Cybersecurity Incident Report (CIR)
Conceptual Database Design Document

Nathaniel Filer and Gabriel Urbaitis

February 2024

This document outlines a conceptual database design for Cybersecurity Incident Reports (CIRs) that could be used by the Cybersecurity and Infrastructure Security Agency (CISA) to fulfill the requirements of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

1 Cybersecurity Incident Reports

All organizations covered by CIRCIA must report cybersecurity incidents to CISA. These reports will contain detailed information about each incident, and the information will be stored in the CIR database.

When a cybersecurity incident occurs, if it is detected, an individual from an affected organization will fill out a CIR and submit it to CISA. That person will then be listed as the point of contact (POC) for that incident, unless they specify another POC. So at most two people can be associated with any given report. If multiple reports are made about a single incident, there may be multiple POCs for the incident. When any report is made, if it is concerning an unrecorded incident, then a new incident record will be created. Otherwise, an existing incident record will be updated accordingly (some attributes may be automatically updated, but others will be updated by someone who manually reviews reports).

Organizations are either part of the critical infrastructure/private sector, the US Federal Government, a foreign government, a US State, Local, Tribal, or Territorial Government, an Information Sharing and Analysis Center, or they are individuals who, while they aren't technically organizations, can be affected by incidents similarly. An incident may also involve other organizations that are indirectly negatively impacted, or needed for support. The database will keep track of which involved organizations have been notified about the incident.

Information about the narrative and categorization of the incident will be recorded. This will include any specific techniques used by attackers, such as known malware (malicious code) or exploits to common software vulnerabilities. When

malicious code is involved, information about antivirus software installed on the affected machines and the network activity of the virus may also be recorded. The database will also hold information about the impact of the incident, including known relevant details about hosts involved and/or data breached. Some details about the incident, such as specific IOCs (indicators of compromise), are not required in the records, but may be included in the incident narrative, if relevant.

This document presents the conceptual schema for the CIR database. It is organized into four sections. This section, section 1, is the introduction to the scope of the mini-world covered by the database. Section 2 contains the notation and definitions for the conceptual schema as found in the template document. Section 3 describes in detail the conceptual schema following the guidelines found in section 2. Section 4 lists the most important queries that may be posed to this specific database, as well as some additional example queries.

2 Notation and Definitions (taken from Dr. Soraya Abad Mota's template)

The notation used: all upper case for the entity names, lower case for the relationship names, and the first letter capitalized for attribute names.

The description of the entities starts with a sentence which explains their meaning. Then the attributes to describe the instances are included. The relationships are also described by a sentence and a list of attributes if they have them.

Each attribute has a four-letter code which describes the type of attribute according to the four classification criteria for attributes. The format for this code is: (xyzw), where

- x tells that the attribute is simple (S) or composite (C),
- y tells that the attribute has a single value (S) or is multivalued (M),
- z tells that the attribute is primitive (stored) (P) or derived (D), in case it is derived, an explanation of how to deduce it from other attributes or a formula/procedure must be specified, and
- w tells that the attribute is fixed (F) (i. e. it must have a value that is not null) or optional (O), i.e. the domain of the attribute allows the null value.

For example, an attribute that has the SSPF code is a simple attribute with a single value which is primitive and fixed. An example of this kind of attribute could be the Social Security Number (SSN). On the other hand, an attribute with the (CSPO)

code is a composite attribute with a single value, primitive and optional. In this case, the date of birth could be an attribute with this code. If there is a single attribute that has the key constraint, it can be underlined. If the key constraint applies to more than one attribute or if there are several combinations of attributes with the key constraint property it is better to list them separately.

If there are attributes that are very common and are used more than once, they can be defined as general types to be used as the type of each attribute which uses the same format.

