端點偵測及應變機制
資料回傳格式說明

國家資通安全研究院

112年3月27日

說明文件更新紀錄(1/2)

- 近期更新之內容記錄

版本	簡報修正內容
111/1/25	初版
111/4/14	第16頁”機關EDR事件回傳格式說明(14/44)” roles備註欄位中”端點偵測及回應機制”調整為” 端點偵測及應變機制”
112/1/4	• 第9頁”機關EDR事件回傳格式說明(7/44)” • 範例中內容中”NCCST”調整為”NICS” • 第13頁”機關EDR事件回傳格式說明(11/44)” • 範例中內容中”技服中心”調整為”國家資通安全研究院” • 第27頁”機關EDR事件回傳格式說明(25/44)” • 壓縮密碼”NCCST”調整為” NICS”

說明文件更新紀錄(2/2)

- 近期更新之內容記錄

版本	簡報修正內容
112/1/7	更新簡報檔背景格式
112/1/30	更新簡報檔背景格式
112/3/27	• 第4頁架構圖原”技服中心LOGO”更換為”國家資通安全研究院LOGO” • 第21頁sample_refs之備註” Artifact Object 頁數”更改為”P29” • 新增附件三”檔案轉Base64方法”

機關EDR事件回傳架構說明

- EDR偵測到異常行為或惡意程式活動，並確認成為資安事件時，由SOC依特定格式透過現有聯防監控資料回傳管道提交至主管機關

機關EDR事件回傳格式說明(1/44)

- EDR設備依偵測結果產製事件單紀錄
  - 每台受駭主機需產生1份該主機對應之事件資料
  - 目前規劃為STIX Json(V2.1)格式，內容分為以下4個物件類型
    - STIX Meta Objects(SMO)
    - STIX Domain Objects(SDO)
    - STIX Cyber-observable Objects(SCO)
    - STIX Relationship Objects(SRO)

機關EDR事件回傳格式說明(2/44)

- 各物件類型詳細內容
  - 本事件單無擴充事項，STIX Meta Objects無需填寫
  - STIX Domain Objects之Grouping、Attack Pattern、Identity及Observed Data為必要物件
  - Indicator、Malware、Malware Analysis若無資料時無須填寫，但有相關資料時必須填寫
    - 例如惡意程式類行為主動式後門，則須填寫中繼站資料，但若惡意程式類型為掃描工具(如nmap)，則無需填寫中繼站資料
  - Report為事件單之選擇性使用物件(無論是否有報告)
  - STIX Cyber-observable Objects皆為必填物件，
    - 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
  - STIX Relationship Objects皆為必要物件

機關EDR事件回傳格式說明(3/44)

- 各物件類型詳細內容

項次	物件類型	物件	必填
1	STIX Domain Objects(SDO)	Grouping(基本資訊)	V
		Attack Pattern(攻擊手法)	V
		Identity(資安監控單位、受駭單位、資安設備)	V
		Indicator(中繼站資訊)	V
		Malware(惡意程式資訊)	V
		Malware Analysis(惡意程式分析資訊)	V
		Observed Data(主機資訊)	V
		Report(EDR報告)	
2	STIX Cyber-observable Objects(SCO)	Artifact Object(檔案Base64 編碼)	V
		Domain Name Object(主機hostname)	V
		File Object(惡意程式詳細資料)	V
		IPv4 Address Object(主機IP)	V
		Process(可疑活動(cmd))	
3	STIX Relationship Objects(SRO)	Sightning	V
		Relationships	V

