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)
AIRT login page

Login
Password

Login using client certificate

Login

AIRT version 20050830.1, Copyright (C) 2004-2005 Tilburg University <airst-dev@ut.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.
AIRT Control Center

Welcome team. Your last login was at 2015-09-12 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
## Incident overview

Enter incident number: [Enter]
Select incident status: [open] [Ok]

### New incident

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Consituency</th>
<th>Hostname</th>
<th>Status</th>
<th>State</th>
<th>Type</th>
<th>Last updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SURFnet-CERT#010021</td>
<td>uvt.nl</td>
<td>pi1250.uvt.nl</td>
<td>open</td>
<td>blockrequest on</td>
<td>infected</td>
<td>06 Sep 2005</td>
</tr>
<tr>
<td>SURFnet-CERT#010023</td>
<td>rug.nl</td>
<td>oos:kicce.rug.nl</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>12 Sep 2005</td>
</tr>
</tbody>
</table>

New State: Leave Unchanged
New Status: Leave Unchanged

Update All Selected

2 incidents displayed.
Incident details: SURFnet-CERT#010021

Basic incident data

- Incident type: infected
- Incident state: infected
- Incident status: unknown
  - update

Affected IP addresses

- 137.56.40.234
- pi1250.uvt.nl
- Unknown

Affected users

- cert@uvt.nl
- UvT, UvT-CERT

Email address of user: [Add help]

- If checked, create user if email address unknown

History
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:

If checked, create user if email address unknown

History

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

New comment
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
IP address search

IP address: 83.65.182.10
Search
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
- Network: Default network (0.0.0.0/0)
- Constituency: default

Constituency Contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
</table>

Previous incidents

No previous incidents

Link address to incident

SURFnet-CERT#010023: 129.125.14.80 (infected)

New Search

IP address: abuse@inode.at

Search
New Incident

Incident type: infected
Incident state: inspection requested
Incident status: open

Affected IP addresses

Hostname or IP address: 33.65.182.10
Constituency: default (default)

Affected users

Email address of user: abuse@node.nl

- [ ] Check to prepare mail
### Available standard messages

#### Messages

<table>
<thead>
<tr>
<th>Function</th>
<th>Message</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>prepare en-test</td>
<td>@INCIDENTID@: Please inspect @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare en-infringement-reply</td>
<td>@INCIDENTID@: Infringement complaint @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-infringement-forward</td>
<td>@INCIDENTID@: Copyright/warez klacht @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-MyNetWatchman</td>
<td>@INCIDENTID@: MyNetWatchman klacht @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-Cymru-bots</td>
<td>@INCIDENTID@: Cymru klacht over besmette @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Create a new message](#)
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
- @USERNINFO@: Will be replaced with detailed information about the user, if that information is available.
- @USERNAME@: 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. Those 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. 
http://www.symantec.com/avcenter/security/Content/2001_05_08.html

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

Kind regards,

SUIT-CERT - @YOURNAME@
### Available standard messages

#### Messages

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>prepare en-test</td>
<td>@INCIDENTID@: Please inspect @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare en-infringement-reply</td>
<td>@INCIDENTID@: Infringement complaint @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-infringement-forward</td>
<td>@INCIDENTID@: Copyright/warez klacht @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-MyNetWatchman</td>
<td>@INCIDENTID@: MyNetWatchman klacht @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare nl-Cymru-bots</td>
<td>@INCIDENTID@: Cymru klacht over besmette @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prepare en-honeypot-3306</td>
<td>@INCIDENTID@: Please inspect @HOSTNAME@</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Create a new message
Send standard message.

To: abuse@innode.at

Subject: SURFnet-CERT#010024. Please inspect 83-65-182-10

From: SURFnet-CERT - Teun <cer@surfnet.nl>

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.innode.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.
Application for incident response teams

IP address search

IP address: pi1250.uvt.nl

Search
Detailed information for host pi1250.uvt.nl

Search results for the following host:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
<th>Network</th>
<th>Constituency</th>
</tr>
</thead>
<tbody>
<tr>
<td>137.55.40.234</td>
<td>pi1250.uvt.nl</td>
<td>137.55.0.0/15 (137.55.0.0/16)</td>
<td>Universiteit van Tilburg</td>
</tr>
</tbody>
</table>

Constituency Contacts

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

Previous incidents

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Created</th>
<th>Type</th>
<th>State</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SURFnet-CERT#010018</td>
<td>31 Aug 2005</td>
<td>administrative</td>
<td>inspection requested</td>
<td>closed</td>
</tr>
<tr>
<td>SURFnet-CERT#010019</td>
<td>31 Aug 2005</td>
<td>administrative</td>
<td>inspection requested</td>
<td>closed</td>
</tr>
<tr>
<td>SURFnet-CERT#010020</td>
<td>31 Aug 2005</td>
<td>administrative</td>
<td>inspection requested</td>
<td>closed</td>
</tr>
<tr>
<td>SURFnet-CERT#010021</td>
<td>03 Sep 2005</td>
<td>infected</td>
<td>blockrequest on</td>
<td>open</td>
</tr>
</tbody>
</table>

