보안은 정보전, 위협 인텔리전스로 대응을 앞당기다

오늘날 가장 많이 언급되는 단어 중 하나는 인텔리전스(Intelligence)다. 인공지능(Artificial Intelligence)을 떠올린다. 하지만 정보보안 분야에서의 인텔리전스는 위협 인텔리전스(Threat Intelligence, TI)라는 의미로도 많이 사용된다.

정보보안에서의 인텔리전스는 정보 수집과 분석의 과정 및 그 결과인 '정보' 그 자체를 나타내는 개념이다. 이는 사이버 위협을 예측하고 방어하는 데 필요한 정보이며, 단순한 데이터가 아니라 조직이 실제 보안 의사결정을 내리는 데 활용할 수 있는 정보다. 반면, AI에서의 인텔리전스는 기계가 사람처럼 학습하고 추론하는 능력을 의미한다. 이 둘은 서로 다른 개념이지만 시간이 지나면서 점점 합쳐지는 추세다.

위협 인텔리전스란?

위협 인텔리전스는 외부에서 끊임없이 발생하는 사이버 위협 정보를 수집하고 분석해 활용할 수 있도록 가공한 정보다. 이를 통해 기업은 사이버 위협을 예측하고 사전에 방어할 수 있다. 그 효용성은 다음 세 가지 키워드로 설명 가능하다.

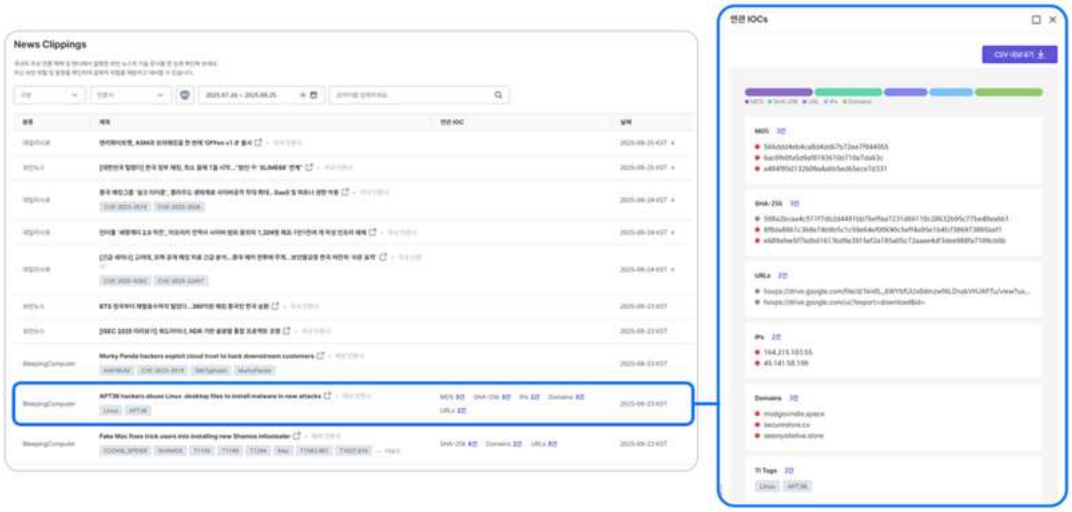
- 타산지석: 해킹 피해 사례와 정보를 교훈 삼아 보안을 강화하고 유사 위협을 차단
- 하인리히 법칙: 큰 사건 이전에 반복되는 경미하거나 잠재적인 패턴을 파악해 위험 신호 조기 감지
- 킬체인 전략: 공격이 발생하기 전에 공격 체인을 끊어 피해를 예방

위협 인텔리전스를 효과적으로 활용하면 기업 내외부에서 발생하는 침해사고를 빠르게 파악하고, 수집한 정보를 바탕으로 공격을 사전에 무력화할 수 있다. 하지만 방대한 정보를 직접 수집하고, 자사에 위협이 되는지를 분석한 뒤 보안 정책에 적용하는 과정은 내부 보안팀이 홀로 감당하기 어렵다. 이때 필요한 것이 바로 위협 인텔리전스 플랫폼(Threat Intelligence Platform, TIP)다.

