EXPERT COLUMN

SECURITY OPERATION METRICS

탐지와 대응 기준의 보안 실행 매트릭스

예기치 못한 위협의 시대, 무엇을 보호하고 어떻게 보안할 것인가

기하급수적으로 증가하고 있는 사이버 위협은 단순 온프레미스, 클라우드 보안이라는 대응의 경계 또한 무너뜨리고 있다. 혼돈이 야기되는 이 때, 기업은 보호할 대상의 가치를 재정의하고 어떻게 보안할 지에 대한 우선순위를 파악해야 한다.
이 글에서는 보안 위협에 대한 탐지와 대응 기준의 보안 실행 매트릭스를 통해 진화 가능한 보안 가이드를 소개한다.

“무엇을 보호하고 어떻게 보안할 것인가?”

이 질문에 대한 해답을 찾기 위해서는 보호해야 할 대상에 대한 가치 산정이 되어야 보안의 우선순위를 정해서 실행 가능하게 할 수 있다. 보안과 보호의 도메인은 광범위하다. 이를테면 시스템, 사용자, 인프라, 개인정보를 포함한 데이터에 이르기까지 다양하며, 보호할 대상에 따라 보안 방법론과 솔루션의 선택이 가능하다. 예를 들어, 엔드포인트 통합 보안 솔루션, 계정/인증관리 솔루션, 로그 감시, 감사 도구, 백업 및 복구 솔루션과 같은 시스템 관련 영역, 이메일 보안과 같은 특정 포인트 솔루션 등이 있다.

그렇지만 한꺼번에 모든 것을 다 보호하고 보안할 수는 없다. 그렇기 때문에 내부 가치 산정이 중요하고 그에 따라 우선 순위를 정해 당장 할 수 있는 보안에 대한 방법론과 솔루션을 채택해야 한다. 그 우선순위는 보호해야 할 대상뿐만 아니라 무엇으로부터 보호해야 하느냐도 함께 고민이 되어야 한다. 결국 그 무엇은 위협(Threat)이라고 볼 수 있다.

위협의 정의

이 위협에 대해서도 우선순위를 정하고 이에 따라 위협의 도메인을 재정의해야 한다. 위협도 다양한 기준에 따라 분류할 수 있지만 큰 틀의 기준을 3가지 정도로 가늠잡아 위협을 재정의해보자.

[그림 1] 위협의 정의

첫 번째, 상대적으로 쉬운 위협을 취약점(Vulnerability)이라고 할 수 있다. 이 취약점의 가장 큰 특징은 '알려져(Known) 있다'는 것이다. 알려진 취약점에 대해서는 각 벤더에서 제공하는 패치를 적기에 적용한다면 해당 위협은 쉽게 대응할 수 있다.

두 번째는 '알려지지 않은(Unknown)' 위협의 영역이다. 알려지지 않은 위협은 APT(Advanced Persistent Threat)라 불리는 지능형 지속 공격이나 다양한 변종, 설정 오류들로 인해 방어자보다 공격자가 쉽게 파악하여 공격에 이용하는 유형이다. 결국 대응책도 하나의 방법론보다는 다차원적인 방법론으로 대응해야 한다.

마지막은 '보이지 않는(Invisible)' 위협이다. 보이지 않는다는 것은 이미 상존하는 위협 요소인데 우리가 위협이라고 파악하지 못하고 느끼지 못하기 때문이다. 이는 예방 차원에서 현 상황의 위험도를 파악하고 위험 요소를 평상시에 추적하는 노력이 있어야만 대응이 가능하다. 이를 파악하기 위해서는 여러가지 방법이 있겠지만 그 중 하나는 취약점과 위협이 될 가능성이 있는 요소들을 파악하고 상관관계나 사업적 임팩트 등을 고려해, 백분율 형태로 정리하여 나름 정량적 기준으로 표기하기도 한다. 이것이 바로 위험(Risk)이다.

위협에 대한 도메인 구성을 크게 세가지로 정의하고, 정량화된 위험도에 따라 취약점, 위협, 위험의 우선순위를 정하게 된다면, 각 위협 도메인에 적합한 다양한 대응 방법론들을 선정해야 한다. 그리고 적용 가능한 실행으로 바로 연결되어야 한다.

