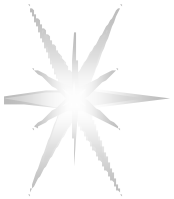
IODEF
and
Extended Incident Handling Framework

TF-CSIRT Seminar

May 31, 2001

Ljubljana



Agenda

- TF-CSIRT Incident Taxonomy and Description WG work process
- IODEF and Extended Incident Handling
- IODEF and IDMEF relations
  - IDMEF development and pilot implementation
  - Presentation and discussion at IETF50

ITDWG work process

Incident Taxonomy and Description WG

- Webpage and charter - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/
- i-taxonomy and iodef mailing lists had been merged
- iodef@terena.nl archive - http://hypermail.terena.nl/iodef-list/mail-archive/
  - historical: i-taxonomy@terena.nl archive - http://hypermail.terena.nl/incident-taxonomy-list/mail-archive/

IODEF Editorial Group

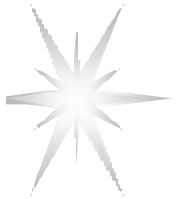
Jimmy Arvidsson, Telia CERT

Andrew Cormack, CERT UKERNA

Yuri Demchenko, TERENA

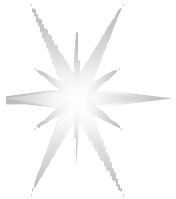
Jan Meijer, CERT-NL

Contribution is welcome!



IODEF/ITDWG – next steps

- Pilot implementation among few CSIRTs in Europe
  - TERENA co-funded Pilot Project
    - First implementation of IODEF in Scandinavia
  - Primary IHS Platform: Remedy ARS
    - Other platforms: Magic TSD, Nortel Clarify
- Next BoF – at 13th FIRST Conference in Toulouse, France
  - Suggestions about Agenda are needed
- BoF at IETF51 in London on Extended Incident Handling
  - agreed with IDWG and IETF Security Area



IODEF Documents

- Incident Object Description and Exchange Format Requirements
  - Published as RFC 3067 http://www.ietf.org/rfc/rfc3067.txt
- XML Data Type Description (XML DTD)
  - Pre-project draft is available
    http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/iodef-xmldtd-00.dtd
  - Document (I-draft) to be drafted before IETF51
  - Problems with name space sharing with IDMEF - TBC
- Incident Object Data Model and Incident Object Elements Description
  - To be drafted before IETF51

Other and external IODEF related Documents

- Best Current Practice on Incident classification and reporting schemes
  - Version 1 http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/BCPreport1.rtf
- Taxonomy of the Computer Security Incident related terminology - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/i-taxonomy_terms.html

Other documents/areas of interest

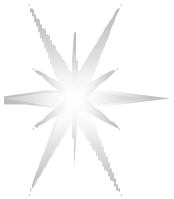
- Evidence Collection and Archiving (current i-draft expired)
  - Cached copy - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/archive/draft-ietf-grip-prot-evidence-01.txt
  - To be taken over by INCH BoF

IODEF and Extended Incident Handling (inch)

- IODEF (Incident Object Description and Exchange Format) is a product of Incident Taxonomy and Description WG – Deliverable C
  http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/
  - IODEF Requirements – RFC3067 (http://www.ietf.org/rfc/rfc3067.txt)
  - Pilot implementation between few European CSIRTs (e.g., CERT-NL, CERT-UK)

Other and previous projects

- CERT/CC (Roman Danyliw)
  - Network of Internet-based security event sensors at various organizations
    http://www.cert.org/kb/aircert/
- Litton-TASC (William Rice and Katarina Auer)
  - http://home.earthlink.net/~wmrice/CIAM_Paper_Final2.pdf
    http://home.earthlink.net/~wmrice/CIAM_FIRST2000.htm
- IETF GRIP WG
  - I-draft on Evidence Collection Guidance – expired



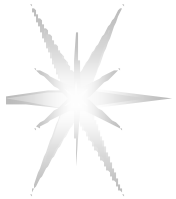
IODEF purposes

A uniform incident description enables applications such as:

- uniform internal incident storage
- incident handling between teams made easier (only one team needs to classify and analyze the complete incident, the other team can re-use this data)
- uniform incident reporting by victims to CSIRTs
- uniform statistic generation and exchange, for both domestic use and exchange of data between teams
- trend-analyses for reoccurrence of incidents, victims, attackers, etc.
- trend-analyses for relations between scans and attacks and thus begin working on pro-active incident response

