정 보 보 호 학 회 지
제 31 권 제5호, 2021. 10

한국형 사이버 위협 정보 공유 기술 및 발전 방향

이 현 진*, 조 학 수**

요 약

사이버 보안 위협은 점차 은밀화·고도화되고 있어 단일 솔루션으로 탐지·분석이 어렵고, 파편화된 정보만으로 대응하는데 한계가 있다. 이에 대응하기 위하여 글로벌 보안업체들은 CTA를 구성하여 신속 위협대응 체계를 구축하고 있다. 국내에서도 이에 발맞추어 다수의 보안 업체 및 기관들이 협업하여 2017년부터 3년간 Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발 과제를 수행하였다. 본 논문에서는 해당 과제의 수행성과 중 CTI 및 정보 공유 체계를 중심으로 정리하고 이를 통해 도출된 시사점과 현재 진행 방향을 정리하고자 한다.

Ⅰ. 서 론

사이버 보안 위협이 은밀화·고도화됨에 따라 단일 솔루션으로 탐지·분석이 어렵고, 파편화된 정보만으로 대응하는데 한계가 있다. 이와 같은 환경에서 효율적으로 사이버 위협에 대응하기 위해서는 5가지의 요구사항을 만족할 수 있어야 한다. 첫 번째는 보안 센서 제품별로 상이한 이벤트 정보를 통합할 수 있어야 한다. 두 번째는 분리된 보안위협 관제 솔루션을 통합할 수 있어야 한다. 세 번째는 새로운 보안 위협에 대해서 신속하게 인지할 수 있어야 한다. 네 번째는 대량으로 발생하는 보안 이벤트를 효율적으로 분석 및 대응할 수 있어야 한다. 마지막으로 자동화된 수집/분석/대응 프로세스 구축을 통한 신속한 보안 체계를 구축할 수 있어야하며, 이를 위해 사이버 위협 대응 컨트롤 센터가 구축되어야 한다. 이와 같은 요구사항을 만족시키기 위하여 Check Point, Cisco, Fortinet, McAfee, Palo Alto Networks 등 글로벌 보안업체들은 공격·방어 중심의 기술에서 피해 최소화를 위한 예방·대응 관점으로 보안 기술을 변화시키고 있으며, CTA(Cyber Threat Alliance) 기반의 신속 위협 대응 체계를 구축하였다. CTA에 가입한 회원사는 의무적으로 각 사가 보유하고 있는 일정량 이상의 침해 위협 정보를 주기적으로 공유해야하며, APT 공격, 지능형 악성코드 등 각 회원사에서 공유한 위협 정보는 CTA 플랫폼을 통해 취합, 실시간으로 자동 공유한다[1].

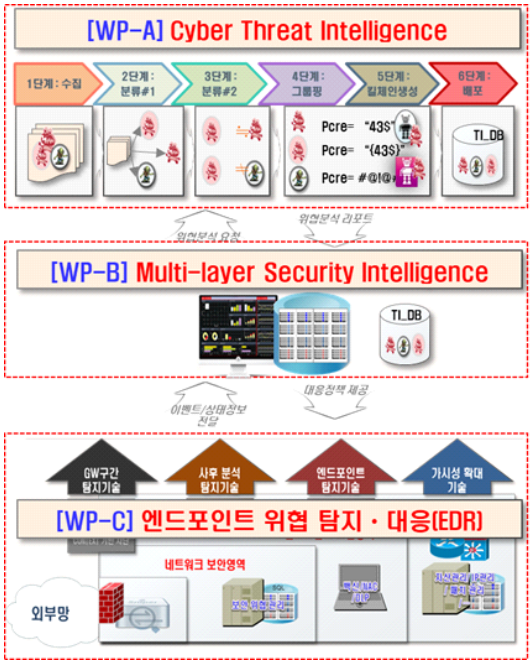
국내에서도 이와 같은 대응체계 구축을 위하여 다양한 시도를 진행하였으며, 대표적인 예로 한국인터넷진흥원(KISA; Korea Internet and Security Agency)에서 운용하고 있는 C-TAS(Cyber Threats Analysis System)를 들 수 있다. C-TAS는 사이버 위협 정보를 체계적으로 수집해 관계기관 간 자동화한 정보 공유를 목적으로 하는 예방·대응 시스템으로 2014년 8월부터 본격적으로 가동되었다[2]. 그러나 특정 고객사에서 접수된 민감 정보의 경우 대외 보안유지 서약 등의 사유로 위협 정보가 실시간으로 공유되지 못하는 경우가 있으며, 정보 공유의 비대칭성으로 인해 공유가 원활하지 못한 한계 및 정보 공유 인터페이스가 국제 표준과 다소 상이함으로 인한 공유 정보 호환의 문제 등 몇 가지 한계가 존재하며 이에 대한 극복 방안 등도 활발히 검토되고 있다[3].

