STIX 2.0 을 이용한 제어 정보 공유 포맷에 대한 연구

박지영
(주)이글루시큐리티

e-mail : charmpa@igloosec.com

A Study on Control Information Sharing System Using STIX 2.0

Jee-Young Park
ICM Team, R&D Center, IGLOO SECURITY, Inc.

요 약

최근 기업, 기관, 개인의 자산들에 대한 사이버 위협이 빈번하게 발생되고 있으며, 시장에는 다양한 업체/제품의 단말/EDR/네트워크 제품들이 경쟁하고 있다. 이로 인해 사이버 위협에 대한 정보 및 제어 정보, 정책 정보들을 사전에 공유하고 해당 정보의 자동화된 해석을 통한 신속한 대응 처리의 중요성이 높아지고 있다. 본 논문에서는 업체들의 장비/제품에 적용 가능한 제어 정보를 정의하고 이를 공유하기 위한 공유 시스템을 제안한다. 이를 위해 STIX 2.0 표준을 도입하여 제어 정보를 설계하고, 확장 표준을 통해 요구되는 속성들을 추가 정의하여 자동화된 해석 및 대응 처리가 가능하도록 설계한다.

1. 서론

최근 IoT 기기의 증가와 기기간 수평적 연결이 늘어나면서 언제 어떻게 기업, 기관, 개인의 자산이 공격 받을지 모르는 상황에 직면해 있다. 만약, 위협 정보를 사전에 공유 받고 해석하는 것이 가능하다면, 이를 분석하여 준비하고, 다양한 보안 장비들에 대응 조치를 지시하거나 취약점 패치 정보를 공유하여 보다 신속한 대응이 가능하게 될 것이다. 그러나 공유되는 정보들이 공통된 기준으로 위협 정보, 제어 정보 등을 표현하지 못하고 있고, 통신 방법도 업체에 따라 다르게 사용하고 있는 것이 현실이다. 이로 인해, 공유되어진 정보의 자동화된 해석과 대응 처리를 위한 자원의 소모가 존재하며 즉각적인 대응 및 사후 조치에 어려움이 존재한다. 이러한 문제의 해결을 위해 위협 정보의 표준화 요구들이 있어 왔다. 현재 여러 표준 중 미국 국토안보부와 MITRE 가 공동 개발한 STIX, TAXII 가 주류로 자리잡고 있다. 본 논문은 STIX 표준에서 정의하고 있는 정보 공유 체계를 이용하여 제어 정보의 처리까지 확장함으로써 다양한 업체의 보안 장비에서 해석 가능한 규격을 설계하고 이를 적용한 시스템을 구현하고자 한다.

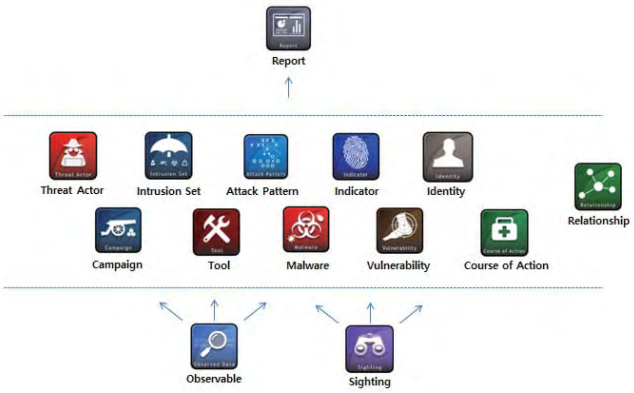
2. 배경

STIX 표준이 2.0 으로 올라가면서 OASIS 에서 표준 제정 및 참조 구현을 담당하고 있다. 이전 1.x 와 비교하여 포맷 정의 언어 등 여러 부분에서 변경 사항이 존재한다.