그렇다면 실제 현장에서 보안 담당자들은 어떤 어려움을 겪고 있으며, 위협 인텔리전스는 이를 어떻게 해결할 수 있을까? 현장 보안 담당자들의 고민과 안랩의 위협 인텔리전스 플랫폼 AhnLab TIP가 제시하는 솔루션을 문답 형식으로 살펴보자.

Q1. 아침마다 여기저기 보안 뉴스 찾아다니기 너무 힘들어요.

매일 쏟아지는 보안 뉴스를 실시간으로 추적해 신뢰할 수 있는 소스인지 판별하고, 기업에 실제 영향을 주는지 분석하는 작업은 기본적으로 많은 시간이 소요된다. 그리고, 항상 반복되는 업무로 인해 보안 담당자에게 큰 피로감을 준다. AhnLab TIP는 이 문제를 해소하기 위해 보안 벤더, 연구기관 보고서, 주요 미디어 등 신뢰할 수 있는 소스를 모니터링하고 중요한 뉴스를 선별하여 한 눈에 확인 가능하도록 정리한다. 그리고, 이를 이메일과 AhnLab TIP 플랫폼 상에서 제공한다.



[그림 1] 뉴스 클리핑 및 연관 IoC 정보

AhnLab TIP는 단순 뉴스 제공에 그치지 않고, 관련 침해지표(Indicator of Compromise, IoC)까지 함께 제공한다. 고객 입장에서는 뉴스와 연관된 IoC 및 상세 분석 정보를 확인해 조직에 미치는 영향도를 파악할 수 있다. 보안 담당자는 매일 뉴스 검색에 쏟던 시간을 줄이고, 곧바로 대응이 필요한 위

협에만 집중할 수 있다.

Q2. 주간/월간으로 위협 동향을 정리해서 보고하는 일이 많아요.

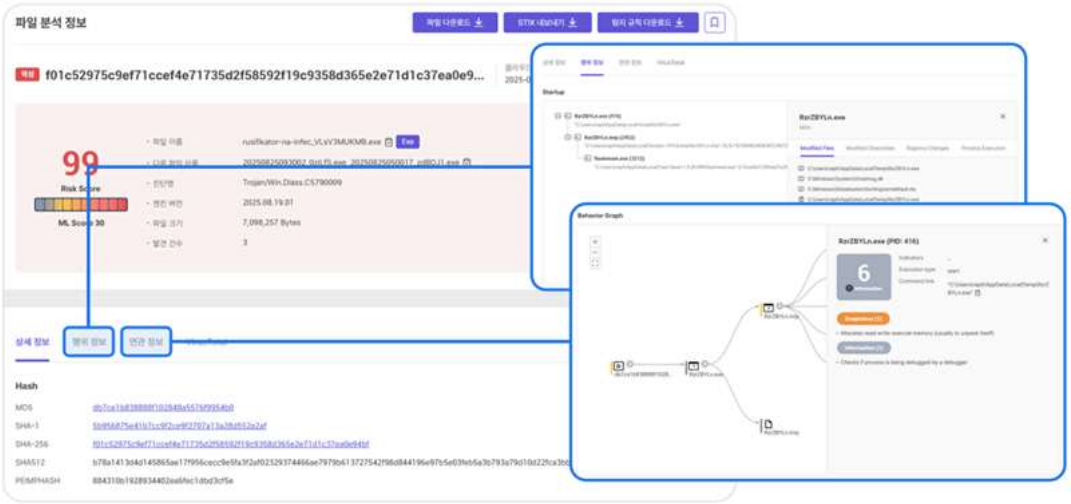
보안 담당자들의 또 다른 고민은 위협 정보를 단순히 모으는 데 그치지 않고 유형과 기간별로 정리해 이해하기 쉽게 보고해야 한다는 점이다. 특히 비전문가도 쉽게 이해할 수 있도록 가공하는 과정에서 큰 부담을 느낀다. AhnLab TIP는 악성코드, 네트워크 침해, 산업별 현황 등에 대한 위협 통계를 대시보드로 제공하여 사용자가 동향을 한 눈에 파악할 수 있도록 한다. 또한, 위협 동향 보고서를 주간, 월간, 연간 단위로 발간한다. 이를 토대로 보안 담당자는 최신 위협 동향을 신속하게 파악하고, 내부 보고서 작성 업무의 부담을 크게 줄일 수 있다.