2017년부터 3년간 정보보호 핵심 원천 기술 개발 사업의 일환으로 진행된 “Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발 과제”(이하, KOSIGN 과제)는 14개의 산/학/연 기관이 모여서 한국형 사이버위협정보 공유 서비스인 K-CTI 서비스와 국내 보안제품을 연동하여, 신속하고 효율

이 논문은 2021년도 과학기술정보통신부의 재원으로 한국인터넷진흥원의 지원(No.KISA 지원-2021-0000, 인공지능 지속학습과 분산 마이닝 기법을 적용한 차세대 SIEM 솔루션 개발, 100%)을 받아 수행된 연구임
* ㈜윈스 기반기술팀 (수석연구원/팀장, l33hyun@wins21.co.kr)
** ㈜윈스 연구개발총괄 (부사장/CTO, marius71@wins21.co.kr)

적인 사이버 위협 대응이 가능한 체계 구축을 위한 기반기술 개발을 목표하였으며, C-TAS의 한계를 극복하기 위한 대안으로 추진되었다.

그림 1은 KOSIGN(Korea Open Security Intelligence Global Network) 과제를 통해 개발하고자한 사이버 위협 정보 공유 서비스 개념도 및 WP 별 관계도를 나타내고 있다. KOSIGN 과제는 3개의 WP(Work Package)로 구성되어 있으며, WP-A는 글로벌 사이버 위협정보를 수집·분석하여, 공격을 추정하고 대응 방안을 제공하는 CTI(Cyber Threat Intelligence) 기술 개발하고, WP-B는 CTI로부터 전송되는 STIX(Structured Threat Information Expression) 포맷의 다양한 이벤트 정보를 빅데이터 기반으로 수집/저장하고, 수집된 정보를 침해지표 기준으로 인과관계를 분석하고, 향후 예상되는 위협까지 대응할 수 있는 MSI(Multi-layer Security Intelligence) 기술을 개발하는 것을 목표로 하였다. 마지막으로 WP-C는 이기종 보안장비들의 보안이벤트를 STIX/TAXII (Trusted Automated Exchange of Intelligence Information) 기반으로 정보 연계하고, 추론된 위협에 효과적으로 대응할 수 있는 EDR(Endpoint Detection and Response) 및 IPS(Intrusion Prevention System) 기술을 개발하는 것을 목표로 하였다.

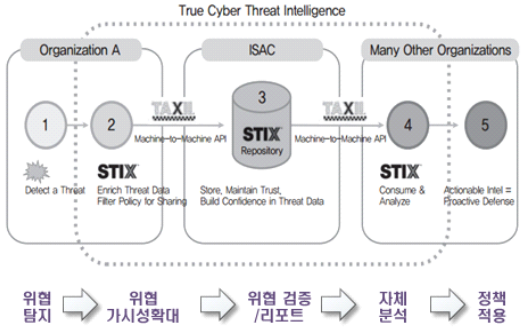


〔그림 1〕 사이버 위협 정보 공유 서비스 개념도 및 과제 WP 별 관계도

본 논문은 4개의 장으로 구성되어 있으며, 2장에서는 KOSIGN 과제 중 WP-A에 해당하는 CTI 시스템의 개발 성과를 정리하고, 3장에서는 CTI 시스템 개발을 통해 획득한 기술을 기반으로 상용화 추진 현황에 대해서 기술한다. 마지막으로 4장에서 KOSIGN 과제의 시사점 및 결론을 맺고자 한다.

Ⅱ. K-CTI 시스템 개발 성과

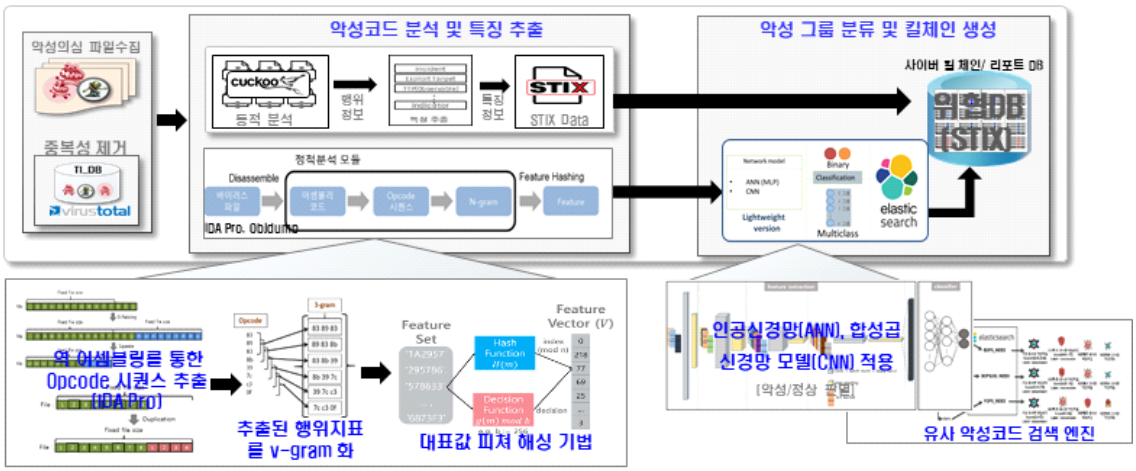
글로벌 보안업체들은 은밀화·고도화되면서 발전하고 있는 사이버 위협에 효과적으로 대응하기 위하여 공격·방어 중심의 기술에서 피해 최소화를 위한 예방·대응 관점으로 보안기술을 개발하고 있으며, CTA를 구성하여 그림 2와 같이 신속 위협 대응 체계를 구축하였다. K-CTI는 글로벌 보안업체들이 구성한 신속 위협 대응 체계와 효과적으로 연동할 수 있도록 시스템을 개발하였으며, 본 장에서는 K-CTI를 구성하는 기능과 연동 인터페이스를 중심으로 개발 성과를 정리하고자 한다.



