Journal of the KIMST, Vol. 21, No. 6, pp. 807-816, 2018
ISSN 1598-9127
DOI http://dx.doi.org/10.9766/KIMST.2018.21.6.807

Research Paper 정보 · 통신 부문

위협 헌팅을 적용한 사이버 상황인식 시스템 개발에 관한 연구

이재연*,1) · 최정인1) · 박상현1) · 김병진1) · 현대원1) · 김관영1)

1) 한화시스템㈜ 지휘통제·통신연구소 C4I·사이버팀

A Study for Cyber Situation Awareness System Development with Threat Hunting

Jaeyeon Lee*,1) · Jeongin Choi1) · Sanghyun Park1) · Byeongjin Kim1) · Dae-Won Hyun1) · Gwanyoung Kim1)

1) *C2·Comm. R&D Center C4I·Cyber Team, Hanwha Systems Co. Ltd., Korea*

(Received 4 July 2018 / Revised 29 August 2018 / Accepted 19 October 2018)

ABSTRACT

Threat hunting is defined as a process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions. The main concept of threat hunting is to find out weak points and remedy them before actual cyber threat has occurred. And HMM(Hunting Maturity Matrix) is suggested to evolve hunting processes with five levels, therefore, CSOC(Cyber Security Operations Center) can refer HMM how to make them safer from complicated and organized cyber attacks. We are developing a system for cyber situation awareness system with pro-active threat hunting process called *unMaze*™. With this unMaze, it can be upgraded CSOC's HMM level from initial level to basic level. CSOC with unMaze do threat hunting process not only detecting existing cyber equipment post-actively, but also proactively detecting cyber threat by fusing and analyzing cyber asset data and threat intelligence.

Key Words : Threat hunting(위협 헌팅), CSOC(사이버 통합보안관제센터), Cyber Situation Awareness System(사이버 상황인식 시스템), Real-Time Threat Information Gathering(실시간 위협 정보 수집), Cyber Asset Management (사이버 자산 관리), Cyber COP(사이버 상황도)

1. 서 론

최근의 사이버 공격은 더욱 조직적이고 목적 지향적이며 오랜 시간에 걸쳐 수행되는데, 이를 지능적 지속 공격인 APT(Advanced Persistent Threat) 공격이라고 한다. APT 공격 집단은 보안 취약점이나 사회공학적 기법, 해킹 도구 사용 및 자체 공격 도구 개발 등을 통해 집단이 목적한 바를 달성할 때까지 공격을 시도하고 진행한다. 이를 관제하기 위해 공공 및 금융, 군이

* Corresponding author, E-mail: jaeyeon46.lee@hanwha.com

나 기업에서 사이버 통합보안관제센터인 CSOC(Cyber Security Operations Center)을 운용하고 있지만, 사이버 공격으로 인한 피해는 지속적으로 보고되고 있다. 또한 많은 제조사에서 다양한 기능으로 보안 제품들을 출시하고 있지만, CSOC의 특성에 맞게 제품을 사용하지 않으면 비용만 발생할 뿐 원하는 효과를 얻기도 어렵다. 그래서 많은 CSOC 운영 방식이 보안 장비의 탐지 성능에 의존하던 보안관제 방식에서 발전하여, SIEM (Security Information and Event Management) 장비를 도입 및 운영하면서 여러 종류의 보안 장비에서 발생하는 로그들을 통합해서 관리하고 있다. 그러나 SIEM을 이용해 보안 장비를 통합관리하고 있다고 하더라도, 장비 업데이트보다 공격자의 취약점 발견 시점이 빠르면 보안 장비에서 탐지하지 못하는 Zero-day 공격을 당할 가능성은 여전히 존재한다. 또한 시그니쳐 기반으로 알려진 위협은 지속적으로 변형되면서 발전하기 때문에, 패턴이나 시그니쳐 기반으로 위협을 탐지하는 IDS/IPS(Intrusion Detection/Prevention System)와 같은 보안 장비의 탐지율이 저하될 수밖에 없는 상황이다.

그래서 등장한 새로운 관제 패러다임이 위협 헌팅(Threat Hunting)이다. 위협 헌팅은 위협이 발생하기 이전에 위협이 발생할만한 사이버 자산의 취약점을 찾아내고, 이를 제거하여 위협이 발생하지 않도록 선조치하는 일련의 활동을 통칭한다. 이런 위협 헌팅 프로세스를 성공적으로 수행하기 위해 위협 헌팅 성숙도 모델 5단계를 정의하며, 성숙도 단계별로 어떤 분야에 어떤 조건을 갖춰야 하는지 위협 헌팅 성숙도 매트릭스도 제안되었다[1].

본 논문에서는 사이버 위협 탐지와 병행하여 위협 헌팅 프로세스를 수행할 수 있도록 unMaze™라는 명칭을 가진 상황인식 시스템을 개발하고, 이를 CSOC에 적용하여 사용시 위협 헌팅 성숙도를 얼마나 확보할 수 있는지에 대해 제안한다. unMaze는 보안장비에서 발생하는 사이버 위협 경보를 표준 인터페이스를 이용해 연동하여 사이버 자산 정보와 융합 후 탐지 결과를 사이버 상황도에 도시하고, 위협 인텔리전스 문서를 분석하여 사이버 자산의 취약점과 매핑시켜 잠재적 위협을 경고한다. 또한 사이버 자산을 데이터베이스를 이용해 관리하며, 네트워크 모니터링을 통해 블랙리스트에 해당하거나 화이트리스트 기반 비인가 트래픽을 검출한다. 위협 헌팅 프로세스가 적용되지 않은 일반적인 CSOC에 본 연구를 통해 개발한 unMaze 시스템을 연동하여 운영시, CSOC은 위협 헌팅 성숙도를 최소 1단계 이상으로 향상시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 CSOC에 위협 헌팅 프로세스를 적용해야 하는 이유에 대해 기술하고, 3장에서는 위협 헌팅 개념 및 성숙도 모델에 대해 기술한다. 4장에서는 unMaze의 각 기능을 설명하고, 5장에서는 unMaze 적용시 CSOC이 획득할 수 있는 위협 헌팅 성숙도에 대해 설명한다. 6장에서 결론 및 향후 연구 방향에 대해 설명하는 순서로 본 논문을 구성한다.

