Communication

# Naming

Name: Open Security Incident Database

Short Form: OSIDB

Domain: osidb.org

Website: www.osidb.org:3000

Email: opensecurityincidentdb@gmail.com

Google Group: Open Security Incident Database

Twitter: osidb

RSS Feed: http://www.osidb.org:3000/feed

# Data Model

Incident

* ID
* Name
* Summary
* Reviewed
* Classification & Description
  + Victim
  + Attacker
  + Attack
  + Target
  + Weakness
  + Country
* Events
  + Sources

|  |  |
| --- | --- |
| **Attacker-Types** | **Description** |
| Internal Accidental | An internal attacker without malicious intent that is/was in a trusted relationship to the victim. This relationship is typically described as an employee or contractor. Through the trusted relationship the attacker had at least partially authorized access to the IT environment. |
| Internal Malicious | An internal attacker with malicious intent that was in a trusted relationship to the victim. This relationship is typically described as an employee or contractor. Through the trusted relationship the attacker had at least partially authorized access to the IT environment. |
| Organized Crime | An organization that systematically aims to make profit with illegal activities. |
| Activist | An attacker that tries to achieve a goal based on his personal believes like moral, politics, culture or religion. |
| Criminal Hacker | An attacker that acts on his own without being part of an organization. |
| Script Kiddie | Usually a young less skillful attacker using techniques he does not fully understand. |
| State Level | A state level (or structured) attacker that acts on behalf of a government. These are usually intelligence services, information operations units. |
| Multiple | Attacker that consists of multiple attacker-types. |
| Unknown | Unknown attacker type. |
| Other | Other, in this list not available attacker type. |

|  |  |
| --- | --- |
| **Victim-Types** | **Description** |
| Finance |  |
| Industry |  |
| Government |  |
| Education |  |
| Retail |  |
| NGO |  |
| Consumer |  |
| Telecommunication |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Target-Types** | **Description** | **Notes** |
| Access Credentials | Any kind of credentials that can be used to access applications, services and systems. | What if they are hashed or encrypted? What if weak or strong crypto is used? |
| Payment Data – General | Any kind of that that can be used to retrieve money or to perform payments. |  |
| Payment Data – Credit Card Data | Credit card data. |  |
| Personal Identifiable Data – General | Data that can be linked to a person. |  |
| Personal Identifiable Data – Sensitive | Highly sensitive data that can be linked to a person. These are typically: information about health, religion or personal believes, social security, criminal prosecution and larger collections of general personal identifiable data that has a profile character. |  |
| Critical Infrastructure | Infrastructure that is important for a country or society because the country’s well being heavily depends on it. Be it because it delivers important resources like electricity or oil or because it may vitally threaten a country when not working properly (i.e. atomic power plant). |  |
| Source code | Non-public source code. |  |
| Confidential Data | Any kind of confidential data that does not fit into the other categories. |  |
| Multiple | Multiple target types. |  |
| Unknown | Unknown target types. |  |

|  |  |
| --- | --- |
| **Attack-Types** | **Description** |
| Website Penetration | Penetration through exploiting websites. |
| Application/Service Penetration | Penetration through exploiting applications (SAP, etc.) or services (web server, database, middleware, etc.). |
| System Penetration | Penetration through exploiting systems (operating system, libraries, utilities, etc.). |
| Malware | Use of malware to persist attack or to steal data. |
| Theft | Theft of IT equipment. |
| Loss | Losing IT equipment. |
| Communication Interception | Intercepting any kind of communication. |
| Simple Access | Simply accessing a system or data without necessarily exploiting vulnerability. |
| Denial of Service | Simple or distributed denial of service |
| Sabotage | Manipulation with the intention of damaging an environment. |
| Multiple | Attack containing multiple attack types. |
| Unknown | No Information about attack available. |
| Other | Other, in this list not available attack. |

|  |  |
| --- | --- |
| **Weakness-Types** | **Description** |
| Vulnerability |  |
| Misconfiguration |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Event-Sources** | **Description** |
| Victim |  |
| Involved Vendor |  |
| Press |  |
| Attacker |  |
| Professionals/Analysts |  |
| Law Enforcement / Government |  |
| Other |  |