〔그림 2〕 해외 CTA가 구축한 신속 위협 대응 체계 개념도

2.1. K-CTI 시스템

사이버 위협 인텔리전스(CTI)는 사이버 시스템의 안전을 위협하는 정보를 수집하여 상황을 분석하고 사이버 보안 위협에 효과적으로 대응하는 방법 또는 현존하거나 발생 가능한 위협에 대한 대응을 결정에 사용할 수 있도록 해당 위협에 대한 맥락, 메커니즘, 지표, 예상 결과 및 실행 가능한 조언 등을 포함한 증거기반의 지식으로 정의하고 있다[4]. 국내의 경우 KISA를 중심으로 주요 민간 보안업체들이 참여하여



〔그림 3〕 WP-A에서 개발한 CTI 플랫폼에서 딥러닝 기반으로 악성코드를 분류하는 개념도

운용하고 있는 C-TAS가 가장 대표적인 예가 될 수 있다.

K-CTI 시스템은 그림 3과 같이 글로벌 CTI와 연동하여 최신 글로벌 위협 정보를 수집하는 것을 포함하여 보안관제 플랫폼에서 제공되는 다량의 이벤트를 가공·분석하여 비정상 행위를 자체적으로 분석하고, 대응방안을 제공하는 것이다[5-6]. 이와 같은 목적을 달성하기 위하여 K-CTI 시스템은 다양한 채널을 통해 위협 정보를 수집하고(수집 단계), 수집된 정보의 분석 전처리 및 유사성 비교를 통해 특징을 추출(분석 전처리 단계)한 후, 기계학습과 딥러닝을 통해 악성코드를 분석(분석 단계)한다. 분석된 악성코드들은 유사도를 분석하여 그룹핑(그룹핑 및 분류 단계)하고, 개별 그룹 내에 포함된 행위를 분석하여 킬체인을 생성(킬체인 생성 단계)하여 DB에 저장한 후 MSI에서 요청할 경우 킬체인 및 분석 정보를 MSI에게 배포(배포 단계)하는 기능을 제공한다.

2.1.1. 데이터 수집

위협 정보는 malshare를 포함한 무료 채널과 웹 크롤링, C-TAS 및 Virussign을 통한 구매 등을 포함하여 약 3,000만 건 (약 9.5 TB)의 악성 코드를 3년에 걸쳐 수집하였다.

데이터 분석을 위하여 악성코드와 정상 파일에 대한 레이블을 생성하는 것이 필요하다. 이를 위해 Virus- total에서 제공하는 리포트를 수집하였으며, 그 중 Kaspersky에서 제공하는 진단명에 따라 정상·악성을 분류하였다. 또한, Virus-total의 public API의 속도 이슈를 극복하기 위하여 AWS에 다수의 EC2 인스턴스를 생성하고, 각각의 EC2 인스턴스에서 Virus-total로 리포트를 요청하는 방식으로 속도 이슈를 회피하였다.

2.1.2. 정적/동적 분석

정적분석은 악성코드의 디스어셈블(disassemble)을 통한 opcode 시퀀스를 활용하였다. 파일의 opcode를 추출하기 위해 IDA(Interactive Dis-Assembler) Pro를 사용하였으며, 동작 지표 추출에 활용하였다[7].

동적 분석을 위해서 오픈소스 기반의 샌드박스 프레임워크인 쿠쿠샌드박스 (cuckoo sandbox)를 활용하였으며 다량의 파일을 분석하기 위하여 하나의 Host에 다수의 Guest를 할당하고 동적 분석 자동화 모듈을 개발하여 사용하였다. 샌드박스 분석 정보는 표 1과 같으며 사이버 킬-체인 정보를 위해 추가 특징 추출을 진행하였다.

