# Web基礎網路參與(WBNP)和發件人基礎網路參與(SBNP)

## 目錄



## 簡介

思科Web和電子郵件內容安全產品可以向思科和Talos提供遙測資料，以提高網路安全裝置(WSA)中網路分類以及連線電子郵件安全裝置(ESA)的IP信譽的有效性。

為WSA和ESA提供的遙測資料是「選擇加入」的。

資料通過二進位制編碼SSL加密資料包傳輸。 以下附件將提供對傳輸的資料的資料、特定格式和說明的深入分析。 無法以直接日誌或檔案格式檢視WebBase網路參與(WBNP)和SenderBase網路參與(SBNP)資料。 該資料以加密形式傳輸。 這些資料在任何時候都不會「閒置」。

### WSA - WebBase網路參與

思科認識到維護隱私的重要性，不會收集或使用個人資訊或機密資訊，如使用者名稱和密碼。此外，主機名後面的檔名和URL屬性會被模糊處理，以確保機密性。

當涉及解密HTTPS事務時，SensorBase網路只接收證書中伺服器名稱的IP地址、Web信譽分數和URL類別。

有關完整資訊，請檢視WSA使用手冊，瞭解裝置上當前運行的AsyncOS for Web Security的版本。 請參閱《使用手冊》中的「Cisco SensorBase網路」。

### ESA - SenderBase網路參與

參與SenderBase網路的客戶允許思科收集有關其組織的聚合電子郵件流量統計資訊，從而提高服務對所有使用者的效用。參與是自願的。思科僅收集有關郵件屬性的摘要資料，以及有關思科裝置如何處理不同型別郵件的資訊。例如，思科不會收集郵件正文或郵件主題。個人身份資訊和標識組織的資訊將保密。

有關完整資訊， p租賃稽核ESA使用手冊 適用於裝置上當前運行的AsyncOS for ESA安全版本。 請參閱《使用手冊》中的「SenderBase網路參與」一章。

## 一般安全顧慮常見問題

問題： 收集的資料儲存在哪裡？
答案： 裝置遙測儲存在思科美國資料中心。
問題： 誰有權訪問收集和儲存的資料？
答案： 僅限分析/使用資料以建立可操作情報的Cisco SBG人員訪問。
問題： 所收集資料的保留時間是多少？
答案： 沒有與裝置遙測相關的資料保留/過期策略。資料可能會無限期保留，也可能由於各種原因被刪除，
問題： 客戶序列號或公共IP地址是否儲存在Talos分類資料庫中？
答案： 否，僅保留URL和類別。WBNP資料包不包含源IP資訊。

## 操作

下面詳細介紹操作、資料型別（按說明）以及演示將傳輸資訊的示例資料：

- SBNP — 與郵件安全相關的特定資料型別（欄位）和示例資料
- WBNP — 與Web安全相關的特定資料型別（欄位）和示例資料
- 威脅檢測操作 — 從操作角度概述威脅檢測

### SenderBase（電子郵件）網路參與

#### 每封電子郵件共用的統計資訊裝置

| 專案 | 示例資料 |
| --- | --- |
| MGA識別符號 | MGA 10012 |
| 時間戳 | 資料從2005年7月1日上午8點 |
| 軟體版本號碼 | MGA版本4.7.0 |
| 規則集版本號 | 反垃圾郵件規則集102 |
| 防病毒更新間隔 | 每10分鐘更新一次 |
| 隔離區大小 | 500 MB |
| 隔離郵件計數 | 目前隔離區中有50封郵件 |
| 病毒分數閾值 | 將郵件傳送到威脅級別3或更高 |

| | |
|---|---|
| 進入隔離區的郵件的病毒分數總和 | 120 |
| 進入隔離區的郵件計數 | 30（平均得分為4） |
| 最長隔離時間 | 12小時 |
| 按進入和退出隔離區的原因劃分的爆發隔離區郵件計數，與防病毒結果相關 | 50個由於.exe規則進入隔離區 |
| 按離開隔離區後執行的操作劃分的爆發隔離區郵件計數 | 10封郵件在離開隔離區後刪除 |
| 郵件在隔離區中保留的時間總和 | 20小時 |

