보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

3C로 이해하는 통합 보안 전략

AhnLab 2022-09-30

월간'안' 독자 여러분들도 "통합 보안이 중요하다", "이제 단일 솔루션으로는 보안에 한계가 있다"라는 말을 한 번쯤 들어봤을 것이다. 이제 통합 보안은 누구나 아는 개념이지만 이를 제대로 구현하는 것은 여전한 숙제로 남아 있다.

그럼, 통합 보안은 어떻게 접근해야 하는 걸까? 그리고 통합 보안의 본질은 무엇일까?

이번 글에서는 3C(Consolidation, CSMA, CNAPP)라는 키워드를 주제로 통합 보안이라는 넓고 깊은 개념에 좀 더 가까이 다가가고자 한다.

우리가 보호해야하는 대상의 보안 가치는 계속해서 변화하고 있다. 예를 들면, OT 환경은 특유의 폐쇄성으로 인해 안전하다고 여겨졌지만, 최근 IT와 OT가 융합되면서 보안의 필요성이 주목받고 있다. 또, 클라우드 역시 과거와 달리 사용자가 늘어나고 실질적인 혜택을 주게 되면서 보안의 가치가 올라가게 되었다.

이와 같은 변화 속에서, 우리가 주목해야 것은 ▲위협의 고도화 ▲보안 영역의 붕괴다. 이제, 네트워크 침입이 발생하면 그 영향은 네트워크에만 국한되지 않는다. 또, 모바일 기기가 침해 당할 경우 비즈니스와 생활 전체에 영향을 준다. 연결된 환경을 노리는 위협이 체계적으로 진화하고 공격 표면도 넓어지는 가운데, 보호 대상의 가치가 달라지면서 통합 보안도 변화하고 있다.

[그림 1] 연결되어 있는 현재의 위협 환경

한 마디로, 환경이 변하니 통합 보안도 달라진다는 뜻이다. 변화를 마주하는 조직들이 해답을 찾으려면, 먼저 과거와 현재의 보안 개념을 양립시키는 것부터 시작해야 한다.

과거의 보안은 내부와 외부(North-South) 경계(Perimeter) 보안이 중심이었다. 반면, 현재는 클라우드의 확대로 말미암아 내부에서의 'East-West' 트래픽 점검이 중요해졌다. 또, 과거에는 정책(Policy) 위주로 보안을 관리했다면, 현재는 올바른 설정을 위한 형상(Posture) 관리의 중요성이 부각되고 있다.

그럼, 미래의 보안을 위해서는 현재 각광 받고 있는 개념을 잘 적용하면 되는 것일까? 반은 맞고 반은 틀리다. 물론 최신 트렌드가 중요하지만, 그렇다고 해서 과거의 개념이 쓸모 없어진 것은 아니다.

최근 East-West 트래픽 보안이 중요하다고 여겨지는 이유는 마이크로서비스 아키텍처에서 애플리케이션 간 통신이 활발해졌기 때문이다. 그렇다고 해서, 기존 네트워크 내외부 경계 보안의 중요성이 낮아진 것은 아니라는 의미다. 결국, 둘 중 하나를 고르는 A or B가 아닌, A and B로 융합하는 것이 이 시대가 지향하는 통합 보안이다.

효과적인 TDR을 위한 '3C'

보안에서 통합은 계속해서 이뤄져오고 있지만, 늘 현재진행형이고 완료된 적이 없다. 앞서 말한대로 지켜야할 대상과 통합의 의미가 계속해서 변화하기 때문이다. 조직들이 유동적이고 어려운 통합 보안을 잘 수행하려면 과거와 현재 보안 개념의 양립을 이해한 뒤, 통합 보안의 본질을 정확히 파악하고 올바른 방향으로 접근해야 한다.

통합 보안의 변치 않는 본질은 모든 영역에서의 위협을 총체적으로 탐지해 효과적으로 대응하는 것, 즉 위협 탐지 & 대응을 잘 하는 것이다.