<표 1> STIX 1.x 와 STIX 2.0 차이 비교

항목	설명
한 개의 표준	STIX 1.x 에서 별도 표준이던 Cybox 객체가 STIX 2.0 에서는 STIX Cybox Observables 로 통합
JSON vs XML	STIX 1.x 는 XML 로 정의하였으나, STIX 2.0 은 JSON 으로 정의
STIX Domain Objects	STIX 2.0 의 모든 객체는 다른 객체에 포함되지 않는 최상위 수준으로 정의하며 대부분의 관계는 최상위 Relatioship 객체를 이용하여 표현
Simpler Model	STIX 2.0 에서는 객체와 속성의 수가 핵심 기능을 표현하고 이해할 수 있는 수준으로 축소
Data Markings	STIX 1.x 는 XPath 를 이용하였으나, STIX 2.0 는 그렇지 않음
Indicator Pattern Language	STIX 1.x 는 XML 구문으로 표현하였으나, STIX 2.0 은 더 간략하고 쉽게 새롭게 정의

STIX 2.0 은 위협 정보의 표현을 위해, 12 개의 SDO(STIX Domain Objects) 객체와 2 개의 SRO(STIX Relationship Objects) 객체를 정의한다.



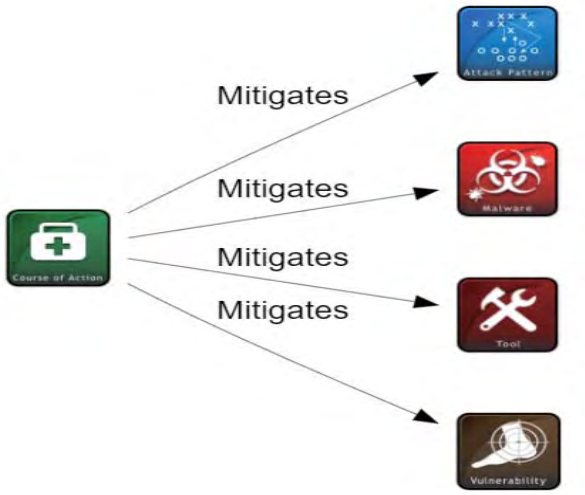
(그림 1) STIX 2.0 객체 구조

Observables 는 STIX 2.0 에서 Observed Data 객체로 표현되며, 관찰되어진 파일 정보(파일명, 해시, 사이즈 등), 레지스트리 키 값, HTTP 요청 등 시스템 네트워

크 운영과 관련 있는 정보들을 정의하고 있다. 현재 19 개의 객체가 기 정의되어 있으며 향후 계속적인 추가가 예상된다.

본 논문에서 다루고자 하는 제어 정보 표현은 위 객체들 중 하나에 속하는 Course of Action SDO 객체를 이용하여 정의한다. Course of Action 객체는 공격을 예방하거나 현재 발생중인 공격에 대응하기 위한 행위를 정의하며, 패치 정보 제공, 방화벽 재설정 등 기술적이고 자동화된 대응은 물론 임직원 대상 보안 교육, 보안 정책 공유 등 수준 높은 행위도 정의할 수 있도록 한다.

STIX 2.0 표준에서 Course of Action 은 Attack Pattern, Malware, Tool, Vulnerability SDO 객체와 'mitigates' 관계 타입으로 연결되어질 수 있다.



(그림 2) Course of Action SDO 객체 관계 흐름도

현 STIX 2.0 표준에서 Course of Action SDO 객체의 action 속성 값은 구체적인 규격이 정의되지 않고 향후 사용 예정으로 분류된 'reserved'로 지정되어 있다.

본 논문에서는 action 값을 STIX 1.x 에 정의되었던 내용을 기반으로 재설계하여 자동화된 해석 및 즉각적인 대응 처리 실행이 가능하도록 하며, 특정한 탐지 패턴에 대해 제어가 가능하도록 하기 위해 그림 3 에서 정의하였던 관계에 Indicator SDO 객체로의 연결을 추가한다. 또한 Course of Action SDO 객체에 확장 속성을 추가적으로 정의하여 소프트웨어 취약점 정보에 대한 패치 파일에 대한 정보를 제공한다.