**每個IP地址共用統計資訊**

| **專案** | **示例資料** | **標準參與** | **有限參與** |
|---|---|---|---|
| 裝置內不同階段的郵件計數 | 防病毒引擎檢測到：100<br>反垃圾郵件引擎檢測到：80 | | |
| 反垃圾郵件和防病毒評分和裁決的總和 | 2,000（所有可見郵件的反垃圾郵件分數總和） | | |
| 遇到不同反垃圾郵件和防病毒規則組合的郵件數 | 100條報文命中規則A和B<br>僅50條消息命中規則A | | |
| 連線數 | 20個SMTP連線 | | |
| 收件人總數和無效收件人數 | 共50個收件人<br>10個無效收件人 | | |
| 雜湊檔名：(答) | 在名為<one-way-hash>.zip的存檔附件中發現檔案<one-way-hash>.pif。 | 未模糊的檔名 | 雜湊檔名 |
| 模糊檔名：(b) | 在檔案aaaaaa.zip中找到檔案aaaaa0.aaa.pif。 | 未模糊的檔名 | 模糊檔名 |
| URL主機名(c) | 在www.domain.com的郵件中找到一個連結 | 未模糊的URL主機名 | 模糊的URL主名 |
| 模糊的URL路徑(d) | 在發往主機名www.domain.com的消息中發現一個連結，該連結具有路徑aaa000aa/aa00aaa。 | 未模糊的URL路徑 | 模糊的URL路 |
| 按垃圾郵件和病毒掃描結果列出的郵件數 | 10個垃圾郵件<br>10個垃圾郵件負數<br>5可疑垃圾郵件<br>4病毒陽性<br>16病毒陰性<br>5病毒無法掃描 | | |
| 按不同的反垃圾郵件和防病毒判定結果顯示的郵件數 | 500個垃圾郵件、300個火腿 | | |
| 大小範圍內的消息計數 | 30K-35K範圍內的125個 | | |
| 不同擴展型別的計數 | 300個「.exe」附件 | | |
| 附件型別、實際檔案型別和容器型別的關聯 | 100個附件具有「.doc」副檔名但實際上是「.exe」<br>50個附件是zip中的「.exe」副檔名 | | |
| 副檔名和實際檔案型別與附件大小的相關性 | 50-55K範圍內有30個附件為「.exe」 | | |
| 按隨機抽樣結果統計的消息數 | 14條消息跳過取樣<br>25條消息排隊等待取樣<br>通過取樣掃描50條報文 | | |
| DMARC驗證失敗的郵件數 | 34條報文未能通過DMARC驗證 | | |

附註：

(a)檔名將以單向雜湊(MD5)編碼。

(b)檔名將以模糊形式傳送，所有小寫的ASCII字母([a-z])替換為"a"，所有大寫的ASCII字母([A-

Z])替換為"A"，任何多位元組UTF-8字元替換為"x"（為其他字符集提供隱私），所有ASCII數字([0-9])替換為。

(c)與IP地址一樣，URL主機名指向提供內容的Web伺服器。不包括使用者名稱和密碼等機密資訊。

(d)對主機名後面的URL資訊進行模糊處理，以確保不洩露使用者的任何個人資訊。

### 每個SDS客戶端共用的統計資訊

| 專案 | 示例資料 |
|---|---|
| 時間戳 | |
| 客戶端版本 | |
| 向客戶端發出的請求數 | |
| 從SDS客戶端發出的請求數 | |
| DNS查詢的時間結果 | |
| 伺服器響應時間結果 | |
| 建立與伺服器連線的時間 | |
| 已建立的連線數 | |
| 到伺服器的併發開啟連線數 | |
| 對WBRS的服務請求數 | |
| 命中本地WBRS快取的請求數 | |
| 本地WBRS快取的大小 | |
| 遠端WBRS的響應時間結果 | |