최근에는 효과적인 위협 탐지 & 대응을 위한 비전을 TDR(Threat Detection & Response)이라 한다. TDR은 위협에 대해 더 나은 가시성을 확보하고 대응할 수 있도록, 보안 솔루션 뿐만 아니라 자산과 인력, 프로세스까지 통합하는 '프랙티스(Practice)'를 일컫는다.

EDR(Endpoint Detection & Response)이나 NDR(Network Detection & Response)처럼 벤더가 탐지 & 대응을 위해 시장에 공급하는 기술들은 'TDR 베스트 프랙티스(TDR Best Practice)'를 위한 방안이자 구성요소 중 하나이다. 다만, EDR이나 NDR을 도입했다고 해서 TDR이 보장되는 것은 아니며, 위에 서술한대로 조직의 자산과 프로세스 등이 어우러져 원활하게 운영되어야 한다.

본 문서의 제목에 등장하는 3C(Consolidation, CSMA, CNAPP)는 TDR 베스트 프랙티스를 위한 주요 방법론이다. Consolidation은 보안 솔루션들의 유기적인 통합, Cyber Security Mesh Architecture(CSMA)는 플랫폼과 플랫폼의 연동, Cloud Native Application Protection Platform(CNAPP)는 개발부터 운영까지 클라우드 전 주기에 걸쳐 보안을 적용하는 것을 의미한다.

1. Consolidation

Consolidation은 클라우드, 엔드포인트, 네트워크 등 기존 보안 영역의 솔루션과 서비스들이 통합된 탐지 & 대응을 위해 융합되는 것을 의미한다.

영역 별로 살펴보면, 클라우드 보안은 클라우드 탄생 이후 CWPP(Cloud Workload Protection Platform)와 CSPM(Cloud Security Posture Management)과 같은 솔루션들이 등장했다. 엔드포인트 보안은 AV(Anti-Virus)에서 시작해 EPP(Endpoint Protection Platform)와 EDR이 등장하고 상호 간 통합되기에 이르렀다. 네트워크 역시 방화벽에서 IPS(Intrusion Prevention System), 그리고 NDR로, 보안 서비스도 보안 유지보수에서 시작해 MSS(Managed Security Service)로 확대됐다. 이제, 해당 솔루션들은 CNAPP, XDR 및 MDR이라는 개념 하에 합쳐지고 있다.

솔루션 통합이 가속화되는 가운데, 이를 도입하는 조직들은 고민에 빠지게 된다. 단일 벤더가 수 많은 솔루션들을 독자적으로 전면 통합하는 것이 불가능하다는 사실을 모두가 알고 있다. 고민은 여러 벤더가 협력한 통합이 나은 것인지, 아니면 단일 벤더가 최대한으로 통합하는 것이 나은지에 관한 것이다.

[그림 2] 프론트엔드와 백엔드 통합의 개념

고민을 해결하려면, 프론트엔드(Front-End)와 백엔드(Back-End) 통합을 구분해서 봐야한다. 일단 백엔드는 가급적 단일 벤더로 통합해야 한다. 위협 인텔리전스(Threat Intelligence), API 등으로 이뤄진 백엔드는 제대로 연동되지 않으면 운영 상의 문제를 일으킬 수 있기 때문이다. 반면, 방화벽, EDR, CWPP 등의 프론트엔드는 백엔드가 제대로 통합되어 있다면 복수의 벤더가 협력해도 무방하다.

결국 통합의 목적은 위협을 잘 탐지해 대응하는 것이고 한 단계 더 들어가면, 전체 보안 영역에서의 다양한 알림(Multi Alert)을 고도화된 분석 역량(Security Analytics)을 통해 하나의 침해(One Incident)로 도출해내는 것이다. 최근 강조되고 있는 '자동화(Automation)'도 이 작업에 효율성을 더한다는 측면에서 중요하다고 볼 수 있다.

