FortiSoar 테스트결과

2020년 7월 20일 월요일

오후 4:23

FortiSoar는 기본적으로 발생하는 이벤트를 HTTP(POST, GET, PUT, DELETE)을 통해 받는 것으로 확인하였습니다. 물론 Fortinet에서 제공하는 Connectors를 통해 Syslog, FortiOS 통신 외 기능을 사용 할 수 있습니다.

아래 예제와 같이 Request를 통해 임의로 원하는 데이터를 Soar에 삽입 할 수가 있습니다.

1. 기본 통신

|  |
| --- |
| Incidents data 조회 결과 ( JSON ) |
| {      "@context": "/api/3/contexts/Incident",      "@id": "/api/query/incidents",      "@type": "hydra:PagedCollection",      "hydra:totalItems": 8,      "hydra:itemsPerPage": 30,      "hydra:firstPage": "/api/query/incidents",      "hydra:lastPage": "/api/query/incidents",      "hydra:member": [          {              "@id": "/api/3/incidents/1e2b890e-f56d-4f87-a349-b0ad5bf37759",              "@type": "Incident",              "ackDate": null,              "slaPercentage": null,              "aftermathDate": null,              "assigneddate": null,              "confirmationDate": null,              "containmentDate": null,              "containmentTime": null,              "dateOfIncident": null,              "description": null,              "destinationIP": null,              "deviceUID": null,              "discoveredOn": null,              "dwellTime": null,              "eradicationDate": null,              "filehash": null,              "identificationDate": null,              "impactAssessments": null,              "incidentsummary": null,    ( . . . ) |

|  |
| --- |
| Incidents data 삽입 요청 |
| Request |
| "source  "name": "Cross Site Script Attack Detected  "severity": {  "itemVaIue" :  "Minimal",  "orderlndex": e  "color" : '  "Icon"  null  "itemVaIue": "Detection"  "Fortis1EM%  "status":  "phase": {  "Open" |
| Response |
| "@context": "/api/3/contexts/Incident",  "@id": "/api/3/incidents/6Ø8b6b5a -df44-461d  "@type": "Incident",  "acOate":  null,  -bfad-7a9db5e4ebb5",  "slapercentage" :  "afternathOate" :  "assigneddate":  null,  null,  null,  "confirmationoate" :  null,  "containnentoate" :  null,  "containnentTime" :  null,  "dateOfIncident":  null,  "description"  null,  "destinationIP": null,  요청에 따른 결과값을 Return 받은 [응답]을 통해서 확인 할 수 있고, 요청이 성공하면  정상적으로 해당 이벤트에 대한 고유 ID가 부여 된 것을 보실 수 있습니다. |

[Incidents data 삽입 요청 결과화면]

Incidents 
Open Incidents By Severity 
Unresolved Incidents By Severity By Type 
1 Items 
21 
O 
Severity 
Na me 
Cross Site Script Attack Detected (TEST) 
Source 
FortiSlEM 
Type 
Phase 
Detection 
Open 

현재까지 확인된 바로는 이미지의 체크박스와 같이 /modules/ 안에 있는 모든 데이터들은 전부 CRUD API 통신을 통해 제어가 가능하다는 점입니다.

C 
A 172.162% 
/modules/i dicators 
Indicators 
Malicious Indicators 

그 리스트는 아래와 같습니다.

|  |
| --- |
| /modules/alerts  /modules/incidents  /modules/tasks  /modules/indicators  /modules/emails  /modules/mitreattack  /modules/vulnerabilities  /modules/assets  /modules/scans  /modules/sla\_template  /modules/attachments  /modules/email\_templates |

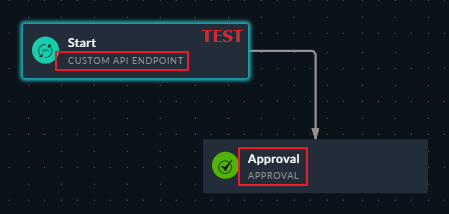
1. Playbook ( 정책 ) 호출

설정해둔 Playbook을 외부에서 호출 할 수 있습니다. 아래 예제를 확인해보겠습니다.

미리 설정해둔 "test" Playbook을 통해 Approval(인증 알림)를 호출하거나 테스트 메일을 발송 할 수 있있는지 확인해보겠습니다.

**# Approval 인증 알림 TEST**

1) CUSTOM API ENDPOINT로 설정 및 Approval 이벤트 생성



2) 외부 요청

C:\AA836065\A1AECE41-8B22-4D9E-A2A2-3BCFB553FE6B.files\image006.png

3) 결과확인

ch 
APPROVALS 
endpoint 
Description: 
Comments: 
8 Items A 

**# TEST MAIL 발송테스트**

1) 설정 및 요청

l!ew 
LN10d0N3 nozsnD 

2) 외부 요청

C:\AA836065\A1AECE41-8B22-4D9E-A2A2-3BCFB553FE6B.files\image006.png

3) 메일 수신

N 
noreply@example.com 
kimduumin@withneb.vorks.com 
14, „ 
/ ap±/3/a1eltB/3ff4e21f-EcES-4cB4-Ec49-Eff39032adfS", 
nul I , "doma±n" 
source" 
Status" 
nul I , "name": "test" 
{"ICI": 118, " 
"dueEy": null, " 
State" 
"Icon" 
B13c-7ce4E141B15a", 
"Open" 
@type": "PI c kl±et", 
nul I, "I±BtName": " / 
„col 01" • 
„ackDate" 
erna ±ITo" 
nul I , "f11 epat 
"Bourcelp": nul I, "userName"• 
nul I, "dev±ceUID": 
" I eepDate" 
services" 
sever±ty": nul 
" erna ± I Body": nul I, "ema±IErom" : 
o chT Ime " 