2. 사이버 상황인식을 위한 사이버 통합보안관제센터

사이버 통합보안관제센터인 CSOC은 모니터링, 검출, 분석 그리고 대응 행위를 포함하는 컴퓨터 네트워크 상에서의 인가되지 않은 행위에 맞춰 공격을 방어하는 행위를 하는 전문가 집단으로 이뤄진 조직이 활동하는 공간이다[2]. CSOC 내에서도 전문적으로 사이버 침해 사고 발생시 이를 분석하고 대응하는 인력으로 구성된 조직을 침해사고 전담 대응팀이라 하여 CERT(Computer Emergency Response Team)라고 하는데, CERT는 정보통신망 등의 침해 사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해복구 등의 임무를 수행한다[3].

상황인식(Situation Awareness)이란 시간, 공간상에서 발생하는 요소와 그에 대한 속성을 인식하고, 가까운 미래에 현재의 상황이 어떤 영향을 미칠 것인지를 인지하는 활동이다. 주로 상황인식 시스템은 복잡하고 역동적인 분야의 의사 결정권자에게 의사 결정에 중요한 현황을 직관적으로 이해할 수 있도록 관련 분야를 연구하는 분야로, 항공이나 교통관제, 선박 항법, 군대 지휘 및 통제 등 상황을 판단하여 의사결정을 수행하는 프로세스를 포함하는 시스템이다[4]. CSOC이 사이버 공간에서 발생하는 위협을 탐지 및 분석하는 기능을 수행하므로, CSOC이 상황인식 시스템 범주에 포함됨을 알 수 있다.

사이버 상황인식 시스템 관점에서 CSOC의 기능 범위를 해석하면, CSOC은 보안 장비를 활용해 위협 탐지를 판단하면서 현재 상황을 분석하는 기능과 더불어, 가까운 미래에 발생 가능성이 높은 잠재적 위협까지 예측하는 기능도 포함되어야 한다. 위협 헌팅은 잠재적인 위협 요소를 사전에 파악하여 대응 조치한다

Table 1. Definition of threat hunting maturity matrix.

		위협 헌팅 성숙(Hunting Maturity: HM) 단계				
위협 헌팅 수행 과정		0단계 – 초기 (Initial – HM 0)	1단계 – 최소 (Minimal – HM 1)	2단계 – 절차적 (Procedural – HM 2)	3단계 – 진보적 (Innovative – HM 3)	4단계 – 선도적 (Leading – HM 4)
	데이터 수집	없음	IT 환경 중 일부에서 몇 가지 종류의 데이터만 수집	IT 환경 전체적으로 특정 종류의 데이터를 지속적으로 수집		
	가설 생성	SIEM, IDS, 방화벽 등 장비가 탐지한 alert에 의존	새로운 가설 생성을 위해 위협 인텔리전스 분석	새로운 가설 생성을 위해 일반적인/ 기적용된[1] 위협 인텔리전스를 분석	새로운 가설 생성을 위해 일반적인/기적용된 위협 인텔리전스를 비롯해 Crown jewel analysis 기법을 사용해 수동으로 사이버 자산을 scoring함	새로운 가설 생성을 위해 일반적인/기적용된 위협 인텔리전스를 비롯해 자동으로 사이버 자산을 scoring함
	가설 검증 도구	alert을 알려주는 콘솔이나 SIEM을 사용한 분석 수행함. 선제적 탐지 없음	full-text나 SQL-like query 등을 통해 SIEM이나 로그 분석기 활용	간단한 도구나 histogram을 활용하여 기존의 헌팅 프로시저를 기반으로 데이터를 분석함	시각화 도구 또는 그래프 분석을 활용함. 새로운 헌팅 프로시저를 개발함	고도화된 시각화 도구 또는 그래프를 활용한 분석 수행. 새로운 헌팅 프로시저를 개발하고 이를 공개함.
	위협 탐지	SIEM/IDS alert만 의존하거나 탐지 장비가 없음	domain, URLs, hash값 등 PoP[2]의 낮은 단계에 해당하는 IOC 식별	도메인명이나 forensic artifact 등 PoP의 중하단 단계의 IOC를 식별하고 이를 시간 기반으로 분석함	PoP의 높은 단계 있는 IOC 상대방의 TTPs를 탐지 가능	자동으로 복잡한 TTPs를 찾아내고 campaign을 추적함. 정보 공유 시스템에 적극적으로 IOC를 공유함.
	분석 자동화	없음	기본적으로 매칭되는 위협 인텔리전스 정보를 alert과 매핑시킴	효율적인 헌팅 프로시저 라이브러리를 생성하고 주기적으로 프로시저를 수행함	효율적 위협 헌팅 프로시저 라이브러리를 생성하여 자주 프로시저를 수행하고, 표준 편차나 이상치 탐지와 같은 기본적인 데이터 사이언스를 수행함	효율적 헌팅 프로시저의 지속적 수행을 자동화하여 경보 시스템을 향상시키고, 머신 러닝과 같은 고도화된 데이터 사이언스를 수행함

는 개념의 관제방법이므로, 사이버 상황인식 시스템이 지향하는 목적에 알맞은 프로세스로 활용할 수 있다.

3. 위협 헌팅 및 위협 헌팅 성숙도 모델

위협 헌팅은 위협이 발생하기 이전에 위협이 발생할만한 사이버 자산의 취약점을 찾아내고, 이를 사전에 조치하여 위협이 발생하지 않도록 선조치하는 일련의 프로세스이다. 위협 헌팅 프로세스를 성공적으로 수행하기 위해 위협 헌팅 성숙도 모델을 5단계로 정의하고, 각 단계별로 어떤 분야에 어떤 조건을 갖춰야 하는지 가이드라인을 제시했다.

