MITRE ATT&CK-D3FEND 지식 그래프 기반의 위협 대응 우선순위 모델

한희수*, 최상훈[1], 박기웅†

세종대학교 Syscore Lab. (학부생, 연구교수[1])
**세종대학교 정보보호학과 (교수†)

A Framework for Optimizing Threat Response Priority using the MITRE ATT&CK and D3FEND Knowledge Graph

Hui-Su Han*, Sang-Hoon Choi[1], Ki-Woong Park†

* SysCore Lab., Sejong University
**Dept. of Computer and Information Security, Sejong U† niversity
(Ungraduate student*, Research Professor[1], Professor†)

요 약

MITRE ATT&CK과 D3FEND 프레임워크의 등장은 사이버 보안 지식의 표준화와 체계화를 촉진하며, 위협 인텔리전스 분석의 공통 언어를 정립한 중요한 전환점을 마련하였다. 그러나 실제 침해 사고 대응 과정에서는 다양한 방어 기술 중 어떤 기술을 우선 적용해야 하는지에 대한 정량적 근거가 부족하다는 한계가 존재한다. 본 논문은 이러한 문제를 해결하기 위해, 방어 기술의 우선순위를 동적으로 산출하는 모델을 제안한다. 우리가 제안한 모델은 기존의 정적인 지식 구조를 데이터 기반의 동적 의사결정 체계로 전환하고, 제한된 보안 자원 내에서 가장 효율적인 방어 활동의 우선순위를 도출하는 데 활용될 수 있다.

I. 서론

MITRE ATT&CK과 D3FEND 프레임워크는 사이버 보안 지식의 표준화와 체계화에 중요한 전환점을 마련했다. [1, 2] ATT&CK은 공격자의 TTPs(전술, 기술, 절차)를, D3FEND는 방어자의 기술 체계를 제공하며 사이버 공격 및 방어 연구의 핵심 기반으로 자리 잡았다.

그러나 두 프레임워크 간의 정량적 연결성이 부족하여, ATT&CK을 통해 위협을 식별하더라도 D3FEND가 제시하는 다수의 방어 기술 중 어떤 것을 우선 적용해야 하는지에 대한 객관적 근거가 부족하다. 이는 풍부한 지식에도 불구하고 실질적인 방어 의사결정을 저해하는 한계로 작용한다.

본 논문은 이러한 한계를 해결하기 위해 MITRE ATT&CK과 D3FEND 간의 연관성을 정량적으로 분석하는 MAD(MITRE ATT&CK - D3FEND) 모델을 제안한다. 본 모델은 단순히 두 프레임워크를 연결하는 것을 넘어, 객관적인 지표를 활용해 방어 기술의 전략적 가치를 평가하고 실질적인 방어 활동의 '우선순위'를 도출한다. 우리가 제안한 모델은 정적 지식을 데이터 기반의 동적 의사결정 근거로 전환하여, 제한된 자원 내에서 효율적인 방어 전략 수립 및 자원 배분을 지원한다.

II. 관련연구

2.1 MITRE ATT&CK 및 D3FEND

MITRE ATT&CK은 실제 관측된 공격 사례를 기반으로 공격자의 행동을 체계적으로 정리한 지식 베이스이다. ATT&CK은 공격 라이프

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 논문은 과학기술정보통신부의 재원으로 실감콘텐츠핵심기술개발 (Project No. RS-2023-00228996, 40%), 한국연구재단(NRF) 중견후속 연구사업(Project No. RS-2023-00208460, 30%), 한국콘텐츠진흥원(KOCCA) 저작권기술 글로벌 인재 양성사업 (Project No. RS-2025-02221620, 30%)의 지원을 받아 수행된 연구임.

사이클에 따른 전술과 개별 기술을 상세히 분류하여, 특정 위협 그룹의 행동을 표준화된 방식으로 모델링하는 데 활용된다.

