Security Monitoring Managed 서비스 소개

네이버 클라우드 플랫폼 Security Monitoring Managed 서비스의 개념과 기본 구조를 설명합니다.

Security Monitoring Managed 서비스란?

네이버 서비스를 외부의 공격으로부터 안전하게 보호하고 있는 보안전문 인력이 네이버 클라우드 플랫폼 고객의 서비스를 24 시간 365 일 보호하는 보안관제 서비스입니다.

Security Monitoring Basic 서비스에서 보다 강화된 모니터링을 원하는 고객에게 유료로 제공되는 상품으로 탐지/차단 서비스 및 분석 서비스를 추가로 제공합니다.

- 탐지/차단 서비스: IDS, IPS, WAF, Anti-Virus, DDoS
- 분석 서비스: 침해사고 기술 지원

상품 용어 설명

Q. IDS 는 무엇인가요?

- IDS(Intrusion Detection System)란 고객의 서비스로 인입되는 공격을 탐지하는 보안 솔루션입니다.
  24 시간 * 365 일 모니터링 함으로써 고객의 서비스가 안전하게 운영될 수 있도록 지원합니다.
  Q. IPS 는 무엇인가요?

- IPS(Intrusion Prevention System)란 고객의 서비스로 인입되는 공격을 탐지/차단하는 보안 솔루션입니다.
  24 시간 * 365 일 모니터링 함으로써 고객의 서비스가 안전하게 운영될 수 있도록 지원합니다.
  Q. Anti-Virus 는 무엇인가요?

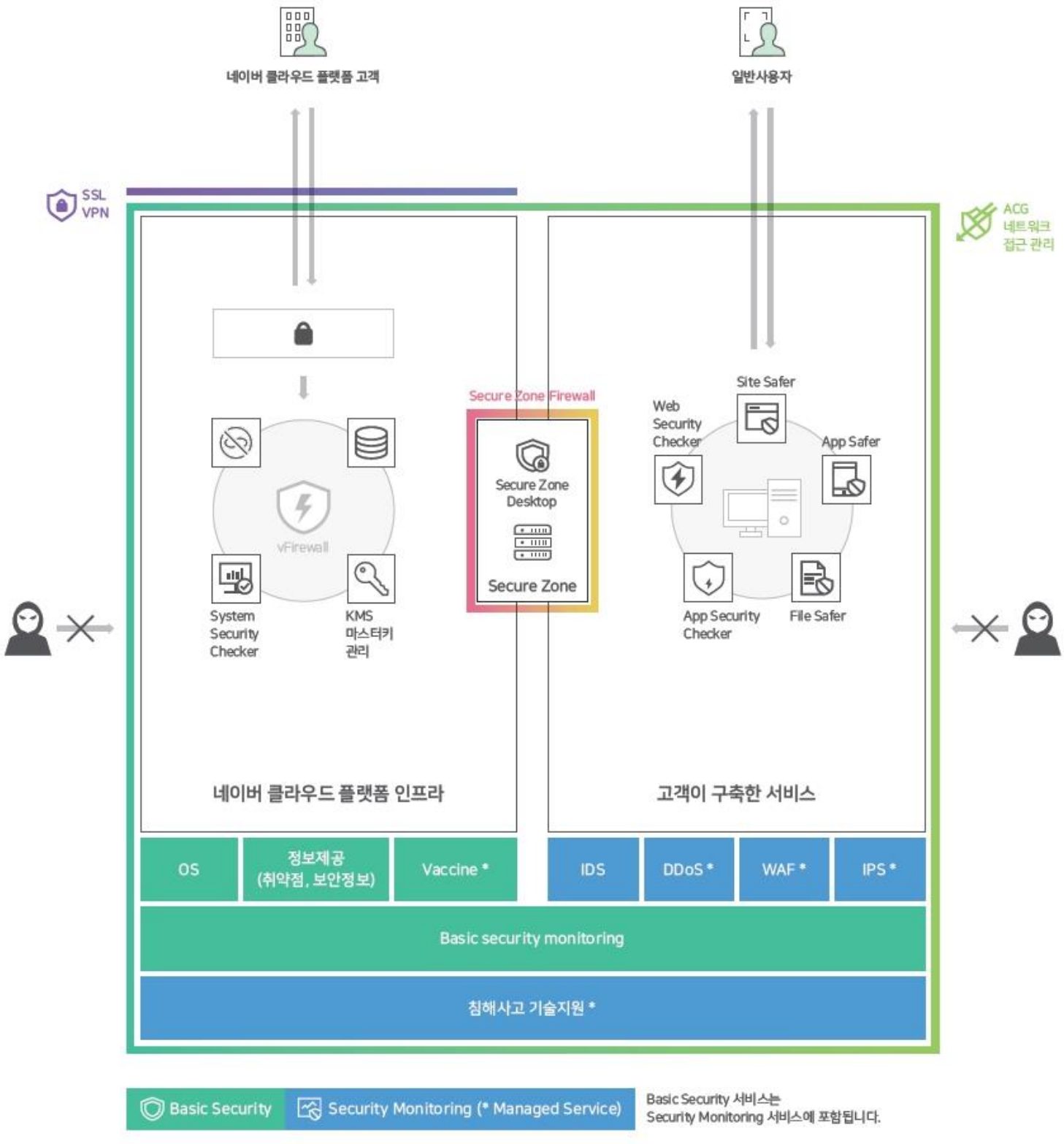
- Anti-Virus 는 악성코드를 탐지/방어하는 보안 솔루션입니다.
  고객이 운영중인 서버에 악성코드를 실시간으로 탐지하고 격리/삭제 조치함으로써 고객의 서비스가 안정적으로 운영될 수 있도록 지원하는 서비스입니다
  Q. DDoS 는 무엇인가요?

