AhnLab

Case Study

BPFDoor 악성코드 차세대 보안 모델로 극복하기

지난 4월, 국내 통신사의 다수 고객 유심 정보가 외부 공격에 의해 유출되는 사고가 발생했다. 본 사건은 통신사의 리눅스 기반 서버에 침입한 해커가 BPFDoor 계열 악성코드를 설치해 벌어진 것으로 알려졌다.

안랩은 지난해 10월, 자사 EDR 솔루션인 AhnLab EDR을 활용해 통신사 공격에 활용된 악성코드와 유사한 BPFDoor 계열 악성코드를 탐지해 분석 내용을 공개했다. 통신사 공격에 사용된 BPFDoor는 당시 탐지했던 악성코드와 몇 가지 차이점이 있지만 주요 기능들은 대부분 동일하다.

AhnLab EDR 외에도 안랩은 샌드박스 솔루션 AhnLab MDS의 동적 분석 역량을 활용해 악성코드와 관련 행위 및 악성 패킷에 대응한다. 리눅스 서버 백신 V3 Net for Linux와 네트워크 보안 솔루션 AhnLab XTG 및 AhnLab AIPS, 클라우드 워크로드 보안 플랫폼 AhnLab CPP의 Host IPS에는 탐지 시그니처를 적용해 BPFDoor를 사전 차단할 수 있도록 지원해오고 있다. 위협 인텔리전스 플랫폼 AhnLab TIP는 BPFDoor와 관련된 위협 정보를 빠르게 공유한다.

더 나아가, 안랩은 고객들이 중장기적으로 BPFDoor와 같은 고도화된 공격으로부터 조직을 효과적으로 보호할 수 있도록 ▲예방 및 차단 ▲탐지 및 대응 ▲운영 및 협업까지 사이버 보안 사이클을 아우르는 솔루션-서비스 연계 보안 모델을 제시하고 있다.

1. BPF와 BPFDoor

BPF(Berkeley Packet Filter)는 네트워크 패킷 필터링을 위해 개발된 메커니즘이다. 커널 영역에 설치되어 외부로부터 전달받은 패킷을 사용자 영역으로 넘길 것인지 결정할 수 있다. BPF는 1992년경 처음 개발되었으며, 2014년에는 eBPF(extended BPF)가 리눅스 커널에 도입되었다. eBPF는 기존 BPF 와 같이 네트워크 패킷 필터링을 지원하면서도 성능, 보안성 및 안정성이 강화되었다.

이번 통신사 공격에 사용된 BPFDoor는 기존 BPF의 패킷 필터링 기능을 악용하는 리눅스 백도어 악성코드다. 패킷 필터링 규칙을 추가해 조작된 특정 패킷인 '매직 패킷'이 수신됐는지 검사한 후 악성 행위를 수행한다. 서버 방화벽과 보안 시스템을 우회할 수 있고, 외부 공격자가 직접 시스템에 명령을 전달할 수 있는 리버스 쉘, 바인드 쉘 등의 기능을 제공한다. 보안 탐지를 회피하고 장기간 시스템에 은밀히 남아 있을 수 있어 공격 수행에 장점이 있다.

BPFDoor 악성코드는 오픈소스이며, 2021년 PwC사 보고서를 통해 처음 공개되었다. 중국 기반 APT 그룹 Red Menshen(Earth Bluecrow)이 사용하는 것으로 알려져 있다.

2. 통신사를 공격한 BPFDoor 변종, 특징은?

안랩은 통신사 해킹 사고 발생 6개월 전인 지난해 10월, AhnLab EDR을 활용해 BPFDoor 계열 악성코드를 탐지하고 분석 내용을 ASEC 블로그를 통해 공개한 바 있다. 당시, 안랩이 탐지했던 BPFDoor 악성코드와 이번 통신사 공격에 활용된 악성코드는 본질적으로 동일하지만 세부적인 기능과 행위에서 몇 가지 차이점이 있었다.