Link address to incident

- SURFnet-CERT#010023: 129.125.14.80 (infected)
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
AIRT Maintenance Center

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
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Location</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>131.174.228.0/22</td>
<td>UMC Nijmegen</td>
<td>edit, delete</td>
</tr>
<tr>
<td>131.174.244.0/22</td>
<td>UMC Nijmegen</td>
<td>edit, delete</td>
</tr>
<tr>
<td>131.180.0.0/16</td>
<td>TUDelft</td>
<td>edit, delete</td>
</tr>
<tr>
<td>131.211.0.0/16</td>
<td>Universiteit Utrecht</td>
<td>edit, delete</td>
</tr>
<tr>
<td>131.224.0.0/16</td>
<td>RIVM</td>
<td>edit, delete</td>
</tr>
<tr>
<td>132.229.0.0/16</td>
<td>Universiteit Leiden</td>
<td>edit, delete</td>
</tr>
<tr>
<td>134.221.0.0/16</td>
<td>TNO</td>
<td>edit, delete</td>
</tr>
<tr>
<td>136.231.0.0/17</td>
<td>WL</td>
<td>Delft Hydraulics</td>
</tr>
<tr>
<td>136.231.128.0/32</td>
<td>Nat Lucht- en Ruimtevaartlab</td>
<td>edit, delete</td>
</tr>
<tr>
<td>137.17.0.0/16</td>
<td>Nat Lucht- en Ruimtevaartlab</td>
<td>edit, delete</td>
</tr>
<tr>
<td>137.56.0.0/16</td>
<td>Universiteit van Tilburg</td>
<td>edit, delete</td>
</tr>
<tr>
<td>137.120.0.0/16</td>
<td>Universiteit Maastricht</td>
<td>edit, delete</td>
</tr>
<tr>
<td>137.224.0.0/16</td>
<td>Wageningen Univ Research</td>
<td>edit, delete</td>
</tr>
<tr>
<td>139.63.0.0/16</td>
<td>TNO</td>
<td>edit, delete</td>
</tr>
<tr>
<td>141.252.0.0/16</td>
<td>Noordelijke Hogeschool Leeuw</td>
<td>edit, delete</td>
</tr>
<tr>
<td>143.121.0.0/16</td>
<td>Universiteit Utrecht</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.2.0.0/16</td>
<td>Saxion Hogescholen</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.3.0.0/16</td>
<td>Geodelft</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.9.0.0/16</td>
<td>WL</td>
<td>Delft Hydraulics</td>
</tr>
<tr>
<td>145.12.0.0/16</td>
<td>Wageningen Univ Research</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.18.0.0/16</td>
<td>Universiteit van Amsterdam</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.19.0.0/16</td>
<td>Hogeschool Zeeland</td>
<td>edit, delete</td>
</tr>
<tr>
<td>145.20.0.0/16</td>
<td>Open Universiteit Nederland</td>
<td>edit, delete</td>
</tr>
</tbody>
</table>
Edit constituency assignments

Current contacts of constituency uvt.nl

(UvT, UvT-CERT) cert@uvt.nl +31 13 466 2014

Assign user(s) to constituency:

admin (Administrator)
(Dhr. G. Panke, Gerard)
(Tisceli, Tisceli BV)
(Boezem, Beoq International)
(Zornet, ZONnet Administrator)
(@Home, @Home Benelux NOC)
(Cello, UPC Nederland)
(Buijs, Hams)
(KPN DirctADSL, Abuse)
(Dhr. Ing. C.B. Okhuysen, Ben)
(Speedlineq, 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. Nederlow, Gjjs)
(Geotronics, Helpdesk)

Assign

Select another constituency | Settings
AIRT Control Center

Welcome teun. Your last login was at 2015-09-12 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
### 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.

<table>
<thead>
<tr>
<th>Start date (day-month-year)</th>
<th>End date</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 July 2005</td>
<td>12 September 2005</td>
</tr>
</tbody>
</table>

[Show statistics]
Welcome true. 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
- WktWespje
- N.E.R.D. flow analysis
- Incident Statistics
- Security news RSS

Null route List of blocked users

Logout
! Overview generated on 2005-Sep-12 17:20:24

! SURFnet-CERT#010021: Created on 03-Sep-2005 22:00:47 by teun
ip route 137.56.40.234 255.255.255.255 Null0

! SURFnet-CERT#010021: Created on since 03-Sep-2005 22:00:47 by teun
no ip route 137.56.40.234 255.255.255.255 Null0
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
- WikiWespe
- N.E.R.D. flow analysis
- Incident Statistics
- Security news RSS
- Null route List of blocked users
- Logout

Are you sure that you want to log out?
Additional Questions and Answers?