Main IODEF actors are CSIRTs – not IDS

IODEF is for human -- not machines/IDS

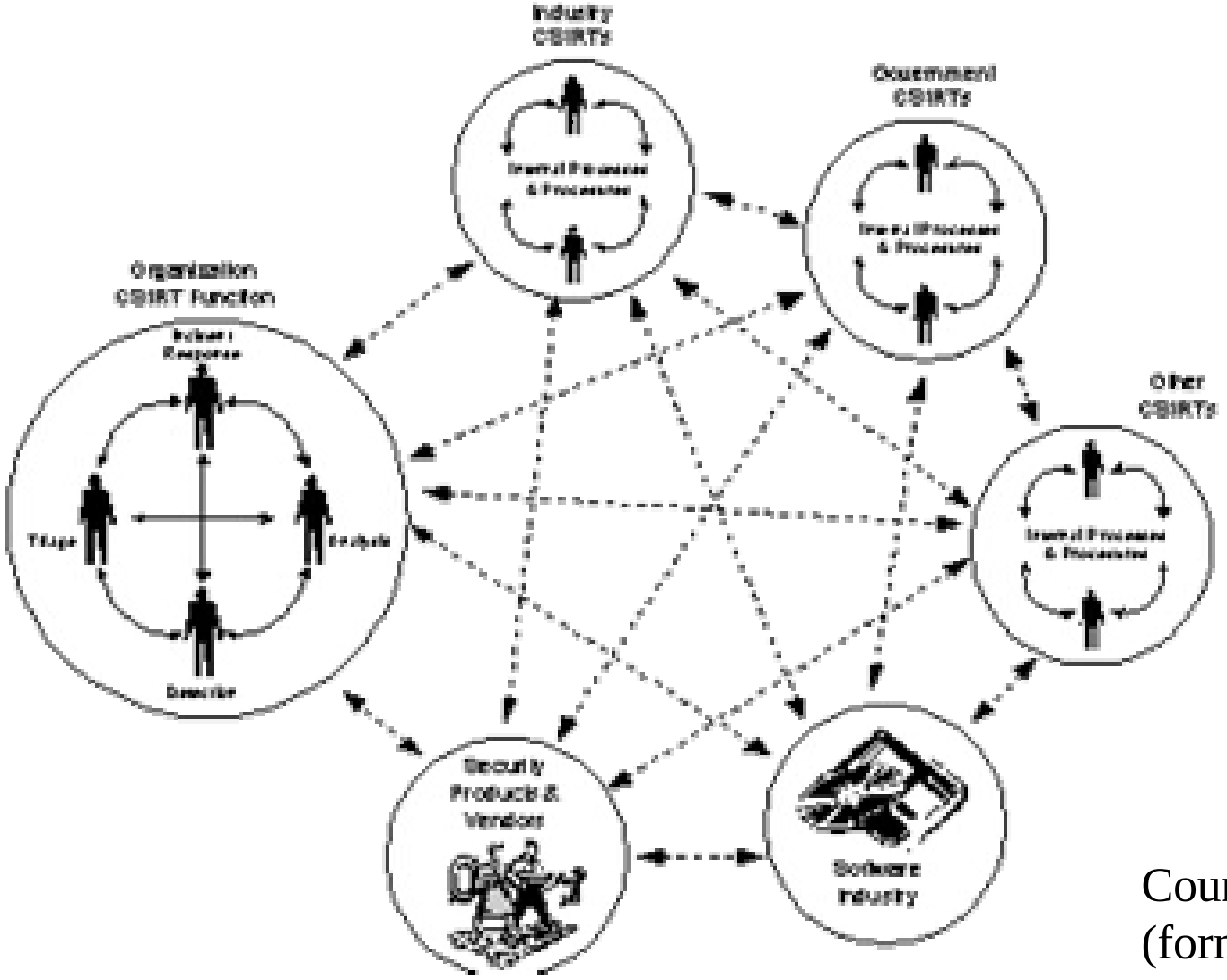


Extended Incident Handling – Scope

Main components/elements of Extended Incident Handling

- Incident Object Description - IODEF
- Incident Information Exchange
- Evidence collection and custody
  - Capable/eligible to be used in law enforcement procedures
- Using/Incorporating Vulnerabilities and Exposures Databases
  - Incident and Vulnerability/Exposure formats compatibility
- Reporting about Vulnerabilities to Software and Hardware vendors
  - Opening and Tracking V/E
- High level statistics and reporting to constituency and sponsors