### AMP SBNP遙測資料

| 格式 | 示例資料 |
|---|---|
| amp_verdicts' :{("verdict"、"spyname"、"score"、"uploaded"、"file_name")、<br>("verdict"、"spyname"、"score"、"uploaded"、"file_name")、<br>("verdict"、"spyname"、"score"、"uploaded"、"file_name")、<br>.....<br>("verdict"、"spyname"、"score"、"uploaded"、"file_name")、<br>} | |
| **說明** | |
| 裁決 — AMP信譽查詢 | 惡意/乾淨/未知 |
| Spyname — 檢測到的惡意軟體的名稱 | [特洛伊木馬測試] |
| 分數 — AMP分配的信譽分數 | [1-100 ] |
| 上傳 — 已指示上傳檔案的AMP雲 | 1 |
| File Name — 檔案附件的名稱 | abcd.pdf |

## WebBase(Web)網路參與

### 每個Web請求共用的統計資訊

| 專案 | 示例資料 | 標準參與 | 有限參與 |
|---|---|---|---|
| 版本 | coeus 7.7.0-608 | | |
| 序列號 | | | |
| SBNP取樣係數（體積） | | | |
| SBNP取樣係數（速率） | 1 | | |
| 目標IP和埠 | | 未模糊的URL路徑段 | 雜湊URL路徑段 |
| 反間諜軟體選擇的惡意軟體類別 | 已跳過 | | |

| | |
|---|---|
| WBRS得分 | 4.7 |
| McAfee惡意軟體類別判定 | |
| 引用URL | 未模糊的URL路徑段　雜湊URL路徑段 |
| 內容型別ID | |
| ACL決策標籤 | 0 |
| 舊版Web分類 | |
| CIWUC網路類別和決策來源 | {'src':'req', 'cat':'1026'} |
| AVC應用名稱 | 廣告和跟蹤 |
| AVC應用型別 | 廣告網路 |
| AVC應用行為 | 不安全 |
| 內部AVC結果跟蹤 | [0,1,1,1 ] |
| 通過索引資料結構的使用者代理跟蹤 | 3 |

**每個Web請求的高級惡意軟體統計資訊**

**AMP統計資訊**

| | |
|---|---|
| 裁決 — AMP信譽查詢 | 惡意/乾淨/未知 |
| Spyname — 檢測到的惡意軟體的名稱 | [特洛伊木馬測試] |
| 分數 — AMP分配的信譽分數 | [1-100 ] |
| 上傳 — 已指示上傳檔案的AMP雲 | 1 |
| File Name — 檔案附件的名稱 | abcd.pdf |

**終端使用者反饋統計資料饋送**

***每個終端使用者共用的統計資訊 分類錯誤 意見回饋***

| **專案** | **示例資料** |
|---|---|
| 引擎ID（數字） | 0 |
| 舊版Web分類代碼 | |
| CIWUC Web分類源 | 'resp' / 'req' |
| CIWUC Web類別 | 1026 |

**提供的示例資料 — 標準參與**

```
# categorized
"http://google.com/": {    "wbrs": "5.8",
   "fs": {
         "src": "req",
         "cat": "1020"
   },
}

# uncategorized
"http://fake.example.com": {    "fs": {
     "cat": "-"
   },
}
```

