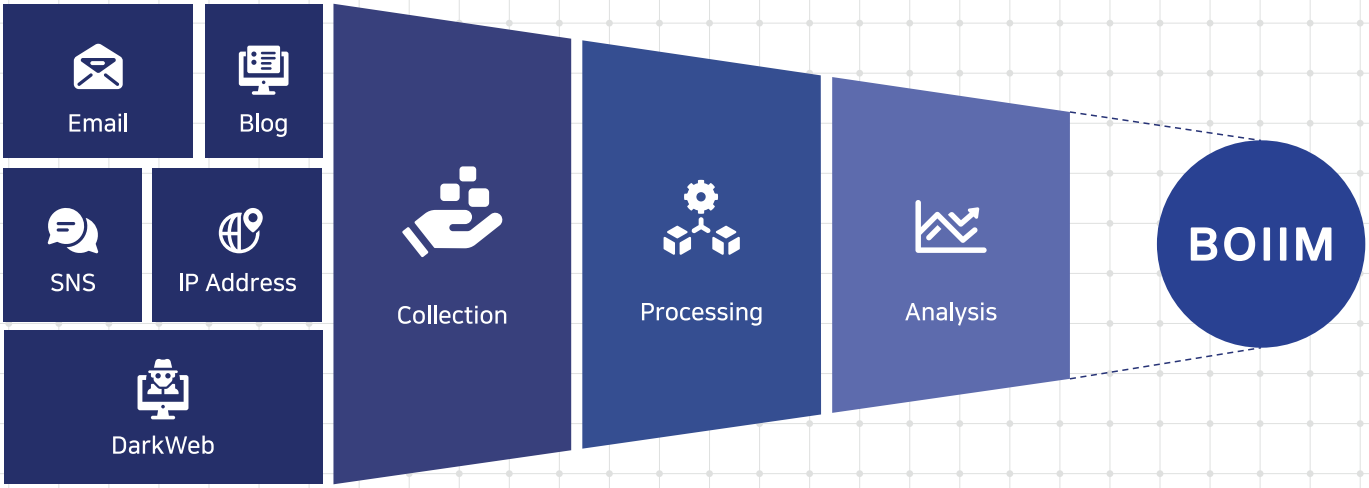
성공적인 비즈니스 운영을 위한 위협 인텔리전스 관리 서비스
Business Operational Information Intelligence Management

BOIIM

비즈니스 정보 유출 및 사이버 위협 정보로부터 자산을 지키는 첫.걸.음!
사이버 위협정보 전문 분석가가 제공하는 관리형 위협 인텔리전스 서비스

조직 내외부 다양한 사이버 위협에 대한 종합적 관리로
성공적인 비즈니스 운영을 돕는 **기업형 위협정보 서비스**

‘ 제로 트러스트 시대에도, 知彼知己 면 百戰不殆 ’
지피지기 백전불태



CTI
사이버 위협 인텔리전스

+ APT 및 사이버 범죄 해킹 그룹의 공격 활동에 대한 분석 자료 제공
+ MITRE ATT&CK Matrix 기반의 해킹 기법에 대한 상세정보 제공
+ 공격 그룹 프로파일링, 유사성 비교, 활동과 특성을 전문가 입장에서 분석

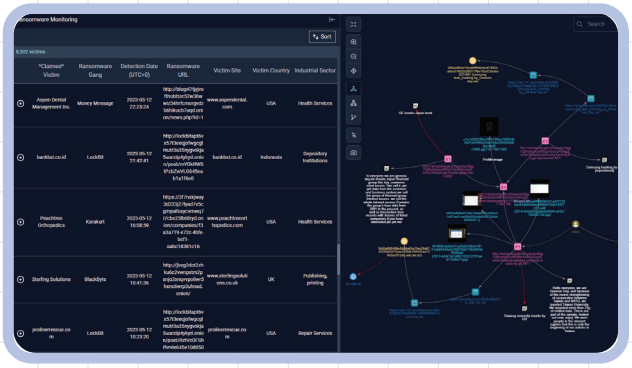
OSINT
다크웹&공개출처 위협 정보

+ 2000억 건 이상의 방대한 다크웹 빅 데이터 기반 유출 정보 검색 제공
+ 다크웹&딥웹에 노출된 기업 도메인 및 해킹된 계정, 디바이스 정보 제공
+ 다크웹&딥웹 공격 최신 동향 제공
+ 위협 정보 연관 관계 추적 시각화

