Headline

위협 중심 보안 전략의 핵심 도구: Rule Framework

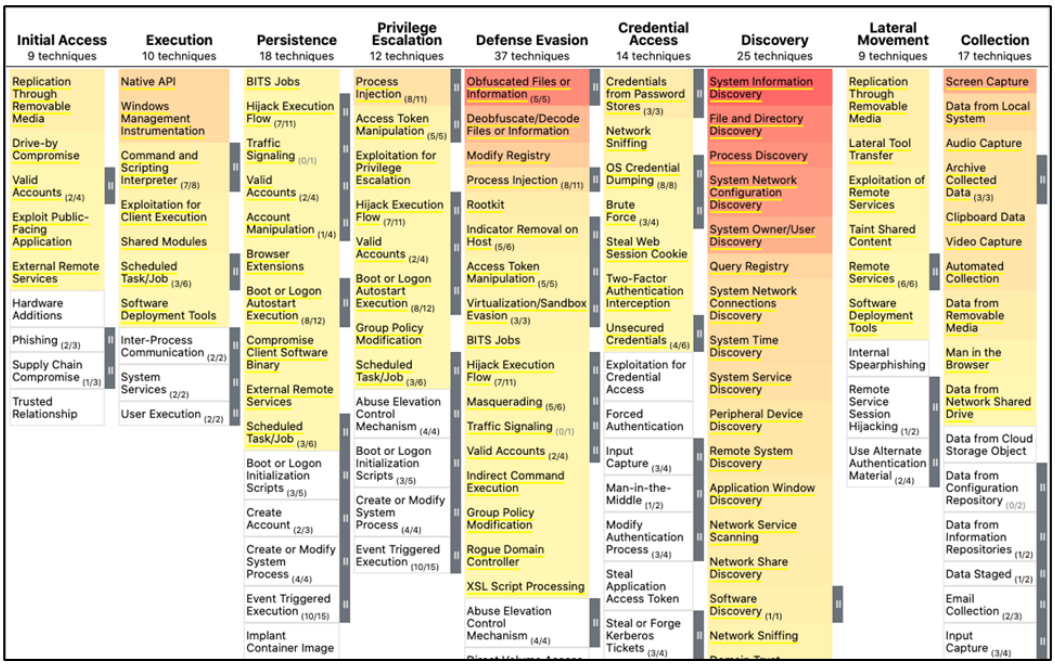
MSS 사업그룹 관제 CERT 팀 서기택 팀장

■ 지능형 위협의 시대

사이버 보안은 이제 단순한 IT 이슈가 아니라 조직의 생존과 직결된 전략적 과제가 되었다. 특히 지능형 지속 위협(APT : Advanced Persistent Threat), 공급망 공격, 랜섬웨어(Ransomware)와 같은 고도화 된 공격은 전 세계의 주요 기업과 공공 기관을 위협하고 있다. 이에 따라 보안 패러다임은 전통적인 예방 중심의 모델에서 위협 탐지 및 대응 중심으로 정보보안을 위한 전략적 이동이 이루어지고 있다. 이 변화의 중심에 탐지룰(Detection Rule-Set) 또는 방법론의 고도화가 큰 비중을 차지하고 있으며, 대표적인 보안 전략 모델로 MITRE ATT&CK 프레임워크가 존재한다. ATT&CK 프레임워크는 공격자의 실제 행위를 기반으로 구성된 지식 베이스로 위협 중심 보안 전략을 효과적으로 수립할 수 있는 기반을 제공한다.

■ MITRE ATT&CK 프레임워크란 무엇인가?

MITRE ATT&CK 는 Adversarial Tactics, Techniques and Common Knowledge 의 약자로 공격자들이 실제로 사용하는 전술(Tactics), 기술(Techniques), 절차(Procedures)을 체계적으로 분류한 지식 기반 매트릭스이다.



