CIA API 整理 (cloud + adapter)

1. CIA cloud: [4 API: Login, Logout, Upload, Lookup]

|  |  |  |  |
| --- | --- | --- | --- |
| Login | | | |
| Description | | 輸入username和password取得session ID。 | |
| URI | | /account/login | |
| Method | | POST | |
| Parameter | | * Username - 帳號 * Password - 密碼，經過base64編碼 | |
| Response code | | * 200 - 正常 * 201 - username或password不正確 | |
| Response content | | 36字元的session ID | |
| Usage | | curl -F "Username=Admin" -F "Password='QWRtaW4xMjM='" 127.0.0.1:9998/account/login | |
| Logout | | | |
| Description | | 登出使session ID無效。 | |
| URI | | /account/logout | |
| Method | | PUT | |
| Parameter | | * Session\_id - 欲登出之session ID，URL參數 | |
| Response code | | * 200 正常 | |
| Response content | | N/A | |
| Usage | | curl -X PUT 127.0.0.1:9998/account/logout?Session\_id=f0d3c08c-8011-45d7-8c6f-fd9b03cedad5 | |
| Upload | | | |
| Description | | 上傳郵件，包含郵件日期、主旨、寄件者、收件者、副本、以及附件。 | |
| URI | | /upload/attachment | |
| Method | | PUT | |
| Parameter | | * Session\_id - 執行動作之session ID，URL參數 * file - 附件檔案，可有一個至多個 * Date - 信件日期 * Size- 檔案大小(byte) * Subject - 信件主旨 * From - 寄件者address * To - 收件者addresses，以”,”相隔 * Cc – 副本addresses，以”,”相隔 | |
| Response code | | * 200 正常 | |
| Response content | | N/A | |
| Usage | | curl -F "file=@./sample1.xls" -F "file=@./sample2.xls" -F "Date=\"2013-07-19\"" –F "Size=10000" -F "Subject=hihi" -F "From=\"john@labma\"" -F "To=\"ted@labma,dasu@labma\"" -F "Cc=\"\"" -F "mail\_attachment=true" 127.0.0.1:9998/upload/attachment?Session\_id=c9eb0a42-36f5-4459-be89-96f6744b3fab | |
| Lookup | | | |
| Description | | 以附件檔案之MD5查詢分析狀況。 | |
| URI | | /report/mtalookup | |
| Method | | POST | |
| Parameter | | * Session\_id - 執行動作之session ID，URL參數 * md5\_list - 欲查詢之MD5s，以”\n”相隔 | |
| Response code | | * 200 正常 | |
| Response content | | 回傳Response為一JSON object，其KEY有Result及查詢的MD5  {  "result": "Success",  "serverstate": "Good/Fail",  "[MD5]": "Report JSON objects"  }  而上述查詢MD5的Report JSON objects由6個objects組成分別為 Result,File,Process,Registry,Network,Sys Error,  當檔案判斷為malicious則會回傳上述6個objects，否則僅回傳Result物件  舉例如下：  {  "TYPE": "Result",  "Response": "[201]Malicious" #Response可參考附件  }  ,  {  "TYPE": "Process",  "Suspicious Rate": 3,  "Path Strings": [  "WINWORD.EXE",  "Hackme.exe"  ]  }  ,  {  "TYPE": "File",  "Suspicious Rate": 3,  "Path Strings": [  "C:\\DOCUME~1\\account\\LOCALS~1\\svchost.txt",  "C:\\DOCUME~1\\account\\LOCALS~1\\svchost2.txt"  ]  }  ,  {  "TYPE": "Registry",  "Suspicious Rate": 3,  "Path Strings": [  "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"  ]  }  ,  {  "TYPE": "Network",  "Suspicious Rate": 3,  "Path Strings": [  "101.1.25.58:TCP:80",  "101.1.25.59:TCP:80"  ]  }  ,  {  "TYPE": "Sys Error",  "Suspicious Rate": 0,  "Reason": App Crashed  ]  } | |
| Usage | | curl -F "md5\_list=6949fe6f06b57e304c31034098671b8f" 127.0.0.1:9998/report/mtalookup?Session\_id=c9eb0a42-36f5-4459-be89-96f6744b3fab | |

2. CIA adapter: [2 API: Upload, Download]

Upload:

|  |  |
| --- | --- |
| Upload | |
| Description | 上傳樣本 |
| URI | <ip:port>/Upload |
| Method | POST |
| Parameter | file : 上傳的樣本, key : Authenticate client ip is valid or not, password: unzip key for uploading zip file this time |
| Response code | Response.status (400): 沒有收到上傳樣本  Response.status (200): 正常收到樣本  Response.status (201): 非允許ip  其他: Http status code |
| Response content | Data format: JSON  Response code = {200,201,400}  Response body:  {  msg: setting message for situations  }  msg: 無論成功或失敗都會有提示訊息 |
| Usage | curl –k -F ‘key=<authenticate key>’ -F ‘password=<password>’ -F file=”@<sample\_path>” https://61.216.83.37:50443/Upload |

Download:

|  |  |
| --- | --- |
| Download | |
| Description | 查詢樣本分析結果,回傳結果將以JSON格式 |
| URI | <ip:port>/Download |
| Method | GET |
| Parameter | md5: hash value self-computed, verifykey: Authenticate client ip is valid or not  Verifykey in Download API是事先預設好的,用來代表合法的使用者ip( valid Source), 因為是事先預設在code中的list, 因此新的使用者再開始使用API前,需要和這邊連絡將代表ip的md5(hashvalue) 新增進list中套用後才能使用API服務 |
| Response code | Response.status (200): 正常查詢完並回傳結果  Response.status (201): 非允許ip  Response.status (300): 正常查詢完但登出有問題,仍回傳結果  Response.status (301): 查詢到非預期回應  Response.status (302): 登入發生問題  Response.status (304): 沒有收到欲查詢的md5  其他: Http status code |
| Response content | Data format: JSON  Response code ={200,201,300,301,302,304}:  {  msg: setting message for situations  result: analysis result  }  msg: 失敗會有提示訊息,成功則沒有此項回傳  result: 若查詢成功,無論是否成功登出都會有此項回傳結果,其它狀況則沒有此項回傳 |
| Usage | curl -k https://61.216.83.37:50443/Download/<verifykey>/<md5> |