[그림 2] 위협 통계 대시보드

Q3. 신뢰할 수 있는 IoC 확보가 필요해요.

침해 정보와 뉴스를 수집한 후 이를 자사 보안 강화에 활용하기 위해서는 검증된 IoC가 꼭 필요하다. 보안의 특성 상 최신 IoC를 빠르게 확인해야 하는 경우가 많지만, IoC를 찾는 것 자체가 쉽지 않고 검증되지 않은 IoC를 활용할 경우 미탐 혹은 오탐과 같은 문제도 발생한다. 이 때문에 신뢰할 수 있는 IoC를 빠르게 확보하는 것이 굉장히 중요하다.

AhnLab TIP는 30년 넘게 축적한 위협 분석 전문성을 바탕으로 침해 뉴스 관련 해시값, 악성코드 진단명, 행위 정보, 연관 지역, 파일·URL·IP 등 신뢰 가능한 IoC를 실시간으로 제공한다. 이 중에는 다른 곳에서는 찾아볼 수 없는 안랩만의 IoC와 중국 및 북한 공격 그룹에 대한 차별화된 IoC들도 포함된다. 이를 통해, 보안 담당자는 위협을 보다 입체적으로 이해하고 선제적으로 대응할 수 있다.

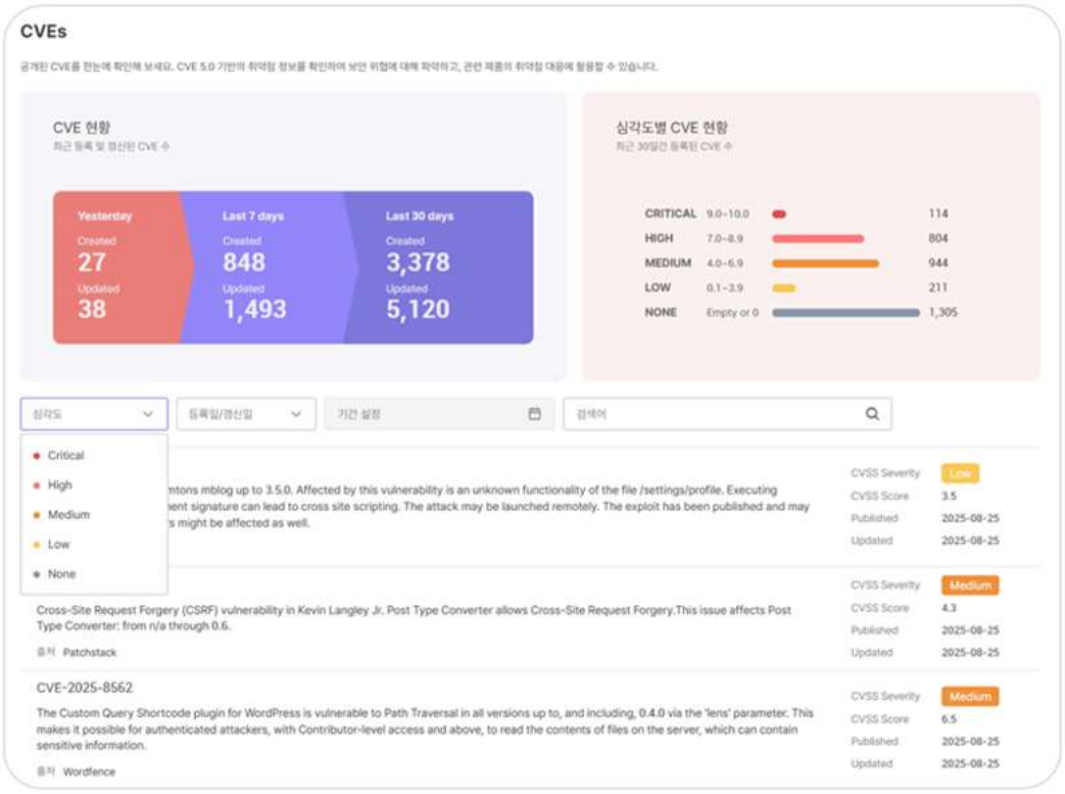


[그림 3] IoC와 상세 분석 정보

또한, AhnLab TIP는 API 연동도 지원하여 고객이 IoC를 IPS, IDS, 방화벽 등 사내 보안 장비 차단 리스트에 신속하게 반영할 수 있도록 한다. 이를 통해, 실제 위협 대응 속도를 크게 높일 수 있다.