2.1.3. 동작 지표 추출

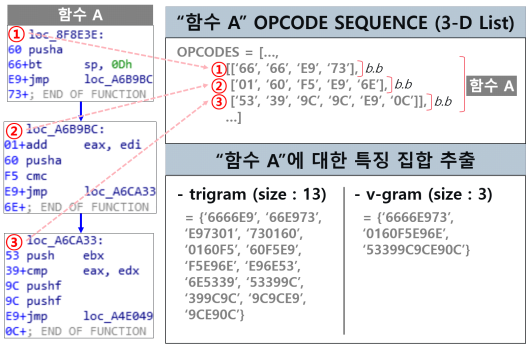
악성코드 동작 분석 지표로 정적 지표인 opcode 시퀀스를 활용하였으며 실행 파일은 2차원 리스트로 구성된 함수와 1차원 리스트로 구성된 기본블록을 구성하였다. n-gram 기법[8]은 입력 문자열에 대해 고정된 길이로 특징을 추출하여 워드를 생성하고, 집합으로 표현하는 방법으로 n-gram 기반의 opcode 특징

〔표 1〕 쿠쿠샌드박스 분석결과 정보

항목	설명
info	실행 환경 정보 및 Host/Guest 머신의 운영체제 정보
signature	호출 API나 위험도에 따른 시그니처 저장
target	파일의 해시값, CRC 정보, 배포시 파일 이름, ssdeep 정보, 파일 크기 등을 저장
buffer	실행 당시 사용했던 버퍼 정보 또는 YARA 규칙에 의한 안티 VM 기능이나 윈도우즈 API 사용 등을 저장
network	분석 파일이 통신한 네트워크 정보를 저장
static	정적정보(pdb 경로, PE 헤더 정보 등)를 저장
dropped	파일 실행 간에 신규로 생성되는 파일에 대한 정보를 저장
behavior	분석 파일의 행위 기반 정보(API 호출 시퀀스, 레지스트리 수정 정보)를 저장
debug	디버깅 정보
screen-shots	분석결과의 스크린샷 정보를 저장
strings	파일의 스트링 정보를 자체 분석하여 저장

추출 시 opcode 시퀀스의 구조를 반영하지 못하고 불용어 생성에 따른 불필요한 저장 공간을 많이 사용하는 단점이 있다. 이러한 문제를 극복하기 위하여 v-gram 기법을 제안하여 적용하였으며, v-gram 기법은 의미를 가지도록 하는 특징을 효율적으로 추출함과 동시에 불용어 생성을 억제할 수 있고, 특징의 개수가 작아 특징 벡터를 생성하는데 소요되는 시간을 감소시켰다[9]. 그림 4는 n-gram으로 특징을 추출한 경우와 v-gram으로 특징을 추출한 경우의 차이를 나타내고 있다.

동작 지표 벡터 생성은 최댓값 기반 피처 해싱(feature hashing) 기법을 제안하여 적용하였다. 해당

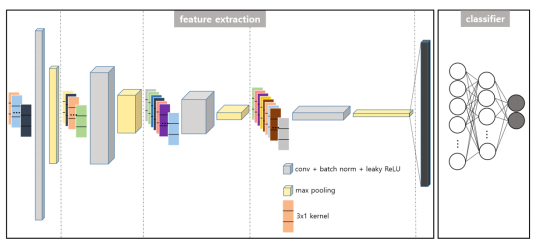


〔그림 4〕 IDA Pro 분석 결과에 따른 예시 및 특징 추출 방법(n-gram VS v-gram)

기술은 입력 특징에 대한 시그니처 값을 대표하는 값을 특징 벡터로 제공하고, 최댓값을 덮어씀으로써, 딥러닝 중 합성곱 신경망(CNN; Convolutional Neural Network)의 max pooling과 같은 대푯값 추출을 기대할 수 있는 장점이 있다. 특징 벡터는 악성코드의 특징 정보를 요약한 동작 지표 벡터로 그룹핑 기술에 활용되었다.

2.1.4. 딥러닝 모델링

딥러닝 모델은 CNN을 적용하였다. CNN은 ANN(Artificial Neural Network)과 달리, 주어진 입력에 대해 특징을 자동으로 추출하는 단계와 추출된 특징을 입력으로 분류하는 단계로 나누어진다. 또한 활성함수는 리키렐루(Leaky ReLU)를 사용하였으며 은닉층을 통과할 때마다 생성된 출력 데이터의 분포가 균일하지 않아 학습을 방해하는 Covariate Shift를 억제하기 위하여 배치 정규화를 수행하였다. 이를 통해 구현된 CNN 모델은 그림 5와 같이 4층으로 구성되어 있으며, 각 층 별로 3X1 필터에 따른 합성곱 연산, 배치 정규화, 그리고 리키렐루 활성함수를 적용한 특징 맵을 적용하였으며, 특징 맵에 대한 max pooling을 적용하였다[10]. CNN 모델의 분류기는 ANN을 적용하였으며 2개의 hidden layer를 구성하였다. 표 2는 딥러닝 모델의 구조 및 파라미터 설정값을 나타내고 있다. 모델 성능 검증은 공인시험기관(한국아이티평가원)을 통해 진행되었으며 약 6.6만개의 레이블링 된 파일 중 임의 추출 방식으로 80%는 학습데이터로 나머지 20%는 검증 데이터로 활용하였다. 파일 1개를 분류하는데 평균 0.053 msec가 소요되었으며 97.15%의 정확도로 악성·정상 유무를 판단하였다.