정리하면, 앞으로 보안 업계에서 행해지는 통합은 백엔드는 단일 통합, 프론트엔드는 복수 통합으로 진행하면서 자동화를 극대화하는 방향으로 진화할 전망이다.

2. CSMA

다음으로, CSMA는 엔드포인트, 네트워크 등 기존 영역의 보안 솔루션들이 통합되어 플랫폼을 이루고 이 플랫폼들이 상호 연동하는 개념이다. CSMA에서는 여러 보안 플랫폼들이 ▲단일 대시보드 ▲통합 매니지먼트 ▲중앙화된 알림 ▲통합 인텔리전스를 기반으로 운영되며, 사용자에게 유연한 구성(Composability), 확장성(Scalability), 상호운용성(Interoperability)을 부여한다. 항상 공격자가 유리한 보안 패러다임에서, CSMA는 무의미한 위협 '노이즈(Noise)'를 최소화할 수 있는 기술적 근거가 된다.

[그림 3] CSMA 개념도

다양한 솔루션으로 구성된 플랫폼이 통합되는 CSMA 아키텍처에서 가장 중요한 것은 바로 '연동'이다. 많은 구성요소들을 갖추고 있다해도, 각각이 제대로 연결되어 있지 않으면 효용성이 떨어질 수 밖에 없는 구조다. 쉽게 비유하면, 블록을 아무리 많이 쌓아도 합을 맞추지 못하면 게임에서 패배하는 테트리스와 비슷하다고 볼 수 있다.

