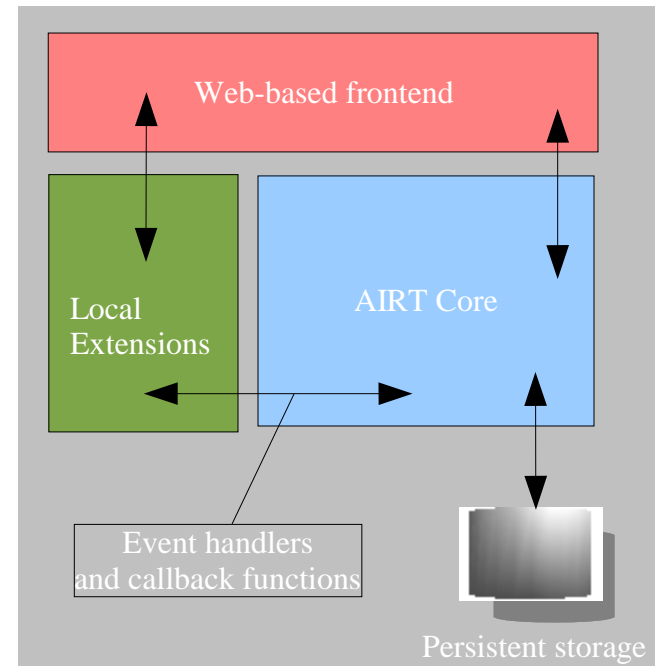
- AIRT Goals and Design Philosophy
- Features: Available and planned
- Demonstration
- Q & A

AIRT Goals

- Development:
 - Rejected: Remedy, TopDesk, RT, RTIR
 - Got: real programmer Kees Leune, Infolab UvT
 - Prototype: collection of tools for UvT-CERT
- Goal: to develop a support system for incident handling which meets the following criteria:
 - Creation of new incident in under 30 sec
 - Comprehensive overview of open incidents
 - Integration with existing tools
 - Support for *outgoing email via templates*

Design Philosophy

- Open
- AIRT-core providing application logic and extension points
- Database-driven
- Extensions which *add* functionality
- Extensions which *alter* functionality
- Human-usable
- Machine-usable



- Community-driven development
- GNU General Public License

AIRT Core Features

- Incident management console
- Address-ranges (Networks, VLANs), constituencies and constituency contacts
- Incident types, states and statuses
- Email templates with PGP GnuPG signing support
- Import queue
- Asynchronous command execution

Plugins

- Automatic importers: Cymru/Flitspaal, MyNetwatchman, Spamcop, Honeyd logging, nmap logging, Nessus logging, other AIRT installations
- Router/firewall/switchport configuration, DHCP server configuration
- Integrated RSS Reader and Wiki environment in management console
- XML SOAP interface to AIRT-Core
- Integration with A-Select for Single Sign-On
- Authentication with client certificates

Demonstration

Honeyd logging indicated a portscan
(output generated by local Perl script)

```
Source ip : 83.65.182.10 Source name: 83-65-182-10.dedicated.sh-wien.inode.at  
time=2005-09-12-13:00:41+0200 proto=tcp dstip=137.56.127.118 dstport=3306  
time=2005-09-12-13:00:41+0200 proto=tcp dstip=137.56.127.119 dstport=3306  
time=2005-09-12-13:00:41+0200 proto=tcp dstip=137.56.127.120 dstport=3306  
time=2005-09-12-13:00:41+0200 proto=tcp dstip=137.56.127.121 dstport=3306  
time=2005-09-12-13:00:42+0200 proto=tcp dstip=137.56.127.121 dstport=3306  
time=2005-09-12-13:00:16+0200 proto=tcp dstip=137.56.44.23 dstport=3306  
time=2005-09-12-13:00:17+0200 proto=tcp dstip=137.56.42.8 dstport=3306  
time=2005-09-12-13:00:18+0200 proto=tcp dstip=137.56.43.159 dstport=3306  
....  
time=2005-09-12-13:26:10+0200 proto=tcp dstip=137.56.36.33 dstport=3306  
time=2005-09-12-13:26:10+0200 proto=tcp dstip=137.56.36.33 dstport=3306
```

