Headline

AI 기반 보안관제 고도화 전략 및 발전 방향

MSS 사업그룹/Secudium 고도화팀 김종현 팀장

■ 개요

한국인터넷진흥원(KISA)에 따르면, 지난해 상반기 침해사고 신고 건수는 664 건으로 전년 동기대비 40% 증가한 것으로 나타났다. 사물인터넷과 커넥티드 기기 사용의 증가, 클라우드 도입과 하이브리드 근무 모델 등을 비롯한 디지털 전환의 가속화로 '공격 표면(Attack Surface)'이 확대되면서 새로운 취약점이 늘고 있다.

보안관제 서비스는 24 시간 365 일 위협 모니터링을 지원한다. 실시간으로 쏟아져 들어오는 수많은 보안 위협에 대한 정확한 판단과 빠른 대응이 필요한만큼, 다양한 사이버 보안 영역 중 특히 힘들고 고단한 업무로 꼽힌다. 무엇보다 해커는 불특정 국가에서 IT 자산을 타깃으로 다양한 방식으로 공격을 시도하고 있으며, 해킹 기술 또한 날로 지능화되고 있기 때문에 밤낮으로 긴장을 늦출 수 없다.

■ 기존 보안관제의 어려움

24 시간 365 일 위협을 모니터링하는 관제 특성상 근본적인 어려움이 존재한다. 이번 보고서를 통해 크게 3 가지 어려움에 대해 살펴보도록 한다.

질문 1. 모든 수집/로그 이벤트를 분석하고 있는가?

