J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr


# 사이버 킬체인 기반 사이버 지휘통제체계 방어 및 공격 모델 연구

# A Study on Defense and Attack Model for Cyber Command Control System based Cyber Kill Chain

이 정 식[1] 조 성 영[1] 오 행 록[1] 한 명 묵[2*]
Jung-Sik Lee Sung-Young Cho Heang-Rok Oh Myung-Mook Han

## 요 약

사이버 킬체인 (Cyber Kill Chain)은 기존의 군사적 용어인 킬체인 (Kill Chain)에서 유래한다. 킬체인은 "파괴를 요구하는 군사 표적을 탐지하는 것에서 파괴하는 것까지의 연속적이고 순환적인 처리 과정 또는 그것을 몇 개의 구분된 행위로 나눈 것"을 의미한다. 킬체인은 핵무기나 미사일과 같이 위치가 변화하고 위험성이 커서 즉각적인 대응을 요구하는 시한성 긴급 표적을 효과적으로 다루기 위해 기존의 작전절차를 발전시켰으며, 방어자가 파괴를 필요로 하는 핵무기나 미사일이 타격점에 도달하기까지의 여러 과정 중 한 단계라도 제 기능을 발휘하지 못하게 하여 공격자가 의도한 목적을 달성하지 못하도록 무력화하는 군사적 개념에서 시작되었다고 볼 수 있다. 이러한 사이버 킬체인의 기본 개념은 사이버 공격자가 수행하는 공격은 각 단계로 구성되어 있으며, 사이버 공격자는 각 단계가 성공적으로 수행되어야 공격 목표를 달성할 수 있으며, 이를 방어 관점에서 보았을 때 각 단계에서 세부적으로 대응 절차를 마련하여 대응하면 공격의 체인 (chain)이 끊어지므로 공격자의 공격을 무력화하거나 지연시킬 수 있다고 본다. 또한 공격 관점에서 보았을 때 각 단계에서 구체적인 대응 절차를 마련하면 공격의 체인이 성공하여 공격대상을 무력화시킬수 있다. 사이버 지휘통제체계는 방어와 공격에 모두 적용되는 체계로 방어시 적의 킬체인을 무력화하기 위한 방어 대응 방안을 제시하여야 하며 공격시에는 적을 무력화하기 위한 각 단계별 구체적인 절차를 제시하여야 한다. 따라서 본 논문은 사이버 지휘통제체계의 방어 및 공격 관점의 사이버 킬체인 모델을 제안하였으며, 또한 방어 측면의 사이버 지휘통제체계의 위협 분류/분석/예측 프레임워크를 제시하였다.

☞ 주제어 : 사이버 지휘통제체계, 사이버 킬체인 모델, 방어 모델, 공격 모델, 위협 분류/분석/예측 프레임워크

## ABSTRACT

Cyber Kill Chain is derived from Kill chain of traditional military terms. Kill chain means "a continuous and cyclical process from detection to destruction of military targets requiring destruction, or dividing it into several distinct actions." The kill chain has evolved the existing operational procedures to effectively deal with time-limited emergency targets that require immediate response due to changes in location and increased risk, such as nuclear weapons and missiles. It began with the military concept of incapacitating the attacker's intended purpose by preventing it from functioning at any one stage of the process of reaching it. Thus the basic concept of the cyber kill chain is that the attack performed by a cyber attacker consists of each stage, and the cyber attacker can achieve the attack goal only when each stage is successfully performed, and from a defense point of view, each stage is detailed. It is believed that if a response procedure is prepared and responded, the chain of attacks is broken, and the attack of the attacker can be neutralized or delayed. Also, from the point of view of an attack, if a specific response procedure is prepared at each stage, the chain of attacks can be successful and the target of the attack can be neutralized. The cyber command and control system is a system that is applied to both defense and attack, and should present defensive countermeasures and offensive countermeasures to neutralize the enemy's kill chain during defense, and each step-by-step procedure to neutralize the enemy when attacking. Therefore, thist paper proposed a cyber kill chain model from the perspective of defense and attack of the cyber command and control system, and also researched and presented the threat classification/analysis/prediction framework of the cyber command and control system from the defense aspect

☞ keyword : Cyber Command Control System, Cyber Kill Chain Model, Defense Model, Attack Model, threat classification/analysis/prediction framework

[1] 2nd R&D Institute - 3rd Directorate, Agency for Defense Development., Seoul Songpa P.O Box 132, 05771, Korea.
[2] School of AI Software, GaChon University., 1342 Seongnamdaero Sujeong-gu Seongnam-si Gyeonggi-do, 13120, Korea.

* Corresponding author (mmhan@gachon.ac.kr)
[Received 16 November 2020, Reviewed 25 November 2020, Accepted 10 December 2020]

# 1. 서 론

사이버 킬체인 (Cyber Kill Chain)은 기존의 군사적 용어인 킬체인 (Kill Chain)에서 유래한다. 킬체인은 “파괴를 요구하는 군사 표적을 탐지하는 데부터 파괴하는 데까지의 연속적이고 순환적인 처리 과정 또는 그것을 몇 개의 구분된 행위로 나눈 것”을 의미한다. 킬체인은 핵무기나 미사일과 같이 위치가 변화하고 위험성이 커서 즉각적인 대응을 요구하는 시한성 긴급 표적을 효과적으로 다루기 위해 기존의 작전절차를 발전시켰다.