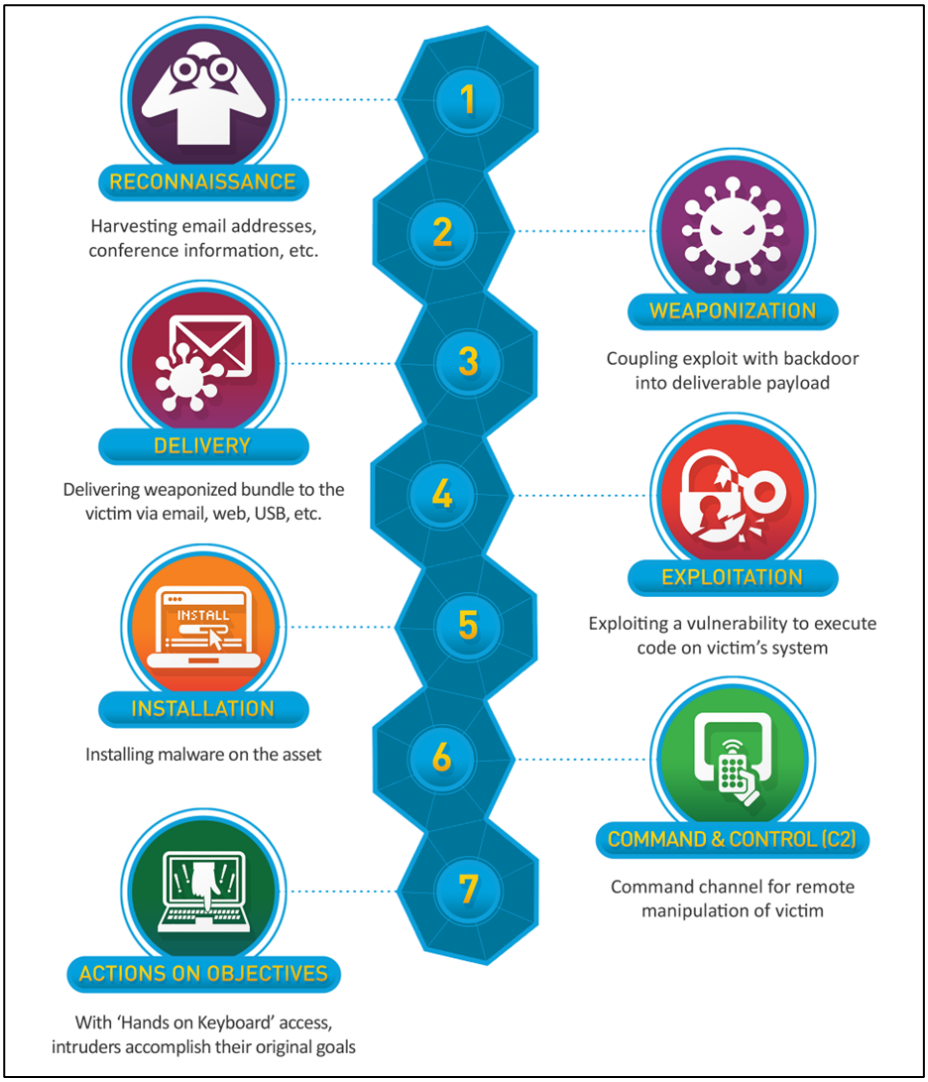
* 출처: MITRE ATT&CK 공식 홈페이지

그림 1. MITRE ATT&CK Metrix - Navigator 중 일부 발췌

공격은 일반적으로 일련의 단계적 행위를 기반으로 진행되며 각 단계는 특정한 전술과 기술로 구분된다. 예를 들어, 공격자는 먼저 초기 접근을 시도하고 그 다음 권한 상승, 내부 정찰, 명령 및 제어(C2), 데이터 유출 등의 단계를 거친다. MITRE ATT&CK 프레임워크는 이러한 각 단계에 따라 공격을 분류하고 기술에 대한 상세 설명과 탐지 지표, 완화 전략 등을 제공한다. 현재 Enterprise, Mobile, ICS 세 가지의 매트릭스를 제공하며 기업 보안, 산업 제어 시스템 보안, 모바일 보안 등 다양한 환경에 적용이 가능하다.

■ MITRE ATT&CK 프레임워크 전술과 기술(TTPs)의 구성

MITRE ATT&CK 프레임워크의 핵심은 공격자의 행동을 단계적으로 모델링한 전술(Tactics)과 그 단계에서 사용되는 구체적인 기술(Techniques)로 구성되어 있다는 점이다. 이 프레임워크는 공격자가 사이버 공격을 수행할 때, 어떤 목표를 가지고 어떤 방식으로 접근하는지를 설명하며 이를 통해 조직은 실제 위협 시나리오를 구조적으로 분석할 수 있다.