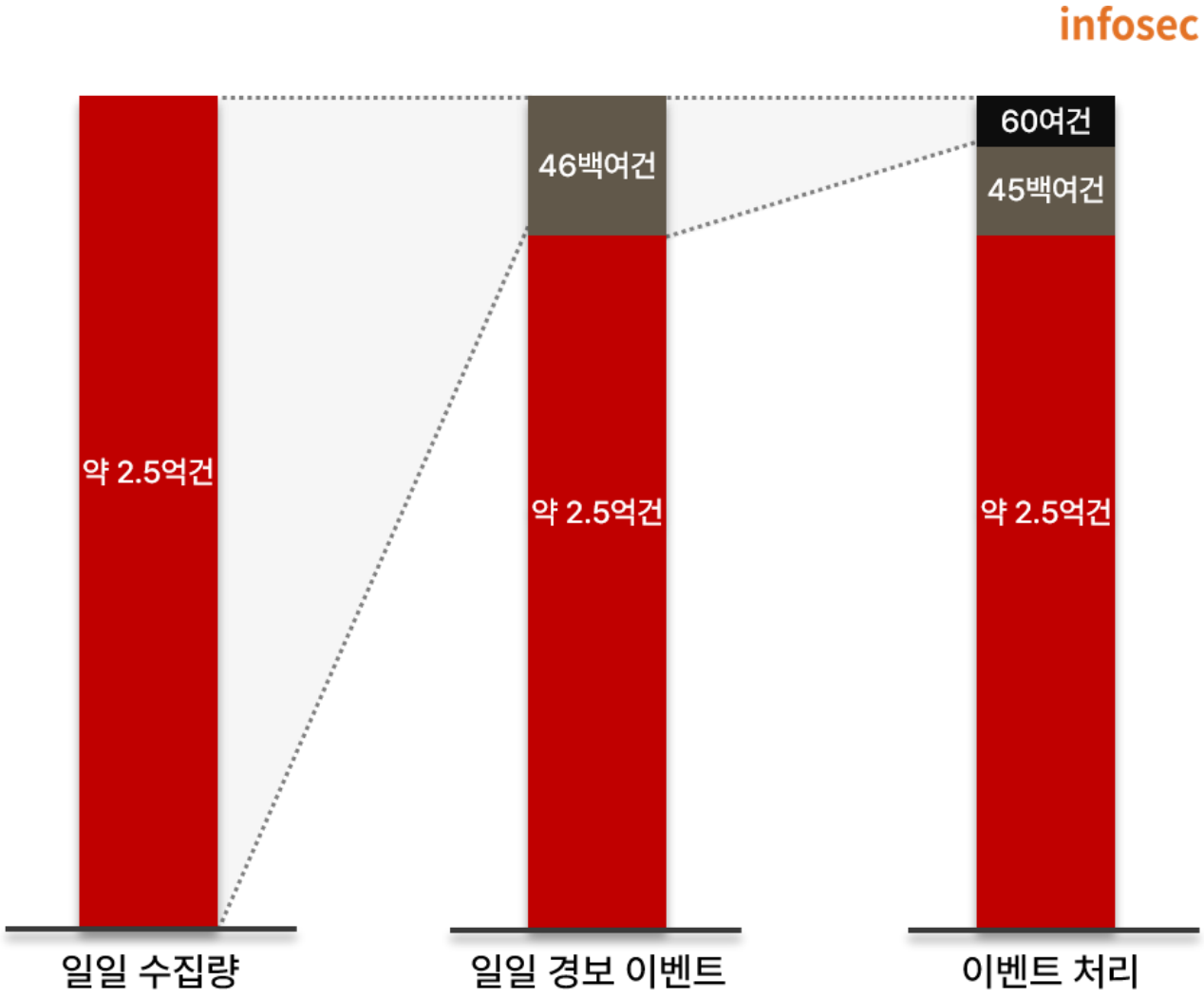


그림 1. 위협 이벤트 현황

위 그림은 A 기업 관제센터에서 수집 및 처리된 위협 이벤트 현황을 나타낸 그래프다. 일일 약 2.5 억 건을 수집하여 관제 플랫폼에서 46 백여 건의 경고를 발생시키고 있으며, 이 중 우선순위에 따라 60 여 건의 위협을 분석/대응하고 있다. 분석되지 않은 경고 45 백여 건은 정말로 안전한 것인지, 경고로 발생되지 않은 약 2.5 억 로그에 보안위협은 없는 것인지 의문을 가질 수 있다.

질문 2. 침해위협 탐지/분석 일관성은 유지되고 있는가?

보안관제사는 위협을 판단하기 위해 수집한 로그의 원본 데이터(Raw-Data)를 확인하거나 바이러스토탈(VirusTotal)과 같은 Reputation DB 또는 Threat Intelligence 등을 활용하고 있다.

그림 2. 위협 판단 시 활용하는 자료

1) Raw-Data 가 난독화 되어 있어 즉시 확인이 안되거나, 복호화 하여도 기술의 난이도에 따라 판단이 어렵다면? 2) VirusTotal 의 91 개 분석 엔진 중 89 개가 정상이고, 2 개의 엔진에서만 의심스럽다고 탐지한다면, 이것은 위협으로 봐야 할까? 정상으로 판단해야 할까? 3) Threat Intelligence 에서 조회결과 C&C IP 로 확인을 했지만, 최종 활동 날짜가 2~3 년 전이라면? 이것을 위협이라고 판단할 수 있을까?

위 3 가지 사항에 대해서는 보안관제사마다 모두 다른 판단을 할 수 있으며, 이에 대해서 문제가 있다고 하기도 어려울 것이다.

질문 3. 새로운 공격, 늘어나는 공격 표면, 이를 탐지하기 위한 신규 보안장비, 늘어나는 보안 로그들에 대해서는 어떻게 대응하고 있는가?