ASM
공격 표면 관리 솔루션

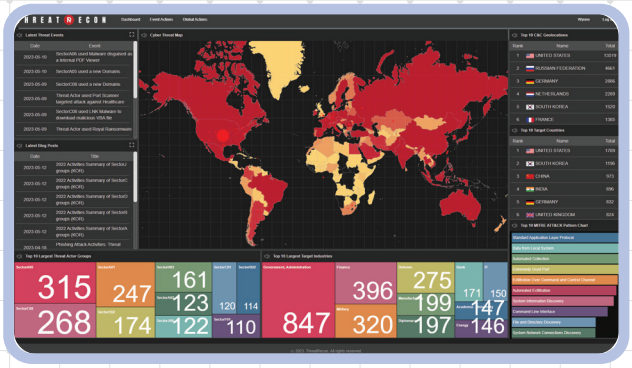
+ 외부에 노출된 (관리/미관리) IT자산 확인 서비스 (진단&스캐닝)
+ 공격 위협에 노출된 자산에 대한 지속적인 실시간 관리 및 모니터링
+ 공격자 관점의 공격 표면 정보 수집 및 보안 위협에 대한 검증(VA/PT)

문의 | service@nshc.net



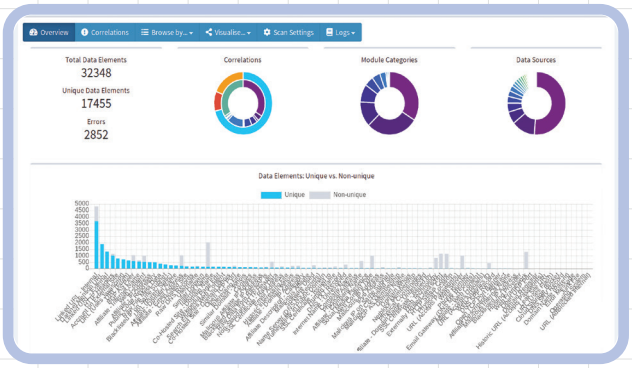
DarkTracer (다크웹 위협 모니터링 플랫폼)

- DarkWeb&DeepWeb 유출 정보 프로파일링
- 등록된 키워드 기반의 유출 콘텐츠 모니터링
- 해킹된 디바이스, 계정정보 데이터베이스 제공



ThreatRecon (사이버 위협 인텔리전스 플랫폼)

- APT 및 사이버 범죄 해킹 그룹 활동 모니터링
- 악성코드 및 사이버 공격 무기 관련 데이터 제공
- 기업 오퍼레이션 내 활용 가능한 CTI 리포트 제공

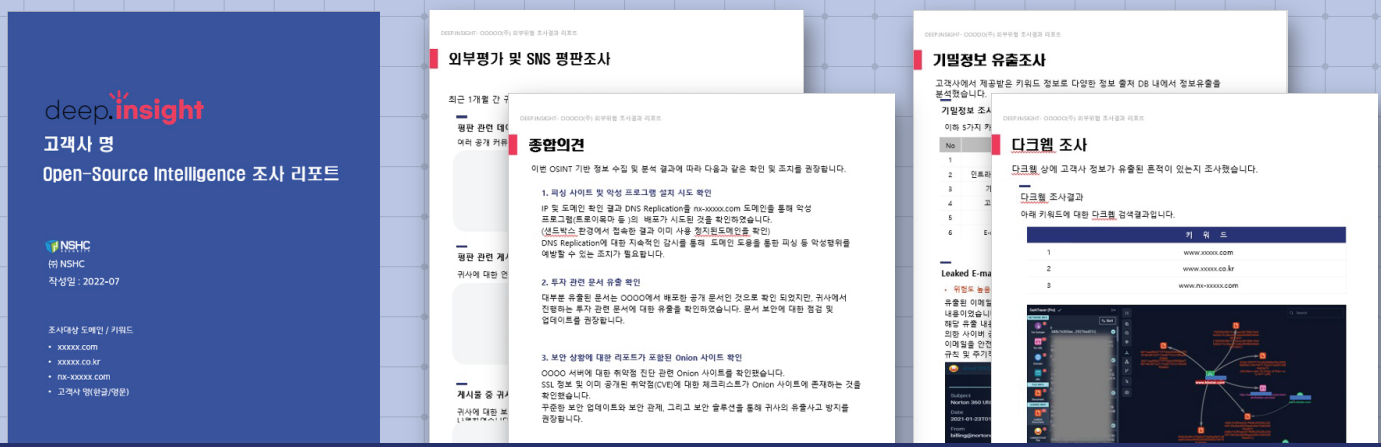


NSHC XTI-ASM (공격표면관리)

- 지속적 보안 노출 위협 관리를 위한 대시보드 제공
- 노출된 보안 위협을 확인하고 취약점을 자동으로 테스트
- 다양한 자동 수집 및 테스트 기능을 제공

deep.insight (기업 외부 위협정보 리포트)

- 공개정보수집(OSINT) DB를 통한 위협정보 분석과 다양한 침해지표(IoC)를 활용한 위협정보 분석
- ID/PW 유출 상황과 감염된 디바이스 데이터 분석