〔그림 5〕 CNN 모델을 통해 악성코드를 이진 분류하는 모델의 네트워크 구조

〔표 2〕 딥러닝 모델의 구조 및 하이퍼파라미터 설정 값

파라미터	값
합성곱 연산 수	16, 32, 64, 128
풀링 방법	max pooling (1X2)
Hidden layer 노드 수	128, 16
목적 함수	크로스 엔트로피
옵티마이저	Adam
활성 함수	Leaky ReLU
에폭	10
학습률	0.0001
배치 크기	256
드랍 아웃	적용 안함

2.1.5. 악성 그룹 분류

악성코드 분류 및 검색은 엘라스틱서치 검색엔진을 사용하였으며, 악성코드의 동작 지표를 추출한 후 유사한 악성코드를 검색하고 분류하는 방향으로 진행하였다. 먼저 데이터의 인덱싱은 IDA Pro로 정적분석한 후 opcode 시퀀스를 추출하고, 기본블록 대푯값(BOPS), 기본블록 대푯값 중 opcode가 30개 이상인 악성코드(BOPS30), 함수대푯값(FOPS)을 인덱싱 할 특징정보로 활용하였다. 유사도 공식은 TF-IDF (Term Frequency – Inverse Document Frequency)[11]를 사용하였으며, 해당 함수는 전체 데이터 중에서 빈도수가 가장 낮은 악성코드에 가중치를 부여한다. 분류 성능은 4개의 엘라스틱서치 인스턴스를 하나의 클러스터로 구성하였다. 표 3은 총 300만개의 악성코드에 대해 BOPS, BOPS30, FOPS 특징정보에 대해서 정확도 및 소요시간 측면에서 측정한 결과를 나타내고 있다. 측정 결과 BOPS30을 적용했을 때, 검색 및 분류 정확도 측면과 소요시간 측면에서 가장 우수한 성능을 보이는 것을 확인할 수 있었다. 이는 악성코드의 특징 정보를 잘 반영하기 위해서는 일정 길이 이상의 정보가 필요함을 의미한다.

〔표 3〕 특징 정보에 따른 정확도 및 소요 시간

구분	BOPS	BOPS (30개 이상)	FOPS
비교한 파일 수	854개	659개	820개
라벨이 맞은 개수	685개	583개	685개
정확도	0.802	0.884	0.835
총 걸린 시간	2084초	132초	2078초
파일 한 개당 찾는데 걸린 시간	2.4초	0.2초	2.5초

2.1.6 킬체인 정보 생성 방안

사이버 킬체인은 록히드 마틴에서 처음 제시한 개념으로 사이버 공격을 프로세스 상으로 분석해 각 공격 단계에서 조직에게 가해지는 위협 요소들을 파악하고, 공격자의 목적과 의도, 활동을 분쇄, 완화시켜 조직의 회복 탄력성을 확보하는 것을 의미한다[12]. APT(Advanced Persistent Threat) 유형의 공격을 탐지·차단하는데 많이 적용되는 개념이다.

공격자는 사이버 킬체인에 명시한 7개의 단계를 거치면서 공격을 진행하므로, 방어자는 최종 단계에 돌입하기 전에 차단함으로써 공격자의 최종 목표 달성을 좌절시키는데 중점을 둘 수 있다. 사이버 킬체인은 악용 가능한 취약점을 확인하고, 자산 정보를 파악하는 정찰(Reconnaissance) 단계, 파악된 취약점을 기반으로 방어 무력화를 위한 은닉화, 난독화 등 방어정책 회피를 위한 무기화(Weaponization) 단계, 다양한 채널을 통해 무기화된 악성코드를 전달하는 유포(Delivery) 단계, 악성코드를 대상 시스템에서 구동하여 악성코드가 설치되도록 하는 취약공격(Exploitation) 단계, 공격자가 지속적으로 대상 시스템을 장악할 수 있도록 백도어 등 원격 접속 가능한 프로그램을 설치하는 설치(Installation) 단계, 공격자가 대상 시스템에 접근하여 공격 목적을 달성하기 위해 명령 채널을 구축하는 명령 제어(Command and Control) 단계, 마지막으로 최종 공격 목표 및 정보를 획득하는 목적 달성(Actions on Objectives)단계로 구성된다. 본 과제에서는 쿠쿠샌드박스의 동적 분석 정보를 일부 선별 및 추출하여 생성하였으며, 7개의 단계 중 4개의 단계에 대해서 유의미한 분류를 진행하였다. 무기화 단계는 Signature 정보와 정적 분석 정보인 PDB 정보를 추출하였고, 설치 단계는 Dropped 정보를 사용하였다. 명령제어 단계는 네트워크의 IP 주소 정보, TCP/UDP 연결 정보, 도메인 정보를 추출하였으며, 목적 달성 단계는 파일 열기/단기, 읽기/쓰기에 해당하는 정보를 추출하였다. 해당하는 정보들은 JSON 형태로 저장하여, 악성코드 정보 전달시 해당 악성코드의 방어 중요도를 인지하는데 활용할 수 있도록 하였다.