3 Conceptual Schema of the CIR Database

The order of presentation of the conceptual schema is:

1. The entities' descriptions, examples, and attributes.

2. The relationships' descriptions and, if they exist, attributes.

3. The EER diagram.

4. The semantic integrity constraints.

3.1 Entities

The entities defined for this database are:

- PERSON
- CONTACT
- INDIVIDUAL
- REPORT
- INCIDENT
- EXPLOIT
- MALWARE
- ANTIVIRUS
- NETWORK ACTIVITY
- IMPACT
- HOST
- DATA
- ORGANIZATION
- CRIT INFR/PRIV SECT
- US FED GOV

- FOREIGN GOV
- SLTT GOV
- ISAC

A detailed description of each entity follows.

PERSON: a person who is the submitter/POC for an incident or is an individual affected by an incident.

Attributes:

- Last_Name (SSPF)
- First_Name (SSPF)
- Phone (SSPF)
- Email (SSPF)

CONTACT: a subclass of Person; someone who submits a report or is the point of contact for a report.

Attributes:

- Job_Title (SSPF)
- Alt_Phone (SSPO)
- Mobile (SSPO)
- Pager (SSPO)
- Fax (SSPO)

INDIVIDUAL: a subclass of person; someone who is affected by an incident as an individual, not as part of an organization.

REPORT: A specific cybersecurity incident report submitted by a contact.

Attributes

- Submission_Date/Time (CSPF)
- Estimated_Recovery_Time_Clock_Hours (SSPO)
- Estimated_Recovery_Time_Staff_Hours (SSPO)
- Estimated_Damage_Accounts ($$$ Loss) (SSPO)

INCIDENT: a specific cybersecurity incident; more than one report may be made about one incident.

Attributes:

- CISA_Incident_ID (assigned upon creation) (SSPF)
- Attack_Start_Date/Time (CSPF)
- Attack_First_Detected_Date/Time (CSPF)
- Incident_Narrative (SSPF)

- Attack_Ended (Y/N) (SSPF)
- Attack_Duration (in hours) (SSPF)
- Observed_Activity_Network_Location (SMPF)
- Attack_Vector (general cause of incident) (SSPF)
- Incident_Type (Phishing, DOS, Password Attack, etc.) (SSPF)
- Suspected_Threat_Actor_Type(s) (SMPO)
- Disclosed_to_Public (Y/N) (SSPF)

EXPLOIT: a subclass of incident that exploits a known software vulnerability that has a CVE (Common Vulnerabilities and Exposures number).

Attributes:

- CVE_ID (e.g. CVE-2019-0709) (SSPF)
- Exploit_Name (e.g. BlueKeep) (SSPO)

MALWARE: a subclass of incident that involves some kind of malware (malicious code).

Attributes:

- Malware_Type (Spyware, Trojan Horse, Worm, etc.) (SSPF)
- Malware_Name (DarkHotel, Emotet, Stuxnet, etc.) (SSPO)
- Signature (SSPO)
- Malware_Description (SSPF)

ANTIVIRUS: an instance of antivirus software that is encountered by malware.

Attributes:

- Antivirus_Name (SSPF)
- Detected_Malware (Y/N) (SSPF)
- Last_Updated (Date) (SSPF)

NETWORK ACTIVITY: an instance of the malware's network activity.

Attributes:

- Port_Number (SSPF)
- Protocol (TCP, UDP, etc.) (SSPF)
- Port_Type (Source or Destination) (SSPF)

IMPACT: details about the specific impact of a specific cybersecurity incident.

Attributes:

- Total_Impacted_Hosts (number) (SSPF)
- Total_Impacted_People (number) (SSPF)
- Total_Impacted_Records (number) (SSPF)
- Functional_Impact (support doc 1, page 4) (SSPF)
- Information_Impact (support doc 1, pages 4-5) (SSPF)

- Recoverability (support doc 1, page 5) (SSPF)
- Severity_Score (SSPF)
- Is_Major (Y/N) (SSPF)
- Potential_Impact (SSPF)
- Remediation_Steps_Taken (SSPO)
- Lessons_Learned (SSPO)

HOST: a specific host or group of hosts (bulk host) included in the impact of an incident.