방어자가 파괴를 필요로 하는 핵무기나 미사일이 타격점에 도달하기까지의 여러 과정 중 한 단계라도 제 기능을 발휘하지 못하게 하여 공격자가 의도한 목적을 달성하지 못하도록 무력화하는 군사적 개념에서 시작되었다고 볼 수 있다. 내용 앞에서 APT 공격은 사이버 공격자가 특정 목표를 달성하기 위하여 특정 조직을 대상으로 지속적이고 지능적인 공격을 수행한다고 언급하였다. 이 과정에서 APT 공격의 공격자는 여러 단계에 걸쳐 은밀하고 지속적이며 데이터 중심의 공격을 수행한다.

사이버 킬체인의 기본 개념은 사이버 공격자가 수행하는 공격은 각 단계로 구성되어 있으며, 사이버 공격자는 각 단계가 성공적으로 수행되어야 공격 목표를 달성할 수 있으며, 이를 방어 관점에서 보았을 때 각 단계에서 세부적으로 대응 절차를 마련하여 대응하면 공격의 체인 (chain)이 끊어지므로 공격자의 공격을 무력화하거나 지연시킬 수 있다고 본다.

본 연구의 목적은 사이버 지휘통제체계의 개발 방향을 체계화 하기 위한 것으로 연구 아이디어는 우리 군의 사이버 지휘통제체계의 방어와 공격을 위한 사이버 킬체인 모델을 제안하고 이를 기반으로 한 방어 관점의 위협 분류체계를 제안하였다. 또한 본 연구는 우리군의 사이버 지휘통제체계 개발의 구체적인 방향과 구조의 체계화에 기여할 것으로 판단된다.

본 논문은 2장에서는 기존의 사이버 킬체인 모델에 대하여 소개하며, 3장에서는 본 논문이 제안하는 시스템 모델을 기술하였으며, 마지막 4장에는 결론을 기술하였다.

# 2. 사이버 킬체인 모델 소개

## 2.1 록히드 마틴 社의 사이버 킬체인 모델

록히드 마틴 社에서는, 사이버 공격은 일련의 과정을 거치며, 방어자가 공격 과정에서 한 단계만 차단해도 공격자가 다음 단계로 진행할 수 없다는 점에 착안하여, 사이버 공격의 절차와 방어 유형을 사이버 킬체인이라는 용어로 명명하고, 다음과 같이 정찰, 무기화, 유포, 악용, 설치, 명령 및 제어, 목적 달성의 7단계로 구성된 사이버 킬체인 모델을 제시하였다.

(표 1) 록히드 마틴 社의 사이버 킬체인 모델
(Table 1) Cyber KillChain Model of LockHeed Martin

| | | |
|---|---|---|
| 1단계 | 정찰 | 공격목표와 표적을 조사, 식별하고 선정 |
| 2단계 | 무기화 | 자동화도구 등을 이용해 공격을 위한 사이버 무기 준비 |
| 3단계 | 유포 | 표적 시스템에 사이버 무기를 전달 |
| 4단계 | 악용 | 사이버 무기의 작동 촉발 |
| 5단계 | 설치 | 표적 시스템에 악성 프로그램 설치 |
| 6단계 | 명령 및 제어 | 표적 시스템을 원격 조작하기 위한 채널 구축 |
| 7단계 | 목적 달성 | 소기의 목적 달성(정보수집, 시스템 파괴등) |

### 2.1.1 정찰 단계

정찰 단계는 공격자가 의도한 목적을 달성하기 위해 공격 대상을 탐색하고 식별 및 선정하는 단계로, 공격자는 표적과 관련된 정보를 수집하기 위해 네트워크를 통해 웹 사이트, 보도자료, 공고문, 공격 대상의 사회관계망 등 다양한 정보를 활용할 수 있다.

### 2.1.2 무기화 단계

무기화 단계에서 공격자는 정찰 단계를 통해 표적을 선정한 후, 표적을 공격하기 위한 사이버 무기를 준비하며, 이 과정에서 사이버 무기는 공격자가 직접 만들거나 공개된 자동화 도구를 이용해 쉽게 만들 수 있다.

### 2.1.3 유포 단계

유포 단계는 앞서 만들어진 사이버 무기를 표적으로 전달하는 단계로서, 록히드 마틴 社의 침해 대응팀의 분석에 따르면, 가장 빈번하게 사용된 전달 방법은 메일 첨부파일, 웹 사이트, USB인 것으로 나타났다.

### 2.1.4 익스플로잇(악용) 단계

악용 단계는 사이버 무기가 표적 시스템에 전달된 후 악성코드의 작동이 촉발되는 단계로서, 대부분은 시스템 및 네트워크 취약점을 이용해 이루어진다.

#### 2.1.5 설치 단계

설치 단계에서 공격자는 표적 시스템에 트로이목마, 백도어 등을 설치하여 일정 기간에 표적 시스템에서 활동할 수 있도록 환경을 조성한다.

#### 2.1.6 명령 및 제어 단계

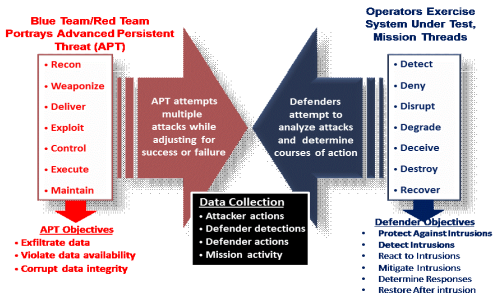
명령 및 제어 단계는 공격자가 외부에서 표적 시스템을 통제할 수 있도록 채널을 구축하는 단계로, 대부분의 APT 공격은 자동으로 수행되기보다 공격자와의 수동적 상호작용을 통해 공격이 이루어지는데, 채널이 구축되면 공격자는 표적 시스템에 자유롭게 접근할 수 있게 된다.