[1]에서는 위협 헌팅 성숙도 모델을 다음과 같은 정의로 제안했다. 초기 0단계는 자동화 경보에 의존하는 단계, 최소 1단계는 CSOC이 위협 인텔리전스를 도입하는 단계, 절차적 2단계는 타 기관에서 진행한 데이터 분석 과정을 적용하는 단계, 진보적 3단계는 새로운 데이터 분석 과정을 창출하는 단계, 선도적 4단계는 자동화된 수준 높은 데이터 분석을 수행하는 단계이다. Table 1은 위협 헌팅 성숙도 매트릭스로, 각 단

1) [1]에서는 “friendly intelligence”로 표현하였으나, 본 연구에서는 운용중인 CSOC에서 이미 적용되어 사용중인 intelligence로 해석하여, 해당 부분을 기적용된 위협 인텔리전스라고 표현했다.

2) PoP(Pyramid of Pain)는 위협 인텔리전스의 IOC(Indicators of Compromise) 형태를 6단계로 구분하며, 상위 단계로 갈수록 IOC를 분석하기 어려운 단계이다. 가장 하위 단계부터 Hash value, IP addresses, domain name, network/host artifacts, tools, 가장 상위 단계로 TTPs(Tactics, Techniques and Procedures)로 정의했다[5].

계별 위협 헌팅 수행 과정이 갖춰야 하는 활동 범위를 정리해놓았다.

위협 헌팅 성숙도 매트릭스는 총 5단계로 구분하며, 0단계인 초기 단계는 보안 장비를 통해 사이버 자산에 위협이 발생하였음을 인지하고 대응하는 일반적인 CSOC의 기능을 나타낸다. 위협 헌팅 수행 과정에서 위협 탐지 항목을 가장 기본 기능으로 제시했다는 것은, 위협 헌팅 프로세스를 수행하려면 위협 탐지 기능을 충분히 수행하고 있어야 함을 의미한다. 위협 탐지 기능을 수행하지 못하는 CSOC이라면 보안장비를 보완하거나, 탐지에 사용되는 위협 인텔리전스를 확대해서라도 발생하는 위협을 탐지할 수 있는 기본적 역량을 먼저 보유해야 할 것이다.

이렇게 장비를 통해 위협을 탐지할 수 있는 CSOC의 경우라면, IT 환경의 일부 데이터 수집을 기존 프로세스에 추가 시켜, 위협 인텔리전스가 적용된 위협 가설을 생성할 수 있는 단계가 기본적 1단계이다. 위협이 발생할 가능성이 있다는 가설을 수립하기 위해서는 관리중인 자산이 해당 위협에 대해 취약점을 갖고 있다는 지식 정보가 있을 때 수립 가능하다. 그러므로 관리중인 자산에서 일부라도 데이터 수집이 반드시 필요하며, 해당 취약점에서 발생 가능한 위협이 어떤 것들이 있는지 매핑시키는 위협 인텔리전스 지식이 있어야 한다. 위협 가설로 가정한 잠재적 위협의 징후가 있는지 확인하기 위해, 가설 검증 도구를 사용해서 공격을 탐지하는데 이때 사용할 수 있는 도구가 SIEM이나 로그 분석기이다. 텍스트 형태로 질의를 하거나 SQL (Structured Query Language) 형태로 질문을 생성해서 로그를 분석함으로써, 공격자가 사용하는 domain이나 URL, 악성코드의 hash값 등을 찾아낼 수 있다. 가정한 공격 행위가 발견되면 잠재적 위협 발생 요소로 파악하여, 이를 사전에 제거 또는 완화하는 대응방책을 적용하여 잠재적 위협 요소를 제거함으로써 하나의 위협 헌팅 가설에 대한 대응 프로세스를 종료할 수 있다.

위협 헌팅 성숙도 2단계 이상의 데이터 수집 기능은 관리중인 IT 환경에서 특정 종류의 데이터를 지속적으로 수집한다는 동일한 범주를 가진다. 그러나 가설 생성 단계는 2단계부터 4단계 까지 구분되어 있다. 2단계에는 가설 생성시 일반적인 위협 인텔리전스에 추가하여 기적용된 위협 인텔리전스를 사용한다. 기적용된 인텔리전스를 활용하기 위해서는 가설을 생성하고, 어떤 위협 인텔리전스를 적용하여 대응을 수행했는지를 관리하는 위협 헌팅 수행 과정이 데이터베이스를 통해 관리될 때만 가능한 업무이다. 이런 가설을 검증하기 위해 위협 헌팅 성숙도 2단계에 해당하는 CSOC은 histogram이나 dashboard 형태의 간단한 도구를 활용하여 가설을 검증할 수 있도록 지원해야 하며, hash 값이나 IP 주소와 같은 PoP 중하단 단계에 있는 IOC(Indicators of Compromise)를 사용해서 이를 시간에 따라 연관 분석할 수 있어야 한다.

3단계와 4단계는 CERT와 같은 분석가 조직이 위협 헌팅 프로세스를 전문적으로 수행할 때 가능하다. 공격자의 TTPs(Tactics, Techniques and Procedures)는 공격 행위 중 가장 분석하기 어려운 단계인데, 이를 파악하고 위협 헌팅 프로시저 라이브러리를 생성하여 데이터 사이언스에 기반한 데이터 분석을 수행할 수 있어야 하기 때문이다. 진보적 3단계에서는 가설 생성시 위협 인텔리전스 뿐만 아니라 자산의 중요도를 측정하여 분석하는 crown jewel analysis 기법을 적용해 가설을 생성할 수 있어야 한다. crown jewel analysis는 관리중인 사이버 자산의 우선순위를 설정하고 가중치를 계산하여 가장 중요한 자산을 선정하는 분석 기법으로, 사이버 위협에 대한 시스템의 민감도 분석 및 위협 발생시 자산의 피해를 최소화하기 위해 적용하기 위한 선행과정이다[6]. 예를 들면, 중요 데이터가 많이 저장된 데이터베이스 서버가 일반 사용자의 단말보다 중요하기 때문에 잠재적 위협이 발생할 가능성이 높아 데이터베이스의 서버 취약점을 우선적으로 분석하는 방식이 적용되는 것이다. 사이버 자산의 crown jewel analysis 분석 기법을 적용하기 위해서는 자산의 중요도를 정량적으로 분석하는 평가 항목을 선정하여[7], 항목별 자산의 점수를 사용자가 설정 및 관리하는 시스템이 동반되어야 한다.