분석 항목	기존 BPFDoor	통신사 공격에 사용된 변종 (2025.04)
자가 복제 경로	/dev/shm/kdmtmpflush	자가 복제 및 삭제 기능 제거
실행 위장 이름	udevd, mingetty 등	smartd, dbus-daemon, hald-addon-volume등
PID 저장 경로	/var/run/haldrund.pid	/var/run/hald-smartd.pid /var/run/system.pid /var/run/hp-health.pid /var/run/hald-addon.pid 등
명령 인증 방식	단순 문자열 기반 (justforfun)	MD5(l5*AYbs@LdaWbsO + 패킷 일부) 계산 방식

[표 1] 기존 BPFDoor와 통신사 공격에 사용된 변종의 차이점

우선, 과거 탐지된 BPFDoor는 앞서 언급한 바와 같이 /dev/shm 경로에 kdmtmpflush라는 이름으로 자가 복제해 실행한 뒤 삭제한 반면, 이번에 확인된 BPFDoor 악성코드들에는 해당 기능이 제거되었다.

PID 파일 경로에도 차이가 있다. 공개된 소스코드에서는 /var/run/haldrund.pid 경로에 PID 파일을 생성한다. 이는 BPFDoor가 정상적으로 실행 중인지 판단하는데 사용된다. 다만, 이번 공격에 사용된 악성코드들은 다른 PID 파일 경로를 갖는다.

비밀번호를 통한 명령 인증 방식도 바뀌었다. BPFDoor는 리버스 쉘과 바인드 쉘 등의 명령을 지원하는데 기존 악성코드의 명령들은 각각 매직 패킷에 포함되는 비밀번호 justforfun과 socket 문자열을 통해 구분됐다. 다만, 이번 공격에 활용된 BPFDoor는 공개된 침해지표(IoC)에 따르면, MD5를 기반으로 명령을 구분했다. 매직 패킷을 통해 전달받은 문자열과 l5*AYbs@LdaWbsO 문자열을 더한 후 MD5를 계산하여 명령을 구분하는 형태였다.

그 외 악성코드가 수행하는 실질적인 기능들은 대부분 동일했다. 다만, 위 내용은 지난 4월 KISA가 공개한 내용을 기반으로 작성되었으며, 이번 통신사 공격에 대한 조사가 진행 중인 관계로 조사 결과에 따라 내용이 업데이트될 수 있다.

3. 안랩은 BPFDoor에 어떻게 대응하고 있나

❶ 개요

안랩은 고객들이 BPFDoor 악성코드를 즉각적으로 탐지해 조치할 수 있도록 다양한 보안 방안을 제공하고 있다. 각 솔루션의 역할은 [표 2]와 같고, 자세한 내용은 후술한다.

제품명	탐지 내용	설명
AhnLab EDR	공격 관련 모든 이벤트	- 방화벽 설정 변경, 포트 리다이렉트 등 행위 탐지 - 보안 솔루션 우회 행위 탐지 - 컨텍스트 분석을 통한 공격 캠페인 이해
AhnLab MDS	알려진 악성코드 및 악성 패킷 공격 관련 이벤트	- 유입 악성코드 시그니처 기반 탐지 및 치료 - 시그니처 기반 '매직 패킷' 차단 - 방화벽 설정 변경, 포트 리다이렉트, 보안 솔루션 우회 행위 등 탐지 (동적 분석)
V3 Net for Linux Server	알려진 악성코드	- 서버 유입 악성코드의 시그니처 기반 탐지 및 치료
AhnLab XTG	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단 (방화벽의 IPS 기능)
AhnLab AIPS	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단
AhnLab CPP(Host IPS)	알려진 악성 패킷	- 시그니처 기반 '매직 패킷' 차단
AhnLab TIP	공격 관련 모든 위협정보	- 악성코드 최신 동향 및 IoC 정보를 보안 운영에 적용