- DDoS(Distributed Denial of Service) 공격은 고객의 서비스가 불가능하도록 자원을 고갈시키는 공격을 의미합니다.
  Anti-DDoS 는 고객의 서비스로 인입되는 DDoS 공격을 탐지/차단하여 고객의 서비스가 안정적으로 운영될 수 있도록 지원합니다.
  Q. WAF 는 무엇인가요?

- WAF(Web Application Firewall)는 웹 공격을 전문적으로 탐지/방어하는 보안 솔루션입니다.
  고객의 웹서비스로 공격이 인입될 경우, WAF 전용 솔루션을 통해 탐지/방어함으로써 즉각적인 대응이 가능하도록 지원하는 서비스입니다.
  Q. 침해사고 기술 지원은 무엇인가요?

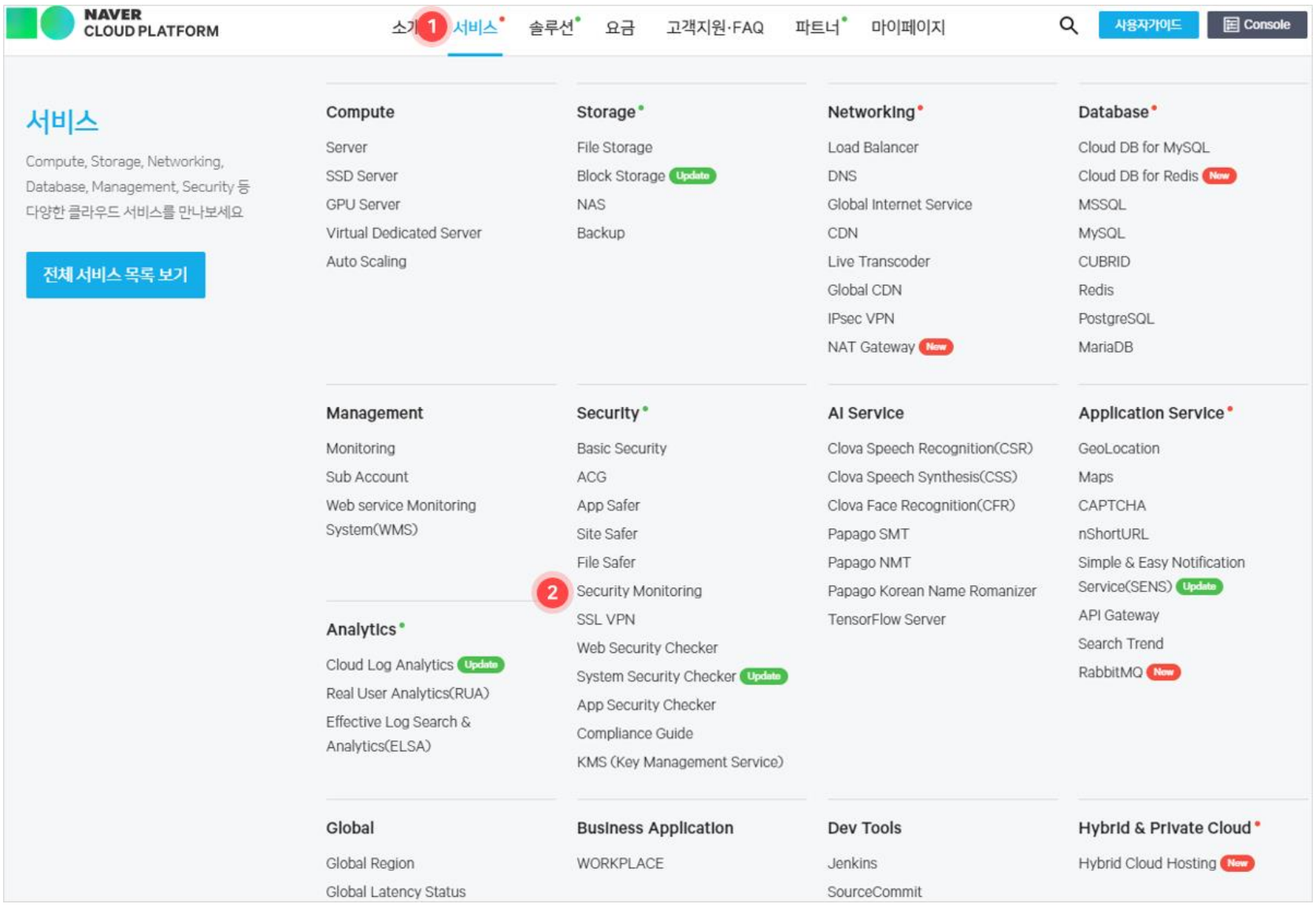
- 고객의 서비스에 침해사고가 발생하면 대응 전문가가 침해사고에 대한 분석을 수행하고, 원인을 파악해 차후 동일한 피해가 발생하지 않도록 지원하는 서비스입니다.