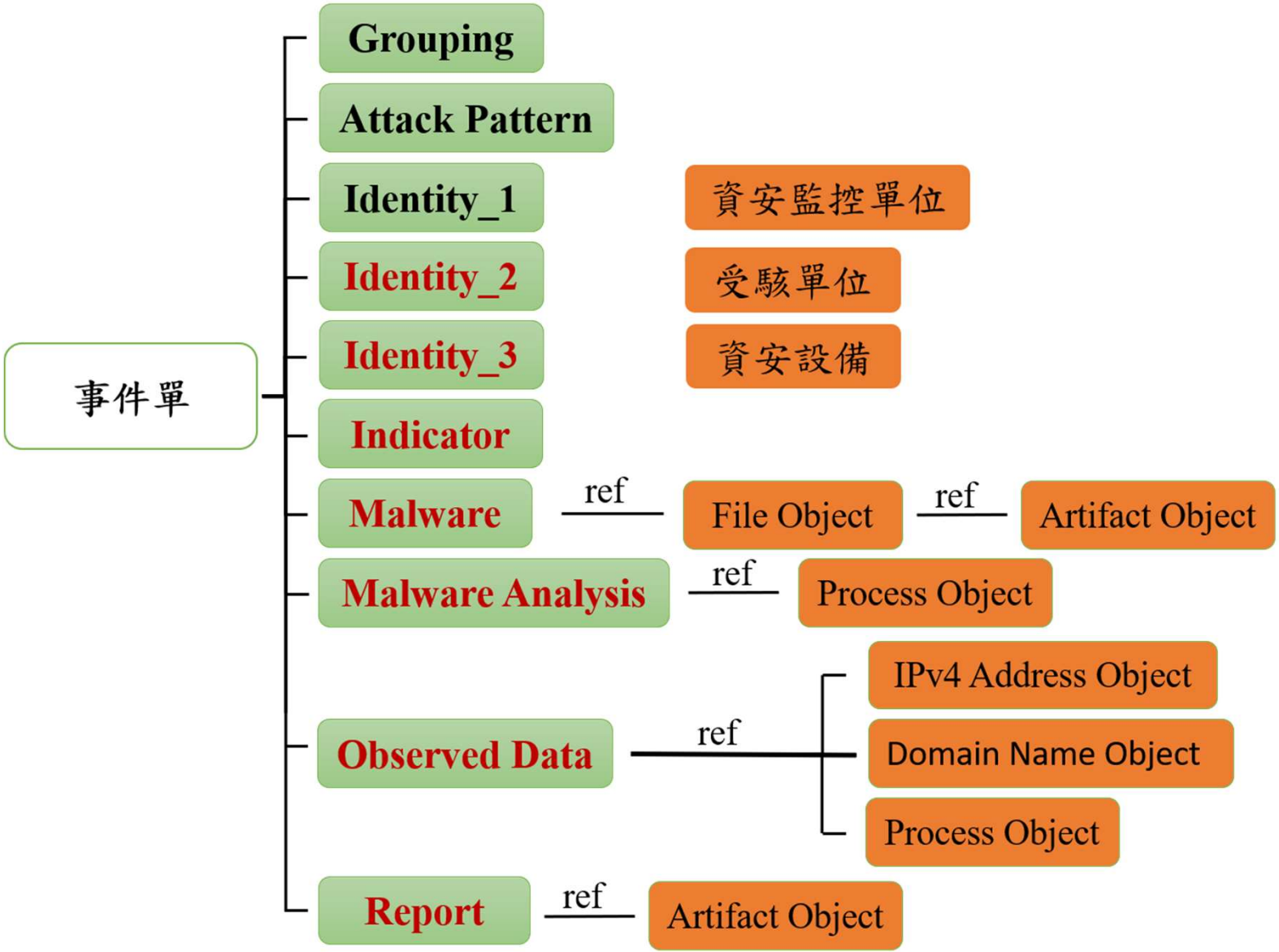
機關EDR事件回傳格式說明(4/44)

- STIX物件基本屬性
  - 參考官方文件或範例

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

機關EDR事件回傳格式說明(5/44)

- 機關EDR事件單架構



機關EDR事件回傳格式說明(6/44)