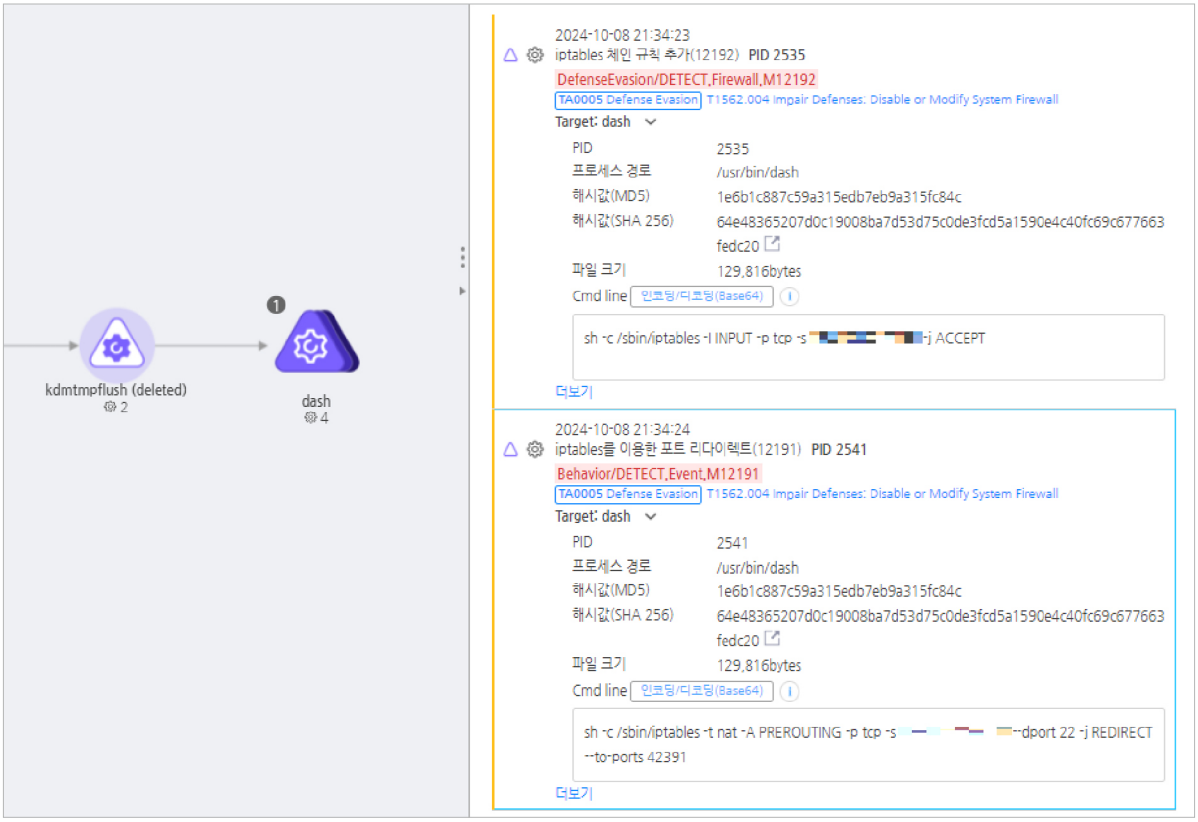
[표 2] 안랩 솔루션의 BPFDoor 악성코드 대응 내용

❷ 2024년 10월, AhnLab EDR이 탐지했던 BPFDoor

지난해 AhnLab EDR의 BPFDoor 탐지 내용을 보면, 실행 과정에서 자신을 /dev/shm 경로에 kdmtmpflush라는 이름으로 복사하는 것이 특징이다. AhnLab EDR은 의심스러운 프로세스가 /dev/shm 경로에 자가 복사하고 실행 권한을 부여하는 행위에 대해 [그림 1]과 같이 위협으로 탐지했다. 이를 통해, 보안 관리자가 위협을 사전에 인지할 수 있도록 지원했다.