AIRT login page - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/login.php

AIRT login page Incident overview

Application for incident response teams

AIRT login page

Home

Incidents

Search

Mail templates

Settings

Logout

Login

Password

[Login using client certificate](#)

Login

AIRT version 20050830.1, Copyright (C) 2004-2005 Tilburg University <airt-dev@uvt.nl>
AIRT comes with ABSOLUTELY NO WARRANTY; for details [click here](#).
This is free software, and you are welcome to redistribute it under certain conditions; See the license for more details.

https://murphy.surfnet.nl/airt/local/certificatelogin.php

murphy.surfnet.nl Proxy: None

AIRT Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

AIRT Control Center Incident overview

Application for incident response teams

AIRT Control Center

Welcome teun. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

Home

Incidents

Search

Mail templates

Settings

Logout

https://murphy.surfnet.nl/airt/incident.php

murphy.surfnet.nl Proxy: None

Incident overview - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/incident.php

Incident overview

Application for incident response teams

Incident overview

Enter incident number Details

Select incident status open Ok

New incident

	Incident ID	Constituency	Hostname	Status	State	Type	Last updated
<input type="checkbox"/>	SURFnet-CERT#010021	uvt.nl	pi1250.uvt.nl	open	blockrequest on	infected	06 Sep 2005
<input type="checkbox"/>	SURFnet-CERT#010023	rug.nl	oosix.icce.rug.nl	open	inspection requested	infected	12 Sep 2005

New State Leave Unchanged

New Status Leave Unchanged

Update All Selected

2 incidents displayed.

https://murphy.surfnet.nl/airt/incident.php?action=details&incidentid=10021

murphy.surfnet.nl Proxy: None

Incident details: SURFnet-CERT#010021 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/incident.php?action=details&incidentid=10021

Incident details: SURFnet-CERT#010... Incident overview

Application for incident response teams

Home
Incidents
Search
Mail templates
Settings
Logout

Incident details: SURFnet-CERT#010021

Basic incident data

Incident type [Help](#)

Incident state [Help](#)

Incident status [Help](#)

infected
probe
spam
content
abusive
administrative
denial

Affected IP addresses

[137.56.40.234](#) [pi1250.uvt.nl](#) [Unknown](#) [edit](#) [remove](#)

IP Address

Affected users

[cert@uvt.nl](#) [UvT, UvT-CERT](#) [remove](#)

Email address of user: [help](#)

If checked, create user if email address unknown

History

Done murphy.surfnet.nl Proxy: None

Incident details: SURFnet-CERT#010021 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/incident.php?action=details&incidentid=10021

Incident details: SURFnet-CERT#010... Incident overview

Affected IP addresses

137.56.40.234 pi1250.uvt.nl Unknown [edit](#) [remove](#)

IP Address Unknown

Affected users

[cert@uvt.nl](#) UvT, UvT-CERT [remove](#)

Email address of user: [help](#)

If checked, create user if email address unknown

History

03-Sep-2005 22:00:47	teun	Incident created
03-Sep-2005 22:00:47	teun	state=inspection requested, status=open, type=infected
03-Sep-2005 22:06:09	teun	Email sent to cert@uvt.nl: SURFnet-CERT#010021: MyNetWatchman klacht pi1250.uvt.nl
03-Sep-2005 22:09:39	teun	Email sent to cert@uvt.nl: SURFnet-CERT#010021: Infringement complaint pi1250.uvt.nl
03-Sep-2005 22:18:59	teun	Email sent to cert@uvt.nl: SURFnet-CERT#010021: Infringement complaint pi1250.uvt.nl
03-Sep-2005 22:55:27	teun	Email sent to cert@uvt.nl: SURFnet-CERT#010021: Cymru klacht over besmette pi1250.uvt.nl
06-Sep-2005 09:20:25	teun	Incident updated: state=blockrequest on, status=open type=infected