Extended Incident Handling – Information flow



Courtesy of William Rice (former Litton-TASC)

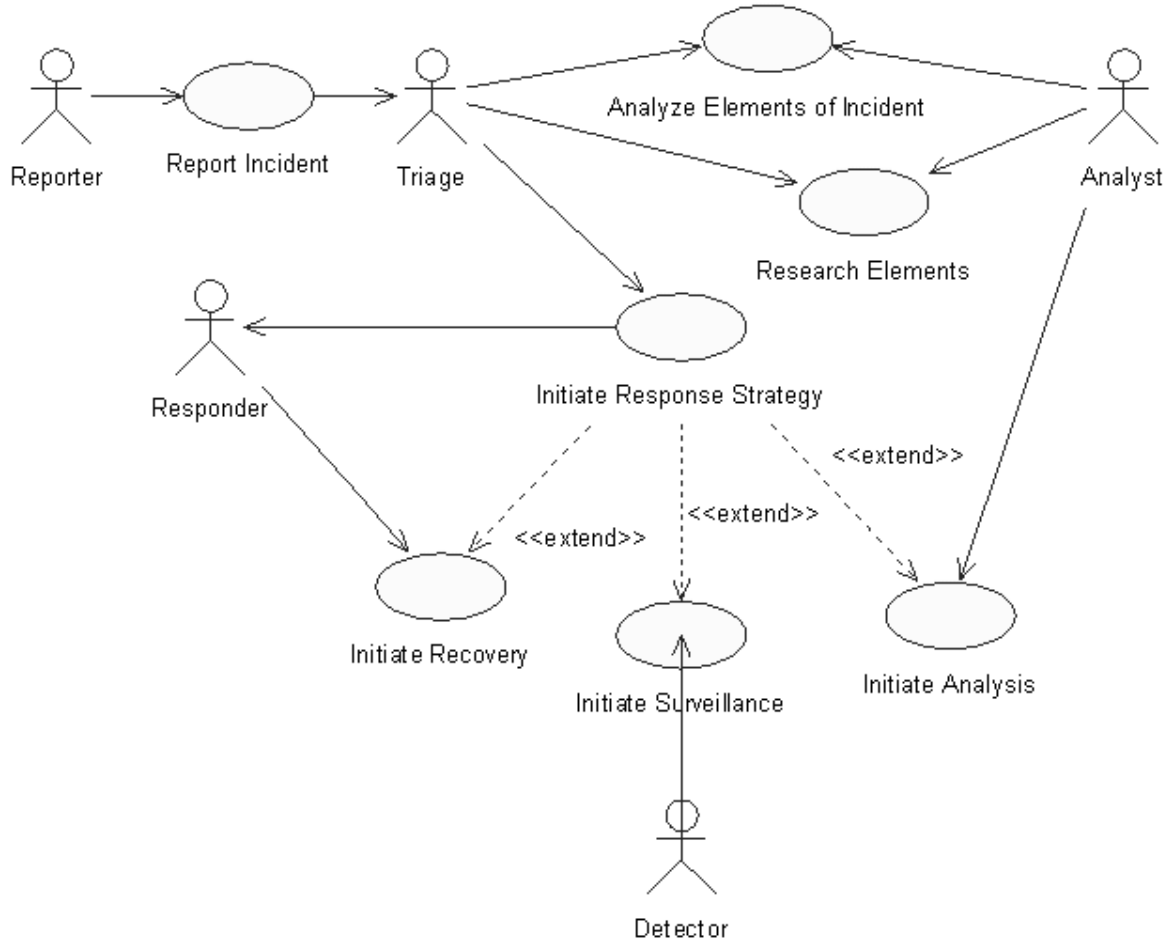
Interaction between IDS, IHS and Vulnerability Reports (Security Alerts)

Yet To Be Described
(including Attack/Incident History)