[그림 1] 의심스러운 경로에 위치한 파일에 실행 권한을 부여 행위 탐지

또한, '매직 패킷'과 매칭되는 비밀번호가 포함된 명령을 전달받으면, 특정 포트를 오픈하고 방화벽 설정을 변경하여 공격자로부터 수신되는 패킷들을 리다이렉트한다. AhnLab EDR은 Iptables를 이용해 새로운 규칙을 추가 및 제거하는 행위와 포트 리다이렉트처럼 의심스러운 행위들을 주요 행위로 탐지했다.



[그림 2] iptables를 이용한 규칙 추가 및 포트 리다이렉트 행위 탐지

위 행위들은 다른 악성코드에서도 나타나는 기법들로, 이것만으로 BPFDoor 악성코드라 단정 짓기는 어렵다. AhnLab EDR은 추가적으로 C2 통신 등 악성코드의 의심스러운 행위들을 분석 및 종합하여 [그림 3]과 같이 BPFDoor로 탐지했다.

[그림 3] AhnLab EDR에서 탐지한 BPFDoor 악성코드

고객 입장에서는 AhnLab EDR을 활용해 BPFDoor와 관련된 의심스러운 행위 분석 정보와 전후 맥락을 확인하여, 원인 파악과 적절한 대응 수행이 가능했다.

BPFDoor와 같은 고도화된 악성코드와 공격 기법을 효과적으로 탐지한 AhnLab EDR은 전 세계적으로 가장 공신력 있는 보안 제품 테스트 중 하나인 '마이터 어택 평가(MITRE ATT&CK Evaluation)'에 국내 보안기업으로는 유일하게 4회 연속 참가해 우수성을 입증하고 있다. 마이터 어택 평가는 주요 위협 그룹들의 공격 기법을 모의수행한 시나리오를 토대로 참가 제품의 위협 탐지 & 대응 역량을 평가한다.

특히, 최근 진행된 라운드 6에서는 주요 랜섬웨어 그룹 클롭(CL0P)과 록빗(LockBit)이 윈도우와 리눅스에 걸쳐 수행하는 실제 공격 기법으로 구성된 시나리오 중 95%를 탐지했다. 이는 전 세계 보안 기업들 중에서도 상위권에 해당하는 성적이다. 뿐만 아니라, 탐지한 56개 세부 단계(substep) 중 49개에서 최고 등급인 Technique을 받았는데, 이는 사용자가 탐지 정보를 통해 위협 행위에 대한 '맥락(Context)'을 포괄적으로 이해할 수 있다는 방증이다.

안랩의 마이터 어택 평가 라운드 6 결과에 대한 자세한 내용은 결과 분석 보고서를 통해 확인할 수 있다.