#### 2.1.7 목적 달성 단계

목적 달성 단계에서 공격자는 의도한 목적을 달성하며, 공격 목적은 내부자료 정찰, 민감한 정보 수집 및 유출, 데이터의 무결성 훼손, 시스템의 파괴 등 다양하다.

### 2.2 美 국방부의 사이버안보 킬체인 모델

美 국방부는 공격과 방어의 주요 활동과 목적 등을 기술한 사이버안보 킬체인을 제시하였다.* 여기서 록히드 마틴 社의 사이버 킬체인 모델의 7단계 중 설치 단계를 포함하고 있지 않았으며, 목적 달성 단계 이후 유지 단계를 추가하였다. 한편 방어자 대응 유형은 사이버 킬체인의 대응 유형과 동일하다. 그림 1은 킬 체인 분석 중에 수행 할 수 있는 활동 유형과 공격자 및 방어자의 목표 및 분석 중에 수집 할 수 있는 데이터 유형을 보여준다.



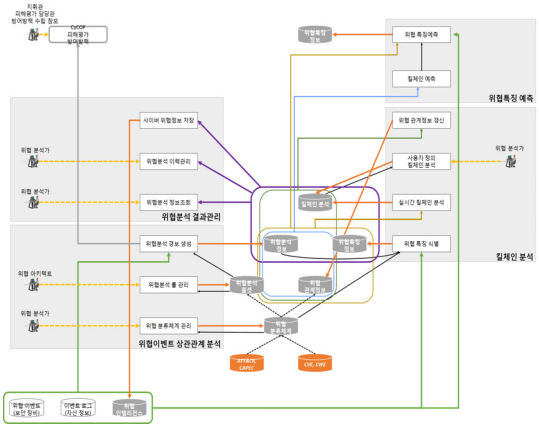

(그림 1) 美 국방부의 사이버안보 킬체인 모델
(Figure 1) Cyber KillChain Model of DoD

* 미 국방연구원 (Institute for Defense Analysis), 사이버안보 시험평가 가이드북, 2015.

## 3. 제안하는 시스템 모델

### 3.1 사이버 킬체인 모델 기반 사이버 지휘통제체계

사이버 킬체인 모델을 기반으로 한 사이버 지휘통제체계 실시간 의사결정지원의 방어를 위한 위협 분류체계, 위협 분석 및 위협예측 프레임워크는 그림 6과 같으며, 공격을 위한 프레임워크는 이슈사항으로 본 논문에서는 제외하고 공격 모델만을 제안하였다.




(그림 2) 사이버 킬체인 모델 기반 사이버 지휘통제체계
(Figure 2) Cyber Kill Chain Model based Cyber Command Control System

### 3.2 제안하는 사이버 킬체인 모델

기존의 사이버 킬체인 모델을 보완하고, 방어적 모델에서는 사이버 위협을 식별하는 방어 관점에서 공격자가 수행하는 공격 패턴을 사이버 킬체인이라는 공격자의 공격 모델을 방어 관점에서 수정하였으며, 공세적 모델에서는 공격 관점에서 허니팟 및 유인시스템을 활용한 공격 패턴을 기존 록히드 마틴 공세적 모델에서 수정하였다.

방어적 모델에서는 록히드 마틴 社의 사이버 킬체인 모델에서, 무기화 단계는 방어 관점에서 보이지 않는 단계(out-of-sight)이므로, 무기화 단계는 배제하였다.

공격자는 시스템의 취약점을 실제로 익스플로잇하고 침해 사후 도구(post-compromise tools) 또는 원격 접근 도구(remote access tools, RATs)와 추가적인 공격 도구를 설치하는 과정에서, 그 시간적 차이는 수 초에 그친다. 따

라서 록히드 마틴 社의 익스플로잇 단계와 설치 단계를 익스플로잇 단계에 통합하였다. 그러나 네트워크의 외부에 노출되어 있는 호스트 또는 서비스에 대한 익스플로잇 시도는 전달 단계로 간주된다. 또한 공격자는 침해한 호스트와 공격자의 인프라 간에 통신을 수행하면서(command and control communication), 공격자의 궁극적인 목표를 달성하기 위한 다양한 행동을 수행한다. 이러한 단계는 록히드 마틴 社의 모델을 기준으로 했을 때 설치 단계, 명령 제어 단계, 목표 달성 단계에 다양하게 분포되어 있다. 따라서 이러한 행동들은 명령 제어 단계에서 수행된다고 정의하였고, 이 단계에서는 침해한 호스트에 대한 제어를 수행하거나, 내부에서 침해 거점을 지속적으로 유지하기 위해 내부 확산(lateral movement)을 수행하거나, 최종 목표를 달성하기 위한 활동(예를 들어 데이터 또는 정보를 유출하기 위해 관련 호스트 또는 데이터의 정보를 발견(discovery)하거나 발견한 정보를 수집(collection)하는 활동)을 수행한다.

마지막으로, 목표 달성 단계에서는 기밀성, 가용성, 무결성 관점에서 공격자의 최종 목표를 달성하기 위한 궁극적 행동을 수행하는 것으로 좁혀 해석하였다. 따라서 사이버 지휘통제체계를 위한 방어 및 공격 관점에서 제안하는 사이버 킬체인 모델은 아래 그림과 같다.


(그림 3) 제안하는 C2시스템 방어적 및 공격적 관점모델
(Figure 3) Proposed C2System Defense and Attack perspective Model

### 3.2.1 방어 모델

#### 3.2.1.1 정찰단계

정찰 단계에서, 공격자는 공격 대상을 식별하고 선택하고, 이후 단계에서 사용할 공격 기술을 판단하기 위해 잠재적 대상 시스템 도는 네트워크에 대한 정보를 수집한다.