New comment:

Done murphy.surfnet.nl Proxy: None

AIRT Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

AIRT Control Center Incident overview

Application for incident response teams

AIRT Control Center

Welcome teun. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

Home

Incidents

Search

Mail templates

Settings

Logout

https://murphy.surfnet.nl/airt/search.php

murphy.surfnet.nl Proxy: None

IP address search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/search.php

IP address search Incident overview

Application for incident response teams

IP address search

Home

Incidents

Search

Mail templates

Settings

Logout

IP address:

Done

murphy.surfnet.nl Proxy: None

Detailed information for host 83-65-182-10.dedicated.sh-wien.inode.at - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/search.php

Detailed information for host 83-65-... Incident overview

Application for incident response teams

[Home](#)
[Incidents](#)
[Search](#)
[Mail templates](#)
[Settings](#)
[Logout](#)

Detailed information for host 83-65-182-10.dedicated.sh-wien.inode.at

Search results for the following host:

IP Address	: 83.65.182.10
Hostname	: 83-65-182-10.dedicated.sh-wien.inode.at
Network	: Default network (0.0.0.0/0)
Constituency	: default

Constituency Contacts

Name	Email	Phone
------	-------	-------

Previous incidents

No previous incidents

Link address to incident

SURFnet-CERT#010023: 129.125.14.80 (infected) ▾

[Link to incident](#) [New incident](#)

New Search

IP address:

Done murphy.surfnet.nl Proxy: None

New Incident - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/incident.php

New Incident Incident overview

Application for incident response teams

Home
Incidents
Search
Mail templates
Settings
Logout

New Incident

Incident type [Help](#)
Incident state [Help](#)
Incident status [Help](#)

affected ip addresses

hostname or ip address
constituency

affected users

email address of user: [help](#)
 if checked, create user if email address unknown

Check to prepare mail

Done murphy.surfnet.nl Proxy: None

Available standard messages - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/standard.php

Available standard messages Available standard messages

Application for incident response teams

Home

Incidents

Search

Mail templates

Settings

Logout

Available standard messages

Messages

prepare	en-test	@INCIDENTID@: Please inspect @HOSTNAME@	edit	delete
prepare	en-infringement-reply	@INCIDENTID@: Infringement complaint @HOSTNAME@	edit	delete
prepare	nl-infringement-forward	@INCIDENTID@: Copyright/warez klacht @HOSTNAME@	edit	delete
prepare	nl-MyNetWatchman	@INCIDENTID@: MyNetWatchman klacht @HOSTNAME@	edit	delete
prepare	nl-Cymru-bots	@INCIDENTID@: Cymru klacht over besmette @HOSTNAME@	edit	delete

[Create a new message](#)

https://murphy.surfnet.nl/airt/standard.php?action=new

murphy.surfnet.nl Proxy: None

Application for incident response teams

- Home
- Incidents
- Search
- Mail templates
- Settings
- Logout

Edit standard message

Update the message and press the 'Save!' button to save the message. The first line of the message will be used as the subject. You may use the following special variables in the template:

@SUBJECT@ .. @ENDSUBJECT@	Delimits the subject line of the message
@HOSTNAME@	Will be replaced with the currently active hostname
@IPADDRESS@	Will be replaced with the currently active IP address
@USERNAME@	Will be replaced with the name of the current user
@USEREMAIL@	Will be replaced with the email address of the current user
@USERINFO@	Will be replaced with detailed information about the user, if that information is available.
@YOURNAME@	Will be replaced with the full name of the logged in incident handler
@YOURFIRSTNAME@	Will be replaced with the first name of the logged in incident handler
@INCIDENTID@	Will be replaced with the current incident id

```
@SUBJECT@@INCIDENTID@: Please inspect @HOSTNAME@@ENDSUBJECT@
Dear abuse team,

SURFnet-CERT is the Computer Security Incident Response Team (CSIRT)
of SURFnet, the National Research and Educational Network of the
Netherlands, and as such the Internet provider of the Dutch
academic community and many research organizations in the
Netherlands. SURFnet-CERT is dealing with all cases of computer
security incidents in which a SURFnet customer is involved as a
victim, intermediate or a suspect.

SURFnet-CERT has detected that a computer known as

@HOSTNAME@ [@IPADDRESS@
contacts honeypot machines within SURFnet. These honeypots
```