Q4. 새로운 취약점 나오면 바로 알고 싶어요.

기업의 지속적인 보안 유지를 위해서는 사용 중인 모든 자산에 대한 신규 취약점을 신속히 파악하고, 심각도에 따라 우선순위를 정해 조치해야 한다. AhnLab TIP는 이와 같은 취약점 정보와 점수를 쉽게 확인할 수 있도록 공개된 CVE(Common Vulnerabilities and Exposures) 정보를 종합해 제공한다.

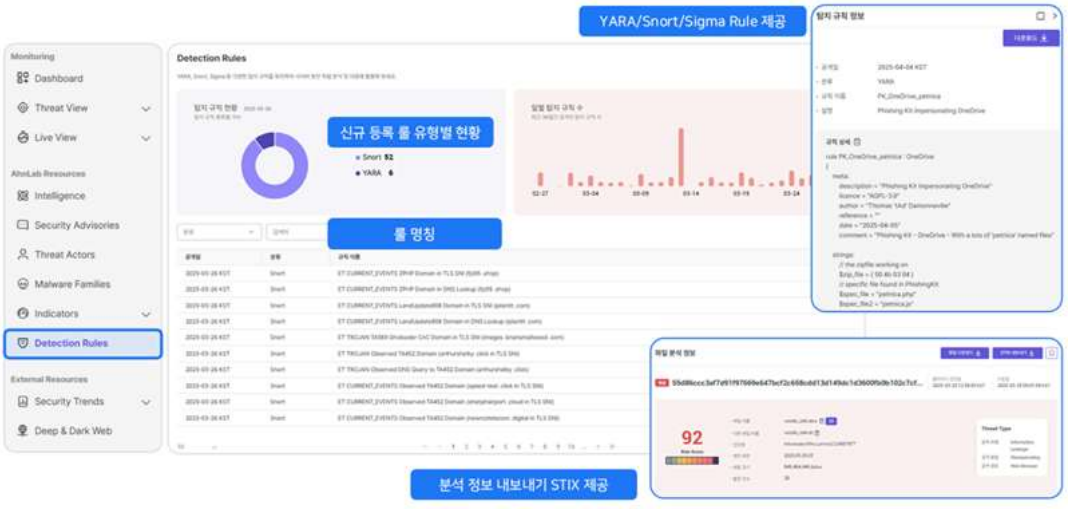


[그림 4] CVE 정보

AhnLab TIP에서는 심각도와 영향도가 높은 취약점은 사용자가 빠르게 확인할 수 있도록 보안 권고문으로 제공한다. 실제 침해에 악용된 취약점은 별도 구분하여 'Notes' 형태로 공유한다. 최신 취약점이 아니더라도 지속적으로 활용되고, 특정 고객에게 영향을 줄 수 있는 취약점은 별도 보고서 제작해 제공한다. 보안 담당자들은 필요한 CVE 정보를 빠르게 파악하고 이를 활용하여 자산을 적시에 패치해 보안을 강화할 수 있다.

Q5. 옆 회사가 해킹 당했다는데, 우리도 위험한지 알고 싶어요.

침해 사고가 발생하면 많은 기업들이 "우리도 비슷한 공격에 노출될 수 있을까?"라는 의문을 갖는다. 하지만 공격 발생 직후에는 상세 정보 접근이 제한되어 필요한 정보를 신속하게 수집하기 어렵다. 정보를 확인했다 하더라도 공격 시뮬레이션 역량이 부족해 실제 활용하지 못하는 경우도 많다. 이러한 이유로 기업들은 해당 공격이 자사와 유사한 환경에서 발생했는지 판단하고 효과적인 대응 전략을 수립하는 데 난항을 겪는다.