3단계인 진보적 단계와 4단계인 선도적 단계의 가장 큰 구분점은 자동화이다. 4단계에서는 사이버 자산의 중요도를 자동으로 설정 및 관리하고, 자동으로 복잡한 TTPs나 전술을 찾아내고 이를 시스템을 통해 외부에 공유하며, 지속적으로 헌팅 프로시저를 자동으로 수행하고 이를 머신러닝과 같은 고도화된 데이터 사이언스의 기초 데이터로 사용하는 차이점이 있다. 선도적인 위협 헌팅 성숙도를 갖게 되면, 최소한의 보안 관제 인력이 자동화된 시스템을 운용하면서 자산의 중요도를 관리하고, 위협 발생 현황을 직관적 시각화로 인지하며, 복잡한 공격자의 공격 행위를 사전에 탐지하여 대응할 수 있게 된다. 이를 위해서 CSOC은 방화벽이나 APT 솔루션과 같은 하나의 시스템이 아

닌, 여러 시스템이 고도로 융합된 최적화 시스템을 구축해야 할 것이다.

위협 헌팅 개념을 도입한 사이버 보안장비는 많은 국내외 제조사에서 개발 중이며, 대표적으로 위협 헌팅 프로세스 개념을 제안한 미국의 Sqrrl Inc.[1], 엔드포인트 솔루션에 위협 헌팅 개념을 적용한 Carbon black Inc.[8], Cybereason Inc.[9] 등이 있다. 위협 헌팅 프로세스를 적용해서 위협 헌팅 성숙도를 만족하는 방법은 제조사의 개발 제품 및 해당 제품을 적용하는 사이트마다 상이할 수 있으나, 위협 헌팅 개념을 CSOC에서 적용했을 때 나타나는 효과는 [10]에서 정리되어 발표되었다. [10]에 따르면, 위협 헌팅에 대해 지식을 가지고 있는 CSOC 담당자는 60 %나 되지만, 현재 보안관제에 위협 헌팅 개념을 적용한 곳은 CSOC 중 1/3에 불과하다고 보고했다. 위협 헌팅 적용시 위협을 탐지하기까지의 기간이 2.5배 단축되었고, 위협을 조사하는데 걸리는 시간은 약 2배 가량이 단축되었다고 설문 조사 결과에서 보고했다. 위협 헌팅 적용시 가장 큰 장점을 응답자의 72 %가 진화된 위협에 대한 탐지 성능이 좋아졌다고 답했다. 본 논문에서 제안하는 위협 헌팅 기법을 적용한 사이버 상황인식 시스템을 기존 CSOC에서 사용 시에도, 진화된 위협 및 발생하지 않은 잠재적 위협에 대한 탐지 성능이 개선될 수 있으며 이는 5장에서 후술한다.

4. 위협 헌팅을 적용한 사이버 상황인식 시스템 – unMaze™

본 연구에서 제안하는 위협 헌팅을 적용한 사이버상황인식 시스템인 unMaze의 시스템 프레임워크는 Fig. 1과 같다. 사이버 정보의 흐름은 정보를 수집하여 필요한 형태로 가공한 후, 관리중인 사이버 자산 정보와 위협 인텔리전스와 융합한다. 융합된 정보는 시각적 정보 전달 형태로 사용자에게 제공되어, 사용자가 사이버 상황에 대한 인식을 하고, 향후 예측을 할 수 있도록 시스템이 지원하는 형태를 갖게 된다[11]. 정보 흐름의 각 단계별로 시스템 구성 요소를 살펴보면, 보안장비에서 발생하는 사이버 위협 정보를 사이버 자산 정보와 융합하여 사이버 상황인식 정보로 가공한 후, 상황도를 통해 사용자가 직관적으로 위협 현황을 이해할 수 있도록 정보를 전달하고자 하는 목적을 갖는다. 또한 사이버 보안 장비로부터 위협으로 식별되어