구체적으로는, 공격자는 잠재적 공격 대상에 대한 정보를 수집하기 위해 네트워크, 포트, 또는 서비스에 대한 스캐닝이나 풋프린팅(footprinting) 등과 같은 능동적 정찰 활동을 수행하거나, 소셜 네트워크 또는 웹사이트 검색과 같은 수동적 정찰 활동을 수행한다.

#### 3.2.1.2 정찰단계 전달 유포 단계

전달 유포 단계에서, 공격자는 이전의 정찰 단계에서 수집한 잠재적 공격 대상에 대한 정보를 활용하여, 공격 대상에 맞추어 제작되어 공격에 사용될 페이로드 또는 악성코드를 공격 대상 시스템 또는 네트워크에 전달하여 침투한다. 이 단계에서 공격자는 다음과 같은 공격을 수행할 수 있다.

- 공격자는 악성코드를 웹사이트(drive-by-download), 이메일(첨부파일, URL 링크, 또는 텍스트 내에 스크립트를 통하여), 또는 USB 메모리를 통해 유포할 수 있다.
- 공격자는 네트워크 바깥에 노출되어 있는 호스트와 서비스(웹 애플리케이션 등)에 침투를 시도한다. 이를 위해 사용할 수 있는 방법은 SQL 인젝션, 크로스 사이트 스크립팅(cross site scripting, XSS)을 이용할 수 있다.

#### 3.2.1.3 익스플로잇 단계

익스플로잇 단계에서, 전 단계인 전달 유포 단계에서 전달된 공격 페이로드 또는 악성코드가 실행되고, 공격자는 대상 시스템 또는 네트워크의 취약점을 익스플로잇한다. 그 결과 공격자는 공격 대상 시스템 또는 네트워크에 거점을 장악하게 된다. 이 과정에서 공격자는 침해 시스템에서 권한 상승을 수행하기도 한다.

관련 연구(Yadav et al. (2015))에서는 익스플로잇 대상 취약점을 크게 운영체제 수준, 네트워크 수준, 애플리케이션 또는 소프트웨어 수준으로 구분할 수 있다고 보았다.

- 운영체제 수준: 일반적으로 커널 또는 장비 드라이버를 대상으로 한다.
- 네트워크 수준: FTP, SMTP, NTP 또는 SSH와 같은

프로토콜을 대상으로 하거나, 라우터와 같은 네트워크 장비를 대상으로 한다.
- 애플리케이션/소프트웨어 수준: 호스트에 설치된 애플리케이션을 대상으로 한다. 애플리케이션에는 웹 브라우저(Internet Explorer, Firefox, Chrome), 문서 관련 프로그램(Microsoft Office, 한글, Adobe PDF), Java, Flash 등이 있다.

#### 3.2.1.4 명령 제어 단계

명령 제어 단계에서, 공격자는 전 단계인 익스플로잇 단계에서 장악한 호스트에서의 최종 목표를 달성하기 위한 다양한 행동을 수행한다.
- 공격자가 장악한 호스트와 공격자의 인프라 간 다양한 채널(포트 또는 프로토콜) 또는 미디어(유·무선 네트워크 또는 이동식 저장장치) 상에서 통신을 수행한다.
- 통신 수행 중에, 공격자는 충분한 사용자 권한을 얻기 위해 계정, 퍼미션(권한), 그룹 정책 등에 대해 새로 생성하거나 기존의 것을 수정한다.
- 내부 정찰을 통해 궁극적 공격 대상을 선택한다.
- 다음 목표 달성 단계에서 실제 유출한 정보 또는 데이터를 수집하기도 한다.

#### 3.2.1.5 목표 달성 단계

목표 달성 단계에서, 앞서 단계들을 성공적으로 달성한 공격자는 궁극적인 최종 목표를 달성하기 위한 행동을 수행한다. 구체적으로 기밀 데이터를 유출하거나(기밀성에 영향), 중요한 시스템 또는 데이터를 파괴 또는 수정하거나(무결성 또는 가용성에 영향), 또는 서비스 거부 공격(무결성에 영향)을 수행한다.

### 3.2.2 공격 모델 관점

#### 3.2.2.1 유인/기만/전달 단계

유인/기만/전달 단계에서, 공격대상자가 공격자의 시스템 또는 일반 사이트에 유인되고 일반적인 시스템으로 기만되어 자신의 정보를 유출하는 행동을 유발하도록 하며, 이를 통해 얻어진 정보는 무기화에 전달되어 공격대상자에 맞는 탐지회피 무기화 기반자료로 활용된다.

또한 무기화 이후 공격대상자의 반복적은 유인으로 무기(악성코드 etc)는 공격대상자에 전달되어 본 단계의 목표를 이루게 된다.

#### 3.2.2.2 무기화 단계

앞서 단계에서 취득한 공격대상자의 정보를 활용하여, 공격대상의 방어/탐지체계를 회피할 수 있는 무기를 생성하는 단계이며, 무기화는 다양한 형태로 구성될 수 있다.

#### 3.2.2.3 익스플로잇 단계

공격 모델의 익스플로잇 단계는 방어모델의 익스플로잇 단계와 동일하며, 본절에서는 설명을 생략한다.

#### 3.2.2.4 명령 제어 단계

공격 모델의 명령 제어 단계는 방어모델의 명령 제어 단계와 동일하며, 본 절에서는 설명을 생략한다.

#### 3.2.2.5 목표 달성 단계

공격 모델의 목표 달성 단계는 방어모델의 목표 달성 단계와 동일하며, 본절에서는 설명을 생략한다.