Done murphy.surfnet.nl Proxy: None

Edit standard message - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/standard.php?action=edit&filename=en-honeypot-3306

Edit standard message

Mail templates
Settings
Logout

@HOSTNAME@	Will be replaced with the currently active hostname
@IPADDRESS@	Will be replaced with the currently active IP address
@USERNAME@	Will be replaced with the name of the current user
@USEREMAIL@	Will be replaced with the email address of the current user
@USERINFO@	Will be replaced with detailed information about the user, if that information is available.
@YOURNAME@	Will be replaced with the full name of the logged in incident handler
@YOURFIRSTNAME@	Will be replaced with the first name of the logged in incident handler
@INCIDENTID@	Will be replaced with the current incident id

```
serve no other purpose than to passively log attacks by other machines;
they supply no services to your machines. SURFnet-CERT assumes that
your system is most likely infected with a computer virus (also known
as a worm or a bot).

--- Begin logfiles ---

--- End logfiles ---

Please note that port 3306 activity can be a result of a
vulnerability of the MySQL server, which is exploited by a worm.
http://www.dshield.org/port_report.php?port=3306
http://www.symantec.com/avcenter/security/Content/2001_05_08.html

If @HOSTNAME@ runs MySQL, it is likely in problems.

Kind regards,

UvT-CERT - @YOURNAME@
```

Save! Cancel

Done

murphy.surfnet.nl Proxy: None

Available standard messages - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/standard.php

Available standard messages Edit standard message

Application for incident response teams

Home
Incidents
Search
Mail templates
Settings
Logout

Available standard messages

Messages

prepare	en-test	@INCIDENTID@: Please inspect @HOSTNAME@	edit	delete
prepare	en-infringement-reply	@INCIDENTID@: Infringement complaint @HOSTNAME@	edit	delete
prepare	nl-infringement-forward	@INCIDENTID@: Copyright/warez klacht @HOSTNAME@	edit	delete
prepare	nl-MyNetWatchman	@INCIDENTID@: MyNetWatchman klacht @HOSTNAME@	edit	delete
prepare	nl-Cymru-bots	@INCIDENTID@: Cymru klacht over besmette @HOSTNAME@	edit	delete
prepare	en-honeypot-3306	@INCIDENTID@: Please inspect @HOSTNAME@	edit	delete

[Create a new message](#)

https://murphy.surfnet.nl/airt/standard.php?action=prepare&filename=en-honeypot-3306

murphy.surfnet.nl Proxy: None

Send standard message. - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/standard.php?action=prepare&filename=en-honeypot-3306

Send standard message. Edit standard message

Application for incident response teams

Home
Incidents
Search
Mail templates
Settings
Logout

Send standard message.

To:

Subject:

From:

Reply-To:

Dear abuse team,

SURFnet-CERT is the Computer Security Incident Response Team (CSIRT) of SURFnet, the National Research and Educational Network of the Netherlands, and as such the Internet provider of the Dutch academic community and many research organizations in the Netherlands. SURFnet-CERT is dealing with all cases of computer security incidents in which a SURFnet customer is involved as a victim, intermediate or a suspect.

SURFnet-CERT has detected that a computer known as

83-65-182-10.dedicated.sh-wien.inode.at [83.65.182.10]

contacts honeypot machines within SURFnet. These honeypots serve no other purpose than to passively log attacks by other machines; they supply no services to your machines. SURFnet-CERT assumes that your system is most likely infected with a computer virus (also known as a worm or a bot).