**提供的示例資料 — 參與有限**

- 來自客戶端的原始請求：www.gunexams.com/Non-Restricted-FREE-Practice-Exams

- 記錄的消息（在遙測伺服器中）：http://www.gunexams.com/76bd845388e0

**完整WBNP解碼**

每個Cisco裝置共用的統計資訊

| **專案** | **示例資料** |
| --- | --- |
| 版本 | coeus 7.7.0-608 |
| 序列號 | 0022190B6ED5-XYZ1YZ2 |
| 型號 | S660 |
| 已啟用Webroot | 1 |
| 已啟用AVC | 1 |
| 已啟用Sophos | 0 |
| 已啟用響應端分類 | 1 |
| 已啟用反間諜軟體引擎 | default-2001005008 |
| 反間諜軟體SSE版本 | default-2001005008 |
| 反間諜軟體Spycat定義版本 | default-8640 |
| 反間諜軟體URL阻止清單DAT版本 | |
| 反間諜軟體URL網路釣魚DAT版本 | |
| 反間諜軟體Cookie DAT版本 | |
| 已啟用反間諜軟體域阻止 | 0 |
| 反間諜軟體威脅風險閾值 | 90 |
| 已啟用McAfee | 0 |
| McAfee Engine版本 | |
| McAfee DAT版本 | default-5688 |
| WBNP詳細級別 | 2 |
| WBRS引擎版本 | freebsd6-i386-300036 |
| WBRS元件版本 | categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215 |
| WBRS阻止清單閾值 | -6 |
| WBRS允許清單閾值 | 6 |
| 已啟用WBRS | 1 |
| 已啟用安全行動化 | 0 |
| 已啟用L4流量監控器 | 0 |
| L4流量監控器阻止清單版本 | default-0 |
| L4流量監控器管理阻止清單 | |
| L4流量監控管理阻止清單埠 | |
| L4流量監控允許清單 | |
| L4流量監控允許清單埠 | |
| SBNP抽樣因子 | 0.25 |
| SBNP取樣係數（體積） | 0.1 |
| SurfControl SDK版本（舊版） | default-0 |
| SurfControl完整資料庫版本（舊版） | default-0 |
| SurfControl本地增量累積檔案版本（舊版） | default-0 |
| Firestone引擎版本 | default-210016 |
| Firestone DAT版本 | v2-310003 |
| AVC引擎版本 | default-110076 |
| AVC DAT版本 | default-1377556980 |
| Sophos引擎版本 | default-1310963572 |
| Sophos DAT版本 | default-0 |
| 已啟用自適應掃描 | 0 |

| | |
|---|---|
| 自適應掃描風險評分閾值 | [10, 6, 3] |
| 自適應掃描負載因子閾值 | [5, 3, 2] |
| 已啟用SOCKS | 0 |
| 交易總數 | |
| 交易總數 | |
| 允許的事務總數 | |
| 檢測到的惡意軟體事務總數 | |
| 管理策略阻止的事務總數 | |
| 按WBRS得分阻止的事務總數 | |
| 高風險交易總計 | |
| 流量監控器檢測到的事務總數 | |
| 與IPv6客戶端的交易總數 | |
| 與IPv6伺服器的事務總數 | |
| 使用SOCKS代理的交易總數 | |
| 來自遠端使用者的事務總數 | |
| 來自本地使用者的事務總數 | |
| 使用SOCKS代理所允許的交易總數 | |
| 允許使用SOCKS代理的本地使用者的事務總數 | |
| 允許使用SOCKS代理的遠端使用者事務總數 | |
| 使用SOCKS代理阻止的交易總數 | |
| 使用SOCKS代理阻止的本地使用者的事務總數 | |
| 使用SOCKS代理阻止的遠端使用者的事務總數 | |
| 自上次重新啟動以來的秒數 | 2843349 |
| CPU利用率(%) | 9.9 |
| RAM利用率(%) | 55.6 |
| 硬碟利用率(%) | 57.5 |
| 頻寬利用率（/秒） | 15307 |
| 開放式TCP連線 | 2721 |
| 每秒交易數 | 264 |
| 客戶端延遲 | 163 |
| 快取命中率 | 21 |
| 代理CPU利用率 | 17 |
| WBRS WUC CPU利用率 | 2.5 |
| 記錄CPU利用率 | 3.4 |
| 報告CPU利用率 | 3.9 |
| Webroot CPU利用率 | 0 |
| Sophos CPU利用率 | 0 |
| McAfee CPU利用率 | 0 |
| vmstat實用程式輸出(vmstat -z， vmstat -m) | |
| 配置的訪問策略數 | 32 |
| 已配置的自定義Web類別數 | 32 |
| 身份驗證提供程式 | 基本，NTLMSSP |
| 驗證領域 | 身份驗證提供程式主機名、協定和其他配置元素 |