Attributes:

- IP_Address(es) (SMPF)
- Host_Type (Attacking, Victim, or Both) (SSPF)
- Host_Name (SSPO)
- Affected_OS (SSPO)
- Affected_Application(s) (SMPO)
- Primary_Purpose (User Desktop, Web Server, etc.) (SSPO)

DATA: an instance of more detailed information about impacted data.

Attributes:

- Impacted_Records (number) (SSPF)
- Impact_Type (Access, Exposure, etc.) (SSPF)
- Relevant_Data_Type(s) (SSN, email, etc.) (SMPF)

ORGANIZATION: The union of all entities containing organizations that are either affected by or involved in incidents.

CRIT INFR/PRIV SECT: an organization in a Critical Infrastructure and/or Private Sector.

Attributes:

- Organization_or_Company_Name (SSPF)
- Org_Type (Hospital, University, etc.) (SSPF)

US FED GOV: an agency in the United States Federal Government.

Attributes:

- Federal_Agency (SSPF)
- Fed_Subagency (SSPF)

FOREIGN GOV: an agency in a foreign government.

Attributes:

- Country (SSPF)
- National_CSIRT (Y/N) (SSPF)

SLTT GOV: an agency in a US State, Local, Tribal, or Territorial Government.

Attributes:

- State (SSPF)
- SLTT_Organization_Name (SSPF)
- Organization_Name (SSPO)

ISAC: an organization that is an Information Sharing and Analysis Center.

Example: Financial Services ISAC

Attributes:

- ISAC_Subagency (SSPF)

3.2 Relationships

There are four regular relationships (reports, updates/creates, affects, and involves), five identifying relationships (encounters, attacks_through, causes, includes, and breaches), two overlapping generalization/specializations, and one union in this schema. The regular and identifying relationships are described below.

reports: the relationship between a cybersecurity incident report and the person who submitted it/is the POC for it.

Attributes:

- Reporter_Type (Submitter, POC, or Both) (SSPF)

updates/creates: the relationship between an incident and a report that updates or creates it.

encounters: the relationship between malware and any antivirus it encounters that is installed on the affected machines.

attacks_through: the relationship between malware and the network activity it attacks through.

causes: relationship between an incident and the impact it causes.

includes: the relationship between an incident's impact and the host(s) included in it.

breaches: the relationship between an incident's impact and a specific set of relevant data breached by it.

affects: the relationship between an incident and an organization that is affected by it.

Attributes:

- Primary_Affected_Sector (SSPO*)
- Location (address of incident location for organization) (CSPF)

involves: the relationship between an incident and an organization that is involved with it because it is indirectly impacted, a supporting organization, or both.

Attributes:

- Involvement_Type (Indirectly Impacted, Supporting, or Both) (SSPF)
- Notified (Y/N) (SSPF)

3.2 Semantic Integrity Constraints

*The Primary Affected Sector attribute of the Affects relationship is fixed if the Organization is Crit Infr/Priv Sect, and optional otherwise.