CSIRT workflow

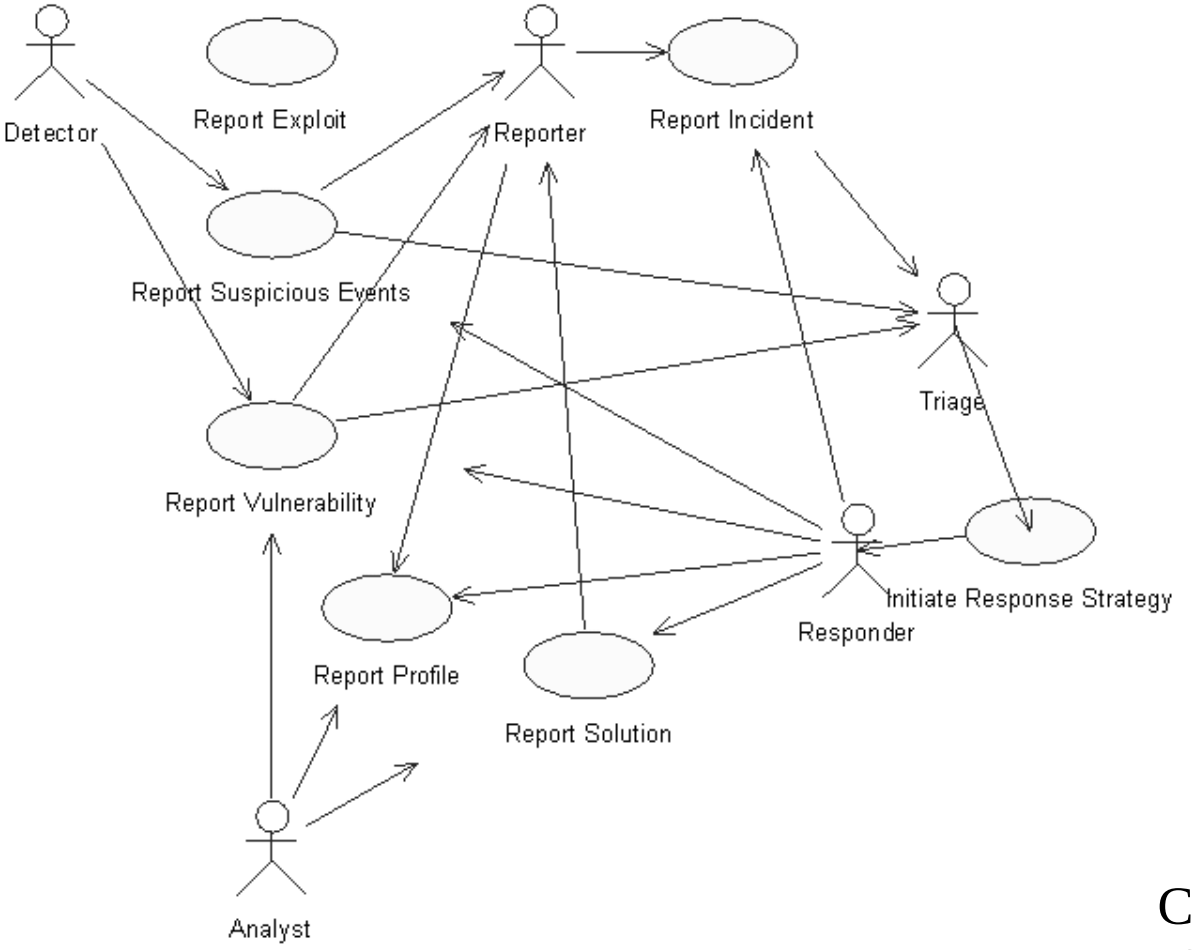
Work in development by Jan Meijer

Litton-TASC: Incident