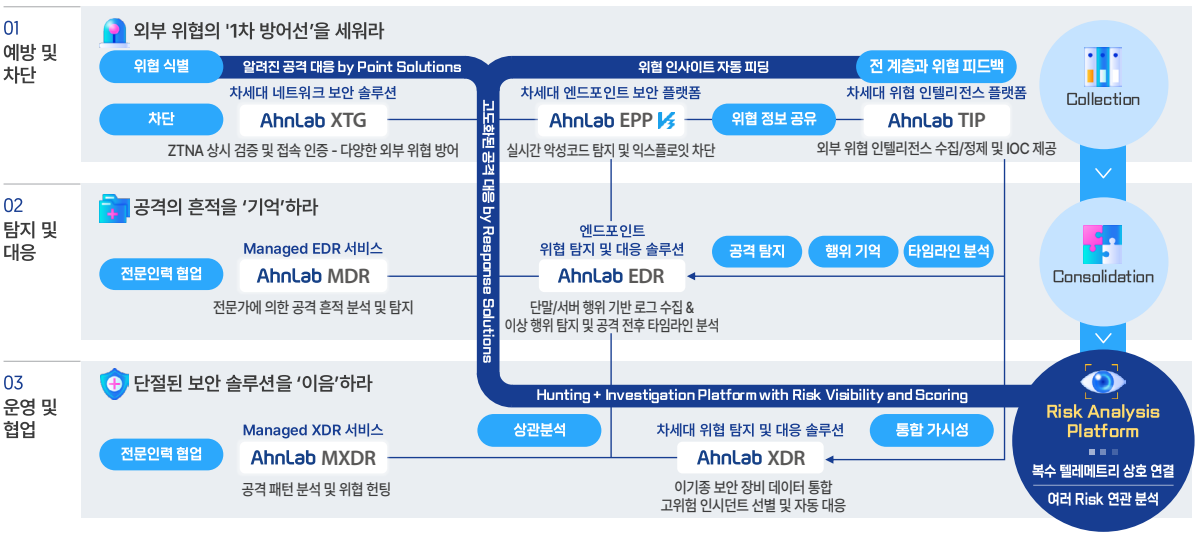
❸ 시그니처와 위협 인텔리전스로 즉각적인 대응 지원

안랩은 AhnLab EDR을 통한 탐지 및 분석 뿐만 아니라, 샌드박스 솔루션 AhnLab MDS의 동적 분석 역량을 활용해 악성코드와 관련 행위 및 악성 패킷에 대응한다. 자사 리눅스 서버 보안 솔루션 V3 Net for Linux Server에는 탐지 시그니처를 적용해 고객들이 BPFDoor 관련 공격을 사전에 탐지해 차단할 수 있도록 지원하고 있다. 차세대 방화벽 AhnLab XTG, 침입차단 솔루션 AhnLab AIPS, 클라우드 워크로드 보안 플랫폼 AhnLab CPP의 Host IPS에는 사용자 정의 시그니처를 추가해 네트워크 단에서 악성 패킷 유입을 차단할 수 있다. 이처럼, 안랩은 IoC 등 공개되는 정보들을 자사 솔루션에 실시간으로 반영하여 BPFDoor로 인한 잠재적인 위협으로부터 고객들을 안전하게 보호하고 있다.

아울러, 위협 인텔리전스 플랫폼 AhnLab TIP에서는 BPFDoor 관련 IoC와 최신 동향 등 보안 정보를 종합적으로 제공해 고객들이 조직을 효율적으로 보호할 수 있도록 지원하고 있다.

4. 차세대 보안 모델로 조직의 미래를 안전하게

이번 BPFDoor 공격은 단순 취약점 악용을 넘어 보안 솔루션 우회해 내부에 잠입하여 장기간 공격을 수행하는 고도화된 기법이 현실화된 케이스다. 물론, 당장 피해 사례가 발생한 BPFDoor에 대응하는 것도 중요하지만, 장기적인 관점에서 여러 위협들을 효과적으로 해소할 수 있는 전략이 필요하다. 이에 대해, 안랩은 ▲예방 및 차단 ▲탐지 및 대응 ▲운영 및 협업까지 사이버 보안 사이클을 아우르는 솔루션-서비스 연계 보안 모델을 제시한다.



[그림 4] 안랩 차세대 보안 모델 아키텍처

❶ 예방 및 차단

차세대 보안 모델에서 가장 선행되어야 하는 작업은 위협을 사전에 예방 및 차단할 수 있는 체계를 갖추는 것이다. 이 단계에서는 안랩의 새로운 차세대 방화벽 AhnLab XTG, 엔드포인트 보안 플랫폼 AhnLab EPP 및 위협 인텔리전스 플랫폼 AhnLab TIP를 연계해 활용하면 큰 효과를 거둘 수 있다.

A. AhnLab XTG: 위협 차단과 네트워크 접속 상시 검증

기존 AhnLab TrusGuard에서 진일보한 차세대 방화벽 AhnLab XTG는 향상된 성능을 바탕으로 네트워크 일선에서 위협을 차단한다. 특히, AhnLab XTG의 ZTNA(Zero Trust Network Access) 기능은 사용자와 기기의 신원 및 보안 상태를 지속적으로 모니터링하여 검증된 사용자만 애플리케이션 및 네트워크 리소스에 접근할 수 있도록 한다. 이를 통해, 비인가 사용자 및 기기의 서버 접속을 사전 차단하여 잠재적 피해를 최소화할 수 있다.

