

# INCH & IODEF update

<http://www.ietf.org/html.charters/inch-charter.html>

<http://www.surfnetters.nl/meijer/inch/>

Warsaw, 29 may 2003

Jan Meijer <[jan.meijer@surfnet.nl](mailto:jan.meijer@surfnet.nl)>

## INCH

- INCident Handling workinggroup
- Develop Incident handling information exchange format
- Not an exchange protocol!
- Requirements doc (FINE)
- Datamodel doc (IODEF)
  - IETF 55 (Nov)
  - Interim meeting (Feb)
  - IETF 56 (Mar)
- Implementation guide

## Implementations

- eCSIRT.net (<http://www.ecsirt.net/>)  
ihsh
- AirCERT (<http://aircert.sourceforge.net/>)
- APCERT (underway)

# INCH-IODEF Datamodel: Incident level

```
+-----+
| IODEF-Document |
+-----+
| STRING version |<-->{1..*}--[ Incident ]
|               |
+-----+

+-----+
| Incident       |
+-----+
| ENUM purpose   |<-----[ IncidentID      ]
| ENUM restriction|<-->{0..1}--[ AlternativeIDs  ]
|               |<-----[ IncidentData    ]
|               |<-->{0..1}--[ RelatedActivity ]
|               |<-->{0..*}--[ AdditionalData ]
+-----+
```

# INCH-IODEF Datamodel: IncidentData level

```
+-----+
| IncidentData |
+-----+
| ENUM restriction | <>--{0..*}--[ Description ]
|                  | <>--{1..*}--[ Assessment ]
|                  | <>--{0..*}--[ Method ]
|                  | <>--{0..1}--[ DetectTime ]
|                  | <>--{0..1}--[ StartTime ]
|                  | <>--{0..1}--[ EndTime ]
|                  | <>-----[ ReportTime ]
|                  | <>--{1..*}--[ Contact ]
|                  | <>--{0..*}--[ Expectation ]
|                  | <>--{0..1}--[ History ]
|                  | <>--{0..*}--[ EventData ]
|                  | <>--{0..*}--[ AdditionalData ]
+-----+
```

# INCH-IODEF Datamodel: Incident.IncidentData.Assessment

```
+-----+
| Assessment |
+-----+
| ENUM restriction |<---{0..*}--[ Impact      ]
|                  |<---{0..*}--[ TimeImpact    ]
|                  |<---{0..*}--[ MonetaryImpact ]
|                  |<---{0..*}--[ LifeImpact     ]
|                  |<---{0..1}--[ Confidence   ]
+-----+
```

# INCH-IODEF datamodel: Incident. IncidentData.Assessment.Impact

```
+-----+  
| Impact |  
+-----+  
| STRING |  
|        |  
| ENUM restriction |  
| ENUM severity   |  
| ENUM completion |  
| ENUM type       |  
+-----+
```

type:

1. admin. Administrative privileges were attempted or obtained
2. dos. A denial of service was attempted or completed
3. file. An action on a file was attempted or completed
4. recon. A reconnaissance probe was attempted or completed
5. user. User privileges were attempted or obtained
6. none. The activity did not have any (technical) impact
7. unknown. The impact of the activity is unknown
8. other. Anything not in one of the above categories

# INCH-IODEF Datamodel: Incident.IncidentData.Method

```
+-----+
| Method |
+-----+
| ENUM restriction |<--{0..*}--[ Classification ]
|                 |
|                 |<--{0..*}--[ Description   ]
+-----+

+-----+
| Classification |
+-----+
| ENUM restriction |<-----[ name ]
| ENUM origin      |
|                 |<-----[ url   ]
+-----+
```

# INCH-IODEF Datamodel: Incident.IncidentData.Contact

```

+-----+
| Contact |
+-----+
| ENUM restriction | <>--{0..1}--[ name          ]
| ENUM role        |
| ENUM type        | <>--{0..*}--[ Description      ]
|   (person/)     |
|   org)          | <>--{0..*}--[ RegistryHandle  ]
|                | <>--{0..1}--[ PostalAddress  ]
|                | <>--{0..*}--[ Email          ]
|                | <>--{0..*}--[ Telephone     ]
|                | <>--{0..1}--[ Fax            ]
|                | <>--{0..1}--[ Timezone     ]
|                | <>--{0..*}--[ Contact      ]
+-----+

```

Role:

1. creator. The entity that generate the IODEF document.
2. admin. An administrative contact for a host or network.
3. tech. A technical contact for a host or network.
4. irt. The CSIRT involved in handling the incident.
5. cc. An entity that is to be kept informed about the the

# INCH-IODEF Datamodel: Incident.IncidentData.Expectation

```
+-----+
| Expectation |
+-----+
| ENUM restriction | <>--{1..*}--[ Description ]
| ENUM priority   |
| ENUM category   | <>--{0..1}--[ StartTime   ]
|                 | <>--{0..1}--[ EndTime     ]
|                 | <>--{0..1}--[ Contact     ]
+-----+
```

1. nothing. Not to take action is requested.
2. contact-site. Contact the listed site in the recipient's constituency.
3. contact-me. Contact the originator of the document.
4. block. Block or investigate machines listed in the document in the recipient's constituency.

