TLP:GREEN

聯防監控資安情資回傳STIX格式規範

國家資通安全研究院

中華民國112年9月

修訂歷史紀錄表

項次	版次	日期	說明
1	V1.0	110/12/8	新編
2	V1.1	111/7/7	修正 Grouping 屬性內容描述
3	V1.2	111/8/25	更新頁尾資訊
4	V1.3	111/9/29	修正受駭單位 Identity 範例
5	V1.4	112/1/1	國家資通安全研究院組織更新
6	V1.5	112/9/1	表 5 情資類別定義更新

國家資通安全研究院整理

目　次

圖 目 次

表 目 次

1. 物件類型

本章節列舉資安監控單與情資分析單所使用之 STIX 2.1 物件，後續章節針對各物件欄位進行介紹。

●STIX Meta Objects 皆為必要物件

●STIX Domain Objects 之 Grouping、Attack Pattern、Identity 及 Observed Data 為必要物件，Indicator、Malware、Malware Analysis、Vulnerability 及 Report 為情資分析單之選擇性使用物件，視情況用以產製相關資訊

●STIX Cyber-observable Objects 皆為選擇性使用物件，視情況用以產製 IP 紀錄、網域/Hostname 紀錄、連線紀錄或電子郵件紀錄

– 資安設備若為端點偵測及應變機制(EDR)，情資須包含一筆受駭單位 IP 紀錄與一筆受駭單位 Hostname 紀錄

– 資安設備若為端點偵測及應變機制以外之類型，情資至少須包含一筆受駭單位連線紀錄或受駭單位電子郵件紀錄

●STIX Relationship Objects 皆為必要物件

表1　SOC 情資使用之 STIX 2.1 物件

項次	物件類型	物件	資安監控單	情資分析單
1	STIX Meta Objects (SMO)	Extension Definition	V	V
2	STIX Domain Objects (SDO)	Grouping	V	V
		Attack Pattern	V	V
		Identity	V	V
		Indicator		V
		Malware		V
		Malware Analysis		V
		Vulnerability		V
		Observed Data	V	V
		Report		V
3	STIX Cyber-observable Objects (SCO)	Artifact Object	V	V
		Domain Name Object	V	V
		Email Address Object	V	V
		Email Message Object	V	V
		File Object		V
		IPv4 Address Object	V	V
		IPv6 Address Object	V	V

項次	物件類型	物件	資安監控單	情資分析單
		Network Traffic Object	V	V
		Process Object		V
4	STIX Relationship Objects (SRO)	Sighting	V	V
		Relationships	V	V

資料來源：國家資通安全研究院整理

2. 物件介紹

STIX 2.1 物件基本屬性詳見表 2，以「*」表示為官方指定必填屬性，後續小節針對 STIX 2.1 物件屬性對應 SOC 欄位進行說明。

表2　物件基本屬性

項次	基本屬性
1	*type
2	*spec_version
3	*id
4	*created
5	*modified
6	created_by_ref
7	revoked
8	labels
9	confidence
10	lang
11	external_references
12	object_marking_refs
13	granular_markings
14	extensions

資料來源：國家資通安全研究院整理

2.1 STIX Meta Objects

本節於 SOC 欄位以「*」表示為 SOC 情資必填屬性

2.1.1 Extension Definition

表3　Extension Definition 屬性

項次	屬性	SOC 欄位	備註
1	name	擴展名稱*	參考官方文件或範例
2	created_by_ref	資安監控單位參照*	填寫資安監控單位 Identity 物件識別碼
3	description	-	-
4	schema	擴展示意*	參考官方文件或範例
5	version	擴展版本*	參考官方文件或範例
6	extension_types	擴展類型*	參考官方文件或範例
7	extension_properties	-	-

資料來源：國家資通安全研究院整理

```
{
    "id": "extension-definition--d83fce45-ef58-4c6c-a3f4-1fbc32e98c6e",
    "created_by_ref": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965918",
    "type": "extension-definition",
    "spec_version": "2.1",
    "name": "Grouping Extension",
    "description": "This schema adds two properties to Grouping object",
    "created": "2021-09-14T08:56:34.935656Z",
    "modified": "2021-09-14T08:56:34.935656Z",
    "schema": "adds two properties to Grouping object",
    "version": "1",
    "extension_types": [ "property-extension" ]
},
```


資料來源：國家資通安全研究院整理

圖1　Exntension Definition 範例

2.2 STIX Domain Objects

本節於 SOC 欄位以「*」表示為 SOC 情資必填屬性

2.2.1 Grouping

情資使用 Grouping 物件封裝基本資訊欄位，其中情資類別參考 N-SOC 情資類別，詳見表 5。

表4　Grouping 屬性

項次	屬性	SOC 欄位	備註
1	name	情資主旨*	
2	description	情資描述*	
3	labels	情資編號*	SOC 英縮寫-機關英縮寫-日期-編號
4	context	情資類別*	參考 N-SOC 情資類別

項次	屬性	SOC 欄位	備註
5	object_refs	相關 SRO、SDO、SCO 參照*	填寫所有相關 SRO、SDO、SCO 識別碼
6	created_by_ref	資安監控單位參照*	填寫資安監控單位 Identity 物件識別碼
7	extensions/ extension_definition_id/ extension_type	擴展類型*	填寫”property-extension”
8	extensions/ extension_definition_id/ x_related_labels	相關情資編號	填寫相關之情資編號

資料來源：國家資通安全研究院整理

表5　N-SOC 情資類別

項次	情資類別	內容說明	情資主旨範例
1	惡意內容	針對透過文字、照片、影片等形式散播不當內容之情資，如： ▪網頁惡意留言 ▪寄送垃圾郵件	外部使用者對多個客戶使用者寄送 SPAM 信件
2	惡意程式	針對與各類型惡意程式有關之情資，如： ▪散播惡意程式 ▪系統存在惡意程式	▪後門/間諜程式連線 ▪內部主機疑似進行惡意程式連線 ▪惡意程式下載行為

