Incident Object Description and Exchange Format

TF-CSIRT at TERENA

IODEF Editorial Group

Jimmy Arvidsson <Jimmy.J.Arvidsson@telia.se>
Andrew Cormack <Andrew.Cormack@ukerna.ac.uk>
Yuri Demchenko <demch@terena.nl>
Jan Meijer <jan.meijer@surfnet.nl>

TeliaCERT CC
Phone: +46 8 713 1872
Fax: +46 705 171 201
E-mail: tcert@telia.se

TELIA

3.2 Incident Description Terms

- Attack
- Attacker
- CSIRT
- Damage
- Event
- Evidence
- Incident
- Impact
- Target
- Victim
- Vulnerability

Purpose:
To define IODEF use and meaning of these terms

Other terms: alert, activity, IDS, Security Policy, etc

References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
- [2] **Incident Taxonomy and Description Working Group Charter** - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/
- [3] Intrusion Detection Exchange Format Requirements by Wood, M. - October 1999. -
- [4] Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition by D. Curry - March 2000 - http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-01.txt
- [5] Guidelines for Evidence Collection and Archiving by Dominique Brezinski, Tom Killalea - July 2000. -
- [6] **RFC 2828. Internet Security Glossary** by R. Shirey. May 2000. -
- [7] **NIST 800-3 Establishing a Computer Security Incident Response Capability (CSIRC).** - November 1991
- **[8] Best Current Practice of incident classification and reporting schemes currently used by active CSIRTs** - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/BCPreport1.rtf
- [9] Multilingual Support in Internet/IT Applications -
- [10] **A Common Language for Computer Security Incidents**; John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667]
- [11] **The Oxford Reference Dictionary**; Oxford University Press, 1986
- [12] **RFC 2350; Best Current Practice; Expectations for Computer Security Incident Response**; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, June 1998

TELIA

Attack vs Attacker

- Attack

An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Attack can be active or passive, by insider or by outsider, or via attack mediator.

- Attacker

Attacker is individual who attempts one or more attacks in order to achieve an objective(s) [Sandia].

For the purpose of IODEF attacker is described by its network ID, organisation which network/computer attack was originated and physical location information (optional).

Target vs Victim

- Target

A computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).

- Victim

Victim is individual or organisation which suffered the incident which is described in incident report.

For the purpose of IODEF victim is described by its network ID, organisation and location information.

Vulnerability

- Vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds.

Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

Damage vs Impact

- Damage

An intended or unintended consequence of an attack which affects the normal operation of the targeted system or service.

In IODEF the description of damage may include free text description of actual result of attack, and, where possible, structured information about the particular damaged system, subsystem or service.

- Impact

Impact describes result of incident expressed in terms of user community, for example the cost in terms of financial or other disruption

Evidence

- Evidence

Evidence is information relating to an event that proves or supports a conclusion about fact of it has occurred, i.e. evidence could be information relating to a security incident, as a computer intrusions, that proves or supports a conclusion about fact of malicious use or attack.

It may include but is not limited to: data dump created by Intrusion Detection System (IDS), data from syslog file, kernel statistics, cache, memory, temporary file system, or other data that caused the alert or were collected after the incident happened.

Special rules and care must be taken when collecting and archiving evidence, particularly to preserve its integrity. When necessary evidence should be stored encrypted.

According to Guidelines for Evidence Collection and Archiving (Evidence) evidence must be strictly secured. The chain of evidence custody needs to be clearly documented.

Event vs Incident

- Event

An action directed at a target which is intended to result in a change of state (status) of the target" [(IEEE96:373) Sandia]. This could be **any** observable occurrence in a system or network.

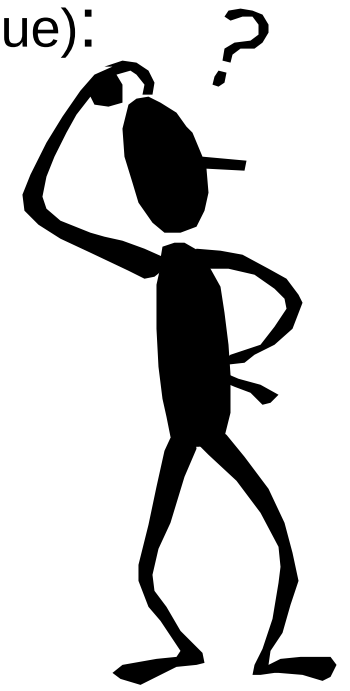
- Incident

The definition of an incident varies between professions, organisations and people. In order to make use of a common and sound vocabulary regarding incident handling within the IT area the following definitions are used.