**每個Web請求共用的統計資訊**

| **專案** | **示例資料** | **標準參與** | **有限參與** |
|---|---|---|---|
| 版本 | coeus 7.7.0-608 | | |
| 序列號 | | | |

| | | | |
|---|---|---|---|
| SBNP取樣係數（體積） | | | |
| SBNP取樣係數（速率） | 1 | | |
| 目標IP和埠 | | 未模糊的URL路徑段 | 雜湊URL路徑段 |
| 反間諜軟體選擇的惡意軟體類別 | 已跳過 | | |
| WBRS得分 | 4.7 | | |
| McAfee惡意軟體類別判定 | | | |
| 引用URL | | 未模糊的URL路徑段 | 雜湊URL路徑段 |
| 內容型別ID | | | |
| ACL決策標籤 | 0 | | |
| 舊版Web分類 | | | |
| CIWUC網路類別和決策來源 | {'src':'req', 'cat':'1026'} | | |
| AVC應用名稱 | 廣告和跟蹤 | | |
| AVC應用型別 | 廣告網路 | | |
| AVC應用行為 | 不安全 | | |
| 內部AVC結果跟蹤 | [0,1,1,1 ] | | |
| 通過索引資料結構的使用者代理跟蹤 | 3 | | |

**每個Web請求的高級惡意軟體統計資訊**

**AMP統計資訊**

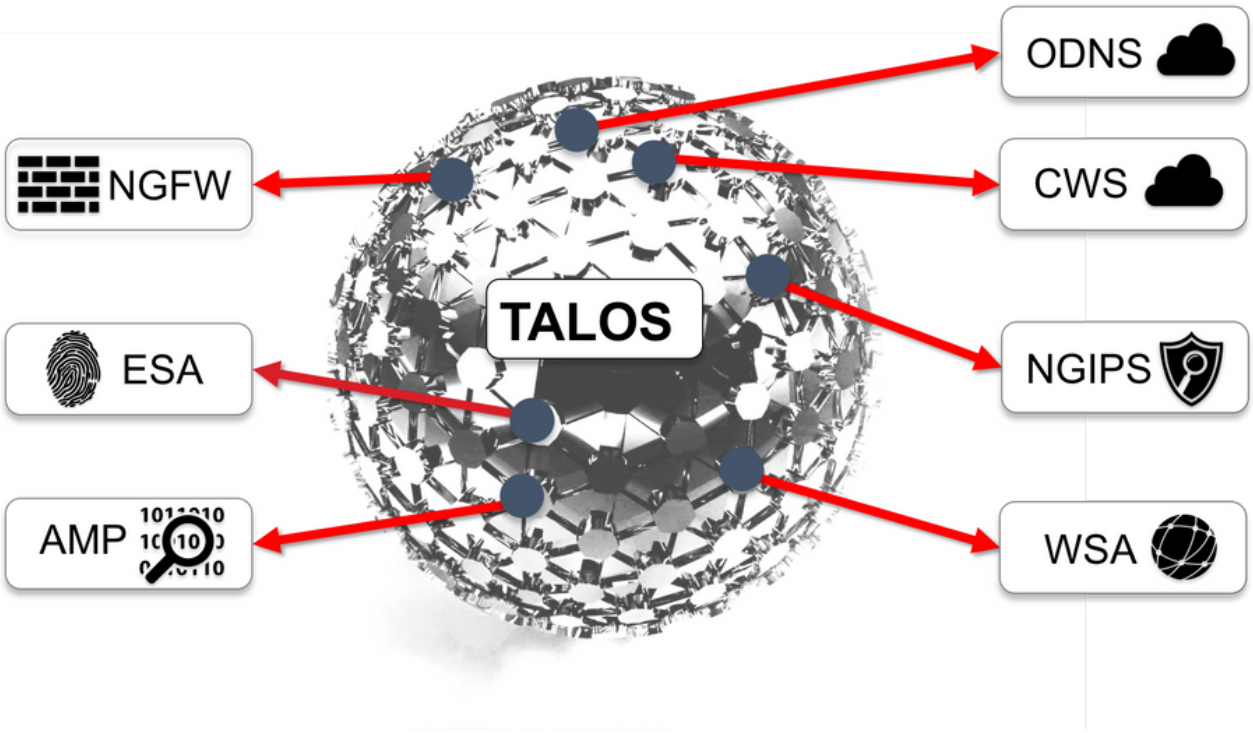
| | |
|---|---|
| 裁決 — AMP信譽查詢 | 惡意/乾淨/未知 |
| Spyname — 檢測到的惡意軟體的名稱 | [特洛伊木馬測試] |
| 分數 — AMP分配的信譽分數 | [1-100 ] |
| 上傳 — 已指示上傳檔案的AMP雲 | 1 |
| File Name — 檔案附件的名稱 | abcd.pdf |