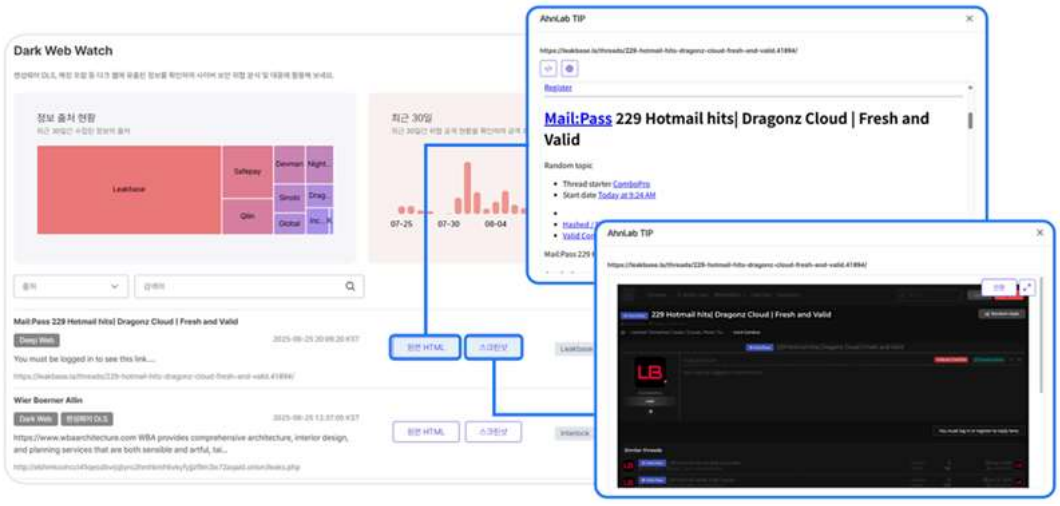


[그림 5] 침해 사고 탐지 룰

안랩은 최근 발생한 침해 사고에 대한 TTPs(Tactics, Techniques and Procedures) 분석 보고서 및 탐지 룰을 제공해 고객들이 유사 위협에 빠르게 대응할 수 있도록 한다. AhnLab TIP에서는 신규 등록된 룰의 유형별 현황, 룰 명칭, YARA, Snort, Sigma 룰 등도 확인 가능하다. 보안 담당자는 이와 같은 정보들을 토대로 유사 공격의 영향도를 판단하고 편리하게 조치를 취할 수 있다.

Q6. 다크웹에 우리 정보 올라왔는지 계속 걱정돼요.

기업들의 유출 정보는 다크웹에서 활발하게 거래된다. 하지만, 다크웹 접근 및 지속적 모니터링을 수행할 전문 역량을 갖춘 기업들은 극히 드물다. 이로 인해, 데이터 유출 여부를 정확히 확인하고 허위 게시물을 판별하는 데 어려움을 겪는다. AhnLab TIP는 이러한 문제를 해결하기 위해 다크웹 모니터링을 핵심 기능 중 하나로 제공하고 있다.