B. AhnLab EPP(V3 Net for Linux Server): 악성코드 차단 및 통합 관리

최근, 리눅스 서버 취약점과 악성코드가 늘어나면서 이에 대한 보안 필요성도 높아지고 있다. 오랜 기간 검증된 리눅스 서버용 백신 V3 Net for Linux Server를 활용하면 BPFDoor와 같이 고도화된 신종 및 변종 악성코드를 사전에 탐지해 차단할 수 있다. AhnLab EPP까지 활용하면 탐지 현황, 정책, 이벤트 등을 통합 관리해 보다 신속한 조치가 가능해진다. 또한, 백신 외에도 패치 관리, 보안 상태 점검, 디바이스 제어 등 EPP가 제공하는 다양한 보안 기능 간 연계 규칙을 활용해 엔드포인트 보안을 한 층 강화할 수 있다.

C. AhnLab TIP: 인텔리전스 기반 전략 수립 및 내부 영향도 점검

AhnLab TIP는 사이버 위협에 대한 최신 IoC, 분석 보고서, 위협 그룹 분석 등 다양한 위협 인텔리전스를 제공한다. 특히, 안랩의 여러 솔루션들을 통해 수집된 데이터를 기반으로 위협을 분석 및 분류하기 때문에 고객들에게 타사에서는 확인할 수 없는 독보적인 위협 인텔리전스를 지원할 수 있다. 고객 입장에서는 AhnLab TIP에서 확인된 최신 IoC를 AhnLab XTG와 EPP에 자동 적용하고 내부 영향도 점검을 수행하여 위협 사전 예방 체계를 갖출 수 있다.

❷ 탐지 및 대응

BPFDoor와 같은 최신 악성코드들은 보안 솔루션 우회 기능을 갖춘 경우가 많다. 만약, 사이버 공격이 1선 차단 체계를 회피해 유입된다면 보다 포괄적인 개념의 탐지 & 대응이 필요하다. 이 때, AhnLab EDR과 MDR 서비스를 활용하면 폭 넓은 가시성을 바탕으로 위협에 대응할 수 있다.

A. AhnLab EDR: 검증된 위협 탐지 & 대응 역량

앞서 소개한 바와 같이 AhnLab EDR은 BPFDoor 연관 행위를 상세하게 탐지해 분석한 바 있다. 이처럼, 엔드포인트에서 발생하는 모든 행위를 모니터링 및 로깅하고 행위 연관관계와 맥락을 분석하여, 어떠한 위협도 올바르게 이해하고 대응할 수 있도록 지원한다. 이처럼 탁월한 맥락 분석 역량은 유입된 공격으로 인한 피해를 최소화할 뿐만 아니라 향후 재발 방지 체계 수립에도 큰 도움이 된다.