**終端使用者反饋統計資料饋送**

***每個終端使用者共用的統計資訊 分類錯誤 意見回饋***

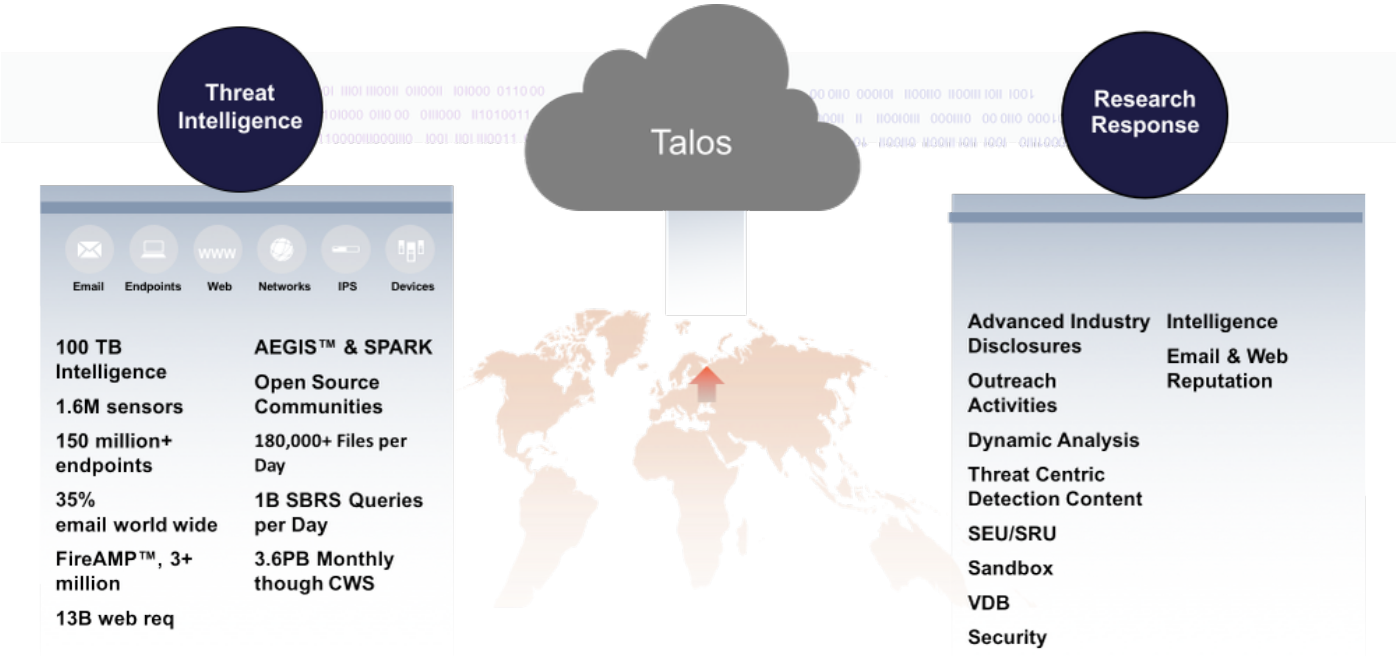
| **專案** | **示例資料** |
|---|---|
| 引擎ID（數字） | 0 |
| 舊版Web分類代碼 | |
| CIWUC Web分類源 | 'resp' / 'req' |
| CIWUC Web類別 | 1026 |