--- Begin logfiles ---

--- End logfiles ---

Please note that port 3306 activity can be a result of a vulnerability of the MySQL server, which is exploited by a worm.

Done

murphy.surfnet.nl Proxy: None

IP address search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/search.php

IP address search Edit standard message

Application for incident response teams

IP address search

Home

Incidents

Search

Mail templates

Settings

Logout

IP address:

Done

murphy.surfnet.nl Proxy: None

Detailed information for host pi1250.uvt.nl - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/search.php

Detailed information for host pi1250.... Edit standard message

Application for incident response teams

Home
Incidents
Search
Mail templates
Settings
Logout

Detailed information for host pi1250.uvt.nl

Search results for the following host:

IP Address : 137.56.40.234
 Hostname : pi1250.uvt.nl
 Network : 137.56.0.0/16 (137.56.0.0/16)
 Constituency : Universiteit van Tilburg

Constituency Contacts

Name	Email	Phone
UvT, UvT-CERT	cert@uvt.nl	+31 13 466 2014

Previous incidents

Incident ID	Created	Type	State	Status
SURFnet-CERT#010018	31 Aug 2005	administrative	inspection requested	closed
SURFnet-CERT#010019	31 Aug 2005	administrative	inspection requested	closed
SURFnet-CERT#010020	31 Aug 2005	administrative	inspection requested	closed
SURFnet-CERT#010021	03 Sep 2005	infected	blockrequest on	open

Link address to incident

Done murphy.surfnet.nl Proxy: None

AIRT Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

AIRT Control Center Edit standard message

Application for incident response teams

AIRT Control Center

Welcome teun. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

[Home](#)

[Incidents](#)

[Search](#)

[Mail templates](#)

[Settings](#)

[Logout](#)

https://murphy.surfnet.nl/airt/maintenance.php

murphy.surfnet.nl Proxy: None

AIRT Maintenance Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/maintenance.php

AIRT Maintenance Center Edit standard message

Application for incident response teams

AIRT Maintenance Center

[Home](#)

[Incidents](#)

[Search](#)

[Mail templates](#)

[Settings](#)

[Logout](#)

User management

[Edit users](#)

Incident management

[Edit incident states](#)

[Edit incident statuses](#)

[Edit incident types](#)

[Edit standard messages](#)

Network management

[Edit networks](#)

[Edit constituencies](#)

[Edit constituency contacts](#)

Appearance

[Edit main menu links](#)

https://murphy.surfnet.nl/airt/networks.php

murphy.surfnet.nl Proxy: None

Networks - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/networks.php

Networks Edit standard message

131.174.228.0/22	131.174.228.0/22	UMC Nijmegen	edit	delete
131.174.244.0/22	131.174.244.0/22	UMC Nijmegen	edit	delete
131.180.0.0/16	131.180.0.0/16	TUDelft	edit	delete
131.211.0.0/16	131.211.0.0/16	Universiteit Utrecht	edit	delete
131.224.0.0/16	131.224.0.0/16	RIVM	edit	delete
132.229.0.0/16	132.229.0.0/16	Universiteit Leiden	edit	delete
134.221.0.0/16	134.221.0.0/16	TNO	edit	delete
136.231.0.0/17	136.231.0.0/17	WL Delft Hydraulics	edit	delete
136.231.128.0/32	136.231.128.0/17	Nat Lucht- en Ruimtevaartlab	edit	delete
137.17.0.0/16	137.17.0.0/16	Nat Lucht- en Ruimtevaartlab	edit	delete
137.56.0.0/16	137.56.0.0/16	Universiteit van Tilburg	edit	delete
137.120.0.0/16	137.120.0.0/16	Universiteit Maastricht	edit	delete
137.224.0.0/16	137.224.0.0/16	Wageningen Univ Research	edit	delete
139.63.0.0/16	139.63.0.0/16	TNO	edit	delete
141.252.0.0/16	141.252.0.0/16	Noordelijke Hogeschool Leeuw	edit	delete
143.121.0.0/16	143.121.0.0/16	Universiteit Utrecht	edit	delete
145.2.0.0/16	145.2.0.0/16	Saxion Hogescholen	edit	delete
145.3.0.0/16	145.3.0.0/16	Geodelft	edit	delete
145.9.0.0/16	145.9.0.0/16	WL Delft Hydraulics	edit	delete
145.12.0.0/16	145.12.0.0/16	Wageningen Univ Research	edit	delete
145.18.0.0/16	145.18.0.0/16	Universiteit van Amsterdam	edit	delete
145.19.0.0/16	145.19.0.0/16	Hogeschool Zeeland	edit	delete
145.20.0.0/16	145.20.0.0/16	Open Universiteit Nederland	edit	delete