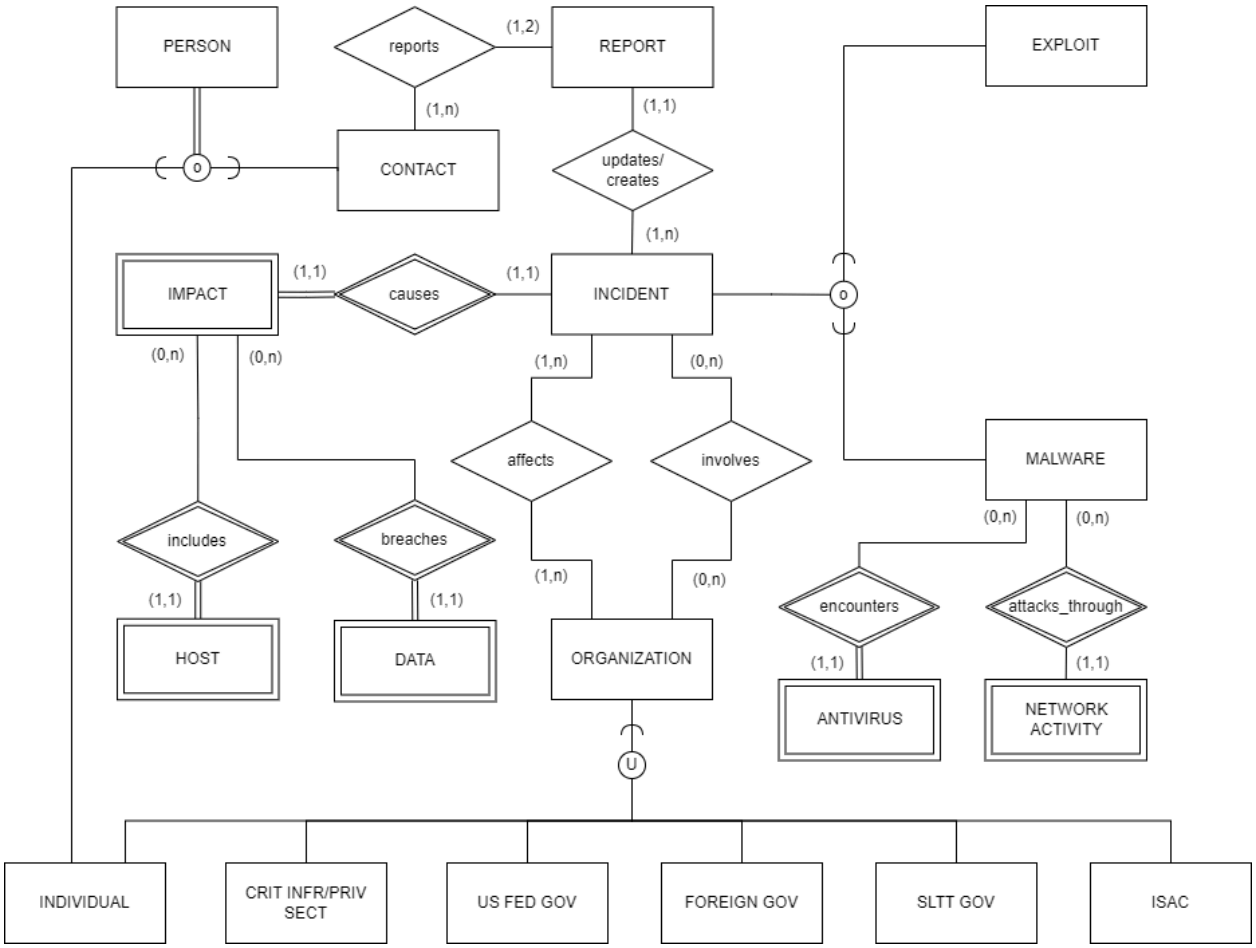

Figure 1: The EER Diagram of the CIR Database

4 Example Queries

1. Kinds of CIR more prevalent at US universities in the past 2 years, 4 years, and 10 years.
2. Statistics of CIRs reported by specific organizations.
3. List the most important cybersecurity incidents that occur in the US in the past year. Most important could mean the number of people or institutions affected, or severity of the attack.
4. Which are new cybersecurity incidents which occurred in the past year.
5. Find a specific cybersecurity incident report given its type, description, and affected organization, or CISA Incident ID number.
6. Find all the cybersecurity incident reports by the malicious code with the same signature.
7. Provide statistics by different criteria of all the CIRs reported in a specific period of time.