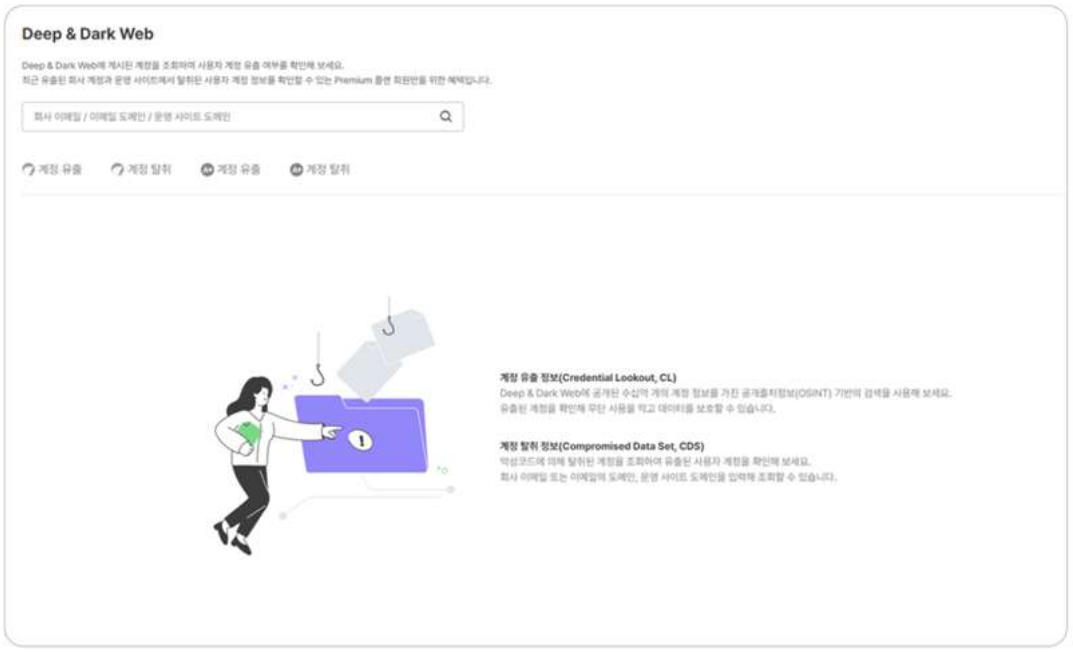


[그림 6] 다크웹 모니터링

AhnLab TIP는 다크웹 포럼과 랜섬웨어 DLS(Dedicated Leak Sites)를 실시간으로 모니터링해 수집된 HTML과 스크린샷 정보를 제공한다. 공격자가 포스팅한 게시물을 분석해 게시 의도, 대상 및 신뢰도에 관한 정보도 함께 전달한다. 실제 피해로 이어질 가능성이 있을 경우 이를 대상 기업에 빠르게 알려 대응할 수 있도록 지원한다.

Q7. 우리 회사 계정은 노출되지 않았을까요?

다크웹에서 흔히 거래되는 정보 중 하나가 기업 계정이다. 공격자들은 초기 침투를 위해 유출된 계정을 구매하고, 이를 공격 캠페인에 사용한다. 계정 노출 여부를 빠르게 확인하는 것이 중요하지만 출처에 대한 접근이 제한적이다. 직원 수가 많을수록 지속적인 모니터링은 더욱 어려워진다.