탐지(Detection)

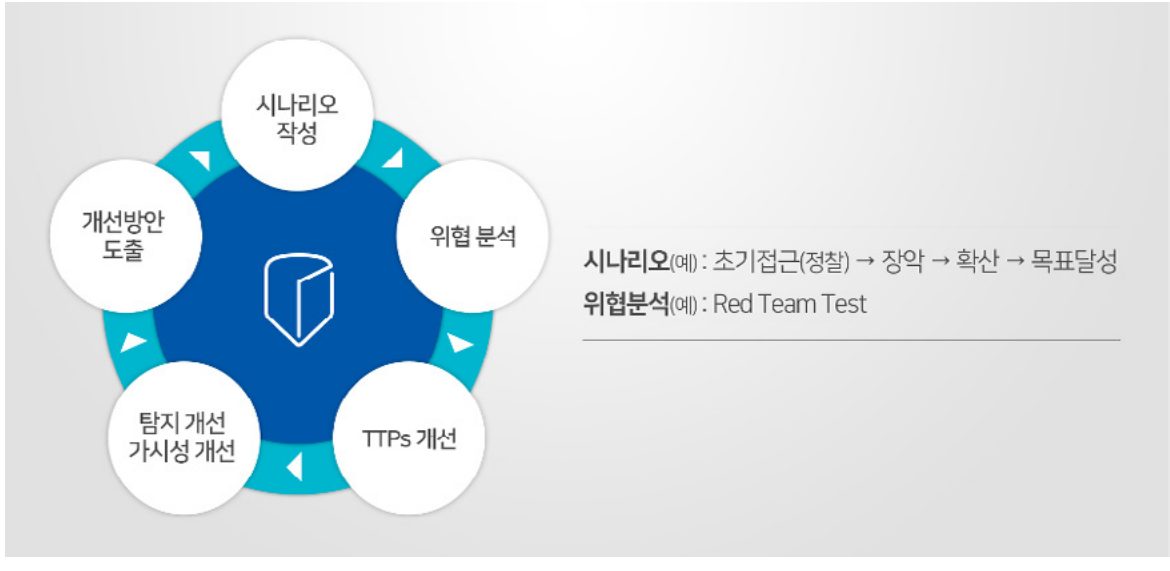
그렇다면 정리된 위협들에 맞춰 제대로 된 실행은 무엇을 어떻게 해야 할까. 그 첫번째 실행 기준은 바로 탐지(Detection)이다. 탐지의 대상과 기법에 대한 이해를 통해서 위협에 대해 무엇을 어떻게 해야 할 지 정하고 실행하는 것이다.

탐지 대상은 여러 형태로 구분할 수 있다. 공격 기법에 따라 구분하면 악성 파일에 의한 공격, 스크립트 형태나 브라우저를 오용하는 인메모리 공격, 혹은 파워쉘을 이용한 파일리스 공격, 정상적인 프로세스를 악용하는 행위 기반 공격까지 다양하게 존재한다.

이러한 공격의 형태를 탐지하기 위해서 다양한 기법들이 필요하다. 시그니처나 룰에 의한 파일 기반 공격 탐지 기법, 파일리스나 프로세스 탐지 대응을 위한 패턴 생성 기법, 그리고 최근에 많이 알려진 마이터어택(MITRE ATT&CK)에서 얘기하고 있는 TTPs(Tactics, Techniques, and Procedures) 기법 등을 통해 대응이 가능하다. 더불어 무수히 많은 탐지 기법들이 효과적으로 적용되기 위해서는 머신러닝(Machine Learning)과 AI(Artificial Intelligence) 기술도 필수적인 요소 기술로 활용된다. 이런 기술들을 통해 방어자 입장뿐만 아니라 공격자 입장에서 공격의 형태를 분석하고 공격 시나리오 설정도 가능해진다. 공격 기법에 대한 프로파일링과 대응 상황, 실제 위협과 피해 사항을 미리 매핑하여 공격 흐름을 기준으로 행위 기반 탐지를 용이하게 한다.

탐지의 한 예를 들어, IOC(Indicators of Compromise)와 IOA(Indicators of Attack)를 구분해보자. IOC는 침해 흔적을 의미하는 방어자의 대응 중심적인 관점의 정의이다. IOC를 탐지하기 위해서는 계정의 속성, 가치(Value)를 중심으로 탐지해서 패턴 생성 기반으로 탐지 기법을 구현한다. IOA는 침해 의도를 의미하며, 어떤 의도를 가지고 공격 기술이나 기법들이 활용될까라는 입장에서의 분석 기법들이 적용될 수 있다.