8. Summarize all the attacks of a specific type that have occurred to a specific organization or type of organization during their lifetime or in a specific period of time.
9. List all the organizations and their classification (federal, government, tribal, etc.) that have reported cybersecurity incidents, how many and of which kind.
10. List all the cybersecurity incidents which have been reported by type and in descending order of the number of incidents.
11. List all incidents that involved the exploitation of a particular known software vulnerability (CVE).
12. List all incidents that a specific person either submitted a report for, is listed as the POC for, or was affected by as an individual.
13. List incidents where a specific type of data (SSN, for instance) was accessed without authorization, and tell how many records were impacted.
14. Show statistics for attacks utilizing a specific type of malware (Ransomware, for instance), including which antivirus software detected the malware and what kinds of protocols the malware was active in.

5 The Logical Relational Schema (LRS) for the CIR Database

The conceptual schema described for the CIR Database is mapped into the Relational Schema presented in this section. All the attributes underlined in the same Relation belong to the primary key. By default all attributes *may not* be null, unless explicitly specified that they *can* be null.

PERSON (*Email, Last_Name, First_Name, Phone*)

CONTACT (*Email, Job_Title, Alt_Phone, Mobile, Pager, Fax*)
Email is a foreign key referencing *PERSON*
Alt_Phone, Mobile, Pager, and *Fax* may be null.

INDIVIDUAL (*Email, Organization_ID*)
Email is a foreign key referencing *PERSON*
Organization_ID is a foreign key referencing *ORGANIZATION*

REPORT (*Submission_Date, Submission_Time, Submitter_Email, POC_Email, Estimated_Recovery_Time_Clock_Hours, Estimated_Recovery_Time_Staff_Hours, Estimated_Damage_Accounts, CISA_Incident_ID*)

Submitter_Email and *POC_Email* are foreign keys referencing *CONTACT*
CISA_Incident_ID is a foreign key referencing *INCIDENT*
Estimated_Recovery_Time_Clock_Hours, Estimated_Recovery_Time_Staff_Hours, and *Estimated_Damage_Accounts* may be null

INCIDENT (*CISA_Incident_ID, Attack_Start_Date, Attack_Start_Time, Attack_First_Detected_Date, Attack_First_Detected_Time, Incident_Narrative, Attack_Ended, Attack_Duration, Attack_Vector, Incident_Type, Disclosed_to_Public*)

Observed Activity Network Location (*CISA_Incident_ID, Observed_Activity_Network_Location*)

CISA_Incident_ID is a foreign key referencing *INCIDENT*

Suspected Threat Actor Type (*CISA_Incident_ID, Suspected_Threat_Actor_Type*)

CISA_Incident_ID is a foreign key referencing *INCIDENT*

EXPLOIT (*CISA_Incident_ID, CVE_ID, Exploit_Name*)

CISA_Incident_ID is a foreign key referencing *INCIDENT*
Exploit_Name may be null

MALWARE (*CISA_Incident_ID, Malware_Type, Malware_Name, Signature, Malware_Description*)

CISA_Incident_ID is a foreign key referencing *INCIDENT*
Malware_Name and *Signature* may be null

ANTIVIRUS (*CISA_Incident_ID, Antivirus_Name, Detected_Malware, Last_Updated*)

CISA_Incident_ID is a foreign key referencing *MALWARE*

NETWORK ACTIVITY (*CISA_Incident_ID, Port_Number, Protocol, Port_Type*)

CISA_Incident_ID is a foreign key referencing *MALWARE*

IMPACT (*CISA_Incident_ID, Total_Impacted_Hosts, Total_Impacted_People, Total_Impacted_Records, Functional_Impact, Information_Impact, Recoverability, Severity_Score, Is_Major, Potential_Impact, Remediation_Steps_Taken, Lessons_Learned*)

CISA_Incident_ID is a foreign key referencing *INCIDENT*
Remediation_Steps_Taken and *Lessons_Learned* may be null