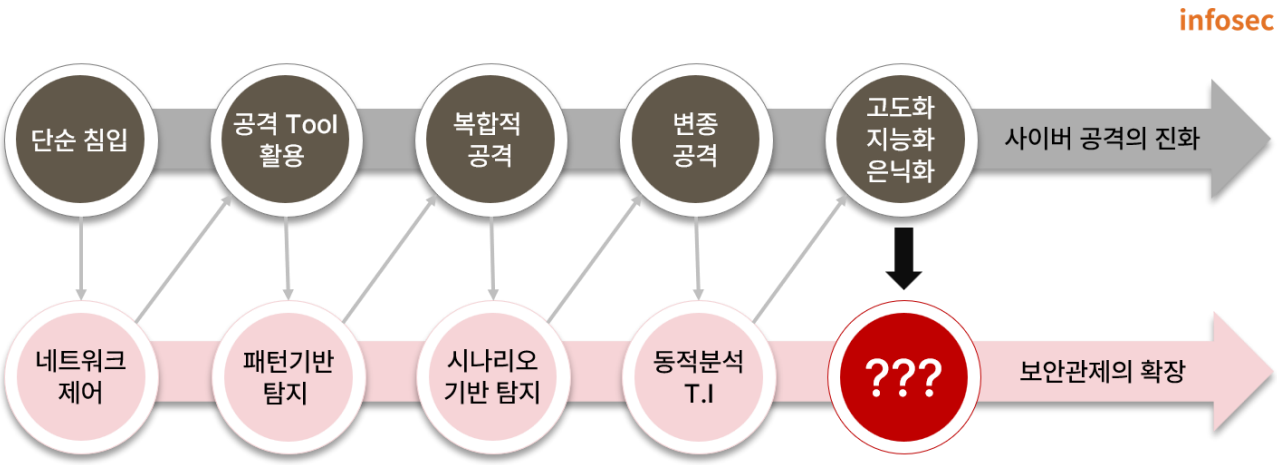


그림 3. 사이버공격 진화 및 보안관제

초기 단순 공격은 방화벽 IP 차단만으로 방어가 가능했다. 자동화 Tool 사용시 IDS/IPS/WAF 에 탐지 패턴을 등록해 방어를 수행했으며, 좀 더 다양한 공격 시도에는 보안 로그 상관분석으로 대응이 가능했다.

최근의 악성 파일 기반 공격에 대해서는 APT 탐지 솔루션을 통해 동적분석/T.I(Threat Intelligence) 탐지,분석,대응을 할 수 있다. 그렇다면 향후 AI 를 활용한 고도화/지능화/은닉화 된 공격은 어떻게 대응할 것인지에 대한 고민이 필요하다.

2023 년 마지막 발표 취약점은 CVE-2023-24151 로 일일 평균 66 개의 취약점이 새로 발표됐으며, 보안 대상도 Cloud, OT/ICS 로 확대되고 있다. 또한, 이를 대응하기 위해 Micro-Segmentation, ASM, SASE 등의 새로운 보안 장비들이 보안관제 대상으로 확대되고 있다.

따라서 보안관제는 늘어나는 보안로그를 분석해 새로운 위협에 대응해야 한다. 보안관제에서 모두 커버할 수 있을지에 대한 우려도 존재한다. 공격자는 한번의 공격만 성공하면 되지만, 보안관제는 한번의 실수도 있어서는 안되기 때문이다.

■ AI 기반 보안관제

지금까지 보안관제가 가지고 있는 한계에 대해 알아보았다. 한계를 보완하기 위해서는 머신의 도움을 받아 “모든 수집 이벤트에 대해 실시간으로 빠르게 분석하고 판단해 대응”하는 것이 중요하다. 특히 AI 를 결합한다면 보안관제가 가지고 있는 많은 한계를 극복하는 데 도움을 받을 수 있다.

앞서 제기된 첫 번째 질문인 “모든 수집/로그 이벤트를 분석하고 있는가?”와 세 번째 질문인 “새로운 공격의 증가”를 좀 더 요약하면, Un-known 위협을 탐지할 수 있는가? 라는 질문이 될 수 있다. 이미 알고 있는 위협이라면 탐지 패턴을 생성하거나 상관분석 Rule 을 만들어 Threat Intelligence 를 통해 탐지할 수 있기 때문이다. 즉, Un-known 위협을 효과적으로 탐지하기 위해서는 전체 수집 로그에서 다른 특성을 가지는 로그가 포함되어 있는지를 모니터링하는 것이 중요하다.