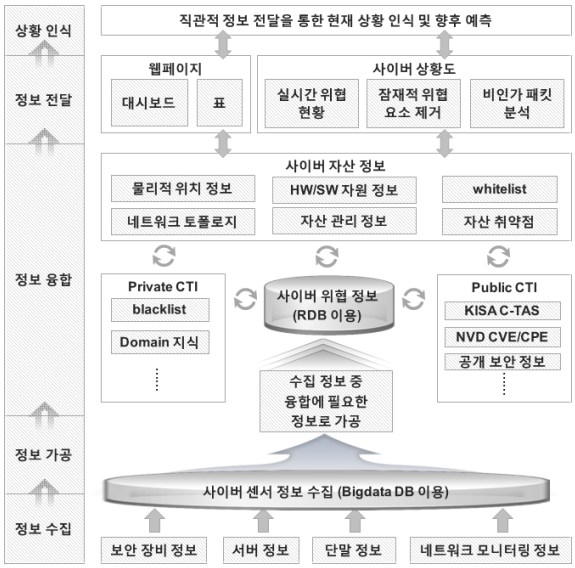

Fig. 1. Proposed system framework for unMaze™

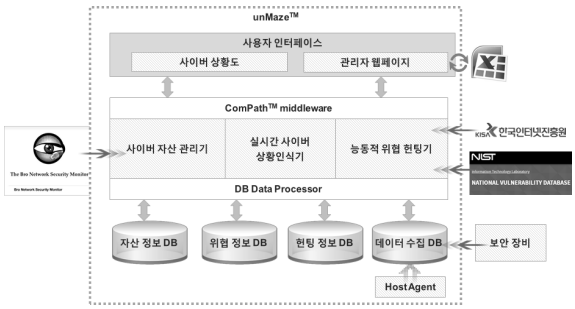

Fig. 2. SW functional block diagram of unMaze™

생성된 경보 외에, 관리중인 사이버 자산의 취약점을 위협 인텔리전스 문서에서 추출한 정보와 매핑하여 사전에 위협이 발생 가능한 요소를 제거하는 위협 헌팅 기능도 포함한다. 제안하는 시스템을 사용하는 사용자는 사이버 상황도를 통해 직관적인 사이버 위협 현황을 시각적으로 전달받음으로써, 피해 현황에 대해 정확히 인지하고 향후 대처방안을 수립할 수 있다.

unMaze는 Fig. 2와 같이 보안장비와 에이전트를 통해 사이버 자산으로부터 정보를 수집하고, 수집한 사이버 위협 정보와 사이버 자산 정보, 위협 헌팅 정보를 융합한다. 융합한 정보를 데이터베이스와 사이버 상황도, 웹페이지를 통해 사용자에게 직관적으로 전달하여, unMaze 사용자들이 빠르게 사이버 상황을 판단하고 의사결정을 수행할 수 있도록 지원한다. 또한 위

협 인텔리전스를 활용한 위협 헌팅 기능을 포함하여, 사이버 자산의 취약점을 분석하고 잠재적 위협 요소를 제거할 수 있도록 지원한다.

4.1 사이버 상황인식 정보 수집 기능

일반적인 보안 장비들이 탐지한 위협 정보만 사용자에게 전달하는 것에 비해, unMaze의 사이버 상황인식 정보 수집 기능은 위협 정보를 사이버 자산 정보와 융합하여 시각적으로 어느 자산에 위협이 발생했는지 직관적으로 도시하는 장점을 갖고 있다.

실시간 사이버 상황인식 정보 수집 기능 구현을 위한 SW 구조는 Fig. 3과 같다. 데이터 수집 모듈에서 정보 수집을 위해 APT 솔루션 장비나 방화벽 등 타 보안 장비와 표준 인터페이스인 RestAPI를 사용하여 보안 장비에서 발생한 정보를 수집한다. 수집한 정보는 ElasticSearch에 미가공된 데이터 형태로 저장되어, 향후 분석가가 전문적인 위협 분석시 활용할 수 있도록 관리된다. 장비를 통해 수집된 가공되지 않은 데이터를 ElasticSesarch에 저장하므로, 사용자가 원하는 형태로 정보를 가공할 수 있는 빅데이터 분석 기능도 포함한다. ElasticSearch를 로그 DB로 사용하고, 데이터 중계 모듈은 kafka를 사용하며, 데이터 수집 모듈은 Logstash를 사용하여 구현하였다[12]. 표준 인터페이스를 통해 장비에서 발생하는 데이터를 수집하는 방식이므로, 기존에 사용 중인 보안장비의 네트워크 토폴로지를 변경하거나 장비를 교체하지 않아도 되는 운용상의 장점을 가진다.

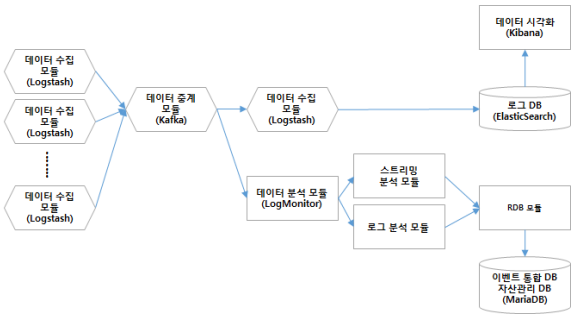

Fig. 3. SW functional diagram for gathering information of cyber assets

4.2 사이버 자산 관리 기능

unMaze의 사이버 자산 관리는 CSOC이 관리하는 사이버 자산에 대한 정보를 관리하는 기능으로, 자산의

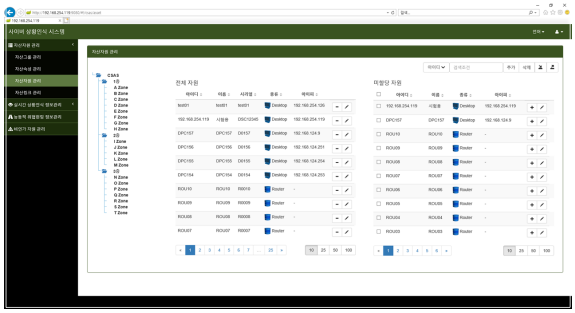

Fig. 4. Implemented web interface for cyber asset management

IP 및 타입, 실행되는 응용 정보 등을 관리한다. 사이버 자산 관리는 데이터베이스를 이용해 관리하지만, unMaze는 Fig. 4과 같이 웹페이지를 통해 직접 DB에 접근하지 않고도 자산 정보를 관리할 수 있도록 사용자 인터페이스를 제공한다. 관리되는 자산 정보는 자산명, 자산 타입, 설치된 운영체제, 운용 응용프로그램명 및 버전 정보 등이다[13]. 사이버 자산 관리자는 웹페이지를 통해 블랙리스트 및 화이트리스트 기반 비인가 자원을 선별할 수 있는 데이터를 생성한다. 블랙리스트는 시큐리티 모니터링을 수행하는 가장 직관적인 방법이며, 화이트리스트 기반 트래픽 분석은 정의된 리스트 외의 정보는 모두 비인가 정보로 분류한다[14]. 블랙리스트/화이트리스트 기반 트래픽 분석은 보안 장비에서 범용적으로 사용하는 모니터링 기법으로, unMaze는 Bro framework[15]을 기반으로 하여 사이버 자산의 관리 외의 블랙리스트 트래픽이 검출되거나, 화이트리스트로 정의되지 않은 비인가 네트워크 트래픽 탐지시 사용자에게 사이버 상황도를 통해 경보로 알려준다.