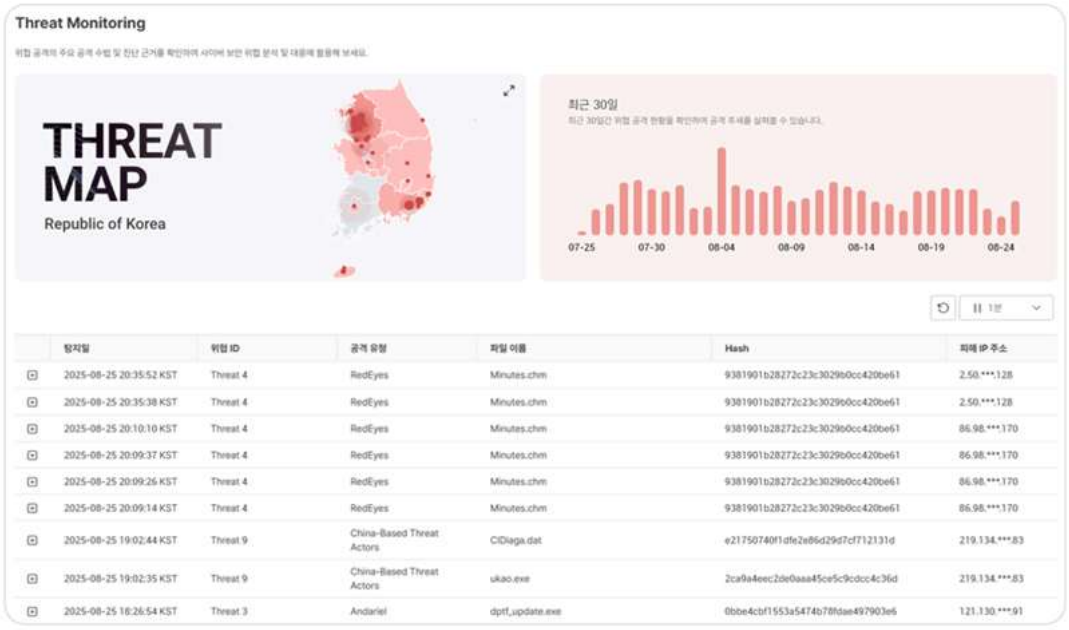


[그림 7] 유출 계정 검색 창

AhnLab TIP에서 회사 도메인 혹은 이메일을 입력하면 유출된 계정 정보를 수집해 보여준다. 또한, 최근 인포스틸러와 C2로 활용되는 텔레그램을 모니터링하여 실시간으로 유출 현황을 파악할 수 있도록 한다. 보안 담당자는 기업 계정의 유출 현황을 실시간으로 파악하고, 유출 정황이 포착되면 신속하게 조치해 피해를 방지할 수 있다.

Q8. 뉴스보다 먼저 공격자의 활동을 알고 싶어요.

해킹 피해를 최소화하기 위해서는 공격자의 활동을 모니터링하고 관련 정보를 수집해 선제적으로 대응할 수 있어야 한다. 하지만, 미디어 등 대외적으로 공개된 정보를 통해 인지할 경우 이미 늦은 경우들도 있다.

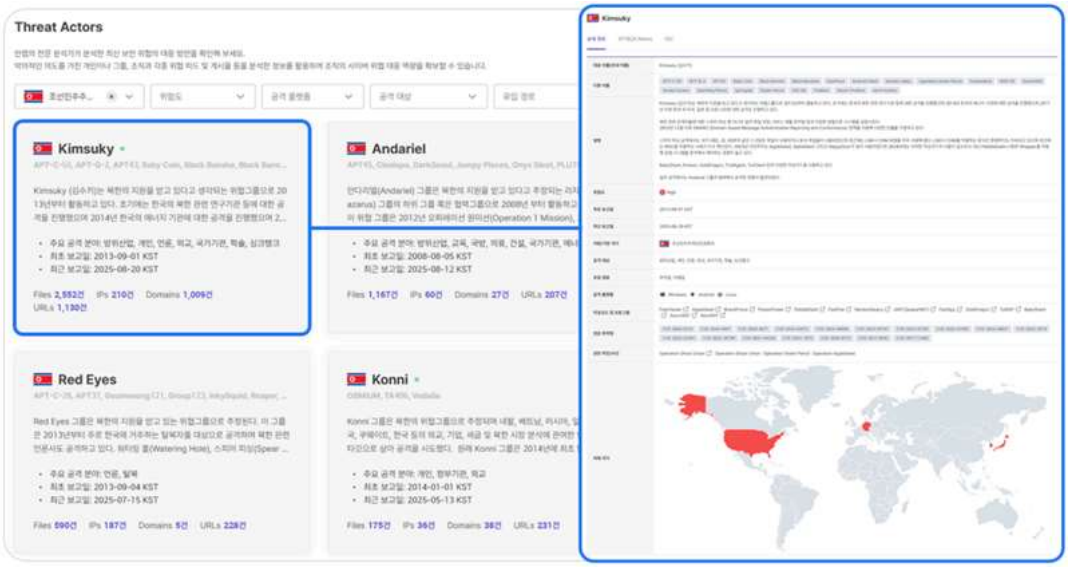


[그림 8] 공격 활동 모니터링

AhnLab TIP는 다양한 탐지 룰을 적용해 공격자와 연관된 IP에서 발생하는 공격 활동을 실시간으로 모니터링한다. 이렇게 수집된 위협 정보는 최신 사건, 이슈, 동향은 물론 보안 전문가의 의견과 조언까지 함께 정리해 제공된다. 기업들은 뉴스보다 빠르게 공격 징후를 파악하고 사이버 위협에 선제적으로 대응하는 데 활용할 수 있다.

Q9. 한국을 목표로 활동하는 국가 기반 공격 그룹 정보가 필요해요.

중국이나 북한 등에서 활동하는 APT 그룹은 국내 기업을 표적으로 삼는 경우가 많다. 한국의 기업/기관들 입장에서는 이들의 활동을 추적하고 대응 정보를 확보하는 것이 중요하다.