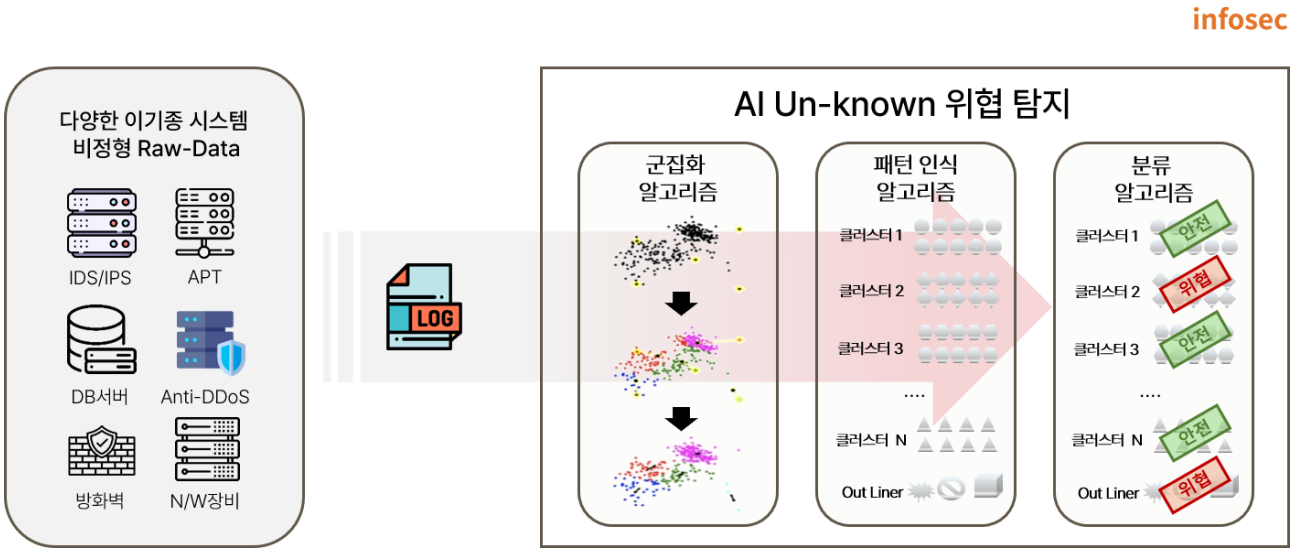


그림 4. AI 기반 Un-known 위협 탐지

AI 는 유사한 항목별로 구분하는 ‘군집화’ 기능이 뛰어나다. 이를 위해서는 아래와 같이 단계를 거쳐 AI 학습 및 활용이 가능하다.

- 초기에는 일정 기간 동안 데이터를 모아 초기 학습 모델을 수행한다. 분류된 각 군집에 대해서 안전한지, 위협인지를 파악하는 라벨링(Labeling)을 수행한다.
- 이후에는 Labeling 을 통해 위협이 될 수 있는 로그를 분석한다.
- 지속적으로 학습을 진행하게 되면, 초기에 어느 군집에도 포함되지 않던 Out-Liner 가 계속적으로 축소된다. 이후 모니터링에서는 “Labeling 된 위협”과 “Out-Liner”를 탐지/분석함으로써 Un-known 위협을 탐지할 수 있다.

두 번째 질문인 **"침해위협 탐지/분석에 대한 일관성은 유지되고 있는가?"**는 관제사들의 정·오탐 판단에 대한 부분이다. 위협 판단에 경험이 필요하기 때문에 신입관제사와 3~4 년 이상의 경력을 가진 관제사의 판단은 서로 다를 수 있다.

이러한 경험에 의한 판단은 어디 있을까? 기존에 판단했던 정·오탐 결과들이 경험을 반영하고 있다. 정·오탐 판정은 기본적으로 개와 고양이를 구분하는 AI 와 동일하다.