項次	情資類別	內容說明	情資主旨範例
3	資訊蒐集	針對蒐集主機、服務或帳號資訊之情資，如： ▪網路主機與服務埠掃描 ▪社交工程(非技術性)	▪外部主機執行掃描探測攻擊 ▪弱點掃描行為
4	入侵嘗試	針對未經授權利用漏洞或攻擊手法嘗試入侵主機之情資，如： ▪透過已知漏洞進行攻擊嘗試 ▪透過密碼猜測或暴力破解等登入嘗試 ▪透過零時差等新形態攻擊手法之入侵嘗試	▪密碼猜測行為 ▪密碼暴力破解 ▪特權帳號使用非允入 IP 登入事件 ▪非上班時間任何登入嘗試
5	入侵攻擊	針對系統遭未經授權存取或取得系統/使用者權限，導致發生異常連線或惡意行為之情資，如： ▪系統遭入侵 ▪殭屍電腦	▪內部電腦連線至 C&C 網站 ▪內部主機單次連線至惡意 IP ▪網頁遭受竄改
6	服務阻斷	針對影響資訊可用性或造成服務中斷之情資，如： ▪阻斷服務攻擊 ▪實體設備損壞	▪外部主機疑似進行阻斷服務攻擊 ▪重要系統疑似遭受阻斷服務攻擊 ▪電子申請服務異常 ▪設備服務中止
7	資訊內容安全	針對系統遭未經授權存取或修改，導致影響資訊機敏性與完整性之情資，如： ▪機敏資訊外洩	▪資料外洩攻擊 ▪應用程式存取 DB ▪新增刪除資料異動

項次	情資類別	內容說明	情資主旨範例
		▪資料遭竄改	
8	詐欺攻擊	針對偽冒他人身分、服務及組織等進行惡意行為之情資，如： ▪釣魚郵件 ▪釣魚網站	發送釣魚郵件
9	系統弱點	針對系統存在弱點之情資，該弱點可能遭利用而影響自身安全或造成他人之威脅	系統疑似存在 RCE 漏洞
10	其他	分享非屬前述情資類別之情資	-

資料來源：國家資通安全研究院整理

```
{
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--9c82a63e-c4fa-4e89-949c-6cad9e430d70",
    "created_by_ref": "identity--0290e9ce-cbdl-4c4c-b23f-9585ba965918",
    "created": "2021-09-14T08:56:34.935Z",
    "modified": "2021-09-14T08:56:34.935Z",
    "labels":["NICS-orgA-20190605-000004"],
    "context": "惡意程式",
    "name": "後門/間諜程式行為",
    "description": "內部電腦遭植入Mirai殭屍網路惡意程式，並持續對外進行報到行為",
    "extensions": {
        "extension-definition--d83fce45-ef58-4c6c-a3f4-1fbc32e98c6e": {
            "extension_type": "property-extension",
            "x_related_labels": ["NICS-orgA-20190601-000001","NICS-orgA-20190601-000010"]
        }
    },
    "object_refs": [
        "identity--0290e9ce-cbdl-4c4c-b23f-9585ba965918",
        "identity--0290e9ce-cbdl-4c4c-b23f-9585ba965919",
        "identity--0290e9ce-cbdl-4c4c-b23f-9585ba965920",
        "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
        "attack-pattern--3f886f2a-874f-4333-b794-aa6075009b1c",
        "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
        "ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd",
        "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
        "ipv6-addr--1e61d36c-a16c-53b7-a80f-2a0016lc96b1",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f527d",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5271",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5273",
        "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6313",
        "email-message--72b7698f-10c2-565a-a2a6-b4996a2f2265",
        "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
        "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436e3",
        "email-addr--e4ee5301-b52d-59cd-a8fa-8036738c7194",
        "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
        "sighting--ee20065d-2555-424f-ad9e-0f8428623c76",
        "sighting--ee20065d-2555-424f-ad9e-0f8428623c79",
        "relationship--b82b2819-3b86-4bd5-afb3-fa36cfbc3f19",
        "relationship--b82b2819-3b86-4bd5-afb3-fa36cfbc3f20"
    ]
},
```


資料來源：國家資通安全研究院整理

圖2　Grouping 範例

2.2.2 Attack Pattern

可直接套用 MITRE ATT&CK 資訊，詳情請參考 MITRE ATT&CK 官網 https://attack.mitre.org/resources/working-with-attack/，並使用官方訂定之 Attack Pattern 物件，亦可參考範例填寫非 MITRE ATT&CK 攻擊手法資訊。

表6　Attack Pattern 屬性

項次	屬性	SOC 欄位	備註
1	name	攻擊手法*	
2	description	攻擊手法補充說明*	
3	aliases	-	
4	kill_chain_phases/ kill_chain_name	駭客狙殺鏈框架名稱	參考官方文件或範例
5	kill_chain_phases/ phase_name	駭客狙殺鏈階段	參考官方文件或範例

