National Forensic Sciences University

An Institution of National Importance
Ministry of Home Affairs, Government of India

Incident Response Management & Threat Intelligence

Data Classification

Presented By:
Mr. Ramya Shah
Assistant Professor,
SCSDF, NFSU


SP
REC
MENU

Data

- In general, data is any set of characters that has been gathered and translated for some purpose, usually analysis.
- It can be any character, including text and numbers, pictures, sound, or video.
- Raw data describes the facts and figures that a company processes every day.

Data Classification

- Data classification is one of the most important steps in data security.
- Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data.
- That's why it's important to classify your data based on how sensitive or valuable it is

Data Classification

Common data classifications include

- Highly Confidential
- Sensitive
- Internal Use Only
- Public

Data Classification

Highly Confidential

- This classification applies to the most sensitive business information that is intended strictly for use within your company.
- Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term.
- It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, etc.

Data Classification

Sensitive

- This classification applies to sensitive business information that is intended for use within your company, and information that you would consider to be private should be included in this classification.

- Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.

Data Classification

Internal Use Only

- This classification applies to sensitive information that is generally not accessible by a wide audience and is intended for use only within your company.

- While its unauthorized disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact your company, employees, business partners, vendors and the like.

Data Classification

Public

- Basically any information that requires no special protection or rules for use

CIA

- Confidentiality, Integrity, Availability
- A model designed to guide policies for information security within an organization
- Considered the three most crucial components of security

CIA

Confidentiality

- Equivalent to privacy
- A set of rules that limits access to information
- Designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it

i.e. Data Encryption, User ID & Password, Two-Factor Authentication, Biometric lock system

CIA

Integrity

- It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people
- i.e. File Permissions, Access Control, Checksums

CIA

Availability

- A guarantee of reliable access to the information by authorized people whenever required
- Best ensured by maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment
- i.e. Load Balancing, Back-up Servers

AAA

Concept relating to the people who use that information

- Authentication
- Authorization
- Non-repudiation

AAA

Authentication

- Authentication is a process of identifying the person before accessing the system.
- It allows user to access the system information only if authentication check got passed.
- Apart from Username & password combination, the authentication can be implemented in different ways like asking secret question and answer, OTP (One Time Password) over SMS, biometric authentication, Token based authentication like RSA Secure ID token etc.

AAA

Authorization

- Once the Authentication passed the Authorization comes in the picture to limit the user as per the permission set for the user.
- The Authorization is generally implemented on Access control list, user role based, user group based and define the permissions & restrictions to specific user group or granting or revoking the privileges for the users.

Access Control

Access control is the selective restriction of access to some kind of resource (a folder, a file, and a device).

There are different types of approaches to access control.

- DAC
- MAC
- RBAC
- MLS

Access Control : DAC

- Discretionary Access Control
- Every user can decide who can, with which permission,read his/her files.

Access Control : MAC

- Mandatory Access Control
- The administrator decides the security policy and all the files in the system will comply

Access Control : RBAC

- Role Based Access Control
- The permissions are not granted per user, but according to the role
- This allows big organizations to assign permission to roles and roles to users, making it easier to create, modify or delete users.

Access Control : MLS

- Multi Level Security
- Each user has a trust level and each item has a confidentiality level.
- The administrator is still the one who is in charge or creating the security policy, as in MAC systems, but the system will ensure that each user will only see the items that have a confidentiality level allowed to him based on some system configurations and the user trust level

Access Control : Non-Repudiation/Accountability

- Tracking who is accessing the systems and which of the requests were denied along with additional details like the Timestamp and the IP address from where the requests came from.

- Means confirmation sent by receiver to sender that the requested services or information was successfully received as Digital confirmation e.g. Digital Certificates, this not only serves as acknowledgement but also helps to validate both sender and receiver is genuine.

Sign of Incidents

“Precursors” and “indicators” – signs of an incident

- Most attacks do not have any identifiable or detectable precursors from the target’s perspective.
- If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack.