Response Use Case



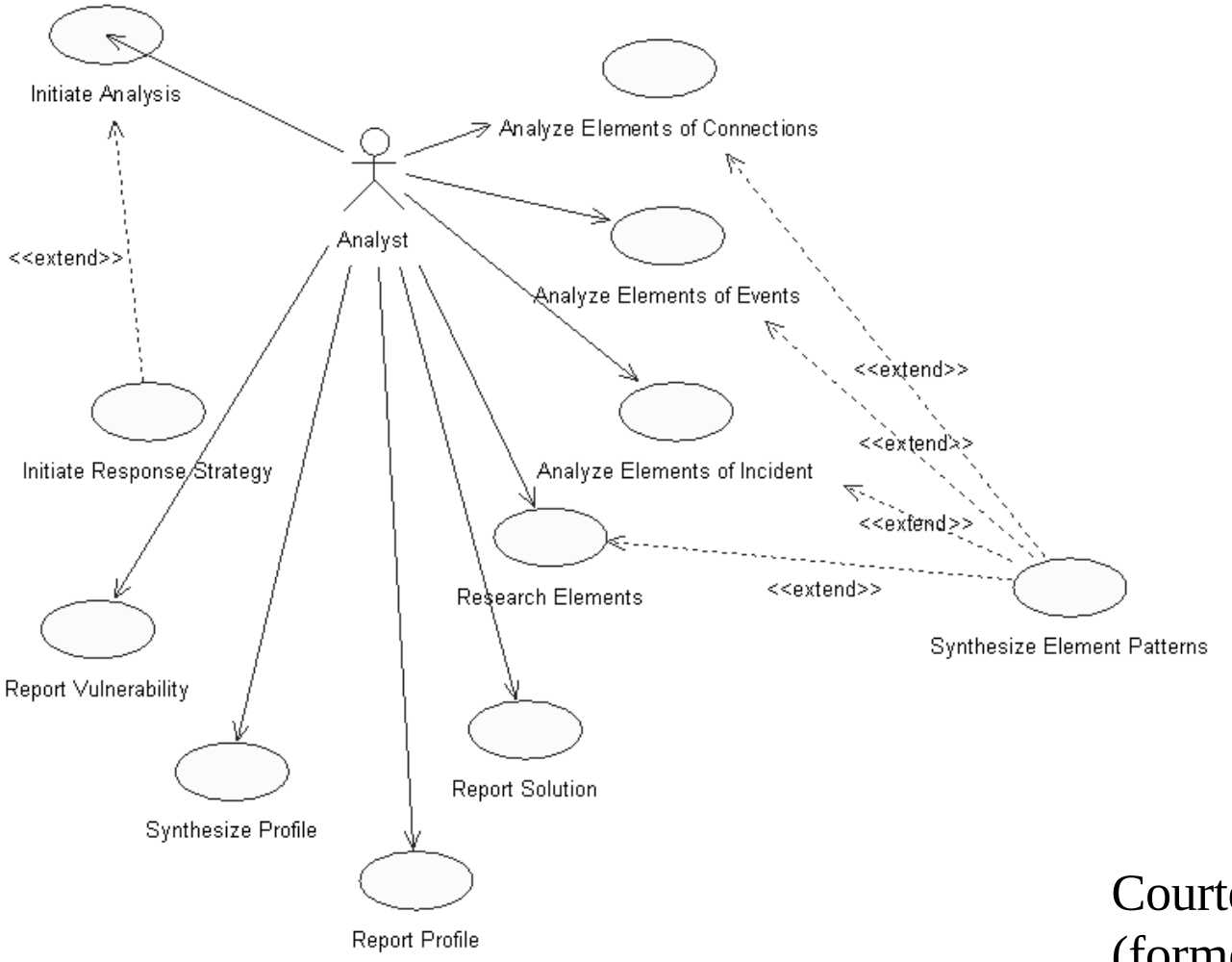
Courtesy of William Rice (former Litton-TASC)