資料來源：國家資通安全研究院整理

```
{
    "id": "attack-pattern--f5bb433e-bdf6-4781-84bc-35e97e43be89",
    "description": "Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot.(Citation: Symantec Chernobyl W95.CIH) Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices could include the motherboard, hard drive, or video cards.",
    "name": "Firmware Corruption",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "external_references": [
        {
            "external_id": "T1495",
            "source_name": "mitre-attack",
            "url": "https://attack.mitre.org/techniques/T1495"
        },
        {
            "source_name": "Symantec Chernobyl W95.CIH",
            "url": "https://www.symantec.com/security-center/writeup/2000-122010-2655-99",
            "description": "Yamamura, M. (2002, April 25). W95.CIH. Retrieved April 12, 2019."
        },
        {
            "url":
            "http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research",
            "description": "Upham, K. (2014, March). Going Deep into the BIOS with MITRE Firmware Security Research. Retrieved January 5, 2016.",
            "source_name": "MITRE Trustworthy Firmware Measurement"
        }
    ],
    "type": "attack-pattern",
    "kill_chain_phases": [
        {
            "kill_chain_name": "mitre-attack",
            "phase_name": "impact"
        }
    ],
    "modified": "2021-04-29T14:49:39.188Z",
    "created": "2019-04-12T18:28:15.451Z",
    "x_mitre_is_subtechnique": false,
    "x_mitre_platforms": [
        "Linux",
        "macOS",
        "Windows"
    ],
    "x_mitre_permissions_required": [
        "Administrator",
        "root",
        "SYSTEM"
    ],
    "x_mitre_impact_type": [
        "Availability"
    ],
    "x_mitre_version": "1.0",
    "x_mitre_detection": "System firmware manipulation may be detected.(Citation: MITRE Trustworthy Firmware Measurement) Log attempts to read/write to BIOS and compare against known patching behavior.",
    "x_mitre_data_sources": [
        "Firmware: Firmware Modification"
    ],
    "spec_version": "2.1",
    "x_mitre_domains": [
        "enterprise-attack"
    ],
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
},
```


資料來源：國家資通安全研究院整理

圖3　Attack Pattern (MITRE ATT&CK)範例

```
{
    "type": "attack-pattern",
    "spec_version": "2.1",
    "id": "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": "更改群組原則",
    "description": "非上班時段竄改群組原則以派送具惡意行為的工作排程",
    "kill_chain_phases": [
        {
            "kill_chain_name": "lockheed-martin-cyber-kill-chain",
            "phase_name": "Exploitation"
        }
    ]
},
```


資料來源：國家資通安全研究院整理

圖4　Attack Pattern (非 MITRE ATT&CK)範例

2.2.3 Identity

情資使用 Identity 產製受駭單位、資安監控單位及資安設備，詳見圖 5 至圖 7。若情資之資安設備類型為端點偵測及應變機制，請產製相關惡意程式資訊(2.2.5)，並封裝成情資分析單。

若無單位 OID 或單位等級，請填寫”N/A”。

表7　受駭單位 Identity 屬性

項次	屬性	SOC 欄位	備註
1	name	單位名稱*	單位中文名稱
2	description	單位代碼*	單位 OID
3	roles	單位等級*	A
			B
			C
			D
			E
4	identity_class	單位資訊*	填寫”government”
5	sectors	單位所屬領域/區域*	中央及地方政府
			能源
			水資源
			通訊傳播
			交通
			金融
			緊急救援及醫院

項次	屬性	SOC 欄位	備註
			科學園區與工業區
			教育
6	contact_information	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965919",
    "created": "2021-09-14T08:56:34.897Z",
    "modified": "2021-09-14T08:56:34.897Z",
    "name": "OO市政府資訊中心",
    "description": "2.16.886.101.OOOOO.XXXXX",
    "roles":["A"],
    "identity_class": "government",
    "sectors":["中央及地方政府"]
},
```


資料來源：國家資通安全研究院整理

圖5　受駭單位 Identity 範例

表8　資安監控單位 Identity 屬性

項次	屬性	SOC 欄位	備註
1	name	資安監控單位*	監控單位(服務業者)全名
2	description	-	-

項次	屬性	SOC 欄位	備註
3	roles	-	-
4	identity_class	資安監控單位資訊*	填寫”SOC”
5	sectors	-	-
6	contact_information	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965918",
    "created": "2021-09-14T08:56:34.897Z",
    "modified": "2021-09-14T08:56:34.897Z",
    "name": "OO_SOC",
    "identity_class": "SOC"
},
```


資料來源：國家資通安全研究院整理

圖6　資安監控單位 Identity 範例

表9　資安設備 Identity 屬性

項次	屬性	SOC 欄位	備註
1	name	設備代號*	-
2	description	設備廠商*	-
3	roles	資安防護類型*	防毒軟體

項次	屬性	SOC 欄位	備註
			電子郵件過濾機制
			應用程式防火牆
			網路防火牆
			入侵偵測及防禦機制
			進階持續性威脅攻擊防禦措施
			端點偵測及應變機制
			目錄服務系統
			核心資通系統
			其他類型可自訂
4	identity_class	設備資訊*	填寫”system”
5	sectors	-	-
6	contact_information	-	-

資料來源：國家資通安全研究院整理

```
{
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965920",
    "created": "2021-09-14T08:56:34.897Z",
    "modified": "2021-09-14T08:56:34.897Z",
    "name": "ESET NOD32 Antivirus",
    "description": "ESET",
    "roles":["防毒軟體"],
    "identity_class": "system"
},
```


資料來源：國家資通安全研究院整理

圖7　資安設備 Identity 範例

2.2.4 Indicator

Indicator 為情資分析單之選擇性使用物件，情資使用 Indicator 物件產製惡意指標，針對惡意 IP、惡意網址或惡意網域，至少填寫一項資訊於 pattern 欄位。

表10 Indicator 屬性

項次	屬性	SOC 欄位	備註
1	name	-	-
2	description	惡意指標描述*	-
3	indicator_types	惡意指標類型*	填寫 IOC 或 IOA
4	pattern	惡意 IP	STIX Patterning 表示法請參考官方文件或範例
		惡意網址	
		惡意域名	
5	pattern_type	惡意指標表示法*	請填寫”stix”
6	pattern_version	-	-