공격자의 입장에서 공격을 꼭 성공시키고자 한다는 가정을 중심으로 목표 지속 행위나 지속적인 권한 탈취 시도 방법들을 탐지하게 하는 기법이 필요하다. 이를 테면, 사이버 킬 체인에 규명된 공격 흐름도나 마이터어택에서 정의된 TTPs 중심의 탐지 기법으로 관리자가 공격의 의도와 목표를 파악할 수 있게 해주기도 한다.



[그림 2] 공격 흐름 기준의 탐지(Detection) 기법

두 번째는 공격 흐름을 기준으로 탐지하는 기법이다. 이를 위해서는 공격 시나리오 작성부터 레드팀(Red Team) 테스트를 통한 위협 분석, 그를 통해 TTPs를 개선하고 탐지와 가시성을 개선해서 시나리오에 다시 반영하는 안이다. 예를 들면 공격의 시나리오는 공격자가 정찰같은 행위를 통해 초기 접근 후 시스템이나 권한을 장악하여 공격을 확산하고 결국 공격의 목표를 이뤄낸다는 과정을 순차적으로 적용해 보는 것이다. 레드팀은 이러한 시나리오 상에서 실제 침투 테스트(Penetration Test)를 통해 위협을 분석하고 탐지 기법 개선의 기반을 마련한다. 실제 침투 테스트와 분석은 기존 탐지 기법들을 더욱 정교하게 다듬고 개선해준다. 이러한 선순환구조를 통해 유사시 대응을 넘어 상시 대응 체제를 이루게 하는 좋은 탐지 기법의 사례가 될 것이다.

이처럼 다양한 탐지 기법에서 시그니처나 룰을 일종의 점이라고 한다면 행위 기반 룰과 패턴은 선 개념이며, 이는 방어자 관점에서의 기법이다. TTPs 를 통해 공격자 입장을 더 반영하여 방어자와 공격자의 관점을 조합한 입체적인 면을 구성한다고 표현해 볼 수도 있다. 이러한 점, 점과 점을 연결한 선, 선이 연결된 면을 가지고 AI나 머신러닝 기술을 통해 다양한 경우의 수를 도출하고 입체적인 탐지 기법을 만들어 여러 공격의 형태를 탐지할 수 있도록 하는 것이다. 결국 탐지 대상과 탐지 기법에 대한 이해를 통해 무엇을 어떻게 탐지 할지에 대한 탐지 기준을 설정할 수 있다.

대응(Response)

그럼 위협에 대한 탐지, 그 다음 실행안은 무엇일까. 바로 대응(Response)이다. 앞서 설명한 위협 분류 및 정의, 탐지도 실질적인 대응을 위한 사전 작업이라고 할 수 있다.

일반적으로 대응이라고 하면 솔루션 도입을 먼저 떠올리게 된다. 대부분 보안 관리자는 탐지된 위협에 대해 자동으로 처리되기를 바랄 것이다. 기존 솔루션을 살펴보면 자동 치료나 삭제, 설정된 정책에 따라서 시스템적으로 차단하는 등의 대응을 해준다. 이를 치료(Remediation)라는 용어로 표현할 수 있다. 이는 알려진 위협을 방어하는데 효과적이다.

알려지지 않은 위협의 경우는 어떨까. 알려지지 않은 것을 탐지하고 자동 치료하는 것 자체가 어렵다는 건 누구나 알고 있는 사실이다. 앞서 알려지지 않은 위협을 탐지하는 기법에 대해 언급했는데 결국 탐지하더라도 판단이나 대응의 주체는 바로 보안 관리자이다. 일반적으로 보안 솔루

션들이 자동 치료 삭제 대응을 하기 위해서는 룰이나 시그니처를 만들고, 오진이나 오탐을 줄이기 위한 검증 작업과 패치 업데이트까지의 시간이 소요되기 마련이다.