2.2. STIX/TAXII 연동 인터페이스

STIX는 보안관련단체별로 상이하게 표현되는 사이버 위협 정보를 규격화된 포맷으로 정의함으로써,

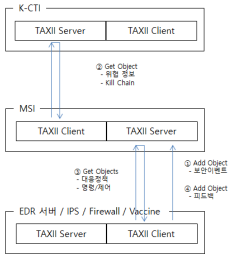
사이버 위협 정보의 신속한 공유와 일관된 분석, 그리고 자동화된 해석을 가능하게 하는 것을 목적으로 정의되었으며, TAXII는 STIX로 표현된 사이버 위협 정보를 HTTPS를 통해 공유하는 프로토콜을 의미한다[13]. 본 과제에서는 이기종 보안 솔루션 간 정보 공유를 위해 STIX/TAXII 관련 모듈 개발 및 표준화를 진행하였다.

2.2.1 STIX/TAXII 연동 모듈 개발

본 과제에서는 참여 업체 간 위협 정보 공유를 위해 STIX 2.0 기반 보안위협정보 생성/조회 API를 Incident, TTP, Campaign, CoA 구조체로 구현하였으며, 12개의 SDO(STIX Domain Objects) 객체(Threat Actor, Intrusion Set, Attack Pattern, Indicator, Identity, Campaign, Tool, Malware, Vulnerability, Course of Action, Observed Data, Report)와 2개의 SRO(STIX Relationship Objects) 객체(Relationship, Sighting)을 생성/파싱하는 Java, Python, C++ 라이브러리를 구현하였다.

위협 정보 연동 프로토콜은 TAXII 2.0 표준을 준용하여 HTTPS RESTful 방식으로 개발하였다. 서버는 Python으로 개발되었고, 클라이언트는 Java, Python, C++로 구현하였다. TAXII 2.0 RESTful API 및 서버·클라이언트 연동 구조는 그림 6과 같다.

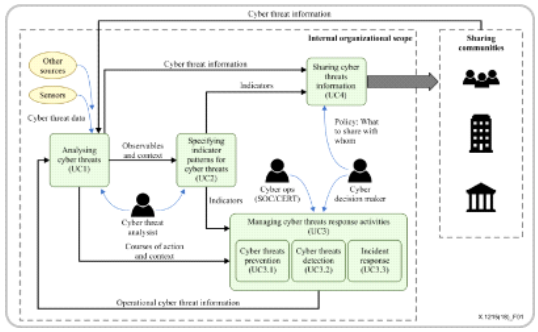
API	METHOD	설명
Server Discovery	GET	TAXII 서버의 일반 정보 조회
Get Api Root	GET	API Root 정보 조회
Get Status	GET	이전 요청 상태 정보 조회
Get Collections	GET	API Root 아래 호스팅되는 Collection 목록 조회
Get a Collection	GET	하나의 Collection 정보 조회
Get Objects	GET	Collection 내의 객체 목록 조회
Add Objects	POST	Collection 에 객체 추가
Get an Object	GET	하나의 객체 조회
Get Object Manifests	GET	하나의 Collection 으로부터 객체들에 대한 manifest 조회



〔그림 6〕 TAXII2.0 RESTful API 및 서버 클라이언트 연동 구조

2.2.2 STIX/TAXII 표준화

본 과제에서는 STIX/TAXII 규격의 국내·외 표준화를 위해 많은 노력을 기울였다. 이를 통해 ITU-T에 STIX에 대한 유즈케이스 권고안이 채택되었으며, 국내 표준도 3건 채택되었다[14]. 채택된 국제 표준안은



〔그림 7〕 STIX 기능 및 유즈케이스

랜섬웨어 공격 대응 정책을 용이하게 수립할 수 있는 STIX의 기능 및 유즈케이스를 제공하는 것을 주요 내용으로 하고 있으며, 그림 7과 같다. 또한 국내 표준화로 TTA에 구조화된 위협 정보 표현 규격 (STIX) 버전 2.0 제 3부 사이버 위협 관측 코어 개념과 제 4부 사이버 관측 객체에 대한 영문 표준으로 채택되었다.

Ⅲ. 상용화 현황

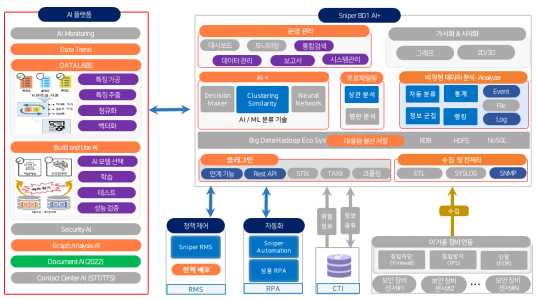
KOSIGN 과제를 참여한 기관들은 과제를 통해 개발된 기술을 다양한 형태로 상용화를 진행하고 있다. 본 장에서는 그중 K-CTI 시스템 개발을 통해 확보된 기술을 기반으로 개발 진행 중인 솔루션을 간단하게 소개하고자 한다. K-CTI 시스템의 가장 큰 특징은 AI 기술을 활용한 악성/정상 판단 기능과 STIX/TAXII 2.0을 기반을 둔 표준화된 연동 인터페이스를 들 수 있다. 해당 기술은 보안 관제 서비스를 제공하는데 있어서 수집된 위협 정보의 정·오탐을 판단하는데 활용될 수 있다. 또한 표준화된 정보 공유 인터페이스는 다양한 이기종 장비와 효과적으로 연동하는데 활용될 수 있다.