- 基本資訊欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	情資主旨	參考附件一	V
2	description	情資描述		V
3	labels	情資編號	SOC英縮寫-機關英縮寫-日期-編號	V
4	context	情資類別	參考N-SOC情資類別(參照附件一)	V
5	object_refs	相關SDO與SCO參照	填寫所有相關SDO與SCO識別碼	V
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	V

機關EDR事件回傳格式說明(7/44)

- 基本資訊欄位說明

  –範例

```
{
    "type": "grouping",
    "id": "grouping--9c82a63e-c4fa-4e89-949c-6cad9e430d70",
    "created_by_ref": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965918",
    "created": "2021-09-14T08:56:34.935656Z",
    "modified": "2021-09-14T08:56:34.935656Z",
    "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Waterbear惡意程式，並主動與中繼站連線",
    "object_refs": [
      "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
      "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333",
      ……,
      "relationship--b82b2819-3b86-4bd5-afb3-fa36cfbc3f20"
    ]
}
```

機關EDR事件回傳格式說明(8/44)

- 攻擊手法欄位說明
  - MITRE ATT&CK
    - 直接複製MITRE ATT&CK官方網站 https://attack.mitre.org/resources/working-with-attack/之該類別STIX格式內容
  - 查不到MITRE ATT&CK

項次	屬性	欄位名稱	備註	必填
1	name	攻擊手法		V
2	description	攻擊手法補充說明		V
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	

機關EDR事件回傳格式說明(9/44)

- 攻擊手法欄位說明
  - –範例1(MITRE ATT&CK)

raw.githubusercontent.com/mitre-attack/attack-stix-data/master/enterprise-attack/enterprise-attack-8.0.json


```
            "x_mitre_attack_spec_version": "2.1.0",
            "x_mitre_domains": [
                "enterprise-attack"
            ],
            "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5"
        },
        {
            "id": "attack-pattern--3f886f2a-874f-4333-b794-aa6075009b1c",
            "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
            "name": "Exploit Public-Facing Application",
            "description": "Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using
software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch,
or a design vulnerability. These applications are often websites, but can include databases (like SQL)(Citation: NVD CVE-2016-6662),
standard services (like SMB(Citation: CIS Multiple SMB Vulnerabilities) or SSH), network device administration and management protocols
(like SNMP and Smart Install(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device
Attacks)), and any other applications with Internet accessible open sockets, such as web servers and related services.(Citation: NVD
CVE-2014-7169) Depending on the flaw being exploited this may include [Exploitation for Defense Evasion]
(https://attack.mitre.org/techniques/T1211). \n\nIf an application is hosted on cloud-based infrastructure, then exploiting it may lead
to compromise of the underlying instance. This can allow an adversary a path to access the cloud APIs or to take advantage of weak
identity and access management policies.\n\nFor websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-
based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)",
            "external_references": [
                {
                    "source_name": "mitre-attack",
                    "external_id": "T1190",
                    "url": "https://attack.mitre.org/techniques/T1190"
                },
                {
```

機關EDR事件回傳格式說明(10/44)

- 攻擊手法欄位說明
  - 範例2(自訂)


```
{
    "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"
      }
    ]
}
```

機關EDR事件回傳格式說明(11/44)

- 資安監控單位欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	資安監控單位	監控單位(服務業者)全名	V
2	identity_class	資安監控單位資訊	填寫”SOC”	V

–範例


```
{
    "type": "identity",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965918",
    "created": "2021-09-14T08:56:34.897484Z",
    "modified": "2021-09-14T08:56:34.897484Z",
    "name": "國家資通安全研究院",
    "identity_class": "SOC  ”
}
```

機關EDR事件回傳格式說明(12/44)

- 受駭單位欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	單位名稱	單位中文名稱	V
2	description	單位代碼	單位OID	V
3	roles	單位等級	A、B、C、D、E	V
4	identity_class	單位資訊	填寫”government”	V
5	sectors	單位所屬領域/區域	能源、水資源、通訊傳播、 交通、金融、教育、 緊急救援及醫院、中央及地方政府、 科學園區與工業區、臺北區域聯防中心、 新北區域聯防中心、桃園區域聯防中心、 臺中區域聯防中心、臺南區域聯防中心、 高雄區域聯防中心	V