Sign of Incidents

“Precursors”

- Precursors can be used to prevent incident from occurring.
  - (by e.g. blocking the source of vulnerability scanning)

Common Examples :

- Web server log entries that show the usage of a vulnerability scanner.
- An announcement of a new exploit that targets a vulnerability of the organization’s mail server.
- A threat from a group stating that the group will attack the organization.

Sign of Incidents

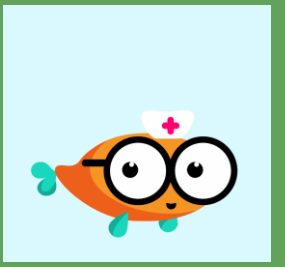
“Indicators”

- Precursors are Rare, but Indicators are all too common.

Common Examples :

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.

Incident Category



Incidents are divided generally into 3 Categories:

1. High
2. Medium
3. Low

Incident Category

Category : High

The severity of a security incident will be considered “high” if any of the following conditions exist:

- Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire UNIT is affected)
- Poses a potential large financial risk or legal liability to the Organization.
- Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information).

Incident Category

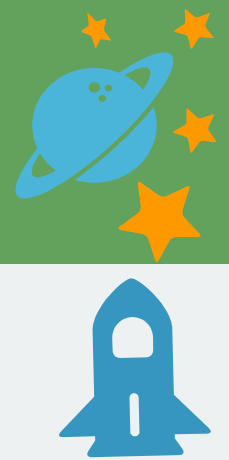
Category : High

- It adversely impacts an enterprise system or service critical to the operation of a major portion of the organization (for example, e-mail, customer information system, Financial information system, human resources information system, etc.).

- It poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.

- It has a high probability of propagating to many other systems on premise and/or off premise and causing significant damage or disruption.

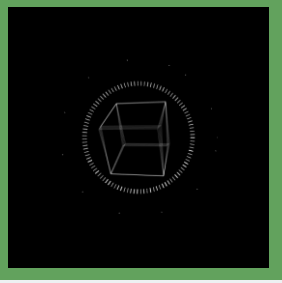
Incident Category



Category : High

- High severity incidents require an immediate response and focused, dedicated attention by the CISO and other appropriate officials and IT security staff until resolved.

Incident Category

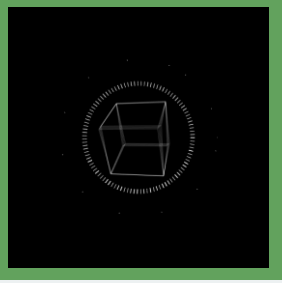


Category : Medium

The severity of a security incident will be considered “medium” if any of the following conditions exist:

- Adversely impacts a moderate number of systems and/or people, such as an
  - individual department, unit, or building
- Adversely impacts a non-critical enterprise system or service
- Adversely impacts a departmental system or service, such as a departmental file server

Incident Category



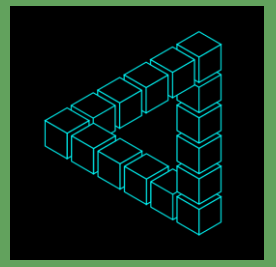
Category : Medium

The severity of a security incident will be considered “medium” if any of the following conditions exist:

- Disrupts a building or departmental network
- Has a moderate probability of propagating to other systems on premise and/or off premise and causing moderate damage or disruption

Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident.

Incident Category

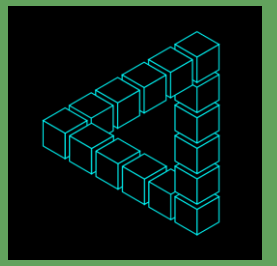


Category : Low

The severity of a security incident will be considered “low” if any of the following conditions exist:

- Adversely impacts a very small number of systems or individuals
- Disrupts a very small number of network devices or segments
- Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

Incident Category



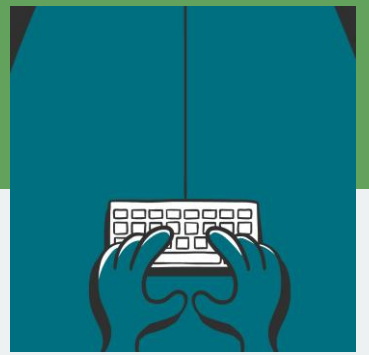
Category : Low

- Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day.