項次	屬性	SOC 欄位	備註
7	valid_from	惡意指標有效起始時間*	YYYY-MM-DDTHH:mm:ss[.s+]Z
8	valid_until	-	-
9	kill_chain_phases	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd32",
    "created": "2016-04-06T20:03:48.000Z",
    "modified": "2016-04-06T20:03:48.000Z",
    "indicator_types": ["IOC"],
    "description": "對外報到惡意伺服器",
    "pattern": "[ ipv4-addr:value = '198.51.100.5' OR ipv4-addr:value = '198.51.100.6' OR url:value
    = 'http://example.com/foo' OR domain-name:value = 'www.5z8.info']",
    "pattern_type": "stix",
    "valid_from": "2021-10-01T00:00:00Z"
},
```


資料來源：國家資通安全研究院整理

圖8　Indicator 範例

2.2.5 Malware

Malware 為情資分析單之選擇性使用物件。若情資欲提供惡意程式雜湊值或惡意程式樣本 Base64 編碼，可將資訊填寫於 sample_refs 欄位，詳見 2.3.1 與 2.3.5 。若情資欲提供惡意程式分析資訊，可另外使用 Malware Analysis 物件並進行關聯，詳見 2.2.6 與 2.4.2 。

表11 Malware 屬性

項次	屬性	SOC 欄位	備註
1	name	惡意程式名稱*	-
2	description	惡意程式描述*	-
3	malware_types	惡意程式類型	請參考官方文件訂定之 malware-type-ov 字典
4	is_family	是否代表惡意程式家族*	填寫 true 或 false
5	aliases	-	-
6	kill_chain_phases	-	-
7	first_seen	-	-
8	last_seen	-	-
9	operating_system_refs	-	-
10	architecture_execution_envs	-	-
11	implementation_languages	-	-
12	capabilities	-	-
13	sample_refs	惡意程式樣本參照	填寫 File Object 識別碼

資料來源：國家資通安全研究院整理

```
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": "China Chopper",
    "description": "This web shell is commonly used by malicious Chinese actors, including advanced persistent threat (APT) groups, to remotely control web servers. This web shell has two parts, the client interface (an executable file) and the receiver host file on the compromised web server.",
    "malware_types": ["webshell"],
    "is_family": false
},
```


資料來源：國家資通安全研究院整理

圖9　Malware 範例

2.2.6 Malware Analysis

Malware Analysis 為情資分析單之選擇性使用物件，若情資欲提供惡意程式執行攻擊指令，可將資訊填寫於 analysis_sco_refs 欄位，詳見 2.3.9 。若情資不提供惡意程式執行攻擊指令，則須將分析結果填寫於 result 欄位。

表12 Malware Analysis 屬性

項次	屬性	SOC 欄位	備註
1	product	惡意程式分析引擎/產品名稱*	以英文小寫與”-”分隔號填寫
2	version	-	-
3	host_vm_ref	-	-
4	operating_system_ref	-	-
5	installed_software_refs	-	-
6	configuration_version	-	-
7	modules	-	-

項次	屬性	SOC 欄位	備註
8	analysis_engine_version	-	-
9	analysis_definition_version	-	-
10	submitted	上傳時間*	YYYY-MM-DDTHH:mm:ss[.s+]Z
11	analysis_started	開始分析時間	YYYY-MM-DDTHH:mm:ss[.s+]Z
12	analysis_ended	結束分析時間	YYYY-MM-DDTHH:mm:ss[.s+]Z
13	result_name	惡意程式威脅程度*	惡意程式等級/最高等級
14	result	分析結果	請參考官方文件訂定之 malware-result-ov 字典
15	analysis_sco_refs	惡意程式執行攻擊指令參照	填寫所有相關 Process Object 識別碼
16	sample_ref	-	-

資料來源：國家資通安全研究院整理

```
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "created": "2021-10-16T18:52:24.277Z",
    "modified": "2021-10-16T18:52:24.277Z",
    "product": "avira",
    "submitted": "2021-10-20T08:36:14Z",
    "analysis_started": "2021-10-20T08:36:14Z",
    "analysis_ended": "2021-10-20T08:36:15Z",
    "result_name": "9/10",
    "result": "malicious",
    "analysis_sco_refs": ["process--d2ec5aab-808d-4492-890a-3c1a1e3cb06e"]
},
```


資料來源：國家資通安全研究院整理

圖10 Malware Analysis 範例

2.2.7 Vulnerability

Vulnerability 為情資分析單之選擇性使用物件，情資使用 Vulnerability 物件產製漏洞資訊，針對 CVE 編號或漏洞名稱，填寫一項資訊於 name 欄位。

表13 Vulnerability 屬性

項次	屬性	SOC 欄位	備註
1	name	CVE 編號	CVE-YYYY-NNNN
		漏洞名稱	
2	description	漏洞描述*	-

資料來源：國家資通安全研究院整理

```
{
    "type": "vulnerability",
    "spec_version": "2.1",
    "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "created": "2016-05-12T08:17:27.000Z",
    "modified": "2016-05-12T08:17:27.000Z",
    "name": "CVE-2019-0604",
    "description": "A remote code execution vulnerability exists in Microsoft SharePoint when the
    software fails to check the source markup of an application package, aka 'Microsoft SharePoint
    Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594."
},
```


資料來源：國家資通安全研究院整理

圖11 Vulnerability 範例

2.2.8 Observed Data

使用 Obersved Data 將所有相關紀錄進行彙整。

表14 Observed Data 屬性

項次	屬性	SOC 欄位	備註
1	first_observed	開始時間*	紀錄彙整開始時間 YYYY-MM-DDTHH:mm:ss[.s+]Z
2	last_observed	結束時間*	紀錄彙整結束時間 YYYY-MM-DDTHH:mm:ss[.s+]Z
3	number_observed	觸發次數*	紀錄彙總觸發次數
4	object_refs	相關 SCO 參照*	填寫所有相關 SCO 識別碼

資料來源：國家資通安全研究院整理