機關EDR事件回傳格式說明(13/44)

- 受駭單位欄位說明
  - 範例


```
{
    "type": "identity",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965919",
    "created": "2021-09-14T08:56:34.897484Z",
    "modified": "2021-09-14T08:56:34.897484Z",
    "name": "OO市政府資訊中心",
    "description": "2.16.886.101.OOOOO.XXXXX",
    "roles":["B"],
    "identity_class": "government",
    "sectors":"中央及地方政府 “
}
```

機關EDR事件回傳格式說明(14/44)

- 資安設備欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	設備代號	填寫”EDR”	V
2	description	設備廠商	EDR廠商名稱	V
3	roles	資安防護類型	填寫”端點偵測及應變機制”	V
4	identity_class	設備資訊	填寫”system”	V

–範例


```
{
    "type": "identity",
    "id": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965931",
    "created": "2021-09-14T08:56:34.897484Z",
    "modified": "2021-09-14T08:56:34.897484Z",
    "name": "EDR",
    "description": "T5",
    "roles":["端點偵測及應變機制"],
    "identity_class": "system  “
}
```

機關EDR事件回傳格式說明(15/44)

- 中繼站資訊欄位說明

項次	屬性	欄位名稱	備註	必填
1	description	惡意指標描述	-	V
2	indicator_types	惡意指標類型	填寫”IOC”或”IOA”	V
3	pattern	中繼站IP	STIX Patterning表示法 請參考官方文件或範例	V
		中繼站域名		
4	pattern_type	惡意指標表示法	請填寫”stix”	V
5	valid_from	惡意指標有效起始時間	YYYY-MM-DDTHH:mm:ss[.s+]Z	V

機關EDR事件回傳格式說明(16/44)

- 中繼站資訊欄位說明
  - 範例


```
{
    "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  domain-name:value = 'www.5z8.info']",
    "pattern_type": "stix",
    "valid_from": "2021-10-01T00:00:00Z"
}
```

機關EDR事件回傳格式說明(17/44)

- 惡意程式資訊欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	惡意程式族群	無惡意程式族群請填"None"	V
2	description	惡意程式描述	-	V
3	malware_types	惡意程式類型	請參考官方文件訂定之malware-type-ov字典(參照附件二)	V
4	is_family	是否代表惡意程式家族	填寫true或false	V
5	sample_refs	惡意程式樣本參照	填寫File Object識別碼(惡意程式可先進行壓縮加密，詳見Artifact Object，P29)	V

機關EDR事件回傳格式說明(18/44)

- 惡意程式資訊欄位說明
  - 範例


```
{
    "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": "Waterbear",
    "description": "惡意程式描述.....",
    "malware_types": ["backdoor"],
    "is_family": false,
    "sample_refs": ["file--e277603e-1060-5ad4-9937-c26c97f1ca69"]
}
```

機關EDR事件回傳格式說明(19/44)

- 惡意程式分析資訊欄位說明

項次	屬性	欄位名稱	備註	必填
1	product	EDR廠商名稱	-	V
2	submitted	EDR掃描受駭主機之結束時間	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
3	result_name	惡意程式威脅程度	惡意程式等級/最高等級	V
4	result	惡意程式威脅程度(官方分級)	填寫Malicious、suspicious、 benign或unknown	V
5	analysis_sco_refs	惡意程式執行命令參照	填寫所有相關Process Object識別碼	

機關EDR事件回傳格式說明(20/44)

- 惡意程式分析資訊欄位說明
  - 範例


```
{
    "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":   “EDR_VENDER",
    "submitted": "2021-10-20T08:36:14Z",
    "result_name": "9/10",
    "result": "Malicious",
    "analysis_sco_refs": ["process--d2ec5aab-808d-4492-890a-3c1a1e3cb06e"]
}
```