HOST (*CISA_Incident_ID, Host_Type, Host_Name, Affected_OS, Primary_Purpose*)

CISA_Incident_ID is a foreign key referencing *IMPACT*
Host_Name, Affected_OS and *Primary_Purpose* may be null

IP Address (*CISA_Incident_ID, IP_Address*)

CISA_Incident_ID is a foreign key referencing *HOST*

Affected Application (*CISA_Incident_ID, Application_Name*)

CISA_Incident_ID is a foreign key referencing *HOST*

DATA (*CISA_Incident_ID, Impacted_Records, Impact_Type*)

CISA_Incident_ID is a foreign key referencing *IMPACT*

Relevant Data Type (*CISA_Incident_ID, Data_Type*)

CISA_Incident_ID is a foreign key referencing *DATA*

ORGANIZATION (*Organization_ID*)

CRIT INFR/PRIV SECT (*Organization_or_Company_Name, Org_Type, Organization_ID*)

Organization_ID is a foreign key referencing *ORGANIZATION*

US FED GOV (*Federal_Agency, Fed_Subagency, Organization_ID*)

Organization_ID is a foreign key referencing *ORGANIZATION*

FOREIGN GOV (*Country, National_CSIRT, Organization_ID*)

Organization_ID is a foreign key referencing *ORGANIZATION*

SLTT GOV (*State, SLTT_Organization_Name, Organization_Name, Organization_ID*)

Organization_ID is a foreign key referencing *ORGANIZATION*

ISAC (*ISAC_Subagency, Organization_ID*)

Organization_ID is a foreign key referencing *ORGANIZATION*

affects (*CISA_Incident_ID*, *Organization_ID*, Primary_Affected_Sector, Location)
CISA_Incident_ID is a foreign key referencing *INCIDENT*
Organization_ID is a foreign key referencing *ORGANIZATION*

involves (*CISA_Incident_ID*, *Organization_ID*, *Involvement_Type, Notified*)
CISA_Incident_ID is a foreign key referencing *INCIDENT*
Organization_ID is a foreign key referencing *ORGANIZATION*

5.1 Additional Integrity Constraints for the Relational Schema

The integrity constraints that must hold for the CIR database and that are not guaranteed by the relational schemas described above are listed in this subsection.

1. Primary_Affected_Sector can be null if the organization with the ID in the tuple is not in the CRIT INFR/PRIV SECT relation.

5.2 Domain definition and constraints

1. Domain *Int* = a positive integer or 0
The following attributes have *Int* as their domain of possible values: Port_Number, Total_Impacted_Hosts, Total_Impacted_People, Total_Impacted_Records, Impacted_Records

2. Domain *Float* = a positive floating point number with two decimal places or 0
The following attributes have *Float* as their domain of possible values: Estimated_Damage_Accounts

3. Domain *Y/N* = {*Yes, No*}
The following attributes have *Y/N* as their domain of possible values: Attack_Ended, Disclosed_to_Public, Detected_Malware, Is_Major, National_CSIRT, Notified

4. Domain *Name* = a short string no more than 50 characters long
The following attributes have *Name* as their domain of possible values: Last_Name, First_Name, Job_Title, Exploit_Name, Malware_Name, Antivirus_Name, Host_Name, Application_Name, Organization_or_Company_Name, Org_Type, Fed_Subagency, SLTT_Organization_Name, Organization_Name

5. Domain *Paragraph* = a long string no more than 5000 characters long

The following attributes have *Paragraph* as their domain of possible values: Incident_Narrative, Malware_Description, Potential_Impact, Remediation_Steps_Taken, Lessons_Learned

6. Domain *Date* = the set of all possible dates
The following attributes have *Date* as their domain of possible values: Submission_Date, Attack_Start_Date, Attack_First_Detected_Date, Last_Updated