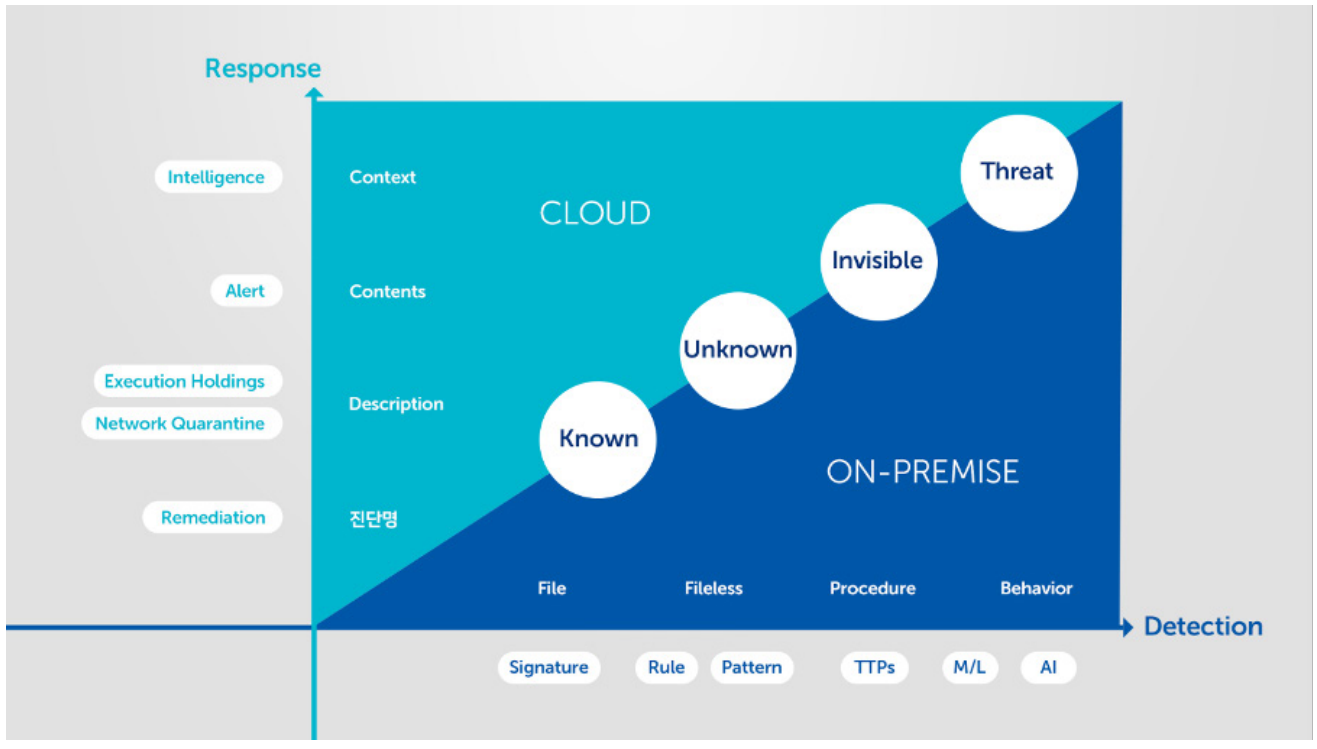
하지만 공격은 그 시간에도 계속될 수 있다. 대표적인 것이 제로데이(Zero-day) 공격이다. 그렇기 때문에 알려지지 않은 위협은 보안 관리자에게 이상 징후나 이상 행위에 대한 알림(Alert)을 주고, 보안 관리자가 직접 실행할 수 있는 판단의 근거를 제시하는 것이 최근 솔루션 대응 방법론으로 대두되었다. 이를 통해 기본적으로 고객은 솔루션이 자동 업데이트되기 전에 의심스러운 파일 실행을 보류시키거나 문제 시 되는 네트워크를 격리하고 격리된 네트워크를 다시 복원하는 대응을 할 수 있다.

이를 통해 기본적으로 보안 관리자는 솔루션이 자동 업데이트되기 전에 의심스러운 파일 실행을 보류시키거나 문제 시 되는 네트워크를 절체하고 이후 다시 복원하는 기본적인 대응법을 수행할 수 있다. 하지만 알려지지 않은 위협을 너머 늘 상존하고 있지만 인지하거나 보이지 않는 위협에 대해서도 대응법이 필요한데, 유사시가 아닌 평상시에 상시 위협 분석을 하는 대응법도 최근 화두가 되고 있다. 이를 위협 추적 대응법이라고 일컫는다.

위협 추적을 효과적으로 하기 위해서는 내부 위협 요소 수집만으로는 판단 기준의 한계가 있기 때문에 산업 전반에 걸친 위협 트렌드와 외부 대응 기법들을 참고한다면 보다 효과적인 위협 탐지와 대응을 할 수 있게 된다. 이것이 바로 위협 인텔리전스(Threat Intelligence)가 필요한 이유다.

이제 기업과 기관에서는 자동 치료·삭제나 차단과 같은 단일화된 초기 대응을 넘어, 다양한 탐지 기법들과 매칭할 수 있는 폭넓은 대응(Response) 체계를 갖춰야 한다.