```
{
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
    "created": "2021-10-19T19:00:00Z",
    "modified": "2021-10-19T19:00:00Z",
    "first_observed": "2021-10-19T19:00:00Z",
    "last_observed": "2021-10-19T19:00:00Z",
    "number_observed": 50,
    "object_refs": [
        "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
        "ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd",
        "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
        "mac-addr--65cfcf98-8a6e-5a1b-8f61-379ac4f92d00",
        "ipv6-addr--1e61d36c-a16c-53b7-a80f-2a00161c96b1",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f527d",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5271",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5272",
        "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5273",
        "email-message--72b7698f-10c2-565a-a2a6-b4996a2f2265",
        "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
        "email-addr--e4ee5301-b52d-59cd-a8fa-8036738c7194"
    ]
},
```


資料來源：國家資通安全研究院整理

圖12 Observed Data 範例

2.2.9 Report

Report 為情資分析單之選擇性使用物件，若情資欲提供完整報告，可將資訊填寫於 object_refs 欄位，詳見 2.3.1 。

表15 Report 屬性

項次	屬性	SOC 欄位	備註
1	name	報告名稱*	
2	description	報告描述	

項次	屬性	SOC 欄位	備註
3	report_types	-	
4	published	報告匯出時間*	YYYY-MM-DDTHH:mm:ss[.s+]Z
5	object_refs	報告內容參照*	填寫 Artifact Object 識別碼

資料來源：國家資通安全研究院整理


```
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
    "created": "2015-12-21T19:59:11.000Z",
    "modified": "2015-12-21T19:59:11.000Z",
    "name": "中國菜刀報告",
    "description": "中國菜刀惡意程式分析完整報告",
    "published": "2021-10-20T17:00:00.000Z",
    "object_refs": [
        "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333"
    ]
},
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
```


資料來源：國家資通安全研究院整理

圖13 Report 範例

2.3 STIX Cyber-observable Objects

本節於 SOC 欄位以「*」表示為 SOC 情資必填屬性。

以下物件皆為選擇性使用物件，視情況使用特定物件產製 IP 紀錄(詳見 2.3.6)、網域/Hostname 紀錄(詳見 2.3.2)、連線紀錄(詳見 2.3.8)或電子郵件紀錄(詳見 2.3.4)

- 資安設備若為端點偵測及應變機制(EDR)，情資須包含一筆受駭單位 IP 紀錄與受駭單位 Hostname 紀錄
- 資安設備若為端點偵測及應變機制以外之類型，情資至少須包含一筆受駭單位連線紀錄或受駭單位電子郵件紀錄

2.3.1 Artifact Object

情資使用 Artifact 物件，針對惡意程式樣本 Base64 編碼、惡意信件 Base64 編碼或報告 Base64 編碼，須填寫一項資訊至 payload_bin 欄位；若為惡意程式樣本 Base64 編碼，將相關 Malware 物件、File 物件與 Artifact 物件進行參照關聯，詳見圖 14。若為惡意信件樣本 Base64 編碼，將相關 Email Message 物件與 Artifact 物件進行參照關聯，詳見圖 15。若為報告 Base64 編碼，將相關 Report 物件與 Artifact 物件進行參照關聯，詳見圖 16。

表16 Artifact Object 屬性

項次	屬性	SOC 欄位	備註
1	mime_type	-	-
2	payload_bin	惡意程式樣本 Base64 編碼	-
		惡意信件 Base64 編碼	
		報告 Base64 編碼	

項次	屬性	SOC 欄位	備註
3	url	-	
4	hashes	-	
5	encryption_algorithm	-	
6	decryption_key	-	

資料來源：國家資通安全研究院整理


```
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6311",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca69",
    "hashes": {
        "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db",
        "SHA-1": "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12",
        "MD5": "9e107d9d372bb6826bd81d3542a419d6"
    },
    "size": 25536,
    "name": "foo.dll",
    "ctime": "2021-10-01T08:17:27.000Z",
    "mtime": "2021-10-12T08:17:27.000Z",
    "atime": "2021-10-12T08:17:27.000Z",
    "content_ref": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6311"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065",
    "created": "2021-05-12T08:17:27.000Z",
    "modified": "2021-05-12T08:17:27.000Z",
    "name": "China Chopper",
    "description": "This web shell is commonly used by malicious Chinese actors, including advanced persistent threat (APT) groups, to remotely control web servers. This web shell has two parts, the client interface (an executable file) and the receiver host file on the compromised web server.",
    "malware_types": ["webshell"],
    "is_family": false,
    "sample_refs": ["file--e277603e-1060-5ad4-9937-c26c97f1ca69"]
},
```


資料來源：國家資通安全研究院整理

圖14 Artifact Object 範例(惡意程式樣本 Base64 編碼)

```
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6313",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
{
    "type": "email-message",
    "spec_version": "2.1",
    "id": "email-message--72b7698f-10c2-565a-a2a6-b4996a2f2265",
    "from_ref": "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
    "to_refs": ["email-addr--e4ee5301-b52d-59cd-a8fa-8036738c7194"],
    "is_multipart": false,
    "date": "2021-10-19T15:55:06.000Z",
    "subject": "Saying Hello",
    "raw_email_ref": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6313"
},
```


資料來源：國家資通安全研究院整理

圖15 Artifact Object 範例(惡意信件樣本 Base64 編碼)


```
{
    "type": "report",
    "spec_version": "2.1",
    "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
    "created": "2015-12-21T19:59:11.000Z",
    "modified": "2015-12-21T19:59:11.000Z",
    "name": "中國菜刀報告",
    "description": "中國菜刀惡意程式分析完整報告",
    "published": "2021-10-20T17:00:00.000Z",
    "object_refs": [
        "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333"
    ]
},
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
```


資料來源：國家資通安全研究院整理

圖16 Artifact Object 範例(報告 Base64 編碼)

2.3.2 Domain Name Object

情資使用 Domain Name 物件，針對來源網域、目的網域、來源 hostname 或目的 hostname，須填寫一項資訊至 value 欄位。

表17 Domain Name Object 屬性

項次	屬性	SOC 欄位	備註
1	value	來源網域	-
		目的網域	
		來源 hostname	
		目的 hostname	
2	resolves_to_refs	-	-

資料來源：國家資通安全研究院整理

