Date :.....
MON TUE WED THU FRI SAT SUN
☐ ☐ ☐ ☐ ☐ ☐ ☐

Name : Krishnaraj P. Thadesar Subject : ARP
Date : 15th April 2025 PRN : 1032210888
Batch : A1

CCA Assignment 2

Q.1. Describe the Incidence object description format and how it helps in Incidence response.

→ IODEF is an XML based standard for sharing cybersecurity incident data (eg. Attack details, impact) between organizations CERT or security team.

→ Structured elements like :

(A) Incident ID, time, severity & Impact level

(B) Attack methods like (malware, phishing, DDOS)

(C) Contact info of reporting parties

(D) Recommended actions (eg. patches & mitigations)

→ It helps in Incidence response by :

Date :.....
MON TUE WED THU FRI SAT SUN
☐ ☐ ☐ ☐ ☐ ☐ ☐

(A) Standardization : Ensure all parties report interpret data consistently (no ambiguity)

(B) Automation : Enables tools to parse / process incidents faster

(C) Collaboration : Allows global teams / CERT to share threat intelligence

(D) Documentation : Creates a clear audit trail for compliance or post incident analysis

Q.2 Which RFC's are published for the format

(1) RFC 7990 :
using XML as the source for multiple outputs (HTML, PDF, TXT)

(2) RFC 7991 :
Specifies the XML v3 Vocabulary for authoring RFCs ~~Cat~~ enabling structured data.

(3) RFC 7992 : Outlines the HTML format for RFCs, improving web ~~se~~ readability

Date :
MON TUE WED THU FRI SAT SUN

④ RFC 7994 :

Updates plain text RFC requirements, supporting Ascii and limited unicode

⑤ RFC 8650 :

marks the adoption of new formats (XML, HTML, PDFs) for RFCs from 2019 onwards.

Q.3 What are the advantages & disadvantages of the IODEF

→ Advantages :

① Standardization : Ensures consistant incident reporting across teams.

② Automation : Speeds up data sharing via machine readable XML

③ Global collaboration : ~~Used~~ used by CERTs worldwide for threat intelligence

④ Flexibility : Supports custom extension for unique needs.

Date :.....
MON TUE WED THU FRI SAT SUN
☐ ☐ ☐ ☐ ☐ ☐ ☐

Disadvantages:

(1) **Complex XML**: Requires technical expertise to implement

(2) **Post incident focus**: Not ideal for real time threat detection.

(3) **Tool dependency**: Needs compatible software for processing.

(4) **Set up overhead**: Requires RTO for real time communication.