7. Domain *Time* = the set of possible times in the day (HH:MM AM/PM)
The following attributes have *Time* as their domain of possible values: Submission_Time, Attack_Start_Time, Attack_First_Detected_Time

8. Domain *Duration* = 2 digits + 2 digits (HH:MM)
The following attributes have *Duration* as their domain of possible values: Estimated_Recovery_Time_Clock_Hours, Estimated_Recovery_Time_Staff_Hours, Attack_Duration

9. Domain *Phone Number* = the set of possible phone numbers
The following attributes have *Phone Number* as their domain of possible values: Phone, *Alt_Phone, Mobile, Pager*, *Fax*

10. Domain *Email Address* = the set of possible email addresses
The following attributes have *Email Address* as their domain of possible values: Email, Submitter_Email, POC_Email

11. Domain *CISA Incident ID* = INC prefix + 9 digits (INC-NNNNNNNNN)
The following attributes have *CISA Incident ID* as their domain of possible values: CISA_Incident_ID

12. Domain *Attack Vector* = {*Unknown, Attrition, Web, Email/Phishing, External/Removable Media, Impersonation/Spoofing, Improper Usage, Loss or Theft of Equipment, Other*}
The following attributes have *Attack Vector* as their domain of possible values: Attack_Vector

13. Domain *Incident Type* = {*Phishing, DOS, Malware, Password, Drive-by, Man-in-the-middle, Theft, Fraud, Data Breach, Privilege Escalation, Sniffing, Anonymous FTP Abuse, Other*}
The following attributes have *Incident Type* as their domain of possible values: Incident_Type

14. Domain *Observed Activity Network Location* = {*Level 1 - Business Demilitarized Zone, Level 2 - Business Network, Level 3 - Business Network Management, Level 4 - Critical System DMZ, Level 5 - Critical System Management, Level 6 - Critical Systems, Level 7 - Safety Systems, Unknown*}
The following attributes have *Observed Activity Network Location* as their domain of possible values: Observed_Activity_Network_Location

15. Domain *Suspected Threat Actor Type* = {*Cybercriminal, Nation-State Actor, Hacktivist, Thrill Seeker, Insider Threat, Cyberterrorist*}
The following attributes have *Suspected Threat Actor Type* as their domain of possible values: Suspected_Threat_Actor_Type

16. Domain *CVE ID* = CVE prefix + year + 4-7 digits (CVE-YYYY-NNNNN)
The following attributes have *CVE ID* as their domain of possible values: CVE_ID

17. Domain *Malware Type* = {*Virus, Trojan, Botnet, Rootkit, Spyware, Adware, Ransomware*}
The following attributes have *Malware Type* as their domain of possible values: Malware_Type

18. Domain *Signature*: a string containing YARA signature rules to identify the specific malware or malware family
The following attributes have *Signature* as their domain of possible values: Signature

19. Domain *Protocol* = {*IPsec, ICMP, IGMP, TCP, HTTP, HTTPS, TLS/SSL, UDP, BGP, EIGRP, OSFP, RIP*}
The following attributes have *Protocol* as their domain of possible values: Protocol

20. Domain *Port Type* = {*Source, Destination*}
The following attributes have *Port Type* as their domain of possible values: Port_Type

21. Domain *Functional Impact* = {*No Impact, No Impact to Services, Minimal Impact to Non-Critical Services, Minimal Impact to Critical Services, Significant Impact to Non-Critical Services, Denial of Non-Critical Services, Significant Impact to Critical Services, Denial of Critical Services/Loss of Control*}
The following attributes have *Functional Impact* as their domain of possible values: Functional_Impact

22. Domain *Information Impact* = {*No Impact, Suspected but Not Identified, Privacy Data Breach, Proprietary Information Breach, Destruction of Non-Critical Systems, Critical Systems Data Breach, Core Credential Compromise, Destruction of Critical System*}
The following attributes have *Information Impact* as their domain of possible values: Information_Impact