機關EDR事件回傳格式說明(21/44)

- 主機資訊欄位說明

項次	屬性	欄位欄位	備註	必填
1	first_observed	EDR掃描受駭主機之開始時間	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
2	last_observed	EDR掃描受駭主機之結束時間	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
3	number_observed	掃描次數	填寫”1”	V
4	object_refs	受駭主機IPv4參照	填寫所有相關SCO-IPv4 Address識別碼	V
		受駭主機Hostname參照	填寫所有相關SCO-Domain Name識別碼	V
		受駭主機執行之可疑command參照	填寫所有相關Process Object識別碼	

機關EDR事件回傳格式說明(22/44)

- 主機資訊欄位說明
  - 範例


```
{
    "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": "2021-10-19T19:05:01Z",
    "number_observed": 1,
    "object_refs":
    [
      "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
      "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
      "process--d2ec5aab-808d-4492-890a-3c1a1e3cb06e"
    ]
}
```

機關EDR事件回傳格式說明(23/44)

- EDR報告欄位說明

項次	屬性	欄位名稱	備註	必填
1	name	報告檔名	不含副檔名	V
2	description	報告描述	-	V
3	published	報告匯出時間	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
4	object_refs	報告內容參照	填寫Artifact Object識別碼	V

機關EDR事件回傳格式說明(24/44)

- EDR報告欄位說明
  - 範例


```
{
    "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": "EDR報告",
    "description": "EDR掃描完整報告",
    "published": "2021-10-20T17:00:00.000Z",
    "object_refs":
    [
        "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333"
    ]
}
```

機關EDR事件回傳格式說明(25/44)

- 檔案Base64 編碼欄位說明
  - 相關物件
    - Report(EDR報告)
    - File Object(惡意程式詳細資料)
      - Artifact Object目前可接受兩種格式
        1. 直接將惡意程式轉換成Base64 編碼
        2. 將惡意程式先壓縮成ZIP格式(密碼：nics)，再將壓縮檔轉換成Base64 編碼

項次	屬性	欄位名稱	備註	必填
1	payload_bin	惡意程式樣本Base64編碼	-	V
		報告Base64編碼		

機關EDR事件回傳格式說明(26/44)

- 檔案Base64 編碼欄位說明

  –範例

```
{
        "type": "artifact",
        "spec_version": "2.1",
        "id": "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333",
        "payload_bin": "VBORw0KGgoAAAANSUhEUgAAADI== ... "
},
{
        "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": "EDR報告",
        "description": "EDR掃描完整報告",
        "published": "2021-10-20T17:00:00.000Z",
        "object_refs": [
          "artifact--ca17bcf8-9846-5ab4-8662-75c1bf6e6333"
        ]
}
```

機關EDR事件回傳格式說明(27/44)

- 主機hostname欄位說明
  - 相關物件
    - Observed Data(主機資訊)

項次	屬性	欄位名稱	備註	必填
1	value	hostname	-	V

機關EDR事件回傳格式說明(28/44)

- 主機hostname欄位說明
  - 範例


```
{
    "type": "domain-name",
    "spec_version": "2.1",
    "id": "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
    "value": "DESKTOP-THXXXX  "
},
{
    "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": "2021-10-19T19:05:01Z",
    "number_observed": 1,
    "object_refs": [
      "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
      "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5"
    ]
}
```

機關EDR事件回傳格式說明(29/44)

- 惡意程式詳細資料欄位說明
  - 相關物件
    - Malware(惡意程式資訊)

項次	屬性	欄位名稱	備註	必填
1	hashes	檔案雜湊值	參考官方文件或範例(至少含MD5)	V
2	size	檔案大小	單位：byte	V
3	name	檔案名稱	含附檔名	V
4	ctime	檔案建立日期	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
5	mtime	檔案修改日期	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
6	atime	檔案存取日期	YYYY-MM-DDTHH:mm:ss[.s+]Z	V
7	content_ref	檔案內容(Base64編碼)參照	填寫Artifact Object識別碼	V