## 3.3 위협 분석 및 예측

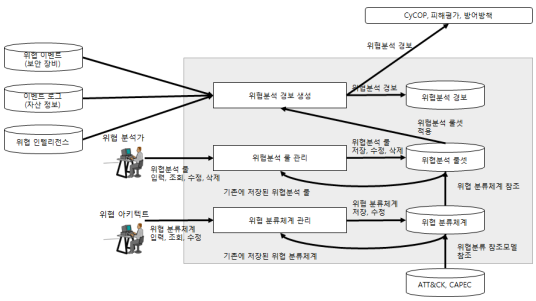
### 3.3.1 위협 분석

#### 3.3.1.1 룰셋 기반 위협 이벤트 상관분석

다양한 보안 센서에서 생성되는 위협 이벤트(events)는 각 보안 센서 관점에서 포함할 수 있는 저수준(low level) 정보를 포함하고 있으며, 한 공격 단계(single attack phase)에서 공격자가 수행하는 공격에 의해 발생되는 보안 이벤트의 수는 매우 많다. 또한 보안 센서의 설정이 완벽하지 않아 오탐(false positive) 또는 미탐(false negative)이 발생할 수 있다.

룰셋 기반 위협 이벤트 상관분석 기능에서는 위협 이벤트를 이용하여 위협을 분석하기 위한 룰셋(rule set)을 기반으로 SIEM에서 상관분석을 수행한다. 그 결과 보다 높은 수준(high level)의 정보를 포함하는 위협분석 경보(alerts)를 생성한다. 위협분석 경보는 크게 오프라인 상관분석 기능과 온라인 상관분석 기능에서 활용된다.

위협 분류체계는 MITRE 社의 ATT&CK과 CAPEC을 참고하고, 해당 공격 기술에 매핑되는 사이버 킬체인 공격 단계 - 공격 전술 - 공격 기술의 3계층으로 구성된다. 이는 SIEM에서 위협 이벤트 간 상관분석을 수행하기 위한 위협분석 룰셋을 구성하는 데 참고 모델로 활용된다.



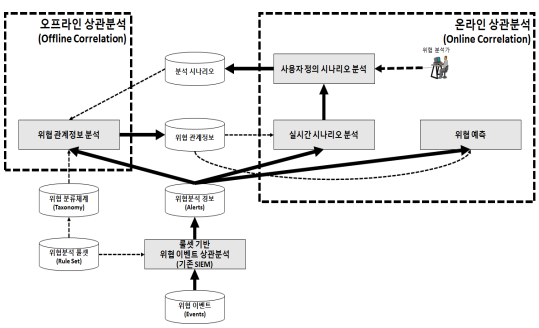

(그림 4) 룰셋 기반 위협 이벤트 상관분석의 기능 흐름
(Figure 4) Function Flow of rule set-based threat event correlation analysis

위협분석 룰 관리는 위협 분류체계를 참고모델로 하여 실제 위협 이벤트를 상관분석할 수 있는 위협분석 룰셋을 관리한다. MITRE CAR의 구조와 내용을 기반으로 체계적으로 위협분석을 위한 룰셋을 관리한다.

위협분석 경보 생성은 실제 룰셋(rule set)을 기반으로 SIEM에서 위협 이벤트 간에 상관분석을 수행하고, 그 결과로 위협분석 경보를 생성한다. 생성된 위협분석 경보는 데이터베이스에 저장되고, 위협분석 경보가 필요한 다른 기능에 전달된다.

### 3.3.1.2 킬체인 분석

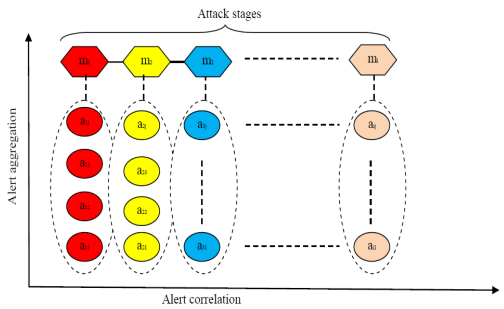
킬체인 분석은 룰셋 기반 위협 이벤트 상관분석에서 위협 이벤트 간 상관분석을 통해 생성된 위협분석 경보에 대해, 과거에 일어났을 것으로 가장 설득력 있는 위협 시나리오를 실시간으로 분석한다.




(그림 5) 킬체인 분석 및 위협 예측의 기능 흐름
(Figure 5) Function Flow of Kill Chain analysis and threat prediction

킬체인 분석과 룰셋 기반 위협 이벤트 상관분석은 다음과 같이 구분하여 설명할 수 있다.

- 룰셋 기반 위협 이벤트 상관분석은 사전에 정의된 룰셋에 의해 여러 위협 이벤트들(low-level data) 간의 상관분석을 수행하는 것으로 볼 수 있다. 즉 그림에서 세로축으로 여러 위협 이벤트(그림의 타원 모형) 간에 묶게 되는 “alert aggregation” 개념에 더 적합하다. 그 결과 하나의 공격 단계(attack stage)에 해당하는 위협 경보(그림의 육각형 모형)가 생성된다.
- 킬체인 분석은 위협 경보(high-level data) 간 상관분석을 수행하는 것으로 볼 수 있다. 즉 그림에서 가로 축으로 여러 위협 경보(그림의 육각형 모형) 간에 체인 형태로 연결되는 “alert correlation” 개념에 더 적합하다. 그 결과 여러 공격 단계(attack stages)로 구성된, 공격 체인(attack chain) 형태의 위협 시나리오가 생성된다.
-