Litton-TASC: Incident Reporting Use Case



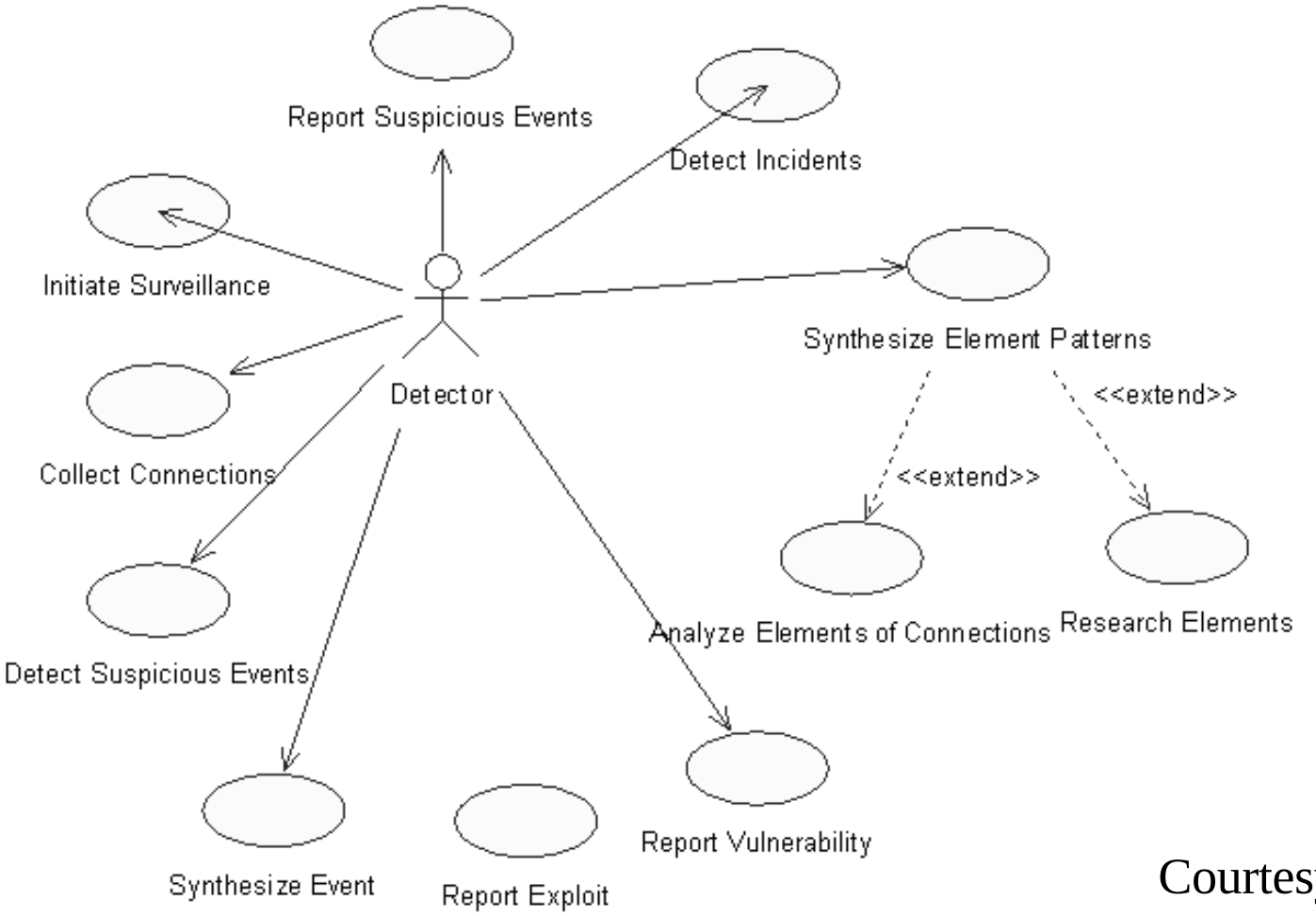
Courtesy of William Rice
(former Litton-TASC)

Litton-TASC: Analyze Incidents Use Case



Courtesy of William Rice
(former Litton-TASC)

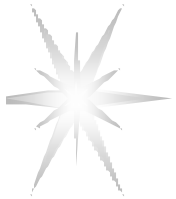
Litton-TASC: Detect Events Use Case



Courtesy of William Rice
(former Litton-TASC)

IDWG Scope and IDMEF Documents

- IDMEF is for Intrusion Detection Systems
  - Main actors - IDS
  - Root element – Alert
    - Short life history
  - Data collected automatically
- Currently on the IETF IDWG std process
  - IDMEF Requirements draft-…-04.txt
  - IDMEF XML DTD and Data Model
  - IDMEF ANS.1 MIBII format – not recommended by IDWG
  - IDMEF transfer protocol - IDXP (XML/BEEP based)
  - Intrusion Alert Protocol (IAP) – not recommended by IDWG
- Design Team and Pilot implementations of XML and MIBII based IDMEF



Pilot implementation of the IDMEF

Design Team: Silicon Defense, ISSS, France Telecom

- **libidmef 0.6** complies with the latest version of the IDMEF specification (0.3), and has a number of fixes and enhancements:
  - More accurate representation of NTP timestamps
  - Revised I/O functionality
  - Compliance with the latest version of **libxml (2.3.9)**
  - Installation as a shared library
- Upcoming release of the next IDMEF XML plugin for the **Snort IDS**
  - It will provide support for the SPADE anomaly detection plugin, as well as the portscan plugin
- IDWG message transfer protocol
  - IDXP should become the IDWG message transfer protocol and will be forwarded as a Proposed Standard RFC
    - IDXP is BEEP based
    - TUNNEL Profile is needed for IDXP to fulfill all the IDWG requirements
  - IAP should NOT be forwarded as an RFC of any kind.