[그림 9] 위협 행위자 분석 화면

안랩은 전 세계 약 400개 위협 행위자(Threat Actor)들의 활동을 모니터링, 분석 및 추적한다. 특히, 한국 조직들을 대상으로 활발하게 공격을 수행하는 중국 및 북한 배후 공격 그룹들에 대해 업계에서 손 꼽히는 분석 역량을 갖추고 있다. 안랩은 자체적으로 개발한 분류 체계에 따라 각 공격 그룹들을 국가별로 관리하고, 사용자들에게 공격 그룹의 개요, 공격 기법, 주요 공격 대상 등의 분석 정보를 제공한다. 또한, 공격 그룹 추적 보고서를 수시로 제공하여 사용자들이 국가 기반 공격 그룹에 효과적으로 대응할 수 있도록 한다.

Q10. 위협에 대한 상세 분석 보고서가 필요해요.

많은 기업이 위협에 대한 상세 분석 보고서를 필요로 하지만 이를 제작할 전문 인력이 부족한 경우가 많다. 특히 보고서에는 공격 체인 시각화, 내부 취약점과 외부 위협 매핑 등 높은 수준의 분석 역량이 필요한 작업이 포함되기 때문에 작성 난이도가 높다.

AhnLab TIP는 위협을 다각도로 분석하고 체계적으로 정리해 아래 표와 같이 다양한 유형의 보고서를 제공한다. 이를 통해 전문 인력이 부족한 기업도 전문성과 신뢰도를 갖춘 분석 보고서를 확보할 수 있다.

유형	설명	종류
위협 Notes	• 고객에 전달이 필요한 다양한 보안 위협 정보 • 신속성에 중점	• 공격자 활동 • 침해사고 • 공격 기법
다크웹 Notes	• 다크웹 포럼, 랜섬웨어 DLS에서 파악한 기업 정보 • 신속성에 중점 • 정보 정확성, 피해 범위 등 검증 후 보강	• 다크웹 노출(정보/계정 유출) • 랜섬웨어 DLS
분석 보고서	• 공격 그룹, 기법, 취약점, 악성코드 등 심층 분석 • 신속성보다 정확하고 유니크한 정보에 중점	• 공격 그룹 분석 보고서 • 공격 기법 분석 보고서 • 취약점 분석 보고서 • 악성코드 분석 보고서 • 포렌식 분석 보고서
동향 보고서	• 각 위협 별 통계 및 동향 정보 • 위협 변화 추이를 지속적으로 파악	• CERT Report • 랜섬웨어 동향 보고서 • 인포스틸러 동향 보고서

		• APT Group 동향 보고서 • 산업별 위협 동향 보고서 (금융) • 지역/국가별 위협 동향 보고서 • 스미싱 동향 보고서 • 연간 보고서

[표] AhnLab TIP 분석 보고서 목록

맺음말

이번 글에서는 보안 담당자들이 현장에서 마주하는 10가지 고민을 중심으로 위협 인텔리전스 활용 방안을 살펴봤다. 수많은 위협 정보 속에서 의미 있는 데이터를 선별하고 맥락을 분석하는 과정은 쉽지 않다. 하지만 갈수록 복잡해지는 위협 환경에서 이 과정은 더 이상 선택이 아닌 필수다.

위협 인텔리전스는 단순히 사고 발생 후 대응하는 수준을 넘어, 공격을 사전에 차단하고 피해 확산을 방지하는 선제적 보안(Proactive Security)으로의 전환을 가능하게 한다. 특히, 단순 IoC 기반 차단이 아니라 공격의 배경과 맥락까지 파악해 기업이 수동적인 방어자가 아닌 능동적인 대응 주체로 자리 잡을 수 있다.

보안은 협력 없이는 완성될 수 없다. 각 기업이 수집한 위협 정보와 안랩과 같은 보안 기업의 전문 분석이 결합될 때 더욱 강력한 방어망을 구축할 수 있다. AhnLab TIP는 앞으로도 양질의 위협 인텔리전스를 신속하게 제공하여 변화하는 사이버 위협 환경에서 신뢰할 수 있는 플랫폼이자 파트너로서 역할을 다해 나갈 것이다.

AhnLab TIP 구독 문의 및 체험 신청은 TIP 포털에서 진행 가능하다.

▶ TIP 포털 바로가기

AhnLab
A-FIRST팀 이명수 팀장