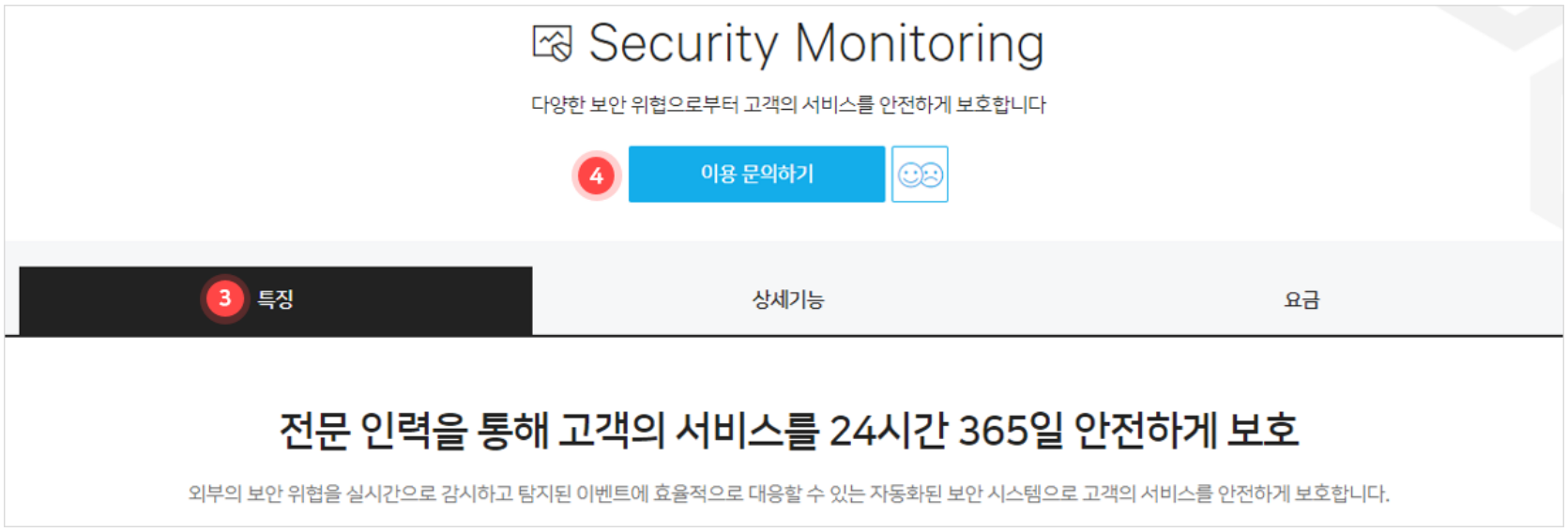
서비스 구조

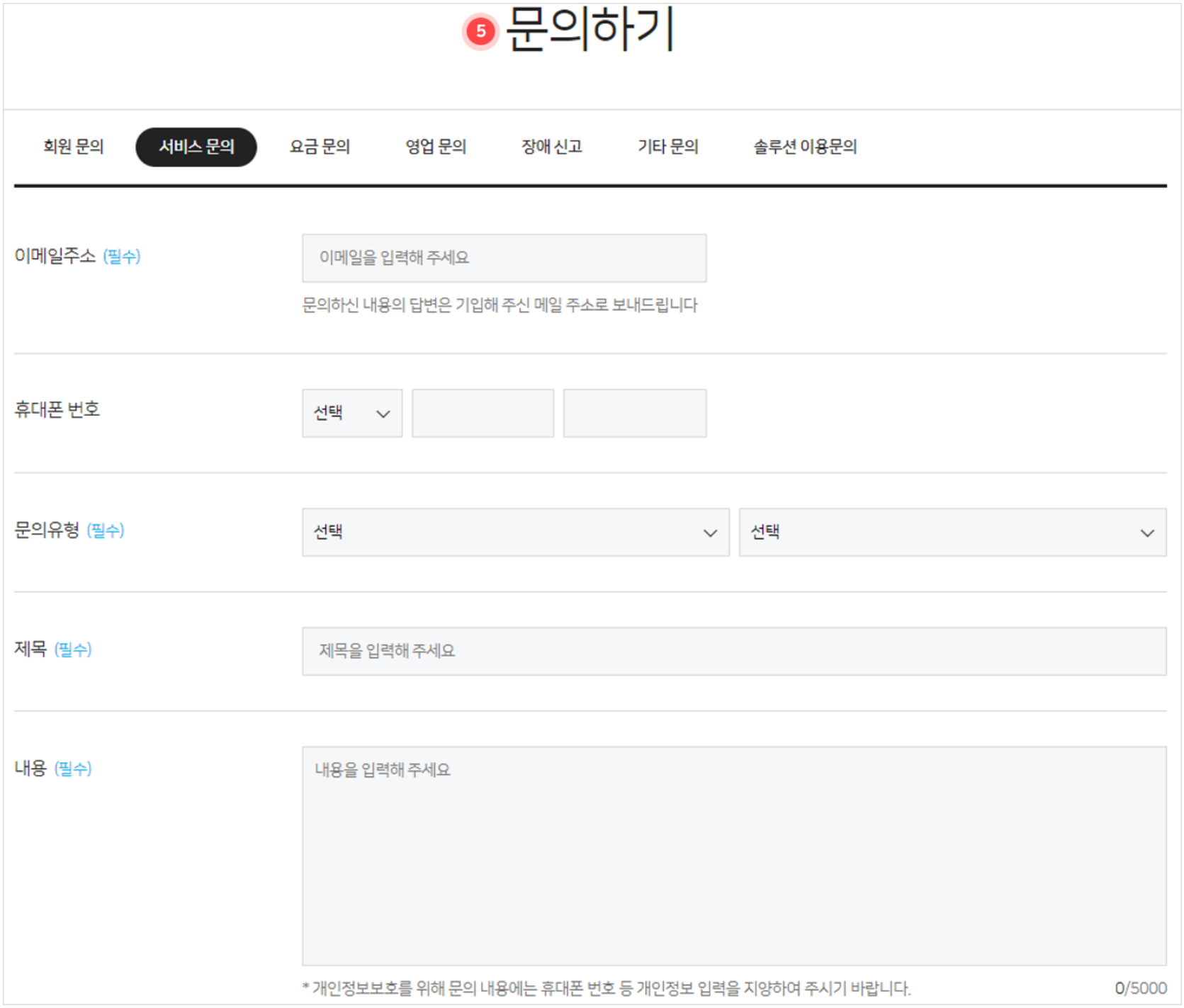


Security Monitoring Managed 는 기본적으로 네이버 클라우드 플랫폼 내부와 외부 사이의 모든 통신에 대한 모니터링 및 차단을 수행합니다.
고객 서비스의 상황과 Security Monitoring 서비스만의 특징을 고려해서 고객의 서비스를 보호하기 위한 최적의 방법을 적용하고 있습니다.