機關EDR事件回傳格式說明(30/44)

- 惡意程式詳細資料欄位說明
  - 範例

```
{
    "type": "file",
    "spec_version": "2.1",
    "id": "file--e277603e-1060-5ad4-9937-c26c97f1ca69",
    "hashes": {
      "SHA-256": "fe90a7….0f25a8915476f5e4bfbac681db",
      "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",
    ...,
    "sample_refs": ["file--e277603e-1060-5ad4-9937-c26c97f1ca69"]
}
```

機關EDR事件回傳格式說明(31/44)

- 主機IP欄位說明
  - 相關物件
    - Observed Data(主機資訊)

項次	屬性	欄位名稱	備註	必填
1	value	主機IP	IPv4地址	V

機關EDR事件回傳格式說明(32/44)

- 主機IP欄位說明
  - 範例


```
{
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
    "value": "198.51.100.2  “
},
{
    "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": "2021-10-19T19:05:01Z",
    "number_observed": 1,
    "object_refs": [
      "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
      "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5"
    ]
}
```

機關EDR事件回傳格式說明(33/44)

- 可疑活動(cmd)欄位說明
  - 相關物件
    - Malware Analysis(惡意程式分析資訊)
    - Observed Data(主機資訊)

項次	屬性	欄位名稱	備註	必填
1	command_line	命令行	-	V

機關EDR事件回傳格式說明(34/44)

- 可疑活動(cmd)說明
  - 範例


```
{
        "type": "observed-data",
        "spec_version": "2.1",
        "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
        ...,
        "last_observed": "2021-10-19T19:05:01Z",
        "number_observed": 1,
        "object_refs": [
          "ipv4-addr--4d22aae0-2bf9-5427-8819-e4f6abf20a53",
          "domain-name--3c10e93f-798e-5a26-a0c1-08156efab7f5",
          "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  "
}
```

機關EDR事件回傳格式說明(35/44)

- Sightning物件
  - 關聯攻擊手法(Attack Pattern)、主機資訊(Observed Data)與資安設備

項次	屬性	欄位名稱	備註	必填
1	description	觸發規則	-	V
2	sighting_of_ref	攻擊手法參照	填寫Attack Pattern物件識別碼	V
3	observed_data_refs	主機資訊參照	填寫Observed Data物件識別碼	V
4	where_sighted_refs	設備參照	填寫資安設備Identity物件識別碼	V

機關EDR事件回傳格式說明(36/44)

- Sightning
  - 關聯攻擊手法(Attack Pattern)、主機資訊(Observed Data)與資安設備
    - 範例


```
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c79",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "description": "ESET_MAL_LNX_ELF_Waterbear_Malware",
    "sighting_of_ref": "attack-pattern--3f886f2a-874f-4333-b794-aa6075009b1c",
    "observed_data_refs": ["observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf"],
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965931"]
}
```

機關EDR事件回傳格式說明(37/44)

- Sightning物件
  - 關聯中繼站(Indicator)、惡意程式(Malware) 與資安設備

項次	屬性	欄位名稱	備註	必填
1	sighting_of_ref	惡意指標、惡意程式參照	填寫Indicator、Malware物件識別碼	V
2	where_sighted_refs	設備參照	填寫資安設備Identity物件識別碼	V

機關EDR事件回傳格式說明(38/44)

- Sightning物件
  - 關聯中繼站(Indicator)、惡意程式(Malware) 與資安設備
    - 範例


```
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623a80",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "sighting_of_ref": "malware--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0065",
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965931"]
},
{
    "type": "sighting",
    "spec_version": "2.1",
    "id": "sighting--ee20065d-2555-424f-ad9e-0f8428623c80",
    "created": "2016-04-06T20:08:31.000Z",
    "modified": "2016-04-06T20:08:31.000Z",
    "sighting_of_ref": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd32",
    "where_sighted_refs": ["identity--0290e9ce-cbd1-4c4c-b23f-9585ba965931"]
},
```