Done

murphy.surfnet.nl Proxy: None

Application for incident response teams

[Home](#)

[Incidents](#)

[Search](#)

[Mail templates](#)

[Settings](#)

[Logout](#)

Edit constituency assignments

Current contacts of constituency uvt.nl

(UvT, UvT-CERT) | [cert@uvt.nl](#) | +31 13 466 2014 | [Remove](#)

admin (Administrator,)
(Dhr. G. Ranke, Gerard)
(Tiscali, Tiscali BV)
(Bezeqint, Bezeq International)
(Zonnet, ZONnet Administrator)
(@Home, @Home Benelux NOC)
(Chello, UPC Nederland)
(Buijserd, Hans)
(KPN Direct ADSL, Abuse)
(Dhr. Ing. C.B. Okhuysen, Ben)
(Speedling, Qinip Operations)
(Wanadoo, Wanadoo Nederland BV)
(Xs4ALL, XS4ALL Internet NOC)
(Bit, BIT BV)
(Dhr. M. Ensink, Martin)
(Dhr. F.W.T. van Leeuwen, Frits)
(Dhr. J. Jagersma, Jeroen)
(Dhr. R. Pronk, Rop)
(Dhr. G. Nederlof, Gijs)
(Getronics, Helpdesk)

Assing user(s) to constituency:

[Select another constituency](#) | [Settings](#)

Find: Highlight Match case

Done murphy.surfnet.nl

AIRT Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

AIRT Control Center Edit standard message

Application for incident response teams

AIRT Control Center

Welcome team. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

[Home](#)

[Incidents](#)

[Search](#)

[Mail templates](#)

[Settings](#)

[Logout](#)

https://murphy.surfnet.nl/airt/local/stats.php

murphy.surfnet.nl Proxy: None

SURFnet-CERT statistics - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/local/stats.php

SURFnet-CERT statistics Edit standard message

Application for incident response teams

SURFnet-CERT statistics

Please select the reporting period of which you would like to see statistics. (note; the start date and the end date are included in the report.)

Start date (day-month-year) 01 - July - 2005

End date 12 - September - 2005

Show statistics

Done murphy.surfnet.nl Proxy: None

Home

Incidents

Search

Mail templates

Settings

Logout

AIR Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

Application for incident response teams

AIRT Control Center

Welcome team. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

[Home](#)

[Incidents](#)

[Search](#)