* 출처: Lockheed Martin 공식 페이지

그림 2. Lockheed Martin 에서 공개한 Cyber Kill Chain 모델

위 [그림 2]와 같이 사이버 위협 행위는 단계적으로 진행된다. 각 단계에 대해 조금 더 자세히 살펴보면, 가장 먼저 공격자는 시스템에 접근하기 위한 '초기 접근(Initial Access)' 단계를 시도한다. 이는 피싱 이메일, 악성 링크, 알려진 사용자 권한 등 사용자의 행위나 외부 접점의 취약점을 노리는 방식으로 나타난다. 이 단계의 목적은 내부 네트워크로 진입할 수 있는 발판을 마련하는 것이다. 다음은 '실행(Execution)' 단계로 공격자가 진입한 후 악성 코드를 실행하여 시스템 제어권을 확보하려는 시도이다. 여기에는 스크립트 실행, 명령어 삽입, 프로세스에 대한 오용 등이 포함된다. 이 과정은 시스템 내에서 공격자가 실제로 악성 행위 등을 동작하도록 만드는 관문이다.

'지속성(Persistence)'은 공격자가 시스템에 장기적으로 머물기 위해 설정하는 메커니즘을 의미한다. 시스템 재부팅이나 사용자 로그아웃 이후에도 공격 코드가 계속 작동할 수 있도록 서비스 등록이나 자동 실행 프로그램 설치 등의 방법이 사용된다. 다음 단계로는 '권한 상승(Privilege Escalation)'으로 정의되며 일반 사용자 권한을 관리자 또는 루트 권한으로 상승시켜 더 넓은 범위의 시스템 접근을 가능하게 만든다. 이후 '방어 회피(Defense Evasion)' 단계에서는 보안 솔루션이나 로그 시스템 등을 우회하거나 무력화시키는 기술이 사용된다. 예를 들어, 악성 파일을 난독화 한다거나 백신 우회를 위한 코드 인젝션 등의 기술이 여기에 해당된다. 이는 탐지를 피하고 지속적인 공격을 가능하게 만드는 중요한 단계이다. '자격 증명(Credential Access)' 단계에서는 공격자가 시스템 내에서 사용자 ID 나 비밀번호를 수집하여 다른 시스템으로 이동하거나 권한을 획득하려고 한다. 이는 메모리에서 비밀번호 해시를 추출하거나 키로거 등을 설치하여 수행된다. '발견(Discovery)' 단계는 내부 네트워크의 구조, 사용자 목록, 시스템 정보 등을 파악하는 과정이다. 공격자는 이 정보를 활용해 다음 공격 단계를 계획하거나 측면 이동(Lateral Movement)의 경로를 설정한다.

악성 행위가 본격적으로 확산되는 단계가 '측면 이동(Lateral Movement)' 단계이다. 이는 공격자가 하나의 시스템에서 다른 시스템으로 이동하는 행위로 자격 증명 도용이나 원격 명령어 실행 등이 주요 수단으로 사용된다. 이 과정을 통해 공격자는 핵심 시스템에 점차 접근하게 된다. 공격의 목적이 구체화되면, '수집(Collection)' 단계가 시작된다. 이때 공격자는 특정 데이터 예컨대 문서, 고객 정보, 인증서, 로그 파일 등을 수집하여 향후 유출이나 조작을 위해 저장한다. 수집된 정보를 외부로 보내는 과정이 '명령 및 제어(Command and Control, C2)' 단계다. 공격자는 악성 소프트웨어를 통해 외부 C2 서버와 연결하고 명령을 주고받거나 데이터를 전송한다. 보통 암호화 된 통신이나 정식 프로토콜을 위장한 전송 방식이 사용된다.

공격의 최종 단계는 '영향(Impact)'으로 이는 시스템의 가용성 저해, 데이터 훼손, 랜섬웨어 감염 등 실제 피해를 일으키는 부분이다. 공격자는 이 시점에 데이터 삭제, 시스템 파괴, 금전 요구 등의 목적을 달성하려 한다.