B. MDR 서비스: 전문가와 함께하는 강력한 탐지 & 대응

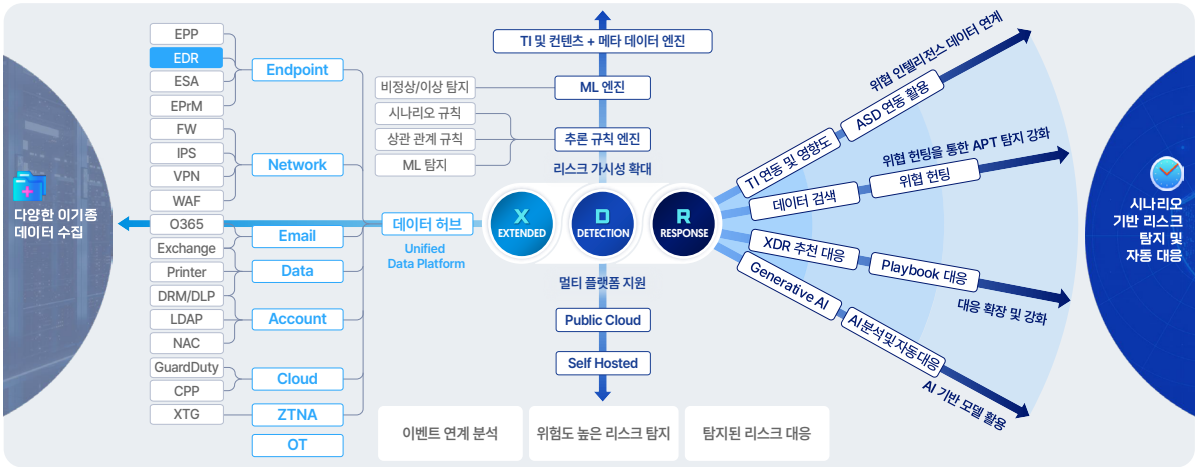
운영에 전문성이 요구되는 EDR은 규모가 작은 기업들에게 관리가 쉽지 않을 수 있다. 안랩의 MDR 서비스는 업계 최고 전문가들이 탐지, 분석 및 맞춤형 대응을 지원하여 고객의 운영 부담을 줄이는 동시에 탐지 & 대응 역량을 한 차원 끌어 올린다.

❸ 운영 및 협업

최신 사이버 위협은 엔드포인트, 네트워크, 클라우드, 이메일 등 다양한 도메인을 넘나들면서 조직의 자산을 노린다. 이러한 위협을 포인트 솔루션 기반으로 대응할 경우, 가시성이 떨어지고 관리 측면에서도 한계가 있다. 따라서, 조직 전반의 리스크를 통합 관리할 수 있는 플랫폼과 전문 서비스 결합의 필요성이 대두되고 있다.

A. AhnLab XDR: 통합 기반 체계적인 리스크 관리

통합 리스크 관리 플랫폼 AhnLab XDR은 다양한 영역에서 수집되는 데이터를 분석 및 정규화하여 리스크를 지수화하고 사이버 공격의 연관관계를 시각화한다. 또한, Open XDR을 지향하여 다양한 보안 솔루션들과 유연하게 연동해 최적의 대응 방안을 제시한다. XDR의 탐지, 분석 및 대응을 지원하는 AI 기술도 탑재되어 있어 한 층 편리한 리스크 관리가 가능하다.



[그림 5] AhnLab XDR 기반 리스크 관리 개념도

B. MXDR 서비스: 고품질 탐지 & 대응과 위협 헌팅

모든 보안 영역을 아우르는 XDR 플랫폼 운영 역시 일정 수준 이상의 전문성을 필요로 한다. 고객의 XDR 운영을 지원하는 MXDR 서비스는 자사 전문가가 XDR의 이벤트를 지속적으로 모니터링하고 탐지된 리스크를 상세하게 분석한다. 뿐만 아니라, 리스크의 내부 영향도를 판단해 대응하고 능동적인 위협 헌팅까지 지원하여 보다 능동적으로 침해를 예방할 수 있다.

5. 맺음말: 최고의 플랫폼과 전문가의 시너지가 필요한 때

최근 글로벌 트렌드를 보면 '협력'의 가치를 강조하는 추세다. 고도화를 거듭하는 사이버 위협 대응을 위해 최고 수준의 솔루션 뿐만 아니라 사람 간 협업이 중요하다는 의미이기도 하다. 그 어떤 보안 솔루션도 완벽할 수 없기에 한계가 존재하기 마련이고, 이 한계는 유연한 연동 기반의 통합 보안 접근과 사람의 전문성을 결합해 극복해 나가야 한다.

안랩은 앞으로도 본 문서에서 소개한 차세대 보안 모델을 기반으로 보안 플랫폼과 전문가의 시너지를 결합하여 고객이 빈틈 없는 보안 체계를 구축해 나갈 수 있도록 앞장 설 계획이다.

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901