Table 1 Common attributes of Software and PMS

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| name | string | product name |
| description | string | Product details |
| vendor | string | Manufacturer name of the product |
| version | string | Product version number |
| created | timestamp | The creation date of the product |
| update | timestamp | The date the product was last updated |
| language | string | The environment language required to run the product |

Table 2 Type ranges of the Malware and Tool classes.

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Name** | **Definition** | **Example** |
| **Tool** | Execution | Tools used to perform malicious actions, including remote code execution and script execution. | PowerShell、WMI、WinRAR SFX |
| Exfiltration | Tools used to transfer data from an infected system to a location controlled by the attacker. | FTP、Exfiltration Over C2 Channel |
| Credential Access | Tools used to obtain, steal, or exploit credentials (such as usernames and passwords). | Mimikatz、Windows Credential Editor |
| Persistence | Tools used to maintain persistent access on an infected system. | Scheduled Task、Registry Run Keys / Startup Folder |
| Defense Evasion | Tools used to evade detection and defensive measures to ensure that attackers can continue to operate without being discovered. | Process Hollowing、User Execution |
| Lateral Movement | Tools used to move within a network and spread to other systems. | PsExec、Windows Remote Management |
| Collection | Tools used to collect information about the infected system, such as file listings, registry information, system configuration, etc. | System Information Discovery |
| Discovery | Tools used to discover resources and network topology on the infected system to help attackers understand the target environment. | Security Software Discovery |
| **Malware** | Adware | Malware that displays advertisements. | **SmartSpyware Cleaner** |
| Spyware | Malware that monitors and steals user information. | **Keylogger** |
| Ransomware | Malware that encrypts files and demands a ransom from the victim to unlock them. | **WannaCry** |
| Trojan | Software that pretends to be legitimate software but performs malicious actions behind the scenes. | **Zeus** |
| Worm | Malware that replicates itself and spreads to other systems. | **ILOVEYOU** |
| Virus | Malware that infects and spreads to other files and systems. | **Melissa** |
| Exploit | Software that exploits system or application vulnerabilities to perform malicious actions. | **Stuxnet** |
| Hybrid | A combination of different types of malware, usually including parts of Trojans and worms, and occasionally viruses. | **Flame** |

Table 3 Unique properties of each subclass of Software and PMS

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **Field** | **Type** | **Description** |
| **Tool** | type | enumeration | Divided into 8 tools according to attack type. |
| kill\_chain\_phases | string[] | Corresponding to different stages of the kill chain. |
| platform | string[] | List of platforms the tool runs on. |
| reference | string | Provide more information about the tool. |
| **Malware** | family | enumeration | Malware family name |
| Associated | string[] | Other related malware names |
| kill\_chain\_phases | string[] | Corresponding to different stages of the kill chain |
| platform | string[] | List of platforms where malware runs |
| reference | string | Provides more information and resource links to malware |
| **Primary equipment** | p\_id | string | A unique identifier for the equipment. |
| p\_type | string | For example, transformer, circuit breaker, generator, etc. |
| p\_voltage | string | The rated operating voltage of the equipment. |
| p\_current | string | The rated operating current of the equipment. |
| p\_rating | string | The power rating of the equipment. |
| p\_loc | string | The physical installation location of the equipment. |
| p\_status | string | The current operational status (e.g., online, offline, fault, etc.). |
| p\_record | string | The maintenance history of the equipment. |
| p\_date | timestamp | The date the equipment was installed. |
| p\_lifespan | string | The expected lifespan of the equipment. |
| **Secondary equipment** | s\_id | string | A unique identifier for the equipment. |
| s\_type | string | For example, relay, sensor, controller, etc. |
| s\_func | string | A description of the equipment's function (e.g., monitoring, protection, control, etc.). |
| s\_protocol | string | The communication protocol used by the equipment (e.g., Modbus, DNP3, etc.). |
| s\_parameter | string | he specific parameters measured by the equipment (e.g., voltage, current, temperature, etc.). |
| s\_acc | float | The measurement accuracy of the equipment. |
| s\_loc | string | The physical installation location of the equipment. |
| s\_status | string | The current operational status (e.g., online, offline, fault, etc.). |
| s\_record | string | The maintenance history of the equipment. |
| s\_date | timestamp | The date the equipment was installed. |
| s\_requirement | string | The power requirements of the equipment. |