4.3 능동적 위협 헌팅 기능

unMaze의 능동적 위협 헌팅 기능은 위협 인텔리전스 정보와 CSOC이 관리하고 있는 자산 정보를 융합하여, 인텔리전스에서 명시한 취약점을 보유한 자산이 있는 경우 잠재적 위협이 발생 가능한 자산으로 간주하고, 사전에 조치하는 능동적 대응을 수행하는 일련의 프로세스를 포함한다.

위협 헌팅은 발생하지 않은 잠재적 위협 발생 요소를 제거하는 활동이므로, 잠재적 위협 요소가 무엇인지를 가정하는 가설을 수립하는 과정이 위협 헌팅의 성능을 결정하는 가장 중요한 단계이다. 위협 헌팅을

위한 가설 수립에는 위협 인텔리전스 정보가 필요한데, 이 정보는 일반적으로 문서 형태로 배포되는 경우가 많다. 위협 인텔리전스 문서를 분석하면, 일반적인 사이버 위협의 증상과 발생 배경, 그리고 해당 위협이 발생한 원인 중 하나인 사이버 자산의 취약점 코드인 CVE(Common Vulnerabilities and Exposures) 등만 기술되어 있다. CERT팀과 같은 전문가라고 하더라도, 일반적인 위협 인텔리전스 문서만 보면 어떻게 위협 헌팅을 위한 초기 가설을 세울지 어려움을 겪을 수 있다. 그러나 unMaze의 위협 헌팅 기능은 위협 인텔리전스와 사이버 자산 정보를 융합하여 초기 가설을 수립하여 시각화하므로, 비전문가라고 하더라도 해당 위협에 대한 취약점을 가진 사이버 자산 정보를 쉽게 파악할 수 있는 장점을 가진다. Fig. 5의 위협 헌팅 적용 예시와 같이, unMaze는 국내외 보안 관련 업체에서 발간하는 위협 분석 정보 및 한국인터넷진흥원인 KISA의 C-TAS(Cyber Threat Analysis & Sharing System)와의 연동을 통해 위협 인텔리전스 문서를 자동으로 수집한다. 위협 인텔리전스 문서의 경우 악성코드나 랜섬웨어와 같이 해당 문서가 다루는 대표적인 위협 이슈가 주어지고, 사이버 위협에 사용된 취약점 코드인 CVE가 같이 공개되는 것이 일반적이므로, 특정 위협 인텔리전스 문서명과 CVE 코드, 그리고 그 CVE 코드값과 맵핑되는 사이버 자산 관련 취약점 코드인 CPE(Common Platform Enumeration)에 해당하는 사이버 자산 정보를 연관 분석하여, unMaze의 사이버 상황도를 통해 사용자에게 직관적으로 정보를 전달할 수 있다.

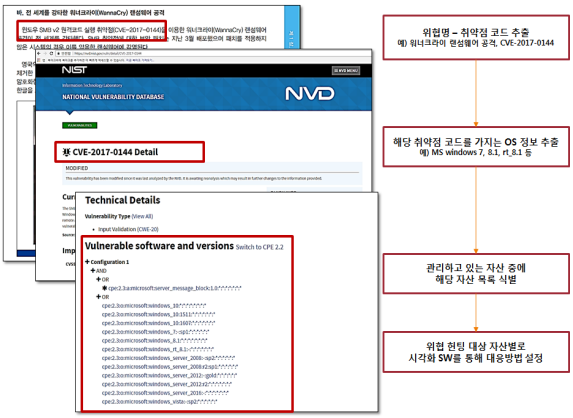

Fig. 5. Proposed threat hunting algorithm with threat intelligence

사이버 위협 관련 정보는 매우 방대한 양으로 매일 생성되고 있기 때문에, 설령 정보를 모두 수집한다 하더라도 어떻게 사용해야 하는지 모르는 상태에서 중요 정보를 식별하지 못하고 위협 분석 대상에서 누락시키는 경우가 많다. 그러나 unMaze는 위협 헌팅 초기 가설 수립을 위해 관리중인 자산과 연관되어 융합정보로 가공된 후 시각적 정보 전달까지 이뤄지기 때문에, 사용자가 위협 인텔리전스 정보를 단순히 정보만으로 획득하는 것이 아니라 관리중인 사이버 자산에 적용한 실질적인 위협 인텔리전스로 활용할 수 있다. unMaze를 활용하여 자산의 취약점을 찾아 잠재적 위협 요소로 식별하고 이에 대한 대응을 반복적으로 수행하면, 사이버 위협이 발생할 확률을 점차 낮추는 결과를 기대할 수 있다.

4.4 사이버 상황도 기능

사이버 상황도는 CSOC에서 지휘관의 상황인식 및 의사결정을 돕는 시각적 도구의 역할을 수행한다. 사이버 상황인식을 위한 프레임워크로 제안된 Cybaware는 시각화 기능의 목표를 '사이버 공간에서 발생하는 상황을 의미상으로 다양한 뷰로 생성하여 여러 디스플레이 플랫폼을 통해 시각화'하는 기능으로 정의했다[16]. unMaze의 시각화 상황도는 dashboard가 가지고 있는 함축적 정보 전달이 아닌 직관적인 정보 전달을 목적으로 개발하였다. unMaze는 Fig. 6과 같이 물리적 사이버 자산의 배치를 모델링하여, 사이버 위협 분야의 전문가 뿐 아니라 비전문가에게도 직관적으로 사이버 위협 정보를 전달한다.