機關EDR事件回傳格式說明(39/44)

- Relationships物件
  - 關聯攻擊手法(Attack Pattern)與受駭單位

項次	屬性	欄位名稱	備註	必填
1	relationship_type	關聯類型	填寫”targets”	V
2	source_ref	攻擊手法參照	填寫Attack Pattern物件識別碼	V
3	target_ref	受駭單位參照	填寫受駭單位Identity物件識別碼	V

機關EDR事件回傳格式說明(40/44)

- Relationships物件
  - 關聯攻擊手法(Attack Pattern)與受駭單位
    - 範例


```
{
    "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--3f886f2a-874f-4333-b794-aa6075009b1c",
    "target_ref": "identity--0290e9ce-cbd1-4c4c-b23f-9585ba965919"
}
```

機關EDR事件回傳格式說明(41/44)

- Relationships物件
  - 關聯中繼站(Indicator)與惡意程式(Malware)

項次	屬性	欄位名稱	備註	必填
1	relationship_type	關聯類型	填寫”indicates”	V
2	source_ref	中繼站資訊參照	填寫Indicator物件識別碼	V
3	target_ref	惡意程式參照	填寫Malware物件識別碼	V

機關EDR事件回傳格式說明(42/44)

- Relationships物件
  - 關聯中繼站(Indicator)與惡意程式(Malware)
    - 範例


```
{
    "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  "
}
```

機關EDR事件回傳格式說明(43/44)

- Relationships物件
  - 關聯惡意程式分析(Malware Analysis)與惡意程式(Malware)

項次	屬性	欄位名稱	備註	必填
1	relationship_type	關聯類型	填寫” analysis-of”	V
2	source_ref	惡意程式分析參照	填寫Malware Analysis物件識別碼	V
3	target_ref	惡意程式參照	填寫Malware物件識別碼	V

機關EDR事件回傳格式說明(44/44)

- Relationships物件
  - 關聯惡意程式分析(Malware Analysis)與惡意程式(Malware)
    - 範例


```
{
    "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  “
}
```

附件一

- NISAC資安事件類型(1/3)

項次	資安事件類型(context)	內容說明	情資主旨範例(name)
1	惡意內容 Abusive Content	針對透過文字、照片、影片等形式散播不當內容之事件，分享相關資訊予特定會員 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 Malicious Code	針對與相關惡意程式之事件，分享相關資訊予特定會員，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
3	資訊蒐集 Information Gathering	針對透過掃描、探測及社交工程等攻擊手法取得資訊之事件，分享相關資訊予特定會員	• 外部主機執行掃描探測攻擊 • 弱點掃描行為
4	入侵嘗試 Intrusion Attempts	針對嘗試入侵未經授權(Authorization)主機之事件，分享相關資訊予特定會員，如 • 試圖透過暴力破解或漏洞等攻擊手法，入侵未經授權主機	• 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

附件一

- NISAC資安事件類型(2/3)

項次	資安事件類型(context)	內容說明	情資主旨範例(name)
5	入侵攻擊 Intrusions	針對系統遭未經授權(Authorization)存取或取得系統/使用者權限之事件，分享相關資訊予特定會員	• 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 Availability	針對影響服務可用性(Availability)或造成服務中斷之攻擊事件，分享相關資訊予特定會員，如： • 阻斷服務攻擊	• 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 Information Content Security	針對系統遭未經驗證(Authentication)存取或影響資訊機敏性(Confidentiality)之事件，分享相關資訊予特定會員，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
8	詐欺攻擊 Fraud	針對偽冒他人身分、系統服務及組織等進行攻擊行為之事件，分享相關資訊予特定會員如： • 釣魚郵件 • 釣魚網站	發送釣魚郵件