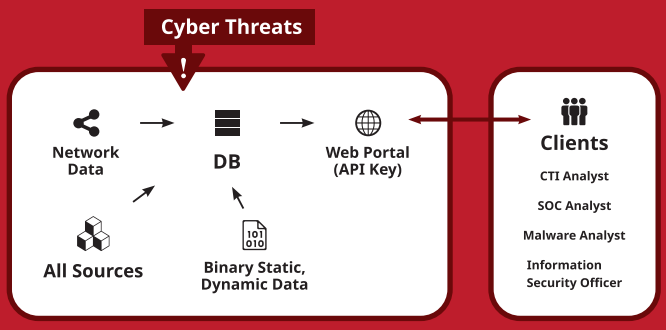
사이버 위협 인텔리전스 플랫폼

THREAT RECON

APT 및 사이버 범죄 해킹 그룹 동향 및 활동 모니터링
악성코드 및 사이버 공격 무기 관련 데이터 제공

▶ 특화된 CTI 서비스

ThreatRecon팀의 특화된 위협 탐지 체계를 이용하여 위협 정보를 수집 및 분석합니다. 이를 바탕으로 기업 환경 내 활용 가능한 CTI (Cyber Threat Intelligence) 서비스를 제공하고 있습니다.



▶ ThreatRecon 특징

THREAT RECON

01 집중 및 차별화
차별화된 동남아시아, 동아시아 및 중동 지역 활동 해킹 그룹 정보 보유

02 정보보안 활동 체계 수립
서비스를 활용한 예방, 탐지 및 대응으로 이어지는 정보 보안 활동 체계 수립 가능

03 특화된 플랫폼
NSHC ThreatRecon Team 자체 플랫폼에 의한 위협 데이터 및 상관 정보 추출

04 특정 이슈 확인
특정 이슈 관련 위협 정보의 확인 가능

문의 | service@nshc.net

▶ ThreatRecon CTI 플랫폼 (2022년 11월 기준)

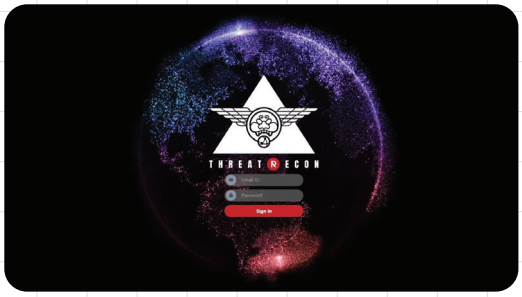
18개 Sector

252개 Group

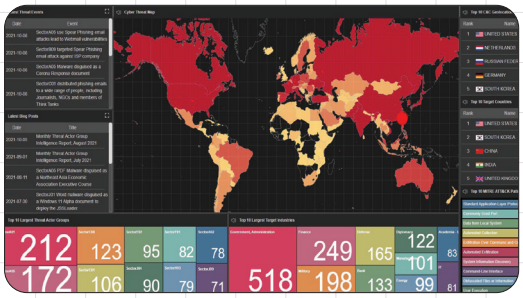
4,222 Event

356,714 Indicator

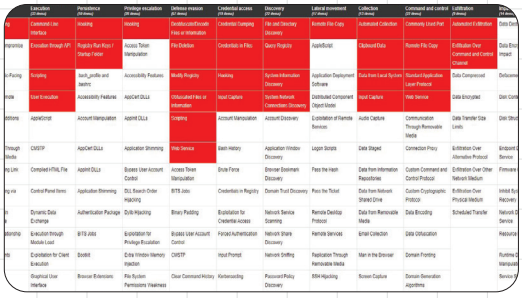
- 동아시아, 동남아시아 및 중동에서 발생하는 위협 정보의 획득이 용이
- CTI 조직 자체 구성이 어려운 만큼, 신뢰적인 정보의 획득이 용이
- 향후 발생할 위협에 대한 정보 수집 체계보다 비용 대비 효과 높음
- 최신 사이버 위협 정보와 동향 파악 용이
- 사이버 위협 인텔리전스 서비스를 활용한 위협 탐지, 차단으로 사전 예방 효과
- 신규 발생 위협에 대한 과거 이벤트와의 상관 정보 확인 용이



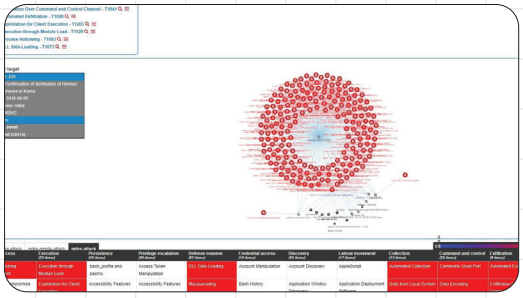
웹 기반 포탈 접속



대시보드



MITRE ATT & CK Framework
기반 공격 단계 정의



수집된 이벤트와의 상관 정보

클라우드 보안 및 자원 관리 통합 솔루션
Cloud Native Application Protector Platform

FRIIM

복잡한 클라우드 인프라 시대, 극한의 감지 성능으로 무장한
클라우드 관리보안 솔루션이 필요한 순간은 바로 지금입니다.