Managed 상품 신청 방법



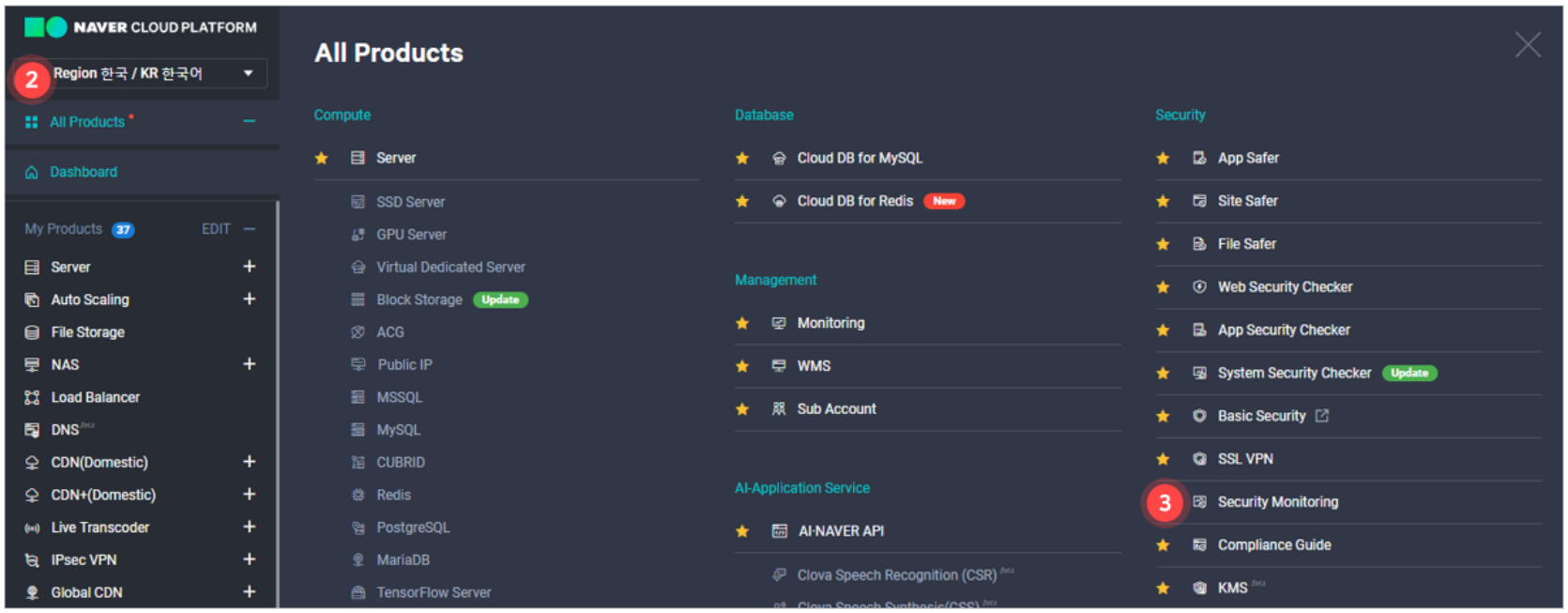


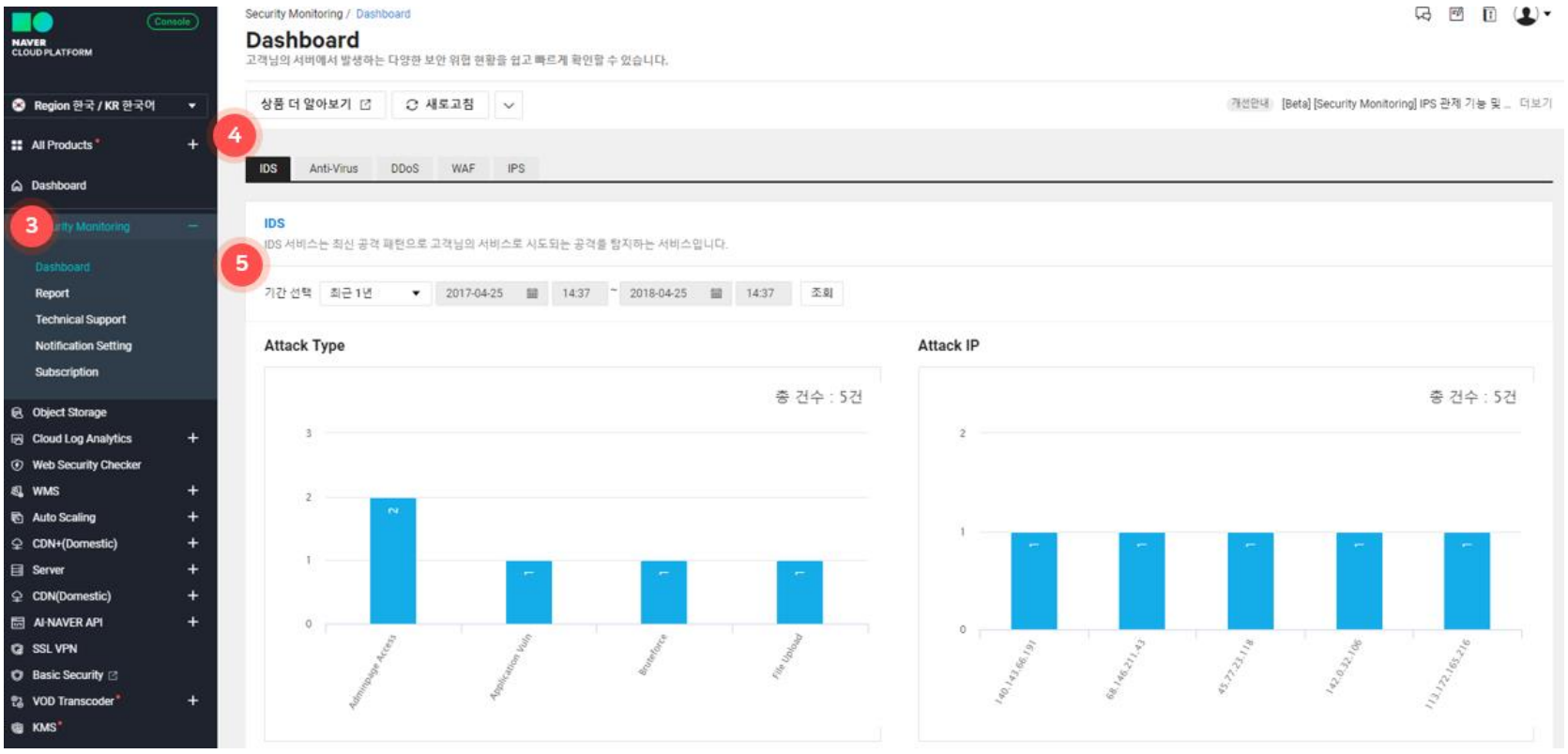


1. **서비스** 메뉴를 선택합니다.
2. **Security > Security Monitoring** 을 선택합니다.
3. **이용안내** 메뉴를 선택합니다.
4. **이용 문의하기** 버튼을 클릭합니다.
5. 고객님의 기본 정보와 Security Monitoring Managed 상품 중 사용하고자 하시는 상품의 종류를 입력해서 문의주시면 빠른 시간 내에 직접 연락드립니다.