지금까지 '무엇으로부터 고객을 보호할 것이냐'라는 것에 대해 위협을 정의했고, 각 위협에 대한 보안 실행의 관점에서 '무엇을 탐지하고 어떻게 대응할 것이냐'에 대한 부분까지도 살펴봤다. 개별 단위로 언급한 탐지와 대응을 종합해 하나의 틀로 정리해 보면 위협에 대한 실행 기준을 만들어 주는 '탐지와 대응 기준의 보안 실행 매트릭스(Security Operation Metrics)'를 떠올릴 수 있다.



[그림 3] 탐지와 대응 기준의 보안 실행 매트릭스 (Security Operation Metrics)

위협은 알려진, 알려지지 않은 그리고 보이지 않은 위협으로 구분하고, 이에 따른 실행 보안의 첫번째 기준인 탐지는 탐지 대상과 탐지 기법 따라 단계적으로 실행 단위를 정의할 수 있다.

탐지에 따른 대응 방법은 솔루션 스스로 자동 치료, 차단하거나 이상 행위, 이상 징후에 대한 알림을 보안 관리자에게 제공한다. 보안 관리자의 직관력과 자체 판단의 기준으로 운영을 해 나가기도 하지만, 이를 넘어 고객이 좀 더 세밀히 판단하고 수행할 수 있도록 외부 위협(Threat Intelligence)를 통해 연관 분석과 상세분석까지도 제공되어야 한다.

이를 종합해 보면 위협 탐지와 대응을 축으로 한 실행 관점의 보안 매트릭스를 만들어 볼 수 있다. 또한 이 매트릭스는 단순 온프레미스를 너머 클라우드 환경까지도 고려되어야 한다.

고객 주도형 & 실행 보안

이 글에서는 3가지 유형으로 정의된 위협을 조망해 보고, 이를 보호할 대상의 가치에 따라 우선순위를 정해서 무엇을 어떻게 할지라는 질문에서 시작했다. 특히, 보안은 준비보다 실행이 중요하다라는 관점에서 관리자가 탐지와 대응 기준의 매트릭스를 통해 실행 방법을 제시했다.

하지만 보안은 보안성이 높을수록 편의성이 떨어지는 상충되는 관계를 갖고 있다. 보안 관리자의 입장에서 우선순위가 높다고 하더라도 사용자 즉, 내부 구성원의 입장에서는 사업 수행의 방해요소로 폄하되어 실행하기 어려운 가이드로만 전락될 수 있다. 어찌 보면 가장 큰 보안 위협이기도 하다. 보안 가이드는 있지만 실행되지 못하는 것은 아무것도 하지 않게 되는 것이다.

그래서 통속적으로 최고 의사결정자의 적극적인 후원 없이는 보안이 제대로 갖춰지거나 실행될 수 없다고 하는 것이다. 따라서 최고 의사결정자가 내부 구성원들과 공감할 수 있는 근거를 마련해주는 것도 보안 관리자의 주요 역할이라고 할 수 있다.

앞서 소개한 탐지와 대응 기준의 보안 실행 매트릭스(Security Operation Metrics)는 한번에 모든 것을 다 갖추기 위한 것이 아니라 하나 하나씩이라도 당장 효과를 볼 수 있는 것을 시작으로 휘발성으로 없어지는 것이 아닌 차곡차곡 쌓아 상호 유기적인 연관관계를 이어 갈 수 있는 큰 그림이 되어야 할 것이다. 우리 자산을 보호하고 보안하는 이유는 바로 사업의 연속성을 확보하고 지속 가능한 사업 성장을 위한 것이기 때문이다. 이제 보안 리스크는 위협 정의에 따라 적절히 대응하지 못했을 때 생기는 사업적 임팩트를 고려해 이를 사업적 리스크로 정량화하여 최고 의사결정자와 구성원들이 공감할 수 있도록 지속적으로 제시되어야 한다.

최근 코로나 이슈로 인해 요원하게 느껴졌던 클라우드 환경이 가까워졌고 재택근무라는 말이 일상화되면서 생산성 제고와 보안성 강화는 더 중요한 숙제가 되었다. 기술이 발전하는 만큼 우리를 향한 위협들은 그 범주가 넓어지고 공격의 형태 또한 더 고도화되었다. 예기치 못한 상황의 연속인 이 시대에, 보안의 중요성, 그 자체는 변하지 않고 있다. 기존 보안의 틀을 유지하면서 기민하게 대응할 수 있기 위해서는 모두가 공감할 수 있는 보안 관리자의 흔들림 없는 근본적인 기준이 필요하다.