```
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
    "value": "example.com"
},
```

資料來源：國家資通安全研究院整理

圖17 Domain Name Object 範例

2.3.3 Email Address Object

情資使用 Email Address 物件，針對寄件人信箱或收件人信箱，須填寫一項資訊至 value 欄位。

表18 Email Address Object 屬性

項次	屬性	SOC 欄位	備註
1	value	寄件人信箱	填寫電子郵件信箱
		收件人信箱	
2	display_name	-	
3	belongs_to_ref	-	

資料來源：國家資通安全研究院整理

```
{
    "type": "email-addr",
    "spec_version": "2.1",
    "id": "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
    "value": "jdoe@example.com"
},
```

資料來源：國家資通安全研究院整理

圖18 Email Address Object 範例

2.3.4 Email Message Object

情資使用 Email Message 物件，針對寄件人信箱參照或收件人信箱參照，至少須填寫一項資訊。

表19 Email Message Object 屬性

項次	屬性	SOC 欄位	備註
1	is_multipart	是否含多段 MIME 內容*	填寫 true 或 false
2	date	寄件日期*	YYYY-MM-DDTHH:mm:ss[.s+]Z

項次	屬性	SOC 欄位	備註
3	content_type	-	-
4	from_ref	寄件人信箱參照	填寫 Email Address Object 識別碼
5	sender_ref	-	-
6	to_refs	收件人信箱參照	填寫 Email Address Object 識別碼
7	cc_refs	-	-
8	bcc_refs	-	-
9	message_id	-	-
10	subject	惡意信件主旨*	-
11	received_lines	-	-
12	additional_header_fields	-	-
13	body	-	-
14	body_multipart	-	-
15	raw_email_ref	信件內容(惡意信件 Base64 編碼)參照	填寫 Artifact 物件識別碼

資料來源：國家資通安全研究院整理

```
{
    "type": "email-message",
    "spec_version": "2.1",
    "id": "email-message--72b7698f-10c2-565a-a2a6-b4996a2f2265",
    "from_ref": "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
    "to_refs": ["email-addr--e4ee5301-b52d-59cd-a8fa-8036738c7194"],
    "is_multipart": false,
    "date": "2021-10-19T15:55:06.000Z",
    "subject": "Saying Hello"
},
```


資料來源：國家資通安全研究院整理

圖19 Email Message Object 範例


```
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6313",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
{
    "type": "email-message",
    "spec_version": "2.1",
    "id": "email-message--72b7698f-10c2-565a-a2a6-b4996a2f2265",
    "from_ref": "email-addr--89f52ea8-d6ef-51e9-8fce-6a29236436ed",
    "to_refs": ["email-addr--e4ee5301-b52d-59cd-a8fa-8036738c7194"],
    "is_multipart": false,
    "date": "2021-10-19T15:55:06.000Z",
    "subject": "Saying Hello",
    "raw_email_ref": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6313"
},
```


資料來源：國家資通安全研究院整理

圖20 Email Message Object 範例(惡意信件 Base64 編碼)

2.3.5 File Object

情資使用 File 物件，針對檔案雜湊值或檔案內容(惡意程式樣本 Base64 編碼)參照，至少須填寫一項資訊；若為檔案內容(惡意程式樣本 Base64 編碼)參照，將相關 Malware 物件、File 物件與 Artifact 物件進行參照關聯，詳見圖 21。若為檔案雜湊值，將相關 Malware 物件與 File 物件進行參照關聯，詳見圖 22。

表20 File Object 屬性

項次	屬性	SOC 欄位	備註
1	extensions	-	
2	hashes	檔案雜湊值	參考官方文件或範例
3	size	檔案大小	
4	name	檔案名稱	
5	name_enc	-	
6	magic_number_hex	-	
7	mime_type	-	
8	ctime	檔案建立日期	YYYY-MM-DDTHH:mm:ss[.s+]Z
9	mtime	檔案修改日期	YYYY-MM-DDTHH:mm:ss[.s+]Z
10	atime	檔案存取日期	YYYY-MM-DDTHH:mm:ss[.s+]Z
11	parent_directory_ref	-	
12	contains_refs	-	

項次	屬性	SOC 欄位	備註
13	content_ref	檔案內容(惡意程式樣本 Base64 編碼)參照	填寫 Artifact Object 識別碼

資料來源：國家資通安全研究院整理


```
{
    "type": "artifact",
    "spec_version": "2.1",
    "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6311",
    "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ..."
},
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca69",
    "hashes": {
        "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db",
        "SHA-1": "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12",
        "MD5": "9e107d9d372bb6826bd81d3542a419d6"
    },
    "size": 25536,
    "name": "foo.dll",
    "ctime": "2021-10-01T08:17:27.000Z",
    "mtime": "2021-10-12T08:17:27.000Z",
    "atime": "2021-10-12T08:17:27.000Z",
    "content_ref": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6311"
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065",
    "created": "2021-05-12T08:17:27.000Z",
    "modified": "2021-05-12T08:17:27.000Z",
    "name": "China Chopper",
    "description": "This web shell is commonly used by malicious Chinese actors, including advanced persistent threat (APT) groups, to remotely control web servers. This web shell has two parts, the client interface (an executable file) and the receiver host file on the compromised web server.",
    "malware_types": ["webshell"],
    "is_family": false,
    "sample_refs": ["file--e277603e-1060-5ad4-9937-c26c97f1ca69"]
},
```


資料來源：國家資通安全研究院整理

圖21 File Object 範例(惡意程式樣本 Base64 編碼)