Relation between IDMEF and IODEF

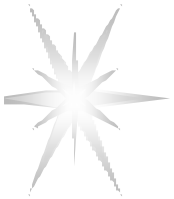
Initial requirements/suggestions:

1. IODEF should be compatible with IDMEF and be capable to use/include IDMEF message into IO, e.g. as or inside of IncidentAlert IO class.

However, backward compatibility is not required, i.e. it's not necessary that IODEF message is understood by IDS (or other automatic system?)

2. If some elements or attributes intersect, options should be considered:
   - change name in IODEF or
   - ask IDWG to consider changing name in IDMEF

Request for comments to ITDWG and IDWG
http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/iodef-idmef-xmldtd-00-rfc.html



IDMEF vs IODEF: (1)

1. Reuse (confirmed) IDMEF to generate in a simplest way **IncidentAlert** (message)?

Possible format for IODEF **IncidentAlert**:

- Some Data
- Authority created IO
- AdditionalData containing **IDMEF**

To Be Considered.

Ask IDWG about lifetime of IDMEF: What happen with confirmed Intrusion?

IDMEF vs IODEF: (2)

4. Compare **(target, source)/IDMEF** and **(target, source)/IODEF.**

Does **source/IDMEF** cover/equal to **Attacker/IODEF?**

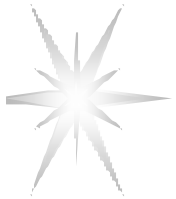
The **Target class** contains information about the possible target(s) of the event(s) that generated an alert. An event may have more than one target (e.g., in the case of a port sweep).

The Target class is composed of four aggregate classes: **Node, User, Process, Service**

The **Source class** contains information about the possible source(s) of the event(s) that generated an alert. An event may have more than one source (e.g., in a distributed denial of service attack).

The Source class is composed of four aggregate classes: **Node, User, Process, Service**

O.K. to reuse



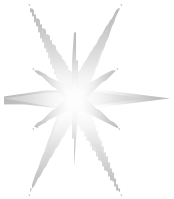
IDMEF vs IODEF: (3)

5. Definition of **impact/IDMEF**

Impact (Optional). The evaluated impact of the event(s) leading up to the alert on the target. The permitted values for this attribute are shown below. The default value is "unknown".

```
<!ENTITY % attvals.impact              "
    ( unknown | bad-unknown | not-suspicious | attempted-admin |
      successful-admin | attempted-dos | successful-dos |
      attempted-recon | successful-recon-limited |
      successful-recon-largescale | attempted-user |
      successful-user )
  ">
```

O.K. to reuse.



IDMEF vs IODEF: (4)

6. IDMEF uses **detectTime/IDMEF**.

The DetectTime class is used to indicate the date and time the event(s) producing an alert was detected by the analyzer. In the case of more than one event, the time the first event was detected.

(This may or may not be the same time as CreateTime; analyzers are not required to send alerts immediately upon detection).

The DetectTime class has one attribute: **ntpstamp** representing the same date and time as the element content.

Can be adopted. TBC.

Consider including element **registrationTime/IODEF**

IDMEF vs IODEF: (5)

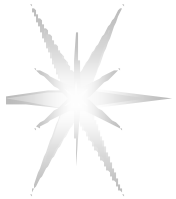
7. It seems that name "**datetime**" is commonly used in XML world but IDMEF use "**date-time**" with dash.

Date-time strings are represented by the **DATETIME data type**. Each date-time string identifies a particular instant in time; ranges are not supported.

Date-time strings are formatted according to a subset of ISO 8601:2000, as show below. Section references in parentheses refer to sections of the ISO 8601:2000 standard.

O.K. to adopt.

Comment to IDWG to change to **datetime**.