MITRE D3FEND는 사이버 보안 방어 기술과 역량을 지식 그래프 형태로 구조화한 프레임워크이다. D3FEND의 핵심 개념은 공격자가 활동 과정에서 필연적으로 생성하거나 조작하는 '디지털 아티팩트'이다. 결과적으로 D3FEND는 디지털 아티팩트를 매개로, 특정 공격 기술(ATT&CK)이 어떤 방어 기술(D3FEND)과 인과적으로 연결되는지에 대한 의미론적 관계를 정립한다.

2.2 기존 CTI 모델의 한계점

CTI(Cyber Threat Intelligence)란 공격자의 TTPs를 분석하여 도출된, 공격의 맥락, 메커니즘, 영향 등을 포함한 증거 기반 지식으로 정의된다. CTI의 핵심 가치는 위협에 대한 조직의 대응을 결정하는 데 사용할 수 있는 '실행 가능성'을 확보하는 데 있다. [3]

진정한 실행 가능성을 확보하기 위해서는, 분석된 위협 정보를 바탕으로 어떤 방어 조치를 선행해야 하는지에 대한 합리적인 기준, 즉 '우선순위'를 제시할 수 있어야 한다.

대표적인 CTI 프레임워크인 사이버 킬 체인(Cyber Kill Chain)과 다이아몬드 모델(Diamond Model)은 공격자의 활동 단계를 식별하고 개별 이벤트를 분석하는 데는 효과적이다. 그러나 다수의 위협에 직면한 조직이 어떤 방어 활동에 제한된 자원을 집중해야 하는지에 대한 구체적인 정량적 지침을 제공하는 데는 한계가 있다. [4] 이러한 한계를 극복하고, 방어 전략의 우선순위를 제시하여 실행 가능성을 확보하는 새로운 CTI 모델이 요구된다.

III. 우선순위 기반 동적 CTI 모델

본 논문에서는 CTI가 제공하는 방대한 위협 정보 속에서 실제 방어 조치의 우선순위를 결정하기 어려운 한계점을 해결하기 위해 우선순위 기반 동적 CTI 모델 MAD를 제안한다.

3.1 전략적 가치 평가를 위한 MAD 모델

D3FEND는 아티팩트를 기반으로 공격과 방어 기술 간의 정적인 관계 매트릭스를 제공한다는 점에서 중요한 기반을 마련한다. 그러나 이는 단순히 가능한 모든 연결성을 나열한 것으로, 특정 위협 행위자나 공격 캠페인에 직면한 조직이 어떤 방어 기술을 우선적으로 적용해야 하는지에 대한 동적인 의사결정 기준을 제시하지 못한다. 이러한 정보의 부재는 CTI의 핵심 목적인 '실행 가능성'을 저해하는 요인으로 작용한다.

MAD 모델은 이러한 한계를 극복하기 위해 D3FEND의 정적 관계에 'TTP 사용 빈도'와 'TTP 영향도'라는 두 가지 핵심 지표를 정량적으로 평가하여 결합한다. 이를 통해 방어 전략의 우선순위를 동적으로 도출함으로써, 정적 정보의 한계를 넘어 CTI의 핵심 가치인 '실행 가능성'을 확보한다. [5]

3.2 우선순위 계산 방법

MAD 모델의 우선순위는 각 방어 기술이 특정 위협 행위자 프로파일로부터 얼마나 많은 위험을 완화할 수 있는지를 정량적으로 평가하여 산출한다.

우선순위 점수 계산에 사용되는 각 지표는 객관적인 데이터 소스를 기반으로 정의한다. TTP 사용 빈도(F)는 특정 공격 기술이 실제 공격 환경에서 얼마나 널리 사용되는지를 나타내는 지표로, MITRE ATT&CK 웹사이트에 등재된 해당 기술의 사용 위협 그룹 및 소프트웨어의 총 개수를 집계하여 산정한다. 이는 기술의 보편성과 실제 위협도를 반영하는 객관적 지표로 활용된다.