3. 제어 정보를 위한 포맷 설계

현재의 STIX 2.0 표준에 정의된 규격은 제어 정보를 자동으로 해석하고 대응 처리를 하기에는 다소 어려움이 존재한다. 이에 아래와 같이 재설계하여 사용한다.

3.1 Course of Action SDO 의 action 값 설계

STIX 1.x 는 다양한 Course of Action 타입을 정의하여 자동화된 처리를 지원하였으나, STIX 2.0 은 아직 규격이 확정되지 않은 상태이다. 이에 STIX 1.x 에 기반하고 또한 다양한 네트워크 보안 장비들에 적용 가능한 action 값을 설계한다. Perimeter Blocking, Internal Blocking, Monitoring, Patching 과 같이 기존 STIX 1.x 표준에 정의된 값을 수용하고, Unblocking 과 같은 추가 속성 값을 정의한다. Unblocking 은 이미 적용된 제어 정보에 대해 해당 제어 명령의 해제나 적용 취소를 의미한다.

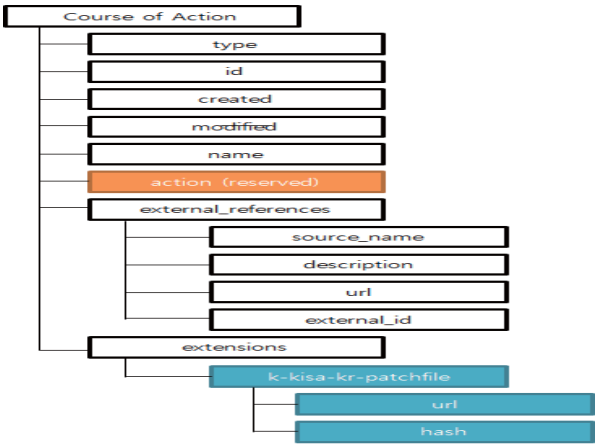
<표 2> Course of Action SDO action 속성값 정의

action 속성 값	설명	참고
Perimeter Blocking	경계 기반 차단	1.x
Internal Blocking	내부 훼손된 출처에서 유입되는 트래픽을 호스트 기반으로 차단.	1.x
Redirection	의심스럽거나 알려진 악성 트래픽을 의도된 대상에서 위협을 보다 안전하게 관찰하고 분석 할 수 있는 영역으로 다시 라우팅.	1.x
Hardening	불필요한 소프트웨어, 실행중인 서비스를 줄임으로써 시스템을 보호.	1.x
Patching	취약점을 가진 소프트웨어에 직접 코드를 작성하여 문제 해결을 적용하는 특정 형태의 강화 (hardening)와 패치.	1.x
Eradication	네트워크에서 멀웨어를 식별, 위치 지정 및 제거.	1.x
Rebuilding	손상된 리소스에 멀웨어가 더 이상 존재하지 않음을 확인하기 위해 간단한 접근에 리소스를 다시 설치.	1.x
Training	위협을 식별하고 완화하는 방법에 대해 사용자와 관리자를 교육.	1.x
Monitoring	네트워크 또는 호스트 기반 센서를 설정하여 위협 요소의 존재를 탐지.	1.x
Physical Access Restrictions	리소스에 물리적 액세스를 제한하는 것과 관련된 활동을 수행.	1.x
Logical Access Restrictions	리소스에 논리적 액세스를 제한하는 것과 관련된 활동을 수행.	1.x
Public Disclosure	위협 또는 위협 요소의 존재, 그리고 적대적 행동에 대하여 긍정적 변화가 있음을 을 공표.	1.x
Diplomatic Actions	위협 행위자와의 의사 소통 및 관계 구축과 같은 행동을 수행.	1.x
Policy Actions	멀웨어의 공격 경로 또는 감염 경로를 감소시키는 정책으로 수정.	1.x
Other	기타.	1.x
Unblocking	적용된 보안 정책의 해제.	확장

3.2 Course of Action 의 확장 속성 설계

소프트웨어 취약점 정보의 공유를 위해서는 패치 파일에 대한 추가 정보를(패치 파일의 URL, 파일 해시 등) 정의할 필요가 있다. 따라서 Course of Action 에 확장 속성을 정의한다.