unMaze의 사이버 상황도는 실시간 위협 상황, 위협 헌팅, 비인가 패킷 관리 등으로 메뉴를 분리하여 목적

Fig. 6. Implemented cyber COP of unMaze™ for cyber situation awareness

에 맞는 사용자 인터페이스를 제공한다. 실시간 위협 상황 도시 기능은 보안 장비를 통해 탐지된 위협을 도시하는 기능으로, 위협 분석 정보 중 필요한 정보만 요약하여 팝업창 형태로 제공한다. 보안장비에서 발생한 위협 정보 중에서 중요 정보만 추출하여 사용자에게 팝업창으로 알리되, 상세 정보를 확인할 수 있는 웹페이지 하이퍼링크 기능을 구현하였다. 위협 헌팅 도시 기능은 위협 인텔리전스 정보와 사이버 자산 정보를 융합하여, 자산의 취약점으로 인해 위협이 발생할 수 있는 잠재적 위협에 대한 정보를 전달하여, 사용자가 사전에 대응할 수 있도록 지원한다. 비인가 패킷 탐지 도시 기능은 화이트리스로 관리 중인 사이버 자산에 해당하지 않는 IP가 네트워크 내에서 유통되는 경우 위협 경보를 발생한다. 사이버 위협으로 식별되지 않더라도 인가되지 않은 패킷이 유통되는 것을 분석하여, 해당 비인가 트래픽으로 인해 사이버 위협이 발생하기 전에 사전에 대응할 수 있도록 지원한다. 사이버 상황도를 통해 사용자는 즉각적으로 위협 발생 여부를 파악하고, 이에 대한 대응을 수행할 수 있어 CSOC의 기능을 더욱 충실히 수행할 수 있게 된다.

5. unMaze 적용시 CSOC의 위협 헌팅 성숙도 향상

unMaze를 사용하여 CSOC을 운용하는 경우, Table 2와 같이 위협 헌팅 성숙도를 획득할 수 있다. 각 항목별 획득 가능한 단계 및 그 이유를 아래에 기술한다.

5.1 데이터 수집: 0단계 → 1단계

위협 헌팅 성숙도 중 데이터 수집 과정은 IT 환경

Table 2. Enhancement of threat hunting maturity level with unMaze™

위협 헌팅 수행 과정	위협 헌팅 성숙 단계별 만족 조건	unMaze 사용시 위협 헌팅 성숙 단계
데이터 수집	[위협헌팅 성숙도 1단계] • IT 환경 중 일부에서 몇 가지 종류의 데이터만 수집	• ElasticSearch를 이용해 발생되는 로그를 미가공 형태로 저장 • 빅데이터 수집 및 검색 솔루션의 기본적인 검색 기능 제공 • 보안장비에서 RestAPI를 통해 위협 탐지 로그 수집
가설 생성	[위협헌팅 성숙도 1단계] • SIEM, IDS, 방화벽 등 장비가 탐지한 alert에 의존 • 새로운 가설 생성을 위해 위협 인텔리전스 분석	• KISA C-TAS를 비롯해 외부의 위협 인텔리전스와 사이버 자산 정보 융합하여 잠재적 위협이 발생 가능한 자산에 대한 가설 생성
가설 검증 도구	[위협헌팅 성숙도 2~3단계] • full-text나 SQL-like query 등을 통해 SIEM이나 로그 분석기 활용 • 간단한 도구나 histogram을 활용하여 기존의 헌팅 프로시저를 기반으로 데이터를 분석함 • 시각화 도구 또는 그래프 분석을 활용함. 새로운 헌팅 프로시저를 개발함	• 수집한 데이터를 직관적 해석이 가능하도록 사이버 상황도 개발 • ElasticSearch의 kibana를 통해 SIEM이나 로그 분석기와 같은 텍스트 기반이나 SQL 기반 데이터 검색 가능
공격 탐지	[위협헌팅 성숙도 1단계] • SIEM/IDS 위협 경보에만 의존하거나 탐지 장비가 없음 • domain, URLs, hash값 등 PoP의 낮은 단계에 해당하는 IOC 식별	• hash 값이나 ip 정보, domain 명 등을 알 수 있도록 보안 장비를 연동
분석 자동화	[위협헌팅 성숙도 2단계] • 기본적으로 매칭되는 위협 인텔리전스 정보를 alert과 매핑시킴 • 효율적인 헌팅 프로시저 라이브러리를 생성하고 주기적으로 프로시저를 수행함	• KISA C-TAS 연동을 통해 주기적으로 위협 헌팅 가설을 생성 • 주기적인 위협 인텔레전스 업데이트에 따라 위협 헌팅 프로시저도 주기적으로 수행됨

중 일부 자산에서 몇 가지 데이터를 수집하는 기능을 수행하면 1단계로 정의했다. unMaze는 APT 솔루션 등 보안장비에서 발생되는 위협 탐지 정보를 RestAPI를 이용해 수집하고, 이를 미가공 데이터 형태로 저장하여 필요한 정보를 분석한다. unMaze는 ElasticSearch를 이용해 빅데이터 수집 및 기본적인 검색을 할 수 있고, 시각화 도구인 Kibana를 통해 dashboard 형태의 웹페이지를 제공하므로, unMaze는 1단계에 해당하는 데이터 수집을 수행한다고 해석 가능하다.

5.2 가설 생성: 0단계 → 1단계

새로운 위협 헌팅 가설을 생성하기 위해 위협 인텔리전스를 분석하는 단계가 위협 가설 생성의 1단계이다. unMaze는 KISA C-TAS 및 외부의 알려진 위협 인텔리전스 문서를 활용하여 위협 헌팅 프로세스를 수행하므로 1단계에 해당하며, 2단계의 기정의된 위협 인텔리전스 적용은 향후 개발 목표로 수행 예정이다.

5.3 가설 검증을 위한 도구 및 기술: 0단계 → 2단계

unMaze는 수집한 데이터를 histogram이나 graph가 아닌 직관적 해석이 가능한 형태로 가공하여 사이버 상황도로 표현하였으므로 가설 검증을 위한 도구 수준은 위협 헌팅 성숙도 2 또는 3단계로 해석할 수 있다. 웹페이지를 통해 수집한 데이터의 검색도 가능하고, dashboard 형태로 정제된 시각화 데이터도 제공한다.