(그림 6) 경보 상관분석의 두 가지 측면에 대한 개념적 설명
(Figure 6) Conceptual description of the two aspects of alert correlation analysis

#### 3.3.1.2.1 위협 관계정보 분석

위협 관계정보 분석 기능은 제안한 위협 분류체계를 이용하여 위협 관계정보를 분석하는 기능과, 위협분석 경보를 이용하여 위협 관계정보를 분석하는 기능을 포함한다. 여기서 위협 관계정보는 위협 분류체계에 포함된 위협 유형(type) 간의 시간적 관계(temporal relationship)와 인과관계(causal relationship)를 나타낸다. 위협 유형은 사이버 킬체인 모델의 각 공격 단계, 각 단계에 속한 공격 전술, 또는 각 공격 전술에 속한 공격 기술이 해당된다. 위협 관계정보는 아래와 같이 Alert Correlation Matrix와 같은 형태로 저장된다. 각각의 행과 열은 위협 유형을 나

타내며, 각 행은 선행되는 위협 유형, 각 열은 각 행에 후행되는 위협 유형을 표현한다.

| | $T_1$ | $T_2$ | ... | $T_j$ | ... | $T_m$ |
|---|---|---|---|---|---|---|
| $T_1$ | $Cor(T_1,T_1)$ | $Cor(T_1,T_2)$ | $Cor(T_1,...)$ | $Cor(T_1,T_j)$ | $Cor(T_1,...)$ | $Cor(T_1,T_m)$ |
| $T_2$ | $Cor(T_1,T_1)$ | $Cor(T_2,T_2)$ | $Cor(T_2,...)$ | $Cor(T_2,T_j)$ | $Cor(T_2,...)$ | $Cor(T_2,T_m)$ |
| ... | $Cor(...,T_1)$ | $Cor(...,T_2)$ | $Cor(...,...)$ | $Cor(...,T_1)$ | $Cor(...,...)$ | $Cor(T_1,T_m)$ |
| $T_i$ | $Cor(T_i,T_1)$ | $Cor(T_i,T_2)$ | $Cor(T_i,...)$ | $Cor(T_i,T_1)$ | $Cor(T_i,...)$ | $Cor(T_i,T_m)$ |
| ... | $Cor(...,T_1)$ | $Cor(...,T_2)$ | $Cor(...,...)$ | $Cor(...,T_j)$ | $Cor(...,...)$ | $Cor(...,T_m)$ |
| $T_m$ | $Cor(T_m,T_1)$ | $Cor(T_m,T_2)$ | $Cor(T_m,...)$ | $Cor(T_m,T_1)$ | $Cor(T_m,...)$ | $Cor(T_m,T_m)$ |

(그림 7) Alert Correlation Matrix
(Figure 7) Alert Correlation Matrix

사전 지식을 이용하여 위협 관계정보를 분석하는 기능은 전문가의 지식 또는 경험치에 의하여 위협 관계정보에 대해 사전에 구축하는 것을 말한다. 이는 시스템이 초기에 구축될 경우 위협 경보 데이터가 충분히 누적되지 않을 경우 사전 지식 기반 위협 관계정보를 이용하여 위협 시나리오를 분석하고 다음 위협을 예측하기 위한 것이다.

위협분석 경보를 이용하여 위협 관계정보를 분석하는 기능은 위협분석 경보를 기반으로 하여 룰셋 기반 위협 이벤트 상관분석 기능에서 생성된 위협분석 경보 데이터 간의 관계를 연관 분석하여 위협 관계정보를 모델링하는 것을 말한다. 가령, 특정 위협분석 경보 $a_i$와 $b_j$가 있을 때, 위협 유형 $A$와 $B$는 다음과 같이 나타낼 수 있다.

$$A = \{a_1, a_2, ..., a_i, ..., a_m\},\ 1 \leqq i \leqq m$$
$$B = \{b_1, b_2, ..., b_j, ..., b_n\},\ 1 \leqq j \leqq n$$

이 때 위협 유형 $A$와 $B$ 간 인과관계(시간적 관계는 이미 형성되어 있을 때)는 $A \rightarrow B$과 같이 표현될 수 있으며, $A$와 $B$의 인과관계 정도를 나타내는 상관 정도(correlativity)는 $Cor(A,B)$와 같이 표현될 수 있다.

전체 위협 유형 간 상관 정도는 위 그림의 경보 상관분석 매트릭스(alert correlation matrix, ACM)에 저장할 수 있다. 매트릭스의 대각선을 기준으로 대칭되는 두 값은 같지 않다. 즉 $a_1 \rightarrow a_2$에 대한 상관 정도인 $Cor(a_1,a_2)$와 $a_2 \rightarrow a_1$에 대한 상관 정도인 $Cor(a_2,a_1)$은 같지 않다.

위협 유형 간의 상관 정도를 구하기 위한 많은 연구들이 진행되어 왔다. 현재는 이 중에서 베이지안 네트워크(Bayesian network)를 기반으로 한 위협 관계정보 분석에 초점을 두고 있다.

위협 관계정보 분석 기능에서는 온라인 상관분석 기능을 통해 도출된 위협 시나리오를 입력 값으로 받아 위협 관계정보를 갱신한다. 위협 관계정보 분석 기능은 실시간으로 수집되는 위협분석 경보와 무관하게 주기적으로 동작하며(오프라인 분석), 수집되는 위협분석 경보의 양에 따라 주기가 조정될 수 있다.