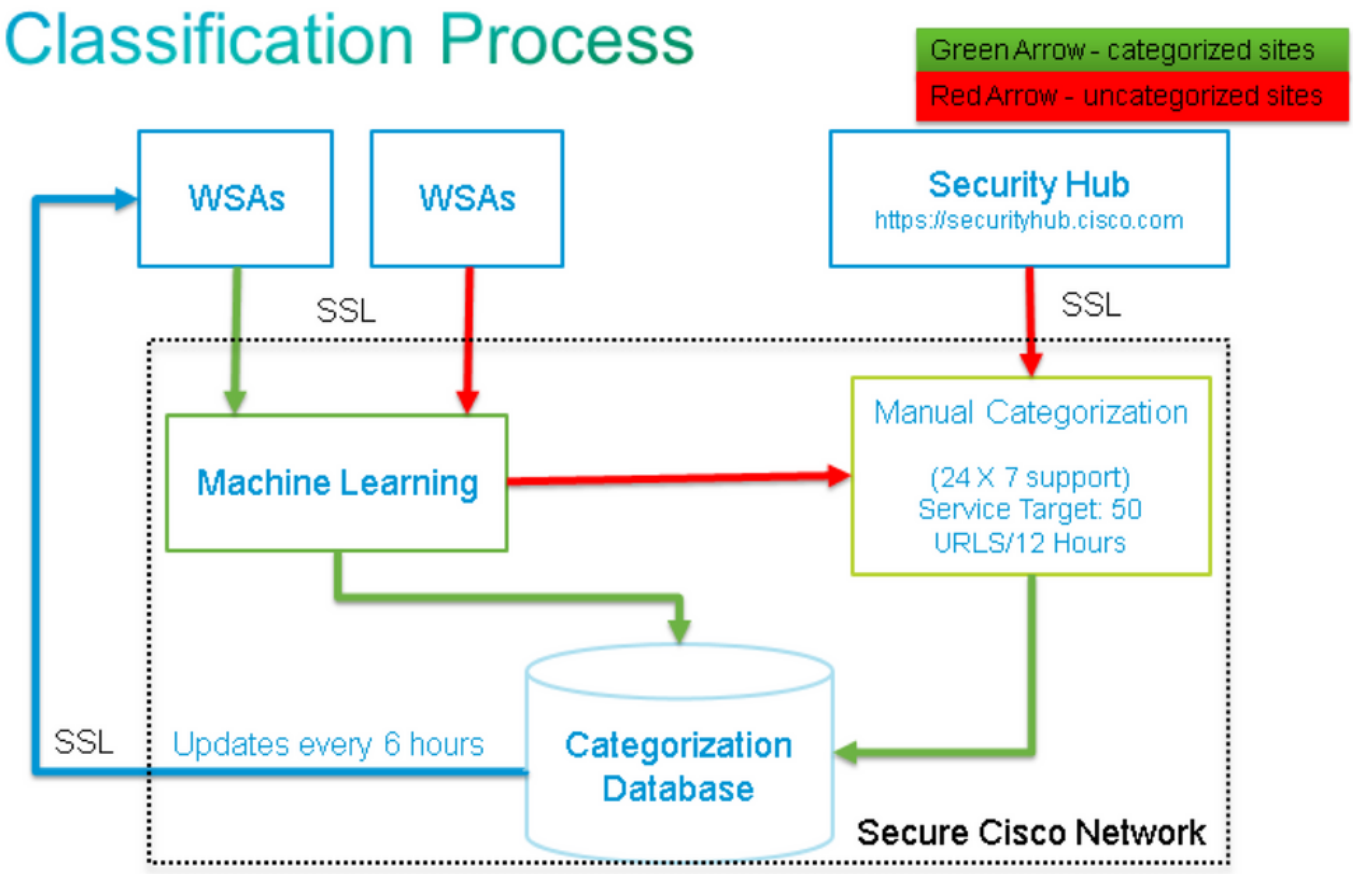
# Talos檢測內容


ODNS
CWS
NGFW
TALOS
NGIPS
ESA
AMP
WSA



# 注重威脅


Threat Intelligence
Talos
Research Response
Email
Endpoints
Web
Networks
IPS
Devices
100 TB Intelligence
1.6M sensors
150 million+ endpoints
35% email world wide
FireAMP™, 3+ million
13B web req
AEGIS™ & SPARK
Open Source Communities
180,000+ Files per Day
1B SBRS Queries per Day
3.6PB Monthly though CWS
Advanced Industry Disclosures
Outreach Activities
Dynamic Analysis
Threat Centric Detection Content
SEU/SRU
Sandbox
VDB
Security
Intelligence
Email & Web Reputation




## 相關資訊

- 思科網路安全裝置 — 產品頁面
- 思科電子郵件安全裝置 — 產品頁面
- 技術支援與文件 - Cisco Systems