이처럼 MITRE ATT&CK 의 전술(Tactics)과 기술(Techniques) - TTPs 은 공격의 각 단계를 논리적으로 설명하며 실제 공격자들의 사고방식과 행동 양식을 추적하고 분석할 수 있도록 돕는다. 이를 통해 위협 대응 조직은 각 단계별 방어 전략을 수립하고 탐지 룰, 대응 시나리오 등을 보다 정교하게 구성할 수 있다.

■ APT 공격 사례 분석

실제 공격 사례를 통해 ATT&CK 프레임워크의 전략과 기술을 실무에 적용하여 이해할 수 있다.

- APT29 (Cozy Bear)

SolarWinds 공급망 공격에서 DLL Side-Loading(T1574.002), 정당한 프로세스 내 악성 코드 삽입(T1055) 등의 기술 사용

- Lazarus Group

금융 기관 공격에 피싱(T1566.001), 권한 탈취(T1003), SMB 를 통한 측면 이동(T1021.002) 등 전술적 조합 수행

- FIN7

POS 시스템 대상 악성 문서 배포(T1203), 정보 수집(T1005), 외부 서버로 데이터 전송(T1041)

위의 사례에서 각 공격 흐름은 MITRE ATT&CK 기술과 전술로 상세하게 매핑되며 이를 바탕으로 공격 재현 또는 탐지 정책 수립이 가능하다. 단순히 공격자 그룹이 사용한 기술을 나열하는 데 그치지 않고 그들의 공격 흐름 전체를 '전술-기술(TTPs) 체계'로 매핑하여 각 단계에서 어떤 탐지와 대응이 가능했는지를 시각화 할 수 있다.

- Lazarus Group: 금융기관 및 암호화폐 거래소 공격

북한과 연계된 것으로 알려진 Lazarus Group 은 금융기관 및 암호화폐 거래소를 집중적으로 노려온 APT 조직이다. 이들은 피싱 메일, 소셜 엔지니어링, 웹 취약점 등을 통해 초기 접근(Initial Access)에 성공한 후 자격 증명(Credential Access)을 탈취하고 측면 이동(Lateral Movement)을 통해 주요 자산 시스템에 접근하는 방식으로 활동한다.

MITRE ATT&CK 프레임워크로 분석해보면, Lazarus 의 피싱 공격은 T1566.001 (Spear phishing Attachment) 기술로 식별된다. 이후 권한 상승은 T1068 (Exploitation for Privilege Escalation), 자격 증명 탈취는 T1003 (Credential Dumping) 기술로 분류된다. 이 그룹은 또한 RDP 연결을 통해 내부 시스템에 접근(T1021.001)하고 외부 C2 서버로 민감 정보를 유출(T1041)했다. 실제 정보보안 실무에서는 이러한 연계 분석을 통해 Lazarus 가 사용하는 전술 및 기술의 시퀀스를 탐지 정책에 반영할 수 있으며, 위협 헌팅(Threat Hunting)의 기준점으로 삼을 수 있다.

표 1. 공격 사례에 대한 MITRE ATT&CK 프레임워크 적용 분석의 예

APT 사례에서 보듯이 MITRE ATT&CK 프레임워크는 이러한 복잡한 공격 흐름을 전술적으로 구조화함으로써 어디서부터 공격이 시작되었고 어떤 기술이 사용되었는지 그리고 어떤 단계에서 탐지 및 방어가 가능했는지를 명확히 파악할 수 있도록 돕는다. 또한 과거 공격 사례를 기준으로 사전 탐지 룰을 구성하거나 위협 헌팅(Threat Hunting) 시나리오를 개발하는 데 효과적인 도구로 활용 가능하다.