IDMEF vs IODEF: (6)

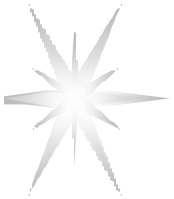
8. IDMEF intends to define tool of the attack by element **ToolAlert**

ToolAlert is subclass of **Alert**.

The **ToolAlert** class carries additional information related to the use of attack tools or malevolent programs such as Trojan horses, and can be used by the analyzer when it is able to identify these tools. It is intended to group one or more previously-sent alerts together, to say "these alerts were all the result of someone using this tool."

The **ToolAlert** class is composed of three aggregate classes: name, command, **alertident**.

No suggestions (Not applicable for IODEF?)



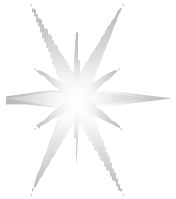
IDMEF vs IODEF: (7)

9. Reuse definition of “**Alertident**” for extended identification of **Incidents**.

AlertIdent - the list of alert identifiers that are related to this alert. Because alert identifiers are only unique across the alerts sent by a single analyzer, the optional "analyzerid" attribute of "alertident" should be used to identify the analyzer that a particular alert came from. If the "analyzerid" is not provided, the alert is assumed to have come from the same analyzer that is sending the ToolAlert.

Not clear at IDMEF specification.

Not applicable for IODEF?



IDMEF vs IODEF: (8)

10. Check definition of “**user**” and “**userId**” in IDMEF.

The **User class** is used to describe user that is receiving the event(s). It is primarily used as a "container" class for the **UserId** aggregate class.

The **UserId** class provides specific information about a user. More than one **UserId** can be used within the User class to indicate attempts to transition from one user to another, or to provide complete information about a user's (or process') privileges.

The **UserId** class is composed of two aggregate classes: **name, number**.

User class in IDMEF is not clearly defined: Comment to IDWG.

Do we need “**user***” element in IODEF?

- In addition to Victim?

IDMEF vs IODEF: (9)

11. IDMEF doesn’t contain elements **Attack** and **Vulnerability** because

- **Attack** is a confirmed **Intrusion** that is being handled by CSIRT/humans

- **Vulnerability** is covered by **Classification** element.

However, it looks a bit indefinite as sub-element of

<!ELEMENT Alert (

Analyzer, CreateTime, DetectTime?, AnalyzerTime?, Source*, Target*, **Classification+**, ToolAlert?, OverflowAlert?, CorrelationAlert?, AdditionalData*)>

The **Classification class** provides the "name" of an alert, or other information allowing the manager to determine what it is (for example, to decide whether or not to display the alert on-screen, what color to display it in, etc.).

The **Classification class** is composed of two aggregate classes: **name** (of vulnerability), **url**.

TBC: What’s the relation between **Alert** and **Attack?**

IDMEF vs IODEF: (10)

13. Check definition of "**classification**" in IDMEF.
    Does it mean known/registered **vulnerability?**

<Classification origin="bugtraqid">
<name>629</name>
<url>http://www.securityfocus.com</url>
</Classification>

Classification class is not clearly defined.

Is it related to Vulnerabilities, Exposure or Attacks? If latter, what's the definition of attack?

IDMEF vs IODEF: (11)

14. Check definition of **method/IDMEF**

IDMEF: Service>webservice>method

The HTTP method (PUT, GET) used in the request

<!ELEMENT WebService (url, cgi?, method?, arg*)>

Contact IDWG to change **method** to **httpmethod**: Using generic term ***method*** is not good in general.

<!ELEMENT Method (Vulnerability, Evidence)>

Otherwise: Consider changing/redefining **Method/IODEF** and/or moving:

- **Vulnerability** to **Attack** and
- **Evidence** to Top level elements/classes or to **AdditionalData**

IDMEF vs IODEF: (12)

15. Consider reusing the following terms from IDMEF:

- **size -** sub-element of **OverflowAlert**
  - N/A
- **number -** sub-element of **userId**
  -
- **url -** (exactly one string)– used in **classification, WebService**
  - O.K.
- **location –** sub-element of **node (location, name address)**
  - Not clearly defined.
- **name –** has diverse number of definitions**:**
  - **name** of a particular tool in **ToolAlert**, **name** of equipment in **node**, **name** of the alert in **Classification** from one of the known origins, etc. Meaning depends on place in IDMEF hierarchy.

  - Not clearly defined.