```
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca69",
    "hashes": {
        "SHA-256": "fe90a7e910cb3a4739bed9180e807e93fa70c90f25a8915476f5e4bfbac681db",
        "SHA-1": "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12",
        "MD5": "9e107d9d372bb6826bd81d3542a419d6"
    },
    "size": 25536,
    "name": "foo.dll",
    "ctime": "2021-10-01T08:17:27.000Z",
    "mtime": "2021-10-12T08:17:27.000Z",
    "atime": "2021-10-12T08:17:27.000Z",
},
{
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065",
    "created": "2021-05-12T08:17:27.000Z",
    "modified": "2021-05-12T08:17:27.000Z",
    "name": "China Chopper",
    "description": "This web shell is commonly used by malicious Chinese actors, including advanced persistent threat (APT) groups, to remotely control web servers. This web shell has two parts, the client interface (an executable file) and the receiver host file on the compromised web server.",
    "malware_types": ["webshell"],
    "is_family": false,
    "sample_refs": ["file--e277603e-1060-5ad4-9937-c26c97f1ca69"]
},
```


資料來源：國家資通安全研究院整理

圖22 File Object 範例(惡意程式雜湊值)

2.3.6 IPv4 Address Object

情資使用 IPv4 Address 物件，針對來源 IP 或目的 IP，須填寫一項資訊至 value 欄位。

表21 IPv4 Address Object 屬性

項次	屬性	SOC 欄位	備註
1	value	來源 IP	IPv4 地址
		目的 IP	
2	resolves_to_refs	-	-
3	belongs_to_refs	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "value": "198.51.100.2"
},
```


資料來源：國家資通安全研究院整理

圖23 IPv4 Address Object 範例

2.3.7 IPv6 Address Object

情資使用 IPv6 Address 物件，針對來源 IP 或目的 IP，須填寫一項資訊至 value 欄位。

表22 IPv6 Address Object 屬性

項次	屬性	SOC 欄位	備註
1	value	來源 IP	IPv6 地址
		目的 IP	
2	resolves_to_refs	-	-
3	belongs_to_refs	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "ipv6-addr",
    "spec_version": "2.1",
    "id": "ipv6-addr--1e61d36c-a16c-53b7-a80f-2a00161c96b1",
    "value": "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
},
```


資料來源：國家資通安全研究院整理

圖24 IPv6 Address Object 範例

2.3.8 Network Traffic Object

情資使用 Network Traffic 物件，針對來源 IP 參照、目的 IP 參照、來源網域參照、目的網域參照、來源 hostname 參照或目的 hostname 參照，至少須填寫一項資訊，以表示連線紀錄。

表23 Network Traffic Object 屬性

項次	屬性	SOC 欄位	備註
1	start	開始時間*	YYYY-MM-DDTHH:mm:ss[.s+]Z
2	end	結束時間	YYYY-MM-DDTHH:mm:ss[.s+]Z
3	is_active	連線是否存活	填寫 true 或 false，若有填寫結束時間，該欄位為 false
4	src_ref	來源 IP 參照	填寫 IPv4 Address Object、IPv6 Address Object 或 Domain Name Object 識別碼
		來源網域參照	
		來源 hostname 參照	
5	dst_ref	目的 IP 參照	填寫 IPv4 Address Object、IPv6 Address Object 或 Domain Name Object 識別碼
		目的網域參照	
		目的 hostname 參照	
6	src_port	來源通訊埠	填寫 0-65535
7	dst_port	目的通訊埠	填寫 0-65535
8	protocols	通訊協定*	參考官方文件或範例
9	src_byte_count	-	-
10	dst_byte_count	-	-

項次	屬性	SOC 欄位	備註
11	src_packets	-	-
12	dst_packets	-	-
13	ipfix	-	-
14	src_payload_ref	-	-
15	dst_payload_ref	-	-
16	encapsulates_refs	-	-
17	encapsulated_by_ref	-	-
18	extensions/ http-request-ext/ request_method	HTTP 請求方法	參考官方文件或範例
19	extensions/ http-request-ext/ request_value	HTTP 請求路徑	參考官方文件或範例
20	extensions/ http-request-ext/ request_version	HTTP 請求版本	參考官方文件或範例
21	extensions/ http-request-ext/ request_header	HTTP 請求標頭	參考官方文件或範例

資料來源：國家資通安全研究院整理

```
{
    "type": "network-traffic",
    "spec_version": "2.1",
    "id": "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f527d",
    "start": "2021-10-19T19:00:00Z",
    "end": "2021-10-19T19:00:01Z",
    "src_ref": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "src_port": 3333,
    "dst_ref": "ipv4-addr--ff26c055-6336-5bc5-b98d-13d6226742dd",
    "dst_port": 443,
    "protocols": [
        "https","tcp"
    ]
},
```


資料來源：國家資通安全研究院整理

圖25 Network Traffic Object 範例


```
{
    "type": "network-traffic",
    "spec_version": "2.1",
    "id": "network-traffic--2568d22a-8998-58eb-99ec-3c8ca74f5271",
    "start": "2021-10-19T19:00:00Z",
    "end": "2021-10-19T19:00:01Z",
    "src_ref": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "src_port": 3333,
    "dst_ref": "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
    "dst_port": 80,
    "protocols": [
        "http","tcp"
    ],
    "extensions": {
        "http-request-ext": {
            "request_method": "get",
            "request_value": "/download.html",
            "request_version": "http/1.1",
            "request_header": {
                "Accept-Encoding": "gzip,deflate",
                "User-Agent": "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113",
                "Host": "www.example.com"
            }
        }
    }
},
```


資料來源：國家資通安全研究院整理

圖26 Network Traffic Object 範例(HTTP 請求)

2.3.9 Process Object

情資使用 Process 物件，須填寫攻擊指令至 command_line 欄位。若攻擊指令由惡意程式產生，將相關 Malware Analysis 物件與 Process 物件進行參照關聯，詳見圖 27。若攻擊指令僅為觀測紀錄，將 Observed Data 物件與 Process 物件進行參照關聯即可。

表24 Process Object 屬性

項次	屬性	SOC 欄位	備註
1	extensions	-	-
2	is_hidden	-	-
3	pid	-	-
4	created_time	-	-
5	cwd	-	-
6	command_line	攻擊指令*	
7	environment_variables	-	-
8	opened_connection_refs	-	-
9	creator_user_ref	-	-
10	image_ref	-	-
11	parent_ref	-	-
12	child_refs	-	-

資料來源：國家資通安全研究院整理