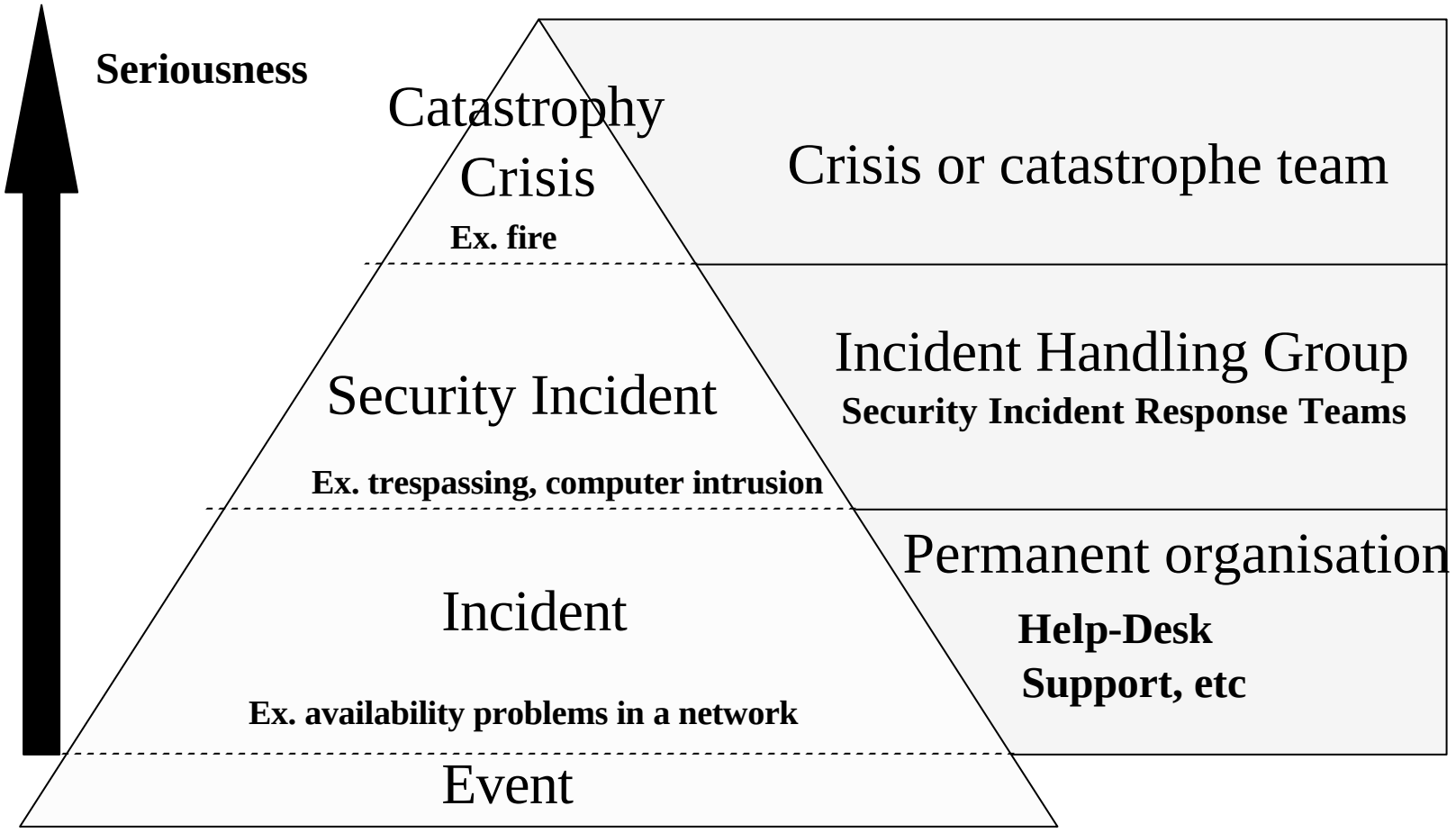
Incident is a root/key element of the discussed IODEF. Incident object data model is described by separate document.

Detailed Examination Of Incident

- The use of the same granularity and preciseness in terms gives us (as a recipient/collegue):
  - guidance of the severity and scope
  - indication of the need for speed
  - efforts of countermeasures
  - possible costs involved



The pyramid of Events



Incident

- Incident

An incident is an event that might lead to an accident or an accident which is not to serious.