확장 속성은 extensions 속성 하위로 정의하며, x-kisa-kr-patchfile 객체를 추가 정의한다. 해당 객체는 패치 파일의 다운로드 경로를 나타내는 url 속성과 해당 파일의 해시 값을 나타내는 hash 속성을 가진다. 이 객체를 해석하는 측은 위 정보를 이용하여 패치 파일의 다운로드 및 패치 작업을 진행할 수 있다.



(그림 3) Course of Action SDO 속성 구성표

3.3 Course of Action 과 다른 SDO 간의 관계 설계

STIX 2.0 표준의 Course of Action SDO 객체는 그림 3 과 같이, Attack Pattern, Malware, Tool, Vulnerability SDO 객체와 'mitigates' 관계를 가지도록 정의되어 있다. 그러나 해당 관계만 가지고 제어 정보를 표현할 수 없으므로 추가적으로 Indicator 가 식별하는 url, ip, 파일에 대한 차단, 탐지, 차단 해제를 표현할 수 있도록 하기 위하여 Indicator SDO 객체와의 'mitigates' 관계를 정의하였다.

<표 3> Course of Action SDO 의 Relationship

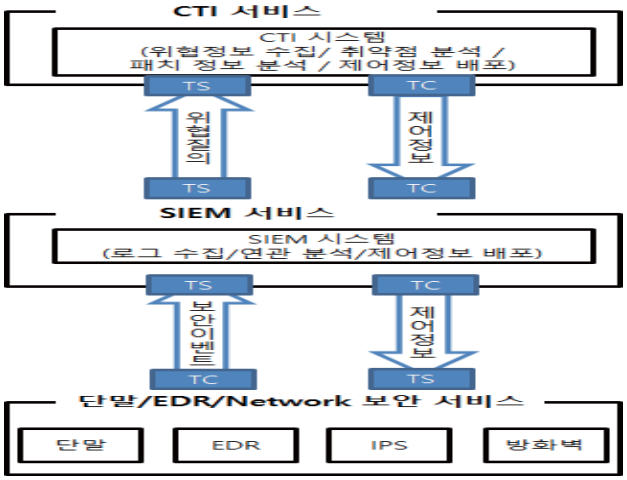
SDO(Source)	Relationship Type	SDO(Taget)	참고
Course of Action	mitigates	Attack Pattern	2.0
Course of Action	mitigates	Malware	2.0
Course of Action	mitigates	Tool	2.0
Course of Action	mitigates	Vulnerability	2.0
Course of Action	mitigates	Indicator	확장

위 설계가 반영된 STIX 2.0 제어 정보를 공유하는 각 업체들의 네트워크 보안 장비들은 해당 정보를 해석하여 공격을 탐지하거나, 특정 IP 나 URL 을 차단/해제할 수 있으며, 또한 패치 정보를 통해 패치 소프트웨어를 다운로드 받아 패치를 진행할 수 있다.

4. 제어 정보 공유 시스템 설계 및 구현

앞서 설계한 제어 정보 공유 포맷을 이용하는 제어 정보 공유 시스템에 대해 설명한다. 시스템은 3 개의 구성 서비스를 가진다. CTI 서비스는 각종 위협 정보 및 패치 정보를 수집/분석하여 제어 정보를 생성하고, SIEM 서비스는 위협 정보 및 제어 정보에 대한 질의를 수행하고 CTI 로부터 제어 정보를 공유 받는다. 하위의 단말/EDR/Network 보안 서비스는 제어 정보를 SIEM 으로부터 공유 받고, 해당 정보의 자동화된 해석을 기반으로 네트워크 혹은 시스템에 적용하며, 결과로 생성되는 다양한 보안이벤트 정보를 SIEM 으로 공유한다.