#### 3.3.1.2.2 실시간 시나리오 분석

실시간 시나리오 분석은, 실시간으로 수집되는 위협 이벤트를 이용하여, 룰셋 기반 위협 이벤트 상관분석 기능에 의해 실시간으로 생성된 위협분석 경보 인스턴스에 대해, 위협 관계정보 분석에서 생성한 위협 관계정보 모델을 이용하여 위협 시나리오를 분석한다. (온라인 분석)

구체적으로 설명하면, 특정 위협분석 경보 인스턴스 $a_i$가 생성되었을 때, 해당 위협 유형 $A$와 관련된 위협 유형을 가지는 위협분석 경보 인스턴스 중 $a_i$의 특징과 비교하였을 때 임계치보다 높은 특징을 가지는 위협분석 경보 인스턴스를 선택한다. 이러한 과정을 해당되는 위협분석 경보 인스턴스가 더 이상 나오지 않을 때까지 반복한다.

#### 3.3.1.2.3 사용자 정의 시나리오 분석

실시간 시나리오 분석 기능에서 도출된 위협 시나리오 목록은 정확하지 않을 수 있다. 이러한 경우 사용자 정의 시나리오 분석 기능에서 위협 분석가의 개입을 통해 필터링할 수 있다. 또는 위협 분석가는 분석 결과가 가장 설득력 있는(plausible) 위협 시나리오라고 판단할 경우, 침해사고 분석 보고서를 생성하기 위해 시나리오에 제목, 설명 등과 같은 메타 정보를 작성하여 저장하게 된다.

### 3.3.1.3 위협 예측

위협 관계정보 분석을 통해 생성된 위협 관계정보 모델을 이용하여, 룰셋 기반 위협 이벤트 상관분석에 의해 실시간으로 생성된 위협분석 경보에 대해 다음 단계에 올

수 있는 가장 설득력 있는 위협 유형과 관련 속성을 예측한다. 이는 위의 그림과 같은 기능 흐름을 통해 수행된다.

구체적으로 설명하면, 특정 위협분석 경보 $a_i$가 생성되었을 때, 해당 위협 유형 $A$와 관련된 위협 유형 중 가장 높은 상관 정도를 가지는 위협 유형을 선택한다. 이는 경보 상관분석 매트릭스(ACM)을 이용하여, 특정 행(특정 위협분석 경보 $a_i$에 대한 위협 유형)에 대해 여러 위협 유형 중 가장 값이 높은 값을 선택하게 된다. 이는 ACM을 기준으로 했을 때, 킬체인 분석이 역방향 상관분석(backward correlation)인 것과 대조되어 정방향 상관분석(forward correlation)으로도 볼 수 있다.

만약 해당 위협 유형이 $C$라면 $C$와 관련된 이전 위협분석 경보$\{c_1, c_2, \ldots, c_p\}$들이 가지는 속성에 대한 통계 분석을 수행하여, 속성들에 대한 확률 분포를 나타내어 예측된 다음 위협이 가질 수 있는 속성 정보를 위협 분석가에게 전달한다. 이는 다가올 수 있는 다음 위협에 대한 사전적인 대응을 수행할 수 있도록 돕는다.

## 4. 결 론

본 논문에서는 우리 군의 사이버 지휘통제체계의 방어와 공격을 위한 사이버 킬체인 모델을 제안하고 이를 기반으로 한 방어 관점의 위협 분류체계를 제안하였다. 이를 위하여 기존의 다양한 사이버 킬체인 모델을 비교분석하고 그들이 가지는 한계를 살펴보았다. 또한 사이버 킬체인 모델에 적용하기 위한 알려진 사이버 위협 분류체계로 MITRE 社의 CAPEC과 ATT&CK을 이용하였으며 위협 분류체계를 정립하면서, 현재 발생하고 있는 사이버 위협은 사이버 킬체인 개념과 모델에 적용할 수 있음을 확인할 수 있었다. 또한 전문가의 지식에 전적으로 의존하지 않고 자동으로 사이버 위협 시나리오를 분석하고(킬체인 분석), 그 결과를 바탕으로 다음 위협 유형을 예측하는 시스템을 제안하였다. 이를 위하여 시나리오 분석 및 위협 예측을 위한 경보 상관분석 분야에 대한 관련 연구를 분석하였다. 관련 연구들은 대부분 전문가의 지식이 전적으로 요구되며, 실시간으로 수집되는 위협 경보에 대한 온라인 분석보다는 데이터베이스에 저장된 주어진 데이터에 대한 오프라인 분석에 초점을 두고 있다는 점에서 한계를 보인다. 제안 시스템에서는 기존의 전문가 지식을 보완하기 위해, 이미 생성된 위협 경보 데이터를 이용하여 베이지안 네트워크를 활용한 알고리즘으로 위협 관계정보를 구축하는 방안을 제안하였다.

위협 관계정보는 경보 상관분석 매트릭스(ACM)과 같은 지식베이스 형태로 구축되어 위협 시나리오를 분석하고 다음 위협을 예측하는 데 활용된다. 위협 관계정보는 앞에서 구축된 위협 분류체계에 속한 위협 유형(type)을 기준으로 위협 유형 간의 관계를 정량화한 수치로 표현된다. 이 때 위협 유형은 사이버 킬체인의 각 공격 단계, 각 단계에 속한 공격 전술(tactic), 또는 각 공격 전술에 속한 공격 기술(technique)이 될 수 있다.

제안한 사이버 킬체인 모델은 여전히 완전하지 못한 문제가 있다. 또한 사이버 킬체인 모델에 맞추어 알려진 공격 패턴 또는 공격 기법을 완전히 매핑하는 것은 어렵다. 실제 공격자는 각 공격 단계별 목적을 달성하기 위한 비용효과적인 방법을 사용하게 되며, 이 과정에서 비슷한 공격 기법이 여러 단계에서 사용된다.