Security Monitoring Managed 서비스 및 보고서 확인 방법

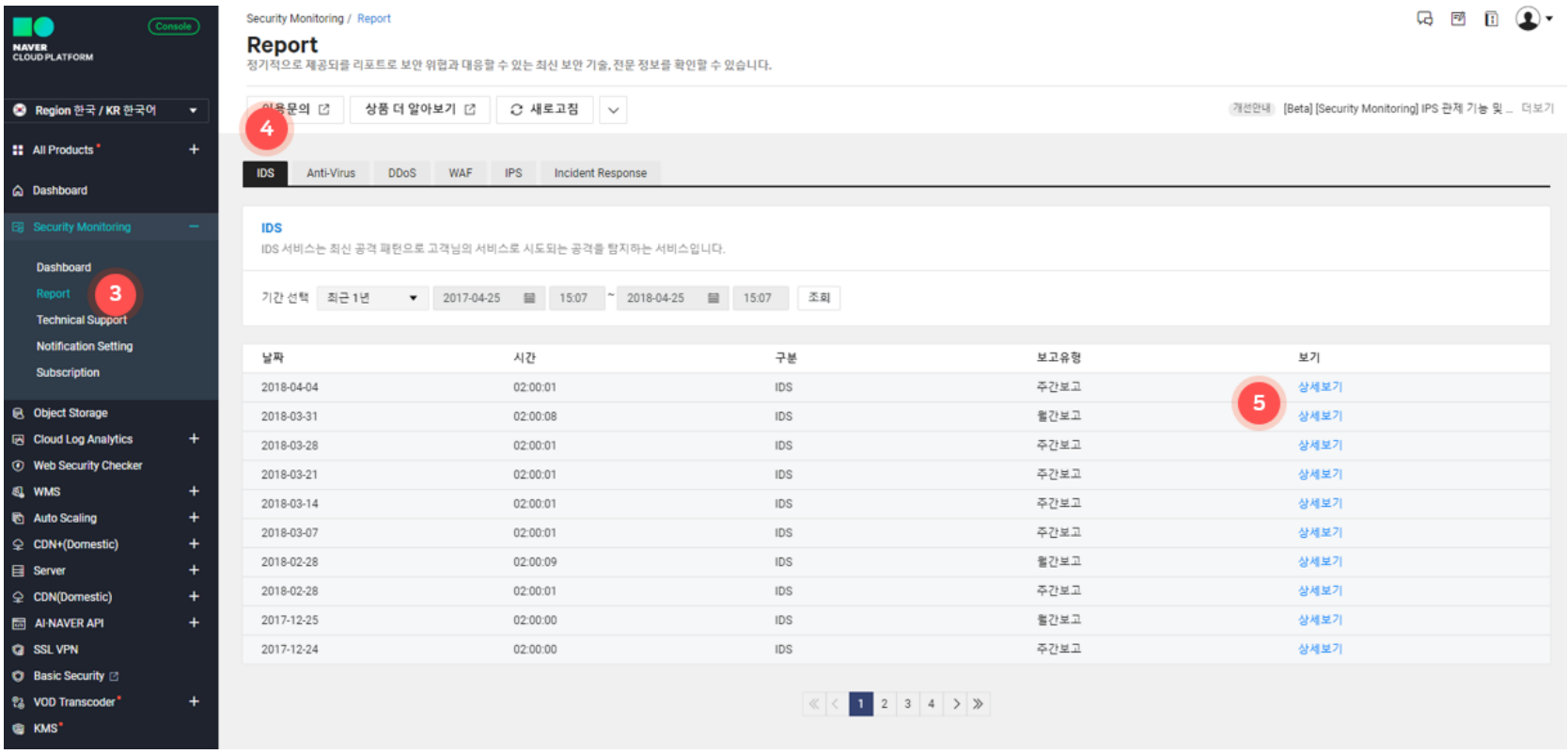
탐지/차단된 공격 정보 확인 방법





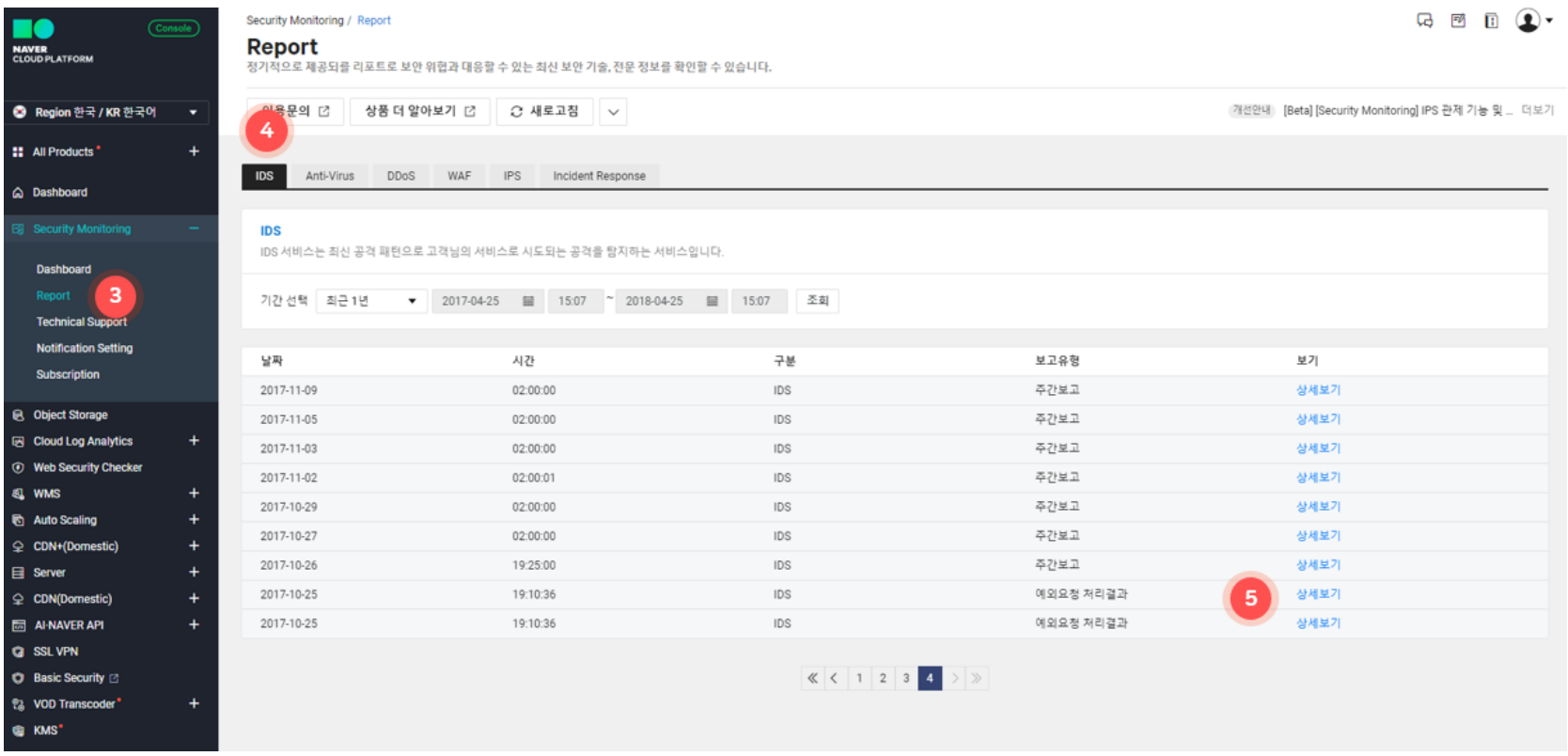
1. **Console** 버튼을 클릭해 Console 화면에 접속합니다.
2. 왼쪽 메뉴에서 **All Product > Security Monitoring** 을 클릭합니다.
3. **대시보드**를 클릭합니다.
4. 현재 사용 중인 Security Monitoring 상품을 확인할 수 있으며 각 상품을 선택하여 탐지된 공격 정보를 확인할 수 있습니다.
5. 탐지된 공격 정보는 공격 유형, 공격자 정보 등 다양한 형태로 제공됩니다.