TTP 영향도(I)는 해당 TTP 성공 시 미치는 잠재적 피해 심각도를 의미한다. 객관적인 평가를 위해 [표 1]과 같이 MITRE ATT&CK의 14개 전술을 공격 라이프사이클 단계에 따라 5개 등급으로 분류하고, 1점에서 5점까지 차등 점수를 부여한다.

[표 1] 공격 전술별 영향도 점수

영향도 점수	영향도 등급	ATT&CK 전술
5점	치명적	Impact
4점	높음	Credential Access, Exfiltration, Command and Control
3점	중간	Persistence, Privilege Escalation, Lateral Movement, Collection
2점	낮음	Execution, Defense Evasion, Initial Access
1점	매우 낮음	Reconnaissance, Resource Development, Discovery

산출 공식은 2단계로, 먼저 개별 TTP의 위험도(Risk)를 '사용 빈도(F)'와 '영향도(I)'의 곱으로 계산한다.

$$Risk = F(TTP_i) \times I(TTP_i)$$

이후, 특정 방어 기술이 대응하는 총 n개의 TTP 위험도를 모두 합산하여 최종 우선순위 점수를 산출한다.

$$\mathrm{Pr}iority = \sum_{i=1}^{n} Risk_i = \sum_{i=1}^{n} [F(TTP_i) \times I(TTP_i)]$$

3.3 적용 예시: 'One-time Password' 방어 기술

제안하는 모델의 적용 예시로, D3FEND의 'Password' 아티팩트와 관련된 방어 기술 '일회용 비밀번호(One-time Password)'를 분석한다. 이 기술의 우선순위를 계산하기 위해, '일회용 비밀번호'와 연관된 공격 기술 중 'Access Token Manipulation: Token Impersonation/Theft (T1134.001)'를 예시로 사용한다.

MITRE ATT&CK에 따르면, 이 기술(T1134.001)은 17개의 위협 그룹 및 소프트웨어에서 사용되므로 사용 빈도(F)는 17이다. 또한, Privilege Escalation 전술에 속하므로 [표 1]의 기준에 따라 영향도(I)는 3점이다. 따라서 해당 TTP의 위험도는 17 x 3 = 51점으로 계산된다.

최종적으로, 'One-time Password'와 관련된 모든 TTP에 대해 이 계산을 반복하여 각 위험도를 합산하면, 해당 방어 기술의 최종 우선순위 점수가 도출된다. 이 점수는 다른 방어 기술들과 비교하여 방어 전략 수립의 근거로 활용된다.

IV. 결론

본 논문은 CTI의 '실행 가능성'을 높이고자, 'TTP 사용 빈도'와 'TTP 영향도' 지표를 활용해 MITRE ATT&CK과 D3FEND 프레임워크를 정량적으로 연계하고 방어 우선순위를 도출하는 MAD 모델을 제안했다.

제안한 모델은 정적 데이터를 실질적인 방어 활동을 위한 동적 의사결정 근거로 전환하여, 데이터 기반의 효율적인 자원 배분을 지원한다는 점에서 의의가 있다. 향후 연구에서는 조직별 자산 중요도와 같은 내부 데이터를 반영하여 모델을 고도화하는 연구를 수행할 예정이다.

[참고문헌]

[1] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G. and Thomas, C. B., MITRE ATT&CK®: Design and Philosophy, The MITRE Corporation, March, 2020.

[2] Kolodenker, M., Spaulding, K. E. and Rios, R. A. M., From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity, Journal of Maritime Research

[3] M.S.Abu, S.R.Selamat, A.Ariffin and R.Yusof, Cyber Threat Intelligence – Issue and Challenges, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 10, No. 1, April, 2018.

[4] Odarchenko, R., Pinchuk, A., Polihenko, O. and Skurativskyi, A., A comparative analysis of cyber threat intelligence models, 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020.

[5] Manocha, H., Srivastava, A., Verma, C., Gupta, R. and Bansal, B., Security Assessment Rating Framework for Enterprises using MITRE ATT&CK® Matrix, SN Computer Science, Vol. 2, No. 393, August, 2021.