# INCH-IODEF Datamodel: IncidentData level

```
+-----+
| IncidentData |
+-----+
| ENUM restriction | <>--{0..*}--[ Description ]
|                  | <>--{1..*}--[ Assessment ]
|                  | <>--{0..*}--[ Method ]
|                  | <>--{0..1}--[ DetectTime ]
|                  | <>--{0..1}--[ StartTime ]
|                  | <>--{0..1}--[ EndTime ]
|                  | <>-----[ ReportTime ]
|                  | <>--{1..*}--[ Contact ]
|                  | <>--{0..*}--[ Expectation ]
|                  | <>--{0..1}--[ History ]
|                  | <>--{0..*}--[ EventData ]
|                  | <>--{0..*}--[ AdditionalData ]
+-----+
```

# INCH-IODEF: Incident.IncidentData.EventData

```
+-----+
| EventData |
+-----+
ENUM restriction <>--{0..*}--[ Description ]
|
| <>--{0..1}--[ Assessment ]
|
| <>--{0..*}--[ Method ]
|
| <>--{0..1}--[ DetectTime ]
|
| <>--{0..1}--[ StartTime ]
|
| <>--{0..1}--[ EndTime ]
|
| <>--{0..*}--[ Contact ]
|
| <>--{0..1}--[ History ]
|
| <>--{0..*}--[ System ]
|
| <>--{0..1}--[ Record ]
|
| <>--{0..*}--[ EventData ]
|
| <>--{0..*}--[ AdditionalData ]
+-----+
```

# INCH-IODEF Datamodel: Incident. IncidentData.EventData.System

```
+-----+
| System |
+-----+
| ENUM restriction |<>-----[ Node    ]
| ENUM category   |
| STRING interface |<>--{0..*}--[ User    ]
| ENUM spoofed    |
|                  |<>--{0..*}--[ Process ]
|                  |<>--{0..*}--[ Service ]
|                  |<>--{0..1}--[ FileList ]
+-----+
```

# INCH-IODEF Datamodel: Incident. IncidentData.EventData.Record

```

+-----+
| Record          |
+-----+
| ENUM restriction | <>--{1..*}--[ RecordData ]
+-----+
| RecordData     |
+-----+
| ENUM restriction | <>--{0..1}--[ DateTime      ]
|                 | <>--{0..*}--[ Description  ]
|                 | <>--{0..1}--[ Analyzer    ]
|                 | <>--{1..*}--[ RecordItem  ]
+-----+
| RecordItem     |
+-----+
| ANY             |
| ENUM type      |
+-----+

```

ip

# <http://www.eCSIRT.net>

## Profile:

IODEF-Message  
Incident

IncidentID  
AlternativeIDs  
IncidentData

Description  
Assessment

Impact

Method

Description

Expectation

Description

Contact

Name  
Description  
email  
telephone  
timezone

EventData

Record

RecordData

RecordItem

**<http://www.eCSIRT.net>**

Exchange protocol (KISS)

States:

- New
- Open <----+  
                  |
- Pending -+
- Closed

# <http://www.eCSIRT.net>

## Exchange protocol

Initiator		Follower
O	-----please investigate----->	(new)
O	-----fyi, no action expected----->	(new)
P	<-----will take care of this-----	(open)
to C/N	<-----no report back when done-----	(open)
P	<-----will report back when done-----	(open)
P	<-----keep you posted-----	(open)
P	<-----need more data-----	(change to pending)
to P	-----status update request----->	(open)
P/O	<-----status update-----	(open)
C	<-----closure of incident-----	(change to close)
C	-----closure ack/nack----->	(change depends on respons)

# Incident Handling System requirements

# Incident Handling System Requirements

- Workflow
- Operational model (Incident, Threads, metadata)
- General requirements (pluggable authentication, modularity, language etc.)
- Modules
  - Triage
  - Core (mail in, mail out, thread-mgt)
  - Incident data
  - Incident management (roles, responsibilities, on a incident basis)
  - User management (for the system)
  - Contact management (constituency, 'tell me all about this IP-address')
  - I/O module(s) (email, IODEF, webform, ?)
  - I/O filters (crypto functions on input/output, ..?)
  - Crypto functions (crypto on internal data?)