Table 4 Property definition of Vulnerability class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| vuln\_id | int | Vulnerability ID |
| CVE\_ID | string | Vulnerabilities are numbered in the CVE database |
| vuln\_name | string | Vulnerability Name |
| vuln\_type | string[] | Vulnerability threat type |
| vuln\_published | string | Date the vulnerability was disclosed |
| last\_modified | string | Date the vulnerability was updated |
| risk\_level | string | Vulnerability severity level |
| CVSS\_score | float | Common Vulnerability Scoring System score |
| influence\_product | string | Configuration of products affected by the vulnerability, using CPE format |
| vuln\_description | string | Vulnerability Details |
| vuln\_vendor | string | Vulnerability Source |
| vuln\_solution | string | Vulnerability Solutions |
| vuln\_patch | string | Vulnerability patch link |

Table 5 Property definition of Weakness class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| weak\_id | int | Weakness Number |
| CWE\_ID | string | The corresponding number of the weakness in the CWE library |
| weak\_name | string | Weakness Name |
| weak\_description | string | A detailed description of the weakness, including its nature, cause, potential risk, etc. |
| weak\_mode | string | The stage at which weaknesses may emerge or be exploited |
| weak\_platform | string | Platform language to which the vulnerability applies |
| weak\_conquence | string | The impact that the weakness may have on the system, including security risks, availability issues, etc. |
| weak\_ordinality | string | Describe the type of correlation or relationship between the weaknesses |
| risk\_level | string[] | Likelihood of the vulnerability being exploited, [high, medium, low] |
| weak\_example | string | Specific manifestations of the weakness, such as sample code |
| detection\_method | String | Weakness Detection Methods |
| weak\_reference | string | Links to standards or reference documents related to the weakness |
| weak\_submission | string | The vulnerability submission information, including date and submitter information |
| weak\_modification | string | Vulnerability modification information, including date, update content, etc. |

Table 6 Property definition of Attacker class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| att\_id | int | The attacker's unique ID |
| ATT\_ID | string | The attacker's corresponding ID in the ATT&CK library |
| att\_name | string | The attacker's common name, alias, or code name |
| att\_created | timestamp | The attacker's initial creation time |
| att\_label | string[] | Describe the threat type of the attacker |
| att\_description | string | A detailed description of the attacker |
| att\_alias | string[] | List of aliases associated with the attacker |
| att\_role | string | Describe the attacker's roles or responsibilities |
| att\_goal | string | Specify the attacker's goals or motivations |
| att\_sophistication | string | Describe the attacker's skill level or sophistication |
| resource\_level | string | Describe the attacker's level of access to resources |
| att\_motivation | string | The main motivation of the attackers |
| att\_domain | string | Industries or sectors that attackers usually target |
| att\_reference | string | Links to previous or future threat activity associated with the attacker |

Table 7 Property definition of Attack Pattern class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| ap\_id | int | The unique ID of the attack mode |
| CAPEC\_ID | string | The corresponding ID of the attack pattern in the CAPEC library |
| ad\_name | string | The name of the attack mode |
| ap\_description | string | A detailed description of the attack mode, including the target, method, impact, etc. |
| ap\_status | string[] | Indicates the maturity and update status of the attack pattern, [Stable, Draft, Deprecated] |
| ap\_abstraction | string[] | Describes the level of abstraction of the attack pattern, [Standard, Detailed, Meta] |
| likelihood\_of\_attack | string[] | The probability or likelihood level of the attack pattern occurring, [High, Medium, Low] |
| severity\_level | string[] | The severity level of the attack mode's impact on the target, [High, Medium, Low] |
| domain\_of\_attack | string[] | Attack patterns commonly used in attack areas, [Software, Hardware, Communications, Supply Chain, Social Engineering, Physical Security] |
| ap\_prerequisite | string | The prerequisites or environmental requirements for an attacker to use the attack pattern |
| ap\_skill | string | Information about the skills required to execute this attack mode |
| ap\_resource | string | The specific resources required to execute this attack mode |
| ap\_mitigation | string | Mitigation measures that can be taken against this attack mode |
| ap\_instance | string | Example describing this attack pattern |
| ap\_reference | string | Links to relevant standards or references for this attack pattern |
| ap\_submission | string | Creation date and submission information of the attack pattern |
| ap\_modification | string | The latest modification date and modification content of the attack mode |