■ 시큐디움 센터(Secudium Center) – Rule Framework

Rule Framework 는 단순한 이론적 도구를 넘어 실제 보안 조직이 공격자의 행동을 체계적으로 이해하고 대응 역량을 강화하는데 매우 중요한 역할을 한다. SK 쉴더스 원격관제 서비스를 담당하고 있는 Secudium Center 에서는 관제 플랫폼 "Secudium v2.0"에 MITRE ATT&CK 프레임워크를 이용한 독자적인 Rule Framework 를 적용하였다. 적용된 프레임워크 구조는 큰 카테고리에서 9 단계로 구성되며, 필수 정보와 선택 정보로 수집 정보를 분류하여 위협 식별 및 대응에 유기적으로 적용 가능한 탐지 전략을 채택하였다.

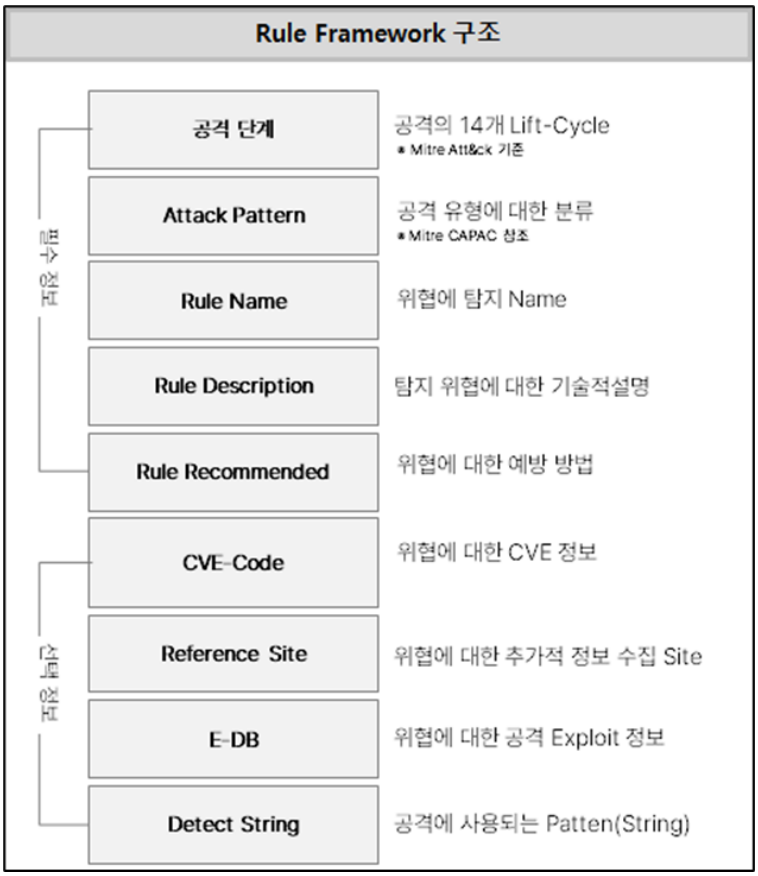


그림 3. Secudium 관제 플랫폼에 적용된 Rule Framework 구조

해당 Rule Framework 를 통해 수집되는 위협 로그를 탐지/분류하여 적절한 대응 기술이 적용된 위협 대응 체계를 구축하는 것이 해당 프레임워크를 활용하는 것의 핵심이다. 또한 위협 헌팅(Threat Hunting)의 구체적인 Feature 를 선정하여 공격자가 사용하는 기술을 선제적으로 탐지해 피해 확산을 방지하고 공격 초기 단계에서 대응 가능성을 높이는데 활용할 수 있다.

지능화 된 사이버 공격에 대항하는 정보 보안의 성공 열쇠는 '체계적 통합과 반복 개선'이다. 이런 관점에서 Rule Framework 를 활용한 탐지 방법론을 정의하는 것은 단순히 새로운 도구를 추가하는 것이 아니라, 보안 운영 전반을 위협 중심의 대응 체계로 재설계하는 과정이다. 전략과 기술을 활용하여 체계적으로 분류 운영하고 반복적인 위협 가능성을 탐색하는 활동을 병행 할 때, 공격자보다 한 발 앞서 방어하는 "능동적 보안 체계"를 구축 할 수 있을 것이다.

■ 참고 자료

[1] MITRE ATT&CK: https://attack.mitre.org

[2] Red Canary: https://redcanary.com

[3] Mandiant Threat Intelligence Reports

[4] Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

[5] Lockheed Martin – cyber kill chain: https://www.lockheedmartin.com