23. Domain *Recoverability* = {*Regular, Supplemented, Extended, Not Recoverable*}
The following attributes have *Recoverability* as their domain of possible values: Recoverability

24. Domain *Severity Score* = {*Baseline - Negligible, Baseline - Minor, Low, Medium, High, Severe, Emergency*}
The following attributes have *Severity Score* as their domain of possible values: Severity_Score

25. Domain *Host Type* = {*Attacking, Victim, Both*}
The following attributes have *Host Type* as their domain of possible values: Host_Type

26. Domain *Affected OS* = {*Linux, MacOS, Windows*}
The following attributes have *Affected OS* as their domain of possible values: Affected_OS

27. Domain *Primary Purpose* = {*User Desktop Machine, User Laptop Machine, Web Server, Mail Server, FTP Server, Domain Controller, Domain Name Server, Time Server, NFS/File System Server, Database Server, Application Server, Other Infrastructure Services*}
The following attributes have *Primary Purpose* as their domain of possible values: Primary_Purpose

28. Domain *IP Address* = 1-3 digits + 1-3 digits + 1-3 digits + 1-3 digits (NNN.NN.NN.NN)
The following attributes have *IP Address* as their domain of possible values: IP_Address

29. Domain *Impact Type* = {*Access, Alteration, Destruction, Exposure*}
The following attributes have *Impact Type* as their domain of possible values: Impact_Type

30. Domain *Data Type* = {*Full Name, SSN, Driver's License Information, Mailing Address, Credit Card Information, Passport Information, Financial Information, Medical Records, Zip Code, Race, Gender, Date of Birth, Place of Birth, Religion*}
The following attributes have *Data Type* as their domain of possible values: Data_Type

31. Domain *Organization ID* = ORG prefix + 9 digits (ORG-NNNNNNNNN)
The following attributes have *Organization ID* as their domain of possible values: Organization_ID

32. Domain *Federal Agency* = the list is too long to put here, but if you go to https://www.cisa.gov/forms/report and under Organization Details, for "What type of Organization are you?" select "United States Federal Government", the list shows up in a drop down from "With which Federal Agency are you affiliated?"
The following attributes have *Federal Agency* as their domain of possible values: Federal_Agency

33. Domain *Country* = one of the 195 countries in the world
The following attributes have *Country* as their domain of possible values: Country

34. Domain *State* = {*Alabama, Alaska, American Samoa, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Northern Mariana Islands, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, United States Virgin Islands, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming*}
The following attributes have *State* as their domain of possible values: State

35. Domain *ISAC Subagency* = {*Automotive ISAC, Aviation ISAC, Communications ISAC, Defense Industrial Base ISAC, Defense Security Information Exchange, Downstream Natural Gas ISAC, Electricity ISAC, Emergency Management and Response ISAC, Financial Services ISAC, Healthcare Ready, Information Technology ISAC, Maritime Transportation System ISAC, Multi-State ISAC, National Health ISAC, Oil and Natural Gas ISAC, Real Estate ISAC, Research and Education Network ISAC, Retail Cyber Intelligence Sharing Center, Supply Chain ISAC, Surface Transportation ISAC, Water ISAC*}
The following attributes have *ISAC Subagency* as their domain of possible values: ISAC_Subagency

36. Domain *Primary Affected Sector* = {*Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors Materials and Waste, Transportation Systems, Water and Wastewater Systems, Private Sector - Not Critical Infrastructure Aligned*}
The following attributes have *Primary Affected Sector* as their domain of possible values: Primary_Affected_Sector

37. Domain *Location* = street number + street address + city + state + zip (NNN AAAAA, CCC, SS ZZZZZ)
The following attributes have *Location* as their domain of possible values: Location

38. Domain *Involvement Type* = {*Indirectly Impacted, Supporting, Both*}
The following attributes have *Involvement Type* as their domain of possible values: Involvement_Type