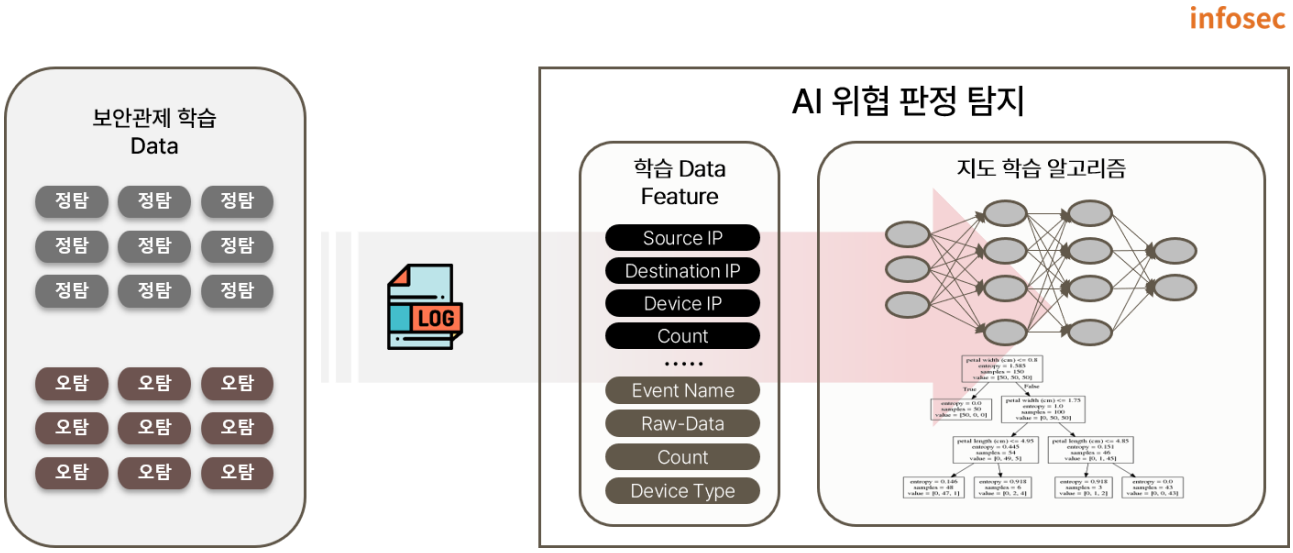


그림 5. 데이터 학습을 통한 AI 위협 판정 탐지

- AI 학습을 위한 데이터(Data)를 확보하는 게 가장 중요하다. 정확한 정·오탐 판정 결과 Data 를 확보해 학습을 진행한다.
- 과대적합[1], 과소적합[2]이 발생되지 않도록 다양한 Data 에 대한 학습을 진행한다.
- Training Data 와 TEST Data 의 준비
  - Training Data 와 TEST Data 는 동일한 비율의 정·오탐 분포를 가져야 한다.
  - Training Data 와 TEST Data 는 중복되는 데이터가 없어야 한다.

지금까지 앞에서 언급한 보안관제의 한계와 AI 를 통해 이를 해결할 수 있는 방안에 대해 살펴봤다. 위협을 탐지하는 관점에서 살펴본 것으로 실제 보안관제는 탐지 이후에 **위협 분석, 긴급 대응, 결과 보고 등의 업무**가 진행된다. 특히, 최근 주목받고 있는 생성형 AI 가 많은 도움이 될 것으로 기대한다.

[1] 과대적합: 지나치게 학습 데이터에 최적화되어, 새로운 데이터에 대한 판단을 하지 못하는 현상

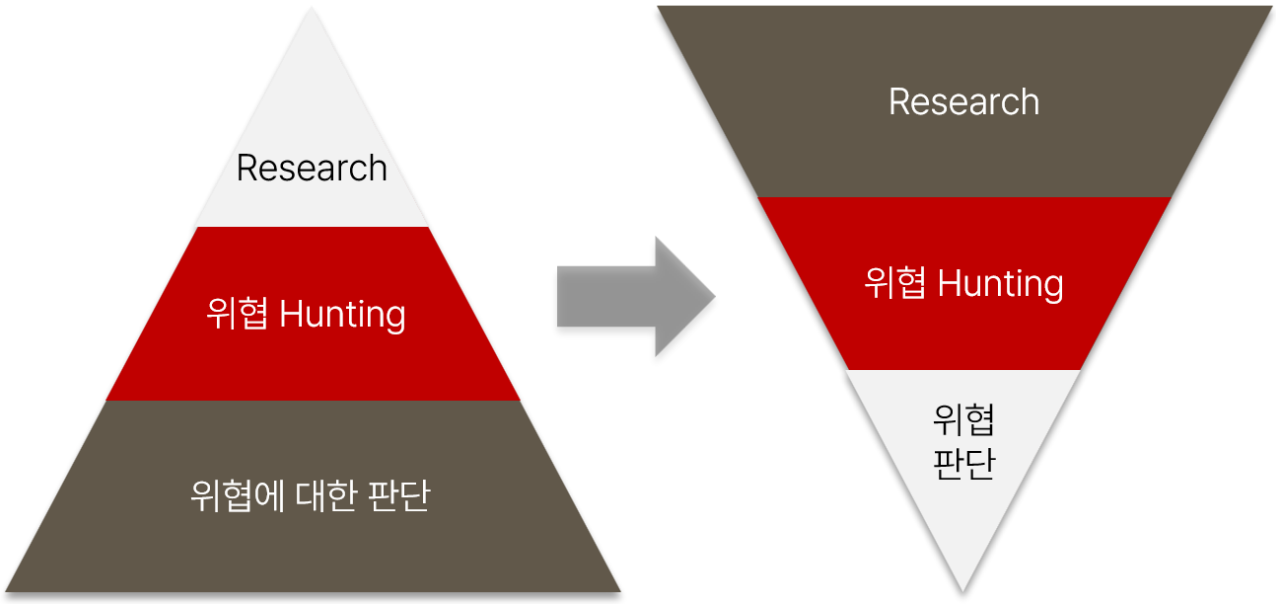
[2] 과소적합: 학습이 부족하여 데이터의 구조/패턴을 반영하지 못하는 현상