This matches well both Oxford and Longman dictionaries, which have these definitions ”*something unusual, serious, or violent that happens*” [Longman] or “*an event or occurrence, especially a minor one*” [Oxford]. An incident may be escalated (reassessed) if it has a more serious impact, i.e. it may be escalated to a security incident, crisis or a catastrophe.

In the IT area, an incident may be availability problems in a network, a zone transfer or computer virus on a single workstation. Normally, we have established units handling incidents daily. These units are a part of the permanent organisation, i.e. help-desk or support units. They are trained to handle incidents and this has become a normal issue in their working day.

Security Incident

- Security Incident

A security incident is an event that involves a security violation. This may be an event that breaks a security policy, UAP, laws and jurisdictions, etc.

A security incident is worse than an incident as it affects the security of or in the organisation. A security incident may be logical, physical or organisational, for example a computer intrusion, loss of secrecy, information theft, fire or an alarm that doesn't work properly. A security incident may be caused on purpose or not. The latter may be if somebody forgets to lock a door or forgets to activate an access list in a router.

This can be narrowed to cover only the IT sector, i.e. security incidents that happens in the IT sphere is called IT-security incidents.

Security Incident

- Other definitions:

NIST declares in the document “Establishing a Computer Security Response Capability” that a security event as “*any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability*”

The “ Internet Security Glossary”[6] states that a security incident is “*A security event that involves a security violation” meaning that “a security-relevant system event in which the system's security policy is disobeyed or otherwise breached*”. This RFC also states that the definition in RFC2350 should not be used "*Any adverse event which compromises some aspect of computer or network security*." [RFC2350] because:

“(a) a security incident may occur without actually being harmful (i.e., adverse) and
(b) this Glossary defines "compromise" more narrowly in relation to unauthorized access”.

This leads us to the definition of a security incident that “*a security incident is any adverse event whereby some aspect of security could be threatened*”. This definition is the same that NIST has declared in the document “Establishing a Computer Security Incident Response Capability (CSIRC)”

IT Security Incident

- IT Security Incident

The Handbook for Computer Security Incident Response Teams (CSIRTs) defines an IT security incident as ”*any real or suspected adverse event in relation to the security of computer or computer networks. Examples of such are: intrusion of computer systems via the network, occurrence of computer viruses or probes for vulnerabilities via the network to a range of computer systems*” [Howard et al].

Typical security incidents are, within the IT area, a computer intrusion, a denial-of-service attack, information theft or data manipulation, etc . This recommendation is proposed by the Internet Security Glossary [RFC 2828] which also recommend not to use the definition proposed in [RFC 2350] which declares a computer security incident as ”*any adverse event which compromises some aspect of computer or network security*."