```
{
    "type": "malware-analysis",
    "spec_version": "2.1",
    "id": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "created": "2021-10-16T18:52:24.277Z",
    "modified": "2021-10-16T18:52:24.277Z",
    "product": "avira",
    "submitted": "2021-10-20T08:36:14Z",
    "analysis_started": "2021-10-20T08:36:14Z",
    "analysis_ended": "2021-10-20T08:36:15Z",
    "result_name": "9/10",
    "analysis_sco_refs": ["process--d2ec5aab-808d-4492-890a-3c1a1e3cb06e"]
},
{
    "type": "process",
    "spec_version": "2.1",
    "id": "process--d2ec5aab-808d-4492-890a-3c1a1e3cb06e",
    "command_line": "wmic /node:172.16.40.227 /password:1qaz@WSX /user:eric service list"
},
```


資料來源：國家資通安全研究院整理

圖27 Process Object 範例

2.4 STIX Relationship Objects

本節於 SOC 欄位以「*」表示為 SOC 情資必填屬性

2.4.1 Sighting

資安監控單與情資分析單皆須使用 Sighting 物件以關聯攻擊手法、連線紀錄與資安設備，詳見表 25；情資分析單若有使用 Indicator、Malware 或 Vulnerability 物件，則須使用 Sighting 物件，以關聯惡意指標、惡意程式、漏洞與資安設備，詳見表 26。

表25 Sighting 屬性 1

項次	屬性	SOC 欄位	備註
1	description	觸發規則*	-
2	first_seen	-	-

項次	屬性	SOC 欄位	備註
3	last_seen	-	-
4	count	-	-
5	sighting_of_ref	攻擊手法參照*	填寫 Attack Pattern 物件識別碼
6	observed_data_refs	連線紀錄彙整參照*	填寫 Observed Data 物件識別碼
7	where_sighted_refs	設備參照*	填寫資安設備 Identity 物件識別碼
8	summary	-	-

資料來源：國家資通安全研究院整理


```
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c76",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "description": "ESET_MAL_LNX_ELF_Mirai_Malware",
    "sighting_of_ref": "attack-pattern--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "observed_data_refs": ["observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"],
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965920"]
},
```


資料來源：國家資通安全研究院整理

圖28 攻擊手法 Sighting 範例

表26 Sighting 屬性 2

項次	屬性	SOC 欄位	備註
1	description	-	-
2	first_seen	-	-
3	last_seen	-	-
4	count	-	-
5	sighting_of_ref	惡意指標、惡意程式或漏洞參照*	填寫 Indicator、Malware 或 Vulnerability 物件識別碼
6	observed_data_refs	-	-
7	where_sighted_refs	設備參照*	填寫資安設備 Identity 物件識別碼
8	summary	-	-

資料來源：國家資通安全研究院整理

```
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c75",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "sighting_of_ref": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965920"]
},
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c77",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "sighting_of_ref": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965920"]
},
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c78",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965920"]
},
```


資料來源：國家資通安全研究院整理

圖29 額外情資 Sighting 範例

2.4.2 Relationships

資安監控單與情資分析單皆須使用 Relationships 物件以關聯攻擊手法與受駭單位，詳見表 27。情資分析單若提供由惡意程式萃取分析之惡意指標，須使用 Relationships 物件以關聯惡意指標與惡意程式，詳見表 28。情資分析單若提供惡意程式分析資訊，須使用 Relationships 物件以關聯惡意程式分析與惡意程式，詳見表 29。

表27 Relationships 屬性 1

項次	屬性	SOC 欄位	備註
1	relationship_type	關聯類型*	填寫”targets”
2	description	-	
3	source_ref	攻擊手法參照*	填寫 Attack Pattern 物件識別碼
4	target_ref	受駭單位參照*	填寫受駭單位 Identity 物件識別碼
5	start_time	-	
6	stop_time	-	

資料來源：國家資通安全研究院整理


```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--b82b2819-3b86-4bd5-afb3-fa36cfbc3f20",
  "created": "2021-09-14T08:56:34.934895Z",
  "modified": "2021-09-14T08:56:34.934895Z",
  "relationship_type": "targets",
  "source_ref": "attack-pattern--5e4a2073-9643-44cb-a0b5-e7f4048446c7",
  "target_ref": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965919"
}
```


資料來源：國家資通安全研究院整理

圖30 Relationships 範例 1

表28 Relationships 屬性 2

項次	屬性	SOC 欄位	備註
1	relationship_type	關聯類型*	填寫”indicates”
2	description	-	
3	source_ref	惡意指標參照*	填寫 Indicator 物件識別碼
4	target_ref	惡意程式參照*	填寫 Malware 物件識別碼
5	start_time	-	
6	stop_time	-	

資料來源：國家資通安全研究院整理


```
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--014841f8-eb38-4673-9904-70f67c93dd8b",
    "created": "2021-10-16T18:52:24.277Z",
    "modified": "2021-10-16T18:52:24.277Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd32",
    "target_ref": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065"
},
```


資料來源：國家資通安全研究院整理

圖31 Relationships 範例 2

表29 Relationships 屬性 3

項次	屬性	SOC 欄位	備註
1	relationship_type	關聯類型*	填寫”analysis-of”
2	description	-	
3	source_ref	惡意程式分析參照*	填寫 Malware Analysis 物件識別碼
4	target_ref	惡意程式參照*	填寫 Malware 物件識別碼
5	start_time	-	
6	stop_time	-	

資料來源：國家資通安全研究院整理


```
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--014841f8-eb38-4673-9904-70f67c92dd8b",
    "created": "2021-10-16T18:52:24.277Z",
    "modified": "2021-10-16T18:52:24.277Z",
    "relationship_type": "analysis-of",
    "source_ref": "malware-analysis--d25167b7-fed0-4068-9ccd-a73dd2c5b07c",
    "target_ref": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065"
},
```


資料來源：國家資通安全研究院整理

圖32 Relationships 範例 3