附件一

- NISAC資安事件類型 (3/3)

項次	資安事件類型 (context)	內容說明	情資主旨範例 (name)
9	系統弱點 Vulnerable	針對系統存在弱點之事件，可能遭利用進而影響系統機敏性(Confidentiality)、完整性(Integrity)或可用性(Availability)，分享相關資訊予特定會員	系統疑似存在RCE漏洞
10	其他 Other	分享非屬前述資安事件類型之事件資訊予特定會員	

附件二

- malware-type-ov字典(1/3)

惡意程式類型 (malware_types)	內容說明
adware	Any software that is funded by advertising. Adware may also gather sensitive user information from a system.
backdoor	A malicious program that allows an attacker to perform actions on a remote system, such as transferring files, acquiring passwords, or executing arbitrary commands [NIST800-83].
bot	A program that resides on an infected system, communicating with and forming part of a botnet. The bot may be implanted by a worm or Trojan, which opens a backdoor. The bot then monitors the backdoor for further instructions.
bootkit	A malicious program which targets the Master Boot Record of the target computer.
ddos	A program that is used to perform a distributed denial of service attack.
downloader	A small trojan file programmed to download and execute other files, usually more complex malware.
dropper	A type of trojan that deposits an enclosed payload (generally, other malware) onto the target computer.

附件二

- malware-type-ov字典(2/3)

惡意程式類型 (malware_types)	內容說明
exploit-kit	A software toolkit to target common vulnerabilities.
keylogger	A type of malware that surreptitiously monitors keystrokes and either records them for later retrieval or sends them back to a central collection point.
ransomware	A type of malware that encrypts files on a victim's system, demanding payment of ransom in return for the access codes required to unlock files.
remote-access-trojan	A remote access trojan program (or RAT), is a trojan horse capable of controlling a machine through commands issued by a remote attacker.
resource-exploitation	A type of malware that steals a system's resources (e.g., CPU cycles), such as a malicious bitcoin miner.
rogue-security-software	A fake security product that demands money to clean phony infections.
rootkit	A type of malware that hides its files or processes from normal methods of monitoring in order to conceal its presence and activities. Rootkits can operate at a number of levels, from the application level — simply replacing or adjusting the settings of system software to prevent the display of certain information — through hooking certain functions or inserting modules or drivers into the operating system kernel, to the deeper level of firmware or virtualization rootkits, which are activated before the operating system and thus even harder to detect while the system is running.

附件二

- malware-type-ov字典(3/3)

惡意程式類型 (malware_types)	內容說明
screen-capture	A type of malware used to capture images from the target systems screen, used for exfiltration and command and control.
spyware	Software that gathers information on a user's system without their knowledge and sends it to another party. Spyware is generally used to track activities for the purpose of delivering advertising.
trojan	Any malicious computer program which is used to hack into a computer by misleading users of its true intent.
unknown	There is not enough information available to determine the type of malware.
virus	A malicious computer program that replicates by reproducing itself or infecting other programs by modifying them.
webshell	A malicious script used by an attacker with the intent to escalate and maintain persistent access on an already compromised web application.
wiper	A piece of malware whose primary aim is to delete files or entire disks on a machine.
worm	A self-replicating, self-contained program that usually executes itself without user intervention.

附件三

- 檔案轉Base64編碼(C#)

```
using System.IO;

public static String encodeBase64File(String FilePath) {
            FileStream inFile = new System.IO.FileStream(FilePath, System.IO.FileMode.Open,
System.IO.FileAccess.Read);
            byte[] binaryData = new Byte[inFile.Length];
            long bytesRead = inFile.Read(binaryData, 0, (int)inFile.Length);
            inFile.Close();
            string base64String = System.Convert.ToBase64String(binaryData, 0,
binaryData.Length);
            return base64String;
}
```