본 논문에서 제안한 연구 수준은 시스템 및 각 구성요소를 식별한 수준이며 향후 각 구성요소, 구체적으로는 위협 관계정보 분석 기능에서 실제로 위협 관계정보를 생성하고 업데이트하기 위한 알고리즘, 위협 관계정보를 이용하여 실시간으로 수집되는 위협 경보에 대해서 위협 시나리오를 분석하고 다음 위협 단계를 예측하기 위해 필요한 구체적인 알고리즘에 대한 연구를 진행할 예정이다. 이러한 알고리즘을 연구하고 검증하기 위한 데이터셋을 개발하기 위해, 현재 군에서 운용하고 있는 네트워크 환경을 모의한 테스트베드를 구축하고, MITRE ATT&CK을 반영한 모의침투 시나리오를 설계하고 수행하여 각 보안 센서에서 위협 경보를 생성하고자 한다. 또한 데이터셋을 통하여 알고리즘을 평가하는 지표를 결정하여 개발하고자 하는 시스템이 얼마나 잘 분석하는지를 평가할 필요가 있다.

따라서 향후 연구에서는 사이버 킬체인 모델을 보다 정교화하고, 사이버 킬체인 모델을 구성하는 각 공격 단계에 대한 전체적인 공격 기술을 (재)분류하고, 이에 대한 대응 방안이 사전에 마련된 프레임워크를 정립할 필요가 있으며, 이를 우리 군의 사이버 지휘통제체계 의사결정지원에도 반영함으로써 보다 체계화된 사이버 작전을 수행할 수 있을 것으로 기대한다.

## 참고문헌(Reference)

[1] Sung-young Cho, Insung Han, YoungSyup Shin, DongJea Lee, ChangWan Lim, Haengrok Oh, "Automation Method ofcyber threat scenario analysis and prediction", CISC-S , pp.564-569, 2018.

[2] Sung-young Cho, Insung Han, Hyunsook Jeong, Sungmo Koo, Moosung Park, "Killchain model and cyber threat classification for cyber situational awareness", CISC-S , pp.149-153, 2017.
[3] Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh and Moosung Park, "Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture", Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2018), 2018 International Conference on. IEEE, pp 1-8. 2018. https://doi.org/10.1109/CyberSA.2018.8551383
[4] Bryan Harris, Eli Konikoff, and Phillip Petersen, "Breaking the DDoS attack chain", Institute for Software Research, 2013.
[5] Dongho Kang and Jungchan Na, "A rule based event correlation approach for physical and logical security convergence", IJCSNS, 12(1), pp.28, 2012. http://paper.ijcsns.org/07_book/201201/20120104.pdf
[6] Bin Zhu and Ali A. Ghorbani, "Alert correlation for extracting attack strategies", IJ Network Security, vol.3, no.3, pp.244-258, 2006. http://ijns.jalaxy.com.tw/contents/ijns-v3-n3/ijns-2006-v3-n3-p244-258.pdf
[7] Tarun Yadav and Arvind Mallari Rao, "Technical aspects of cyber kill chain", International Symposium on Security in Computing and Communication, pp.438-452, Springer, 2015. https://arxiv.org/pdf/1606.03184.pdf
[8] MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), https://attack.mitre.org/wiki/Main_Page
[9] Ali Ahmadian Ramaki and Abbas Rasoolzadegan, "Causal knowledge analysis for detecting and modeling multi-step attacks", Security and Communication Networks, 9(18), pp.6042-6065, Wiley Online Library, 2016. https://doi.org/10.1002/sec.1756|
[10] Chih-Hung Wang and Ye-Chen Chiou, "Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights", International Journal of Computer and Communication Engineering, 5(1), pp.1, IACSIT Press, 2016. https://doi.org/10.17706/IJCCE.2016.5.1.1-10

## ◐ 저 자 소 개 ◑

**이 정 식(Jung-Sik Lee)**
1994년 서울과학기술대학교 전자계산학과(공학사)
1996년 숭실대학교 대학원 전자계산학과(공학석사)
1996년~현재 국방과학연구소 연구원
관심분야 : 사이버 지휘통제체계, 사이버 킬체인, 공격 그래프 etc.
E-mail : godsider@add.re.kr

**조 성 영(Sung-Young Cho)**
2009년 한국과학기술원 정보통신공학과(공학사)
2013년 한국과학기술원 정보보호대학원(공학석사)
2013년~현재 국방과학연구소 연구원
관심분야 : 사이버 상황인식, 사이버 킬체인, 사이버 공격 캠페인 etc.
E-mail : sycho@add.re.kr

## ◐ 저 자 소 개 ◑

**오 행 록(Haeng-rok Oh)**
1987년 인하대학교 전산학과(공학사)
1989년 인하대학교 전산학과 석사(공학석사)
2004년 고려대학교 컴퓨터학과 박사 수료
1990년~현재 국방과학연구소 연구원
관심분야 : 사이버 지휘통제체계, 사이버 킬체인, 사이버전 etc.
E-mail : haengrok@add.re.kr

**한 명 묵(Myung-Mook Han)**
1980년 연세대학교 공과대학(공학사)
1987년 뉴욕공과대학교 대학원 컴퓨터공학과(공학석사)
1997년 오사카시립대학교 대학원 정보공학부(이학박사)
1998년~2018년 가천대학교 컴퓨터공학과 교수
2018년~현재 가천대학교 소프트웨어학과 교수
관심분야 : XAI, 공격자 식별, 정보보호, 알고리즘, 데이터 마이닝, 기계 학습
E-mail : mmhan@gachon.ac.kr