주간/월간 보고서 확인 방법



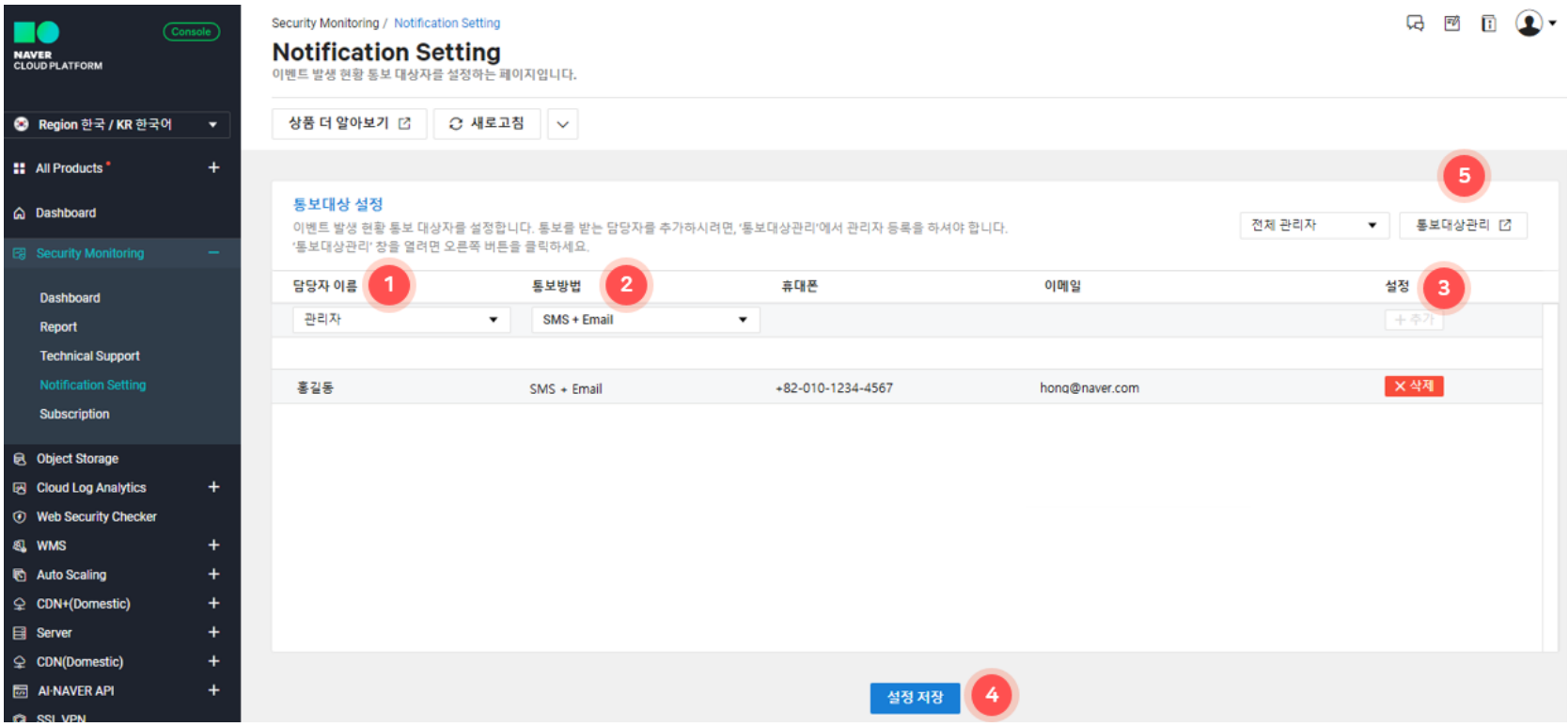
1. **Console** 버튼을 클릭해 Console 화면에 접속합니다.
2. 왼쪽 메뉴에서 **Security > Security Monitoring** 을 클릭합니다.
3. **Report** 를 클릭합니다.
4. 현재 사용 중인 Security Monitoring 상품 탭을 클릭합니다.
5. **보고유형** 중 **주간보고**, **월간보고**에 해당하는 항목의 **상세보기**를 클릭합니다.

예외 처리 결과 확인 방법



1. **Console** 버튼을 클릭해 Console 화면에 접속합니다.
2. 왼쪽 메뉴에서 **Security > Security Monitoring** 을 클릭합니다.
3. **Report** 를 클릭합니다.
4. 예외 처리 요청한 상품 탭을 클릭합니다.
5. **보고유형** 중 **예외요청 처리결과**에 해당하는 항목의 **상세보기**를 클릭합니다.

Notification Setting



1. **통보대상관리**에 등록된 담당자의 리스트가 표시됩니다. 통보대상 담당자를 선택합니다.
   만약 통보대상 담당자가 없다면, (5)번의 '통보대상관리'에서 추가합니다.
2. Security Monitoring 에서 탐지되는 보안 이벤트의 내용을 통보 받을 방법을 선택합니다.
3. 담당자와 통보 방법을 선택한 후, **추가** 버튼을 누르면 통보 대상자로 추가됩니다.
4. **설정저장** 버튼을 선택하여 변경된 정보를 저장합니다.
5. '통보대상관리'에 등록된 담당자만 Security Monitoring 통보 대상자로 등록할 수 있습니다.
   탐지되는 보안 이벤트의 알림을 받으시려면, '통보대상관리'에 먼저 추가해 주시기 바랍니다.

참고 사항

Security Monitoring Managed 상품은 한국/싱가폴/일본/미국(서부)/독일 리전에서 제공됩니다.
추후 모든 글로벌 리전에서 제공 가능하도록 준비 중에 있습니다.

연관 정보 바로가기

아래 가이드에서 연관 정보를 확인할 수 있습니다.

- 서버 생성 가이드
- 로드밸런서 생성 가이드
- DNS 사용 가이드
- Global Region 사용 가이드