보안 관제 서비스를 제공하는 SOC(Security Operation Center)는 다양한 관제 솔루션을 운용하여 위협 발생 여부를 감시·차단하는 역할을 수행한다. SIEM(Security Information and Event Management) 솔루션은 SOC를 운용하는데 가장 중요한 역할을 수행하는 솔루션으로 다양한 보안 장비로부터 수집된 보안 로그 정보를 정규화하여 위협 발생 유무를 감시하고 예측하는 기능을 제공한다. 그러나 보안 위협의 발생 빈도 및 복잡도가 증가함에 따라 업무 부하가 발생하고 이로 인한 관제 인력 이탈 및 관제 품질 감

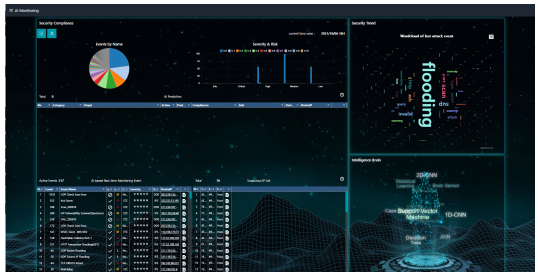
소는 현재 대다수의 SOC가 격고 있는 문제이다. 또한, 다양한 보안 센서 장비를 운용하는 상황에서 위협 발생 시 해당 위협을 탐지한 보안 센서 장비에 수동으로 접속하여 보안 정책을 적용하여 업무 난이도가 높은 문제도 있다.

㈜윈스에서는 이러한 문제를 인지하여 기존의 SIEM 솔루션에 수집된 위협 로그를 분석하여 보안 관제사와 협업하여 위협의 정·오탐 유무를 판단할 수 있는 AI 기반의 위협 식별 기능과 STIX/TAXII 인터페이스를 통한 보안 정책을 제공할 수 있는 기능을 추가한 새로운 솔루션을 개발하고 있다. 개발 진행 중인 AI 기반의 SIEM 솔루션은 기존의 SIEM 기능인 관제 운영, 위협 로그 수집/정규화/저장기능과 수집된 위협 로그 정보로부터 특징을 추출하고 학습할 AI 학습 모델을 선택하여 적용하는 AI 플랫폼으로 구성되어 있다. 그림 8은 현재 상용화를 추진 중인 AI 기반 보안 관제 솔루션의 기능 구성도를 나타내고 있다. AI 플랫폼은 AI에 의해 예측하고 브레인 센서 정탐을 식별한 위협 정보 제공, 현재 기준으로 활성화된 IP 및 이벤트를 추적할 수 있는 AI 모니터링 기능, 이벤트·호스트 랭킹 및 공격이벤트 발생 빈도를 분석하는 데이터 트랜드 기능, 데이터의 특징을 추출/가공/정규화/벡터화를 수행할 수 있는 데이터 랩 기능, AI 알고리즘을 선택하여 학습/테스트/성능검증을 수행하는 빌드앤유즈 AI 기능, 위협 IP 예측, 위협 IP 행위 분석, 공격 유형 및 시간별 공격 성향을 분석하는 시큐리티 AI 기능, RWR(Random Work and Restart) 기반 객체간 관계 분석을 통한 APT 형태의 위협을 예측할 수 있는 그래프 분석 기능을 제공한다. 그림 9는 AI 플랫폼에서 제공하는 다양한 기능 중 AI 모니터링 기능의 화면 GUI를 나타내고 있다.

또한, AI 및 관제사에 의해 위협이 정탐으로 판단



〔그림 8〕 AI 기반 보안 관제 솔루션의 기능 구성도



〔그림 9〕 AI 플랫폼의 AI 모니터링 기능 화면 GUI

될 경우, 방어 정책을 입안하고 STIX/TAXII로 방어 정책을 배포하면, 개별 보안 센서 장비에 해당 정책을 배포하고 관리하는 솔루션과 위협 발생 정보 분석, 시스템 정상 운용 여부를 확인하는 리포트 생성 등 다양한 보안 관제 업무를 자동화할 수 있는 보안 관제 자동화 솔루션에 대한 개발도 활발히 진행되고 있다.