5.4 패턴 및 TTP 탐지: 0단계 → 1단계

unMaze는 hash 값이나 IP 정보, domain 명 등을 알 수 있도록 보안 장비를 연동하므로 1단계에 해당한다. hash 값이나 IP 등은 PoP의 낮은 단계에 해당하는 패턴이나 알려진 시그니쳐에 속하는 IOC이므로, 향후 2단계나 3단계로 발전하기 위해서는 위협 인텔리전스를 분석하는 CERT 인력의 능력이 보완되어야 가능하므로, 이는 시스템적인 개발 요소보다는 CSOC의 운용으로 해결하는 것이 효율적이다.

5.5 분석 자동화: 0단계 → 2단계

unMaze는 KISA C-TAS 연동을 통해 주기적으로 위협 헌팅 가설을 생성하므로 2단계로 해석 가능하다. KISA C-TAS에서 주간 또는 월간으로 인텔리전스 문서가 발간되고, 이를 수신하면 연관 분석 및 사이버 상황도로로 경보를 생성하는 일련의 프로시저가 시스템적으로 개발되어 운용할 수 있다.

6. 결론 및 향후 연구 방향

사이버 해커 조직이 목적을 달성하기 위해 지속적으로 여러 기술을 사용하여 사이버 공격을 수행하는 집단을 APT 공격 집단이라고 하는데, 이들의 공격 대상은 군을 비롯해 금융, 일반적인 기업에 이르기까지 매우 광범위하다. 대부분의 CSOC은 위협이 발생한 후 보안장비를 통해 발생 결과를 탐지하는 post-active 한 통합보안관제 정책을 사용 중인데, 위협 발생 후 탐지하는 기존의 보안관제 패러다임으로는 지속적으로 진화하며 어떤 형태로 발생할지 모르는 APT 공격을 방어하기 부족하다. 위협 탐지와 더불어 pro-active 하게 위협을 헌팅하고 취약점 및 잠재적 위협을 제거하는 활동을 수행하는 위협 헌팅 기법을 반드시 적용해야 한다.

본 논문에서 제안하는 사이버 상황인식 시스템인 unMaze는 기존에 운영 중인 CSOC에 unMaze 시스템을 연동하여 위협 헌팅을 수행할 수 있도록 지원한다. unMaze는 보안 장비에서 발생하는 경보를 수집하여 데이터로 관리하고, 이를 시각화하여 직관적으로 사용자에게 정보를 전달하며, 위협 인텔리전스 문서에서 관리중인 자산과 정보 융합하여 어떤 자산이 잠재적인 위협을 가지고 있는지 분석한 후 선대응할 수 있도록 데이터를 제공한다. 사이버 자산 데이터를 관리하고 비인가된 네트워크 트래픽 정보 탐지시 이를 가공하여 사이버 상황도를 통해 사용자에게 직관적으로 제공한다. unMaze 적용시 CSOC의 위협 헌팅 성숙도를 초기단계인 0단계에서 최소한의 위협 헌팅을 수행하는 1단계 이상으로 향상시킬 수 있다.

향후 unMaze는 위협 헌팅 성숙도를 절차적인 2단계 이상으로 획득할 수 있도록 추가적인 기능을 구현할 예정이다. 실시간 사이버 상황인식 정보 수집 기능의 경우, 성능 저하 없이 수평적인 데이터 수집하고, 시간에 따라 IOC를 연관 분석하는 기능도 추가할 예정이다.

References

[1] Sqrrl Inc., “A Framework for Cyber Threat Hunting,” https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper-web.pdf, 2016.

[2] Carson Zimmerman, “Ten Strategies of a World-Class

Cybersecurity Operations Center," The MITRE Cooperation, pp. 8-9, p. 33, p. 45, 2014.
[3] KISA, "A Manual for CERT Management," https://www.kisa.or.kr/public/laws/laws3.jsp, p. 3, p. 72, 2010.
[4] George P. Tadda and John S. Salerno, "Overview of Cyber Situation Awareness," in Cyber Situation Awareness, Springer, pp. 15-35, 2010.
[5] David J. Bianco, "The Pyramid of Pain," http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html, 2014.
[6] The MITRE Corporation, Systems Engineering Guide, pp. 175-183, https://www.mitre.org/publications/all/systems-engineering-guide, 2013.
[7] The MITRE Corporation, Crown Jewels Analysis, http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis, 2013.
[8] Carbon Black Inc., "Eradicate Concealed Threats: Advanced Threat Hunting with Carbon Black," https://www.carbonblack.com/wp-content/uploads.2017/05/Cb_Threat_Hunting_Whitepaper_fin-1.pdf, 2017.
[9] Cybereason Inc., "Threat Hunting: Answering Am I Under Attack?," https://hi.cybereason.om/threat-hunting-answering-am-i-under-attack, 2017.
[10] Cybereason Inc., "Threat Hunting 2017 Survey Findings Report," https://hi.cybereason.com/2017-threat-hunting-report, 2017.
[11] Jaeyeon Lee, "A SW Framework Design for Defense Cyber Situation Awareness System," KIMST Autumn Conference Proceedings, pp. 567-568, 2017.
[12] Byeongjin Kim, "Opensource based Security Equipment and Asset Monitoring System," KIMST Annual Conference Proceedings, pp. 1367-1368, 2018.
[13] Dae-Won Hyun, "A Study on Intelligent Cyber Situation Awareness System for Cyber Attacks," KIMST Annual Conference Proceedings, pp. 1478-1479, 2018.
[14] Chris Fry and Martin Nystrom, "Security Monitoring," O'reilly, pp. 12-13, 2009.
[15] Bro Framework, https://www.bro.org/sphinx/intro/index.html.
[16] Richard A. Kemmerer, "Cybaware: A Cyber Awareness Framework for Attack Analysis, Prediction, and Visualization," In ARO/MURI Annual Review, 2014.