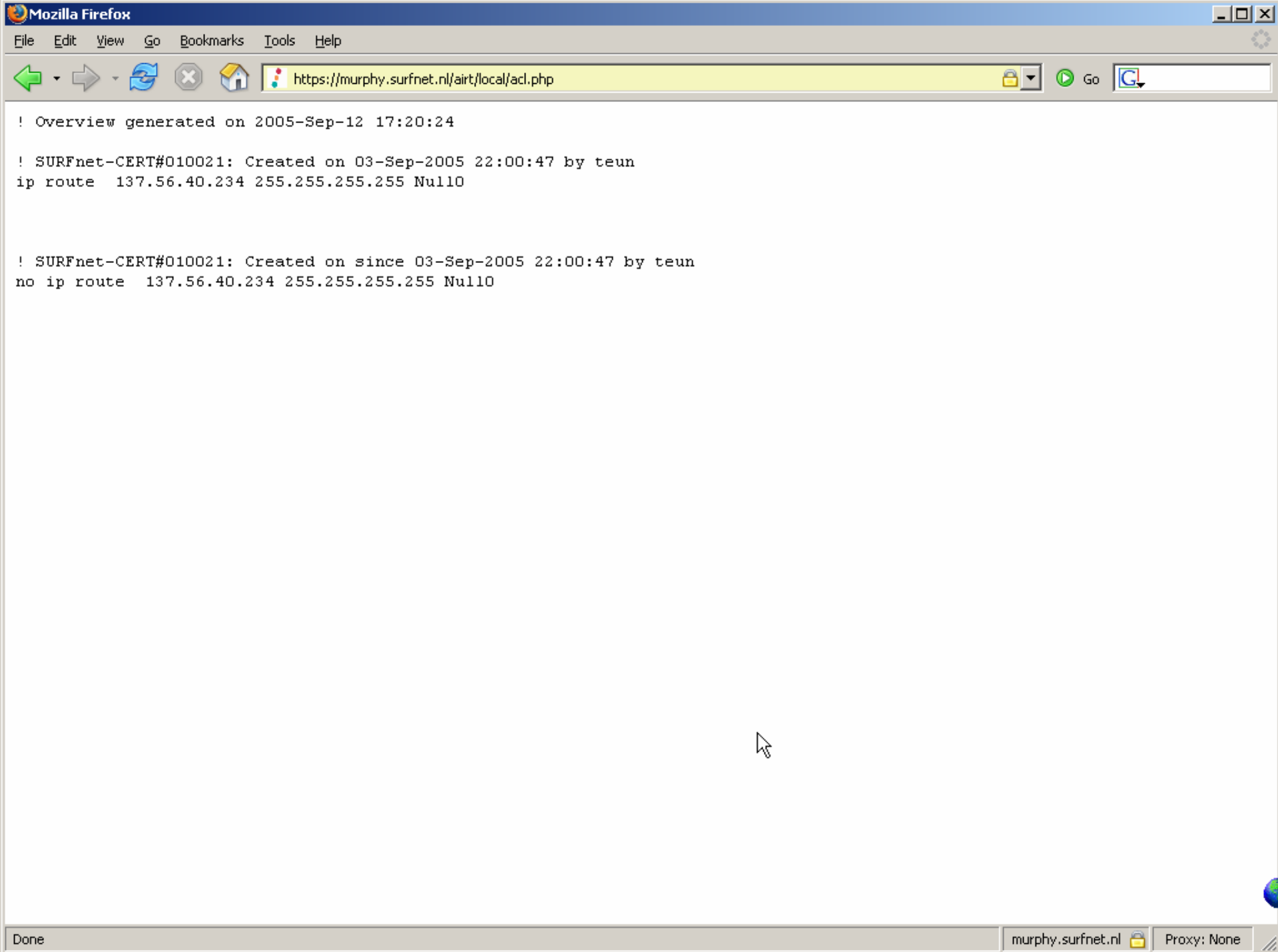
[Mail templates](#)

[Settings](#)

[Logout](#)

https://murphy.surfnet.nl/airt/local/acl.php

murphy.surfnet.nl Proxy: None



AIR Control Center - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://murphy.surfnet.nl/airt/index.php

Application for incident response teams

AIRT Control Center

Welcome teun. Your last login was at 2005-09-12 16:36 from 137.56.40.234.

Main tasks

- [Incident management](#)
- [IP Address lookup](#)
- [Mail templates](#)
- [Edit settings](#)
- [WikiWespje](#)
- [N.E.R.D. flow analysis](#)
- [Incident Statistics](#)
- [Security news RSS](#)
- [Null route List of blocked users](#)
- [Logout](#)

Home

Incidents

Search

Mail templates

Settings

Logout

https://murphy.surfnet.nl

i Are you sure that you want to log out?

OK Cancel

Done

murphy.surfnet.nl Proxy: None

Additional Questions and Answers?