Ⅳ. 결 론

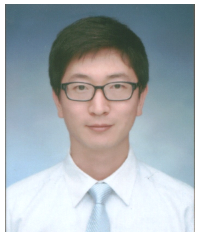
보안 위협은 점차 고도화·은밀화 되고 있다. CTA는 이러한 보안 위협의 발전 방향에 발맞추어 공격·방어 중심의 기술에서 피해 최소화를 위한 예방·대응 관점으로 보안 기술을 변화시킨 점을 주목할 필요가 있다. 또한 KOSIGN 과제를 통해 개발된 K-CTI 시스템은 CTA와 원활하게 연동할 수 있도록 표준화된 인터페이스를 기반으로 개발되었다는 점과 기존 CTI 시스템과 연동하여 정보를 수집하는 것뿐만 아니라 독자적으로 AI 기술을 활용하여 위협 정보를 생성·보관·배포하는 것을 강점으로 둘 수 있다. 또한, C-TAS 시스템과 달리 민간 주도의 분산 형태로 운용된다는 점에서 정보 교환의 확산을 활성화시킬 수 있다. 현재 시점에서 K-CTI 시스템은 그 활용이 미비한 상태이나 향후 C-TAS 시스템의 한계를 극복하는데 도움을 줄 수 있을 것으로 예상된다. 마지막으로 K-CTI 시스템 개발을 통해 확보된 기술은 참여업체에서 다양한 형태로 상용화를 진행하고 있어, 과제의 목적을 충분히 달성했다고 볼 수 있다.

참 고 문 헌

[1] E.M. Sedenberg, and J.X. Dempsey, Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoff,

arXiv preprint arXiv:1805, 12266, 2018.
[2] 김동희, 박상돈, 김소정, 윤오준, “사이버 위협정보 공유체계 구축방안에 관한 연구-미국 사례를 중심으로”, 융합보안논문지, 17(2), pp. 53-68, 2017.
[3] 진희승, 심미나, 양민호, “소프트웨어안전 정보공유체계에 관한 연구,” SPRi 소프트웨어정책연구소, Research Report, 2018. 04.
[4] 김용준, 손태식, “Sysmon과 ELK를 이용한 산업제어시스템 사이버 위협 탐지,” 정보보호학회논문지, 29(2), pp. 331-346, 2019.
[5] 임원식, 윤명근, 조학수, “KOSIGN: 정보보호제품 관점의 사이버위협정보 공유 체계,” 정보보호학회지, 28(2), pp. 20-26, 2018년 4월
[6] 박지백, 최병환, 조학수, “사이버 위협 정보의 공유 활성화 방안,” 한국통신학회지, 35(7), pp. 41-48, 2018년 6월.
[7] IDA Pro, https://hex-rays.com/ida-pro/
[8] C.Y. Suen, “N-Gram Statistics for Natural Language Understanding and Text Processing,” IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. PAMI1, No. 2, pp.164-172. Apr. 1979.
[9] S.M.A. Naqvi and M. Yoon, “Finding Widespread Events with Simple Bitmaps,” IEICE Transactions on Information and System, vol. 101, no. 12, pp. 3246-3248, 2018.
[10] 정성민, 이식, 장지만, 윤명근, “심층학습과 악성코드 분석 연구,” 정보과학회지, 36(2), pp. 37-42, 2018년 2월
[11] H. Christian, M.P. Agus, and S. Suhartono, “Single document automatic text summarization using term frequency inverse document frequency,” ComTech: Computer, Mathematics and Engineering Applications, vol. 7, no. 4, pp. 285-294, 2016.
[12] M.S. Khan, S. Siddiqui, and K. Ferens, “A cognitive and concurrent cyber kill chain model,” Computer and Network Security Essentials, pp. 585-602, 2018.
[13] 최종원, 김예솔, 민병길, “CTI 모델 활용 제어시스템 보안 정보 수집 방안 연구,” 정보보호학회지, 28(2), pp. 471-484, 2018년 4월
[14] ITU-T X.1215 “Use cases for structured threat information expression,” ITU-T, Jan. 2019.

〈저 자 소 개〉



이 현 진 (Hyun-Jin Lee)
정회원
2004년 8월 : 아주대 전자공학과 졸업
2006년 8월 : 아주대학교 전자공학과 공학석사
2013년 8월 : 아주대학교 전자공학과 공학박사
2014년 1월~2015년 1월 : 단암시스템즈 선임연구원
2015년 4월~2020년 2월 : 솔빛시스템 책임연구원/팀장
2020년 3월~현재 : ㈜윈스 수석연구원/팀장
<관심분야> 네트워크 보안, 5G 및 5G 보안, 보안관제, AI 모델, 자동화, 사이버 공격 모델링, 네트워크 모델링 등

조 학 수 (Harksu Cho)
정회원
1997년 2월 : 서울대학교 계산통계학화 전산과학전공 졸업
1999년 2월 : 서울대학교 자연과학대학원 전산과학과 석사
2001년~현재 : ㈜윈스 부사장, CTO
2017년~2019년 : 4차산업혁명위원회 과학기술혁신분과 혁신위원
<관심분야> 네트워크 보안, 침입방지시스템, 침입차단시스템, 악성코드 자동분석, AI 보안관제