Table 8 Property definition of Technique class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| tech\_id | int | Unique ID of the technology |
| ATT\_ID | string | The corresponding ID of the technology in the ATT&CK library |
| tech\_name | string | Technology Name |
| tech\_description | string | A detailed description of the technique, including how an attacker could use it and the possible consequences |
| sub\_technique | string | Sub-techniques of a technology that assist the technology in achieving its goals |
| tech\_complexity | string | The complexity of technical implementation, [High, Medium, Low] |
| tech\_platform | string | The operating system or environment that the technology is applicable to, such as Windows, Linux, macOS, etc. |
| tech\_version | string | Versions or variants of a technology, used to describe different variations of a technology |
| tech\_created | timestamp | Creation date of the technology |
| last\_modified | timestamp | The date the technology was last modified |
| tech\_example | string | Examples of how technology is used |
| tech\_detection | string | Describes methods for detecting or defending against the technique, including data sources to consider when detecting the technique |
| tech\_reference | string | Links to standards or references related to the technology |

Table 9 Property definition of Mitigation class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| mi\_id | int | Unique ID of the mitigation measure |
| ATT\_ID | string | The corresponding ID of the mitigation measure in the ATT&CK library |
| mi\_name | string | Name of the mitigation |
| mi\_description | string | A detailed description of the mitigation measure, including how it will work, how it will be implemented, and its likely effectiveness. |
| security\_control | string | Describe the security controls involved when applying mitigations |
| mi\_version | string | Mitigation version number |
| mi\_created | timestamp | Date the mitigation is created |
| last\_modified | timestamp | Date the mitigation is last modified |

Table 10 Property definition of Tactic class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| ta\_id | int | The unique ID of the tactic |
| ATT\_ID | string | The corresponding ID of the tactic in the ATT&CK library |
| ta\_name | string | Name of the tactic |
| ta\_description | string | A brief description of the tactic, explaining the attacker's general goals and strategies in implementing the tactic. |
| ta\_severity | string | Measures the level of impact of tactics on the target, [High, Medium, Low] |
| ta\_created | timestamp | Creation date of the tactic |
| last\_modified | timestamp | The date the tactic is last modified |

Table 11 Property definition of Consequence class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| con\_id | int | The unique ID of the attack consequence |
| con\_name | string | Name of the attack consequence |
| con\_description | string | Details of the aftermath of the attack |
| con\_type | string | Describe the type of impact the attack had on the affected system or device |
| con\_severity | string | Measuring the severity of the consequences of an attack |
| con\_duration | string | Duration of the aftermath of the attack |
| con\_created | timestamp | When the attack starts to have an impact |

Table 12 Property definition of Indicator class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| in\_id | int | The unique ID of the indicator |
| in\_name | string | Name of the indicator |
| in\_description | string | Details of the indicator |
| in\_type | string | The form of the indicator, such as IP address, domain name, etc. |
| in\_source | string | Sources of indicator information, such as log data, threat intelligence, etc. |
| in\_lifecycle | string | The life cycle of an indicator, that is, the period from when it becomes effective to when it becomes invalid |

Table 13 Property definition of Detection class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
| de\_id | int | The unique ID of the detection method |
| de\_description | string | Detailed description of the assay |
|  | string[] | Describe the available data sources for detecting specific techniques, such as logs, network traffic, endpoint events, etc. |
|  | string | Some of the data actually used by the detection technology |
|  | string | Specify the execution platform of the detection technology |
|  | string | Describe the limitations and possible pitfalls of the detection technology |
|  | string | Actual detection example |
|  | string | Tools used to implement detection technology |
|  | string | References related to detection technology |

Table 14 Property definition of Solution class

|  |  |  |
| --- | --- | --- |
| **Field** | **Type** | **Description** |
|  | int | The unique ID of the solution |
|  | string | Describe the solution details |
|  | string[] | Different stages of the software development life cycle where solutions can be applied |
|  | string | Evaluate the cost of implementing the measure, including the investment of time, manpower and resources |
|  | string | Evaluate the effectiveness of the solution and the extent to which it reduces the risk |
|  | string | Indicates how easy it is to implement the solution |
|  | string | Describe the extent to which the solution was implemented in a timely manner |
|  | string | Provide any special considerations or limitations that you need to be aware of when implementing your solution |