Identify an Incident

HOW WILL YOU IDENTIFY AN INCIDENT?

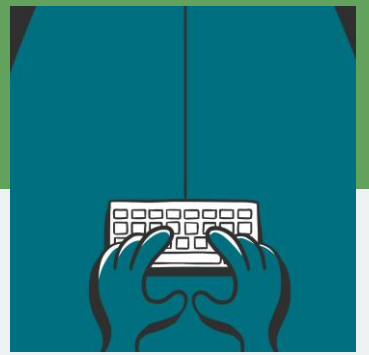
Identify an Incident



Event Management

- Event Management provides qualified alerts when one or more Configuration Items (CI) have have encountered a disruption in its normal functioning or may encounter disruption in its normal functioning. In practice, Event Management may lead to generation of a manual incident OR an automated incident creation.

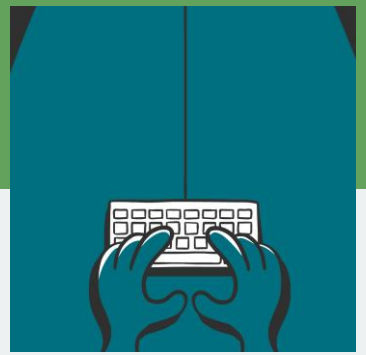
Identify an Incident



From Web Interface

- Web interface is a very efficient method to identify incidents as it involves no human interface to log the ticket. Organization need to provide a intuitive interface to the end users to log incidents.

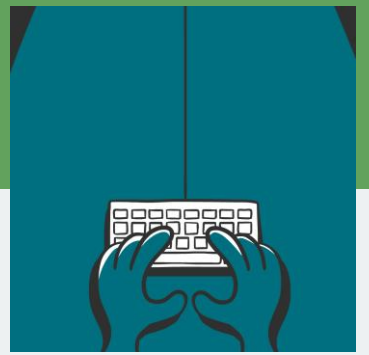
Identify an Incident



From Phone Calls

- Phone calls is the most common way of reporting incidents. This is a labor intensive method to report incidents. However this method has its own merits as end-user incidents can be quickly resolved via First Call Resolution, thus improving customer satisfaction substantially.

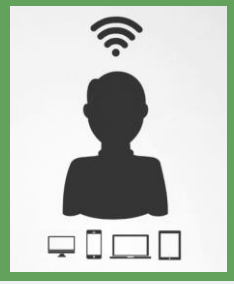
Identify an Incident



From Email Interface

- Emailing incident details to Service Desk is the easiest method to report an incident. However, in most cases, this mode of incident reporting is rigged with lot of inefficiencies.

Identify an Incident

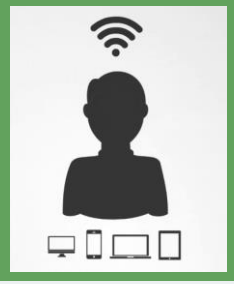


In an MNC, there was a complaint that one of the computers sends out spam messages about women. They checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send spam emails without the computer owner's knowledge.

HOW HAS THE HACKER GOT INTO THE COMPUTER TO SET THIS UP ?

Answer It in Google Form

Identify an Incident



a) Denial of Service might have happened at the server's side which automatically send the spam mails from the attacker's server.

b) Heavy network traffic might have happened which resulted in sending the spam mails.

c) Attacker should have sent many network packets to the server and made it to crash.

d) This must have happened through hacked passwords, out of date patches/updates, no antivirus software or out of data antivirus software

Identify an Incident

According to the common standards / rules on data privacy, name, home address, telephone number, e-mail address are...

Identify an Incident

a) Special Data

b) Sensitive Data

c) Personal Data

d) General Data