생성형 AI 는 자연어를 인식해 다양한 행위를 할 수 있다. 분석 과정에서는 다양한 조회, 검증을 위한 코드 작성 등을 수행할 수 있고, 대응 과정에서는 SOAR(Security Orchestration, Automation and Response)와 연계해 실시간 위협 대응 조치 수행, 대응 전략 수립 및 위협도를 평가할 수 있다. 또, Chat 을 통한 고객 소통 및 문의 대응과 결과 보고를 위한 보고서 작성 등을 수행할 수 있을 것으로 기대하고 있다.

그림 6. 보안관제에서의 AI 활용

SK 쉴더스 시큐디움(Secudium) 센터는 과탐 및 오탐 최소화를 위한 목적으로 AI 를 개발한 뒤 2022 년 6 월 이후 플랫폼에 적용해 운영 중이다. 전체 탐지 위협 중 47%를 AI 를 활용해 자동으로 업무를 수행하고 있으며, 이를 위해 약 7,800 만 건의 Data 가 학습에 사용됐다.

■ 맺음말



지금까지 보안관제 업무의 어려움과 AI 기반 보안관제의 고도화 전략 및 발전 방향에 대해 알아봤다. AI 를 보안관제에 적용 시 '효율화'를 가장 먼저 떠올릴 수 있다. AI 를 활용하는 만큼 관제센터의 인력과 비용을 줄이는 게 가능해질 것이라는 기대감 때문이다.

하지만, AI 는 관제사의 업무 수행을 돕는 보조적인 도구다. AI 를 활용하더라도 최종 결정은 관제사가 수행해야 한다. 현재 관제사는 반복적인 '위협 정·오탐 판단' 업무를 가장 많이 수행하고 있다. 이와 같이 반복적이고 단순한 업무는 이제 AI 에게 맡기고, 관제사는 고도화된 위협을 분석하기 위한 신규 위협 추적(Threat Hunting)과 셀 수 없이 쏟아지는 최신 위협에 대한 연구를 진행해야 한다. 이를 통해 보안관제의 level 을 한단계 끌어올리고 안전한 사이버 세상이 될 수 있도록 노력해야 될 것이다.

국내 정보보안 1 위 기업인 SK 쉴더스는 기업의 비즈니스 환경을 24 시간 365 일 안전하게 보호하고 있는 정보보안관제 서비스를 제공하고 있다. 원격 보안관제 서비스를 통해 다양한 보안 시스템에서 발생하는 로그와 이벤트를 수집해 지능화된 사이버 위협을 탐지/대응하고 있다.

특히, 자체 보유한 글로벌 수준의 보안관제센터 Secudium 센터를 통해 기업의 보안 솔루션 및 시스템 설치/연동에서부터 침해 예방 활동, 모니터링 및 분석, 대응, 보고 등 종합적인 보안관제 서비스를 원격으로 제공한다. SK 쉴더스 보안관제를 도입하면 별도의 전문인력이나 시스템 구축 등 번거로운 절차 없이 합리적인 비용으로 쉽고 빠르게 사이버 위협에 대응할 수 있다.

SK 쉴더스는 업계 최다 전문 보안관제 및 침해사고 대응 인력을 보유하고 있다. 또한, 보안관제 프레임워크와 검증된 자체 보안관제 방법론 ISMM 을 보유하고 있다. 보안관제와 관련한 자세한 내용은 SK 쉴더스 홈페이지에서 확인할 수 있다.