공유되는 STIX 2.0 정보는 TAXII 2.0 표준을 기반으로 연동하기 때문에, 각 구성 성분들은 TAXII 서버/클라이언트의 기능을 모두 포함한다.



(그림 4) 제어 정보 공유시스템 구성

-TC : TAXII 클라이언트
-TS : TAXII 서버

4.1 소프트웨어 취약점 패치 제어 정보

CTI 에서 생성하여 단말/EDR/Network 보안 서비스로 공유된 소프트웨어 취약점 패치를 위한 제어 정보는 action 값이 'Patching' 값을 가지고, x-kisa-kr-patchfile 확장 객체를 가진다. 해당 확장 객체의 url, hash 속성은 패치파일의 다운로드 경로 및 파일의 해시 값을 가진다. 또한 관련 취약점 정보를 표현하는 Vulnerability SDO 객체 및 해당 Vulnerability SDO 와의 'mitigates' 관계를 포함하여 표현된다.

(그림 5) 패치 제어 정보 표현


```
{
  "id": "course-of-action--769b7ba6-0651-41af-9a08-cff573240ba6",
  "spec_version": "2.1",
  "type": "course-of-action",
  "created": "2018-09-06T14:13:39.076Z",
  "modified": "2018-09-06T14:13:39.076Z",
  "confidence": 0,
  "name": "cpe:/a:ruby-lang:ruby:2.1.3",
  "action" : "Patching"
  "description": "Adobe recommends users update their software
    installations to the latest versions by following the instructions
    below\nThe latest product versions are available to end users via one
    of the following methods: Users can update their product installations
    manually by choosing Help > Check for Updates\nThe products will
    update automatically, without requiring user intervention, when
    updates are detected\nThe full Acrobat Reader installer can be
    downloaded from the Acrobat Reader Download Center\nFor IT
    administrators (managed environments): Download the enterprise
    installers from ftp://ftp.adobe.com/pub/adobe/, or refer to the
    specific release note version for links to installers\nInstall updates
    via your preferred methodology, such as AIP-GPO, bootstrapper, SCUP
    /SCCM (Windows), or on Macintosh, Apple Remote Desktop and SSH\nAdobe
    categorizes ",
  "extensions": {
    "x-kisa-kr-patchfile": {
      "url": "http://www.adobe.com/support/downloads/product.jsp?product
        =1&platform=Windows",
      "hash": "d6cd1e2bd19e03a81132a23b2025920577f84e37"
    }
  }
}
```


(그림 6) 패치 제어 정보의 Course of Action SDO


```
{
  "type": "relationship",
  "id": "relationship--5237f6ef-68c9-404f-aaaa-c2c4515ea27f",
  "created": "2018-09-06T14:13:56+09:00",
  "modified": "2018-09-06T14:13:56+09:00",
  "relationship_type": "mitigates",
  "source_ref": "course-of-action--769b7ba6-0651-41af-9a08-cff573240ba6",
  "target_ref": "vulnerability--ffac8686-7a3e-4462-819b-bf6a9639ef7b"
}
```


(그림 7) 패치 제어 정보의 Relationship SRO

```
{
  "id": "vulnerability--ffac8686-7a3e-4462-819b-bf6a9639ef7b",
  "spec_version": "2.1",
  "type": "vulnerability",
  "created": "2006-07-21T23:03:00.000Z",
  "modified": "2012-10-23T11:07:57.000Z",
  "external_references": [
    {
      "source_name": "CVE",
      "description": "Unspecified vulnerability in CORE: Repository for
        Oracle Enterprise Manager 9.0.1.0 and 9.2.0.1 has unknown impact
        and attack vectors, aka Oracle Vuln# EM01.",
      "url": "http://nvd.nist.gov/vuln/detail/2006-3719",
      "external_id": "cve-2006-3719"
    }
  ],
  "confidence": 0,
  "name": "cve-2006-3719",
  "extensions": {
    "x-kisa-kr-vulnerailities-ext": {
      "cvss_v2": "5.5",
      "cvss_v3": "0.0",
      "cwe": null,
      "related_cpe": null
    }
  }
}
```


(그림 8) 패치 제어 정보의 Vulnerability SDO

4.2 C&C IP 차단 제어 정보

위와 동일한 방식으로 공유된 IP 차단을 위한 제어 정보는 action 값이 'Perimeter Blocking' 값을 가지고, 관련 IP 정보를 식별하는 Indicator SDO 객체 및 해당 Indicator SDO 와의 'mitigates' 관계를 포함하여 표현된다.