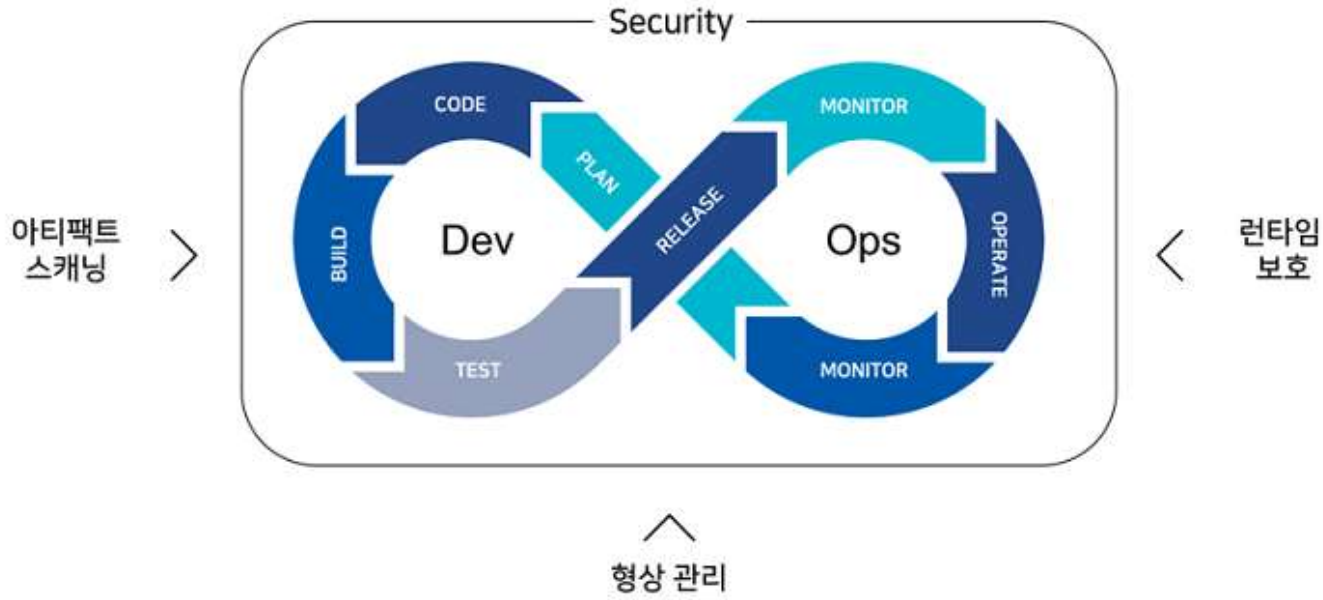
3. CNAPP

클라우드 서비스 영역이 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)를 넘어, CaaS(Container as a Service), fPaaS(Function Platform as a Service)까지 발전하면서, 워크로드를 보호하는 CWPP(Cloud Workload Protection Platform)와 보안 형상을 관리하는 CSPM(Cloud Security Posture Management) 등 보안 솔루션들의 역할이 융합 및 재정의되고 있다.

이 과정에서 클라우드 네이티브(Cloud Native)를 지향하는 통합 보안이 요구되고 있으며, 그 결과로 CNAPP(Cloud Native Application Protection Platform)가 성장하고 있다.

그렇다면, CNAPP의 구체적인 역할은 무엇일까? 시장에서는 개발부터 운영까지 포괄하는 프로세스를 데브옵스(DevOps)라 하고, 이 라이프사이클 전 주기에 보안을 적용하는 것을 데브섹옵스(DevSecOps)라 한다. CNAPP의 역할

은 데브섹옵스(DevSecOps) 라이프사이클에 걸쳐 기본적인 워크로드 보안 뿐만 아니라 ▲취약점 점검 ▲런타임 보호 ▲올바른 설정 관리 등의 기능을 제공해 클라우드 네이티브 보안을 구현하는 것이다.



[그림 4] 데브섹옵스 라이프사이클과 보안 기능

이와 관련해 최근 'Shift-Left' 개념이 부각되고 있는데, 그 동안 운영 단계([그림 4] 기준 오른쪽)에서 주로 수행했던 보안 점검을 개발 단계(왼쪽)으로 옮겨와야 한다는 의미다. 간단히 하면, 소프트웨어 개발 초기부터 취약점이나 설정에 대한 관리를 지속적으로 수행하여 보안을 강화하는 것으로 이해하면 된다.

결론

지금까지 변화하는 통합 보안의 의미와 TDR 베스트 프랙티스를 위한 3C(Consolidation, CSMA, CNAPP)의 개념을 알아봤다. 필자는 효과적인 탐지 & 대응 체계 수립을 고민하는 독자 여러분께 다음 3가지를 제언한다.

▲무조건 새로운 것을 지향하기 보다는 조직 보안 요구사항에 맞춰 과거와 현재를 양립시킬 것
▲민첩하게 움직일 것
▲실현가능한 것부터 바로 시작할 것

서두에 강조한대로, 새로운 트렌드가 나온다고 해서 과거의 것이 무의미해지지는 않는다. 따라서, 과거와 현재 보안의 균형을 토대로 미래를 준비해야 한다. 그 준비는 빠르게 진행해야 하며 이를 위해서는 실행 가능한 것부터 바로 시작해야 한다. 특히, 빠르게 고도화되는 위협 환경을 고려했을 때, 아무런 움직임 없이 가만히 있는 것 자체가 보안 홀(hole)을 발생시킬 수 있다.

안랩은 국내 유일의 통합 보안 벤더로서, 자사가 보유한 포괄적인 솔루션들의 연동을 가속화해 나갈 것이다. 우선적인 목표는 자사 통합 보안 플랫폼을 기반으로 위협을 단순 차단(Protection)하는 것을 넘어 종합적으로 추적(Hunt) 및 추천(Recommend)하는 체계를 확립하는 것이다. 이를 통해, 고객들이 유사시가 아닌 평상시에 조직을 보호하고 궁극적으로 TDR 베스트 프랙티스를 구현할 수 있도록 최선을 다할 것이다.

AhnLab 이상국 마케팅본부장