Howard's events

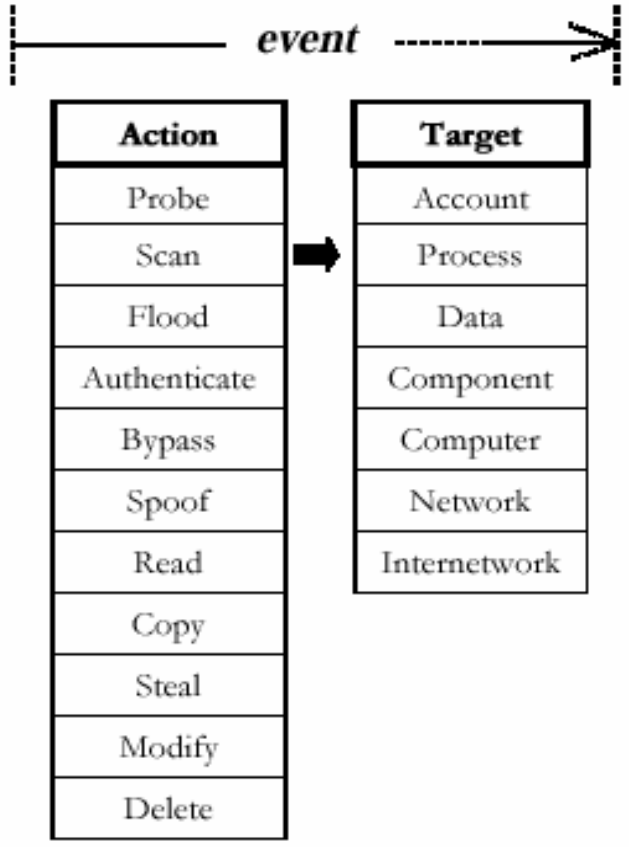


Figure 5.1. Computer and Network Events

Howard's attacks

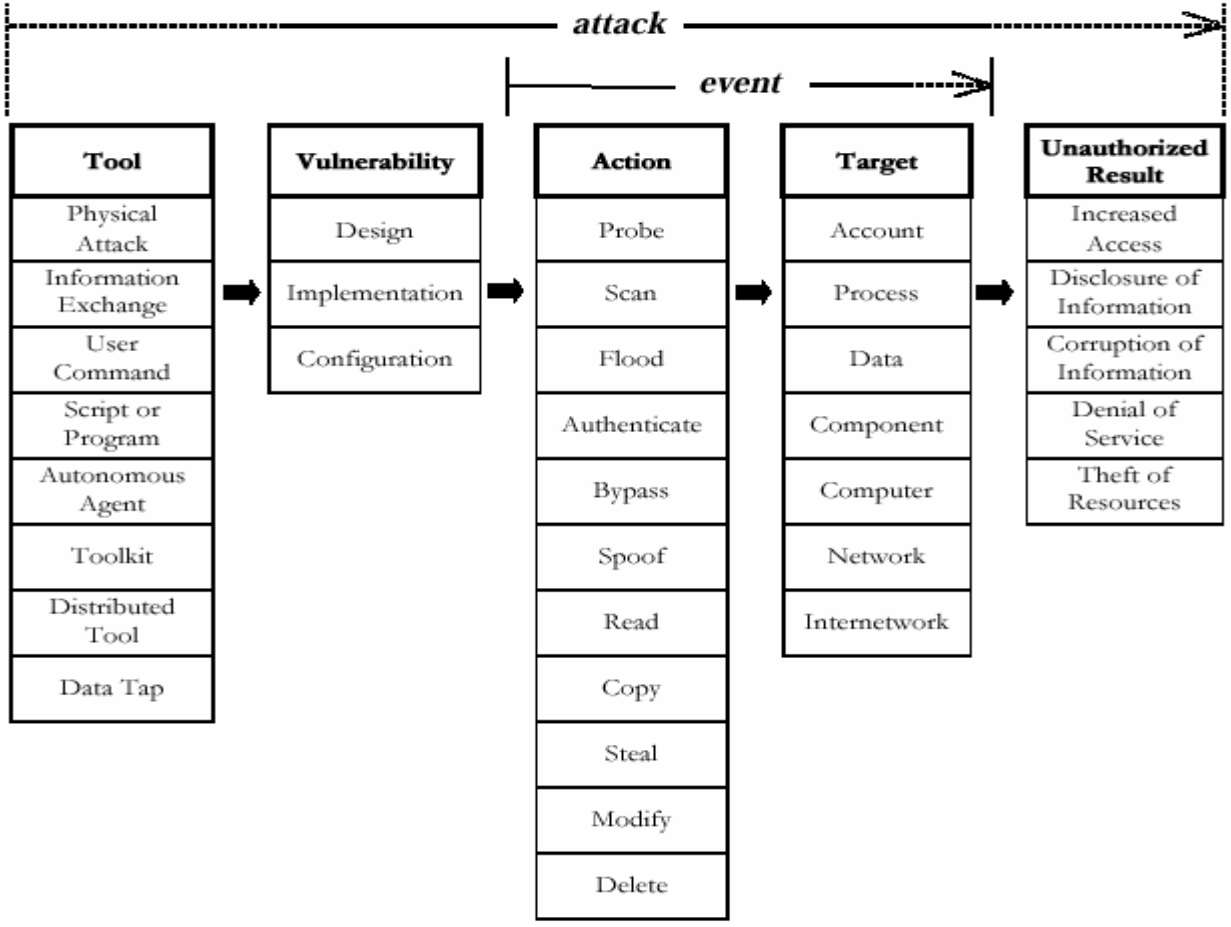


Figure 5.2. Computer and Network Attacks

Howard's scheme

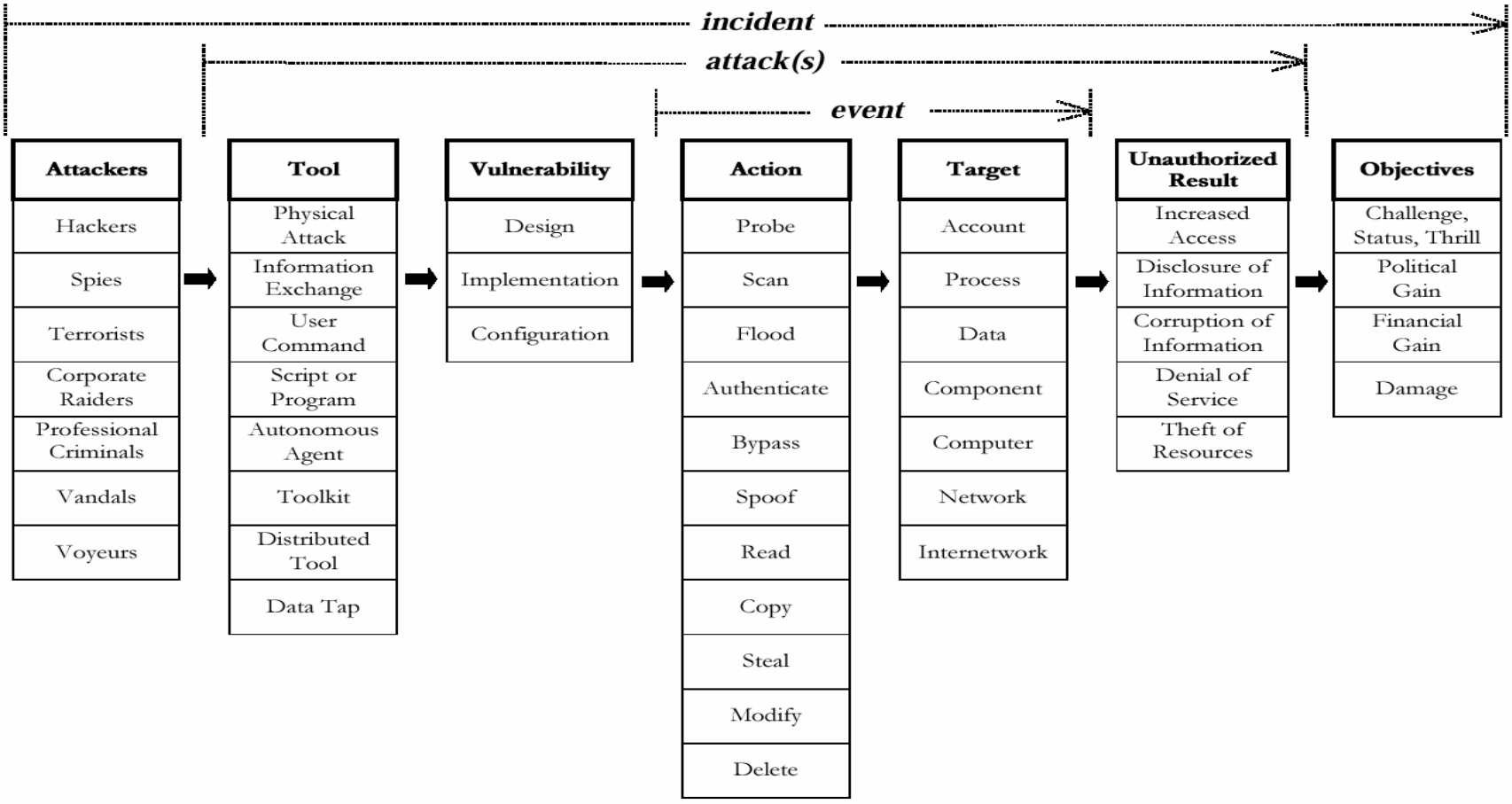


Figure 5.4. Computer and Network Incident Taxonomy

Example: IT Security Incidents

- Malicious Software:
  Computer Viruses, Trojan Horses, Computer Worms, Logical Bombs etc.
- Misuse of System & Services:
  Spamming, Flooding, Abusive Content
- Mapping:
  Scans and Probes
- Computer Sabotage and Damage
- Computer Intrusions
- Information Theft and Espionage

Incident (conclusion)

- Incident

Note that the overall and general term incident is used by IODEF, instead of the more precise IT security incident. This choice of terms depends heavily on the fact that far from all organisations have stated an incident handling policy, in which incident taxonomy is described or referred.

By using the broader term INCIDENT, IODEF does not discriminate or disregard organisations that do not make use of the difference in taxonomy.

Although it is most likely that CSIRTs focussing in handling IT security incidents only.