(그림 9) C&C IP 차단 제어 정보 표현


```
{
  "type": "course-of-action",
  "id": "course-of-action--dfbbdf95-06a2-4e32-8c2c-f9d561ad9bf0",
  "created_by_ref": "identity--9456ef80-991b-4ceb-a83b-8b494efbe249",
  "created": "2018-06-20T08:30:21.936Z",
  "modified": "2018-06-20T08:30:21.936Z",
  "name": "Block incoming 198.51.100.12/24 Ipv4 Address",
  "action": "Perimeter Blocking",
  "description": "The C&C IPv4 address 198.51.100.12/24 is used sample
    ransomware for command and control.\n\t\tAdd ipv4 address to block
    list\n\t\tSee related indicator of indicator id : indicator
    --f3b98274-ceb1-4e7b-9918-306b32c88669"
}
```


(그림 10) 차단 제어 정보의 Course of Action


```
{
  "type": "relationship",
  "id": "relationship--5237f6ef-68c9-404f-aaaa-c2c4515ea27f",
  "created": "2018-09-06T14:13:56+09:00",
  "modified": "2018-09-06T14:13:56+09:00",
  "relationship_type": "mitigates",
  "source_ref": "course-of-action--dfbbdf95-06a2-4e32-8c2c-f9d561ad9bf0",
  "target_ref": "indicator--403af14b-4102-430d-af7d-9fb93b492b11"
}
```


(그림 11) 차단 제어 정보의 Relationship SRO


```
{
  "type": "indicator",
  "id": "indicator--403af14b-4102-430d-af7d-9fb93b492b11",
  "created": "2018-06-20T07:17:37.363Z",
  "modified": "2018-06-20T07:17:37.363Z",
  "name": "ind_rule",
  "description": "ip in CTI reputation",
  "pattern": "[ipv4-addr:value = '198.51.100.12/24']",
  "valid_from": "2018-06-20T07:17:37.363527Z",
  "labels": [
    "malicious-activity"
  ]
}
```


(그림 12) 차단 제어 정보의 Indicator SDO

5. 결론

소프트웨어 업체별 다양한 보안 장비/제품들에 대해 공통의 제어 정보를 정의하는 것은 제품별 특성들의 다양함으로 인하여 정의 범위에 한계가 있을 수 밖에 없다. 그리고 현재 STIX 2.0 Course of Action SDO 객체의 action 속성이 'reserved' 로 정의되어 있어 확정된 표준으로 존재하지 않는다. 이로 인하여 본 논문에서 제안한 설계/구현 방안은 STIX 2.0 표준 발전 방향에 따라 다소 수정될 필요가 있을 것으로 예상된다. 이와 관련하여, 향후 STIX 2.0 에서 정의될 action 값 정의 및 관련 Course of Action SDO 객체 변경 내용들이 다양한 제품들의 제어 정보 표현이 가능한 방향으로 정의 및 보완될 수 있도록 지속적인 연구가 필요하다.

Acknowledges 이 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2016-0-00193, IoT 보안 취약점 검색 · 공유 및 시험 기술 개발)

참고문헌

[1] MITRE, "STIX 1.2" https://stixproject.github.io/releases/1.2/
[2] MITRE, "TAXII 1.1" https://taxiiproject.github.io/releases/1.1/
[3] OASIS, "STIX 2.0" https://oasis-open.github.io/cti-documentation/resources#stix-20-specification
[4] OASIS, "TAXII 2.0" https://oasis-open.github.io/cti-documentation/resources#taxii-20-specification