다양한 멀티 테넌트 & 하이브리드 클라우드의 **설정 오류 탐지** 및 예방
클라우드 워크로드 별 고유 **보안 관리** 및 다양한 **요구사항**에 대응

‘ 클라우드 보안도 제로 트러스트, 제로 스트레스 ’

멀티 테넌트 &
하이브리드 클라우드 지원

AWS, MS Azure 부터 NCP, NHN, KT Cloud 등
국내 CSP 및 컨테이너, 프라이빗 클라우드 총 11개
CSP 지원!

국내외 컴플라이언스부터
자체 기준까지

ISMS-P, CSAP, 금융보안원 등 국내 컴플라이언스와
PCI-DSS, CIS, HIPPA 등 해외 컴플라이언스 지원

CSPM
컴플라이언스 및 형상관리

+ 운영 현황 및 보안 준수율 대시보드
+ 클라우드 리소스 시각화 토플로지
+ CIS, ISMS 등 주요 Best Practice,
  컴플라이언스 진단 및 이력 관리
+ 클라우드 형상 및 설정 변경 관리
+ 설정 변경 및 보안 상태 알람 기능

CWPP
취약점 분석 및 보안관리

+ (CCE) 주요정보통신기반시설
  취약점 분석·평가 기준(과기부),
  클라우드 보안인증(KISA),
  고객사 보안 기준따른 취약점 분석
+ (CVE) NVD, MITRE, 고객사
  보안 기준 등에 따른 취약점 관리

CIEM
클라우드 사용자 및 권한관리

+ IAM/AAD 시각화
+ 인사정보 매칭을 통한 계정관리
+ 부여된 정책과 권한, KEY 관리
+ 계정 or 그룹 단위 정책과 권한 관리
  계정 API & 콘솔 접속 로그 관리
  사용자 행위 분석을 통한 알람 기능

문의 | service@nshc.net

> FRIIM 도입효과

클라우드 **운영 비용 및 관리 체계** 개선 서비스 점검 **시간 단축**
클라우드 보안 준수율 100% 달성!

운영 비용
최대 50% 절감

관리 체계
최대 40% 개선

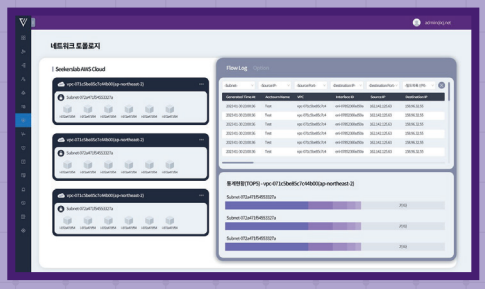
서비스 점검시간
최대 2시간 단축

클라우드 보안준수율
최대 100% 달성

> FRIIM 특장점

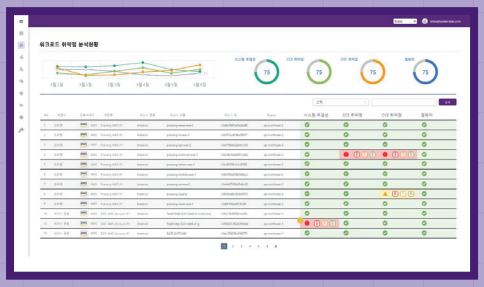
클라우드 보안 통합 대시보드

- 컴플라이언스 준수율 및 미준수 항목 확인
- 보안 이벤트 및 WAF 로그 추이, 탐지 내역 확인
- 고객맞춤형 대시보드 커스터마이징 서비스



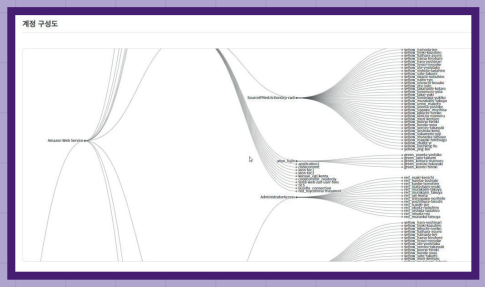
클라우드 네트워크 토폴로지

- 네트워크 자산 배치 상황 및 리소스 점유율 확인
- 미사용 VPC 등의 불필요 자산 검출 기능
- On-Demend 서버와 하이브리드 네트워크도 인식



워크로드 현황 대시보드 & 클라우드 로그

- 클라우드 로그(Flow Log, WAF Log 등)을 인식하여 이벤트 중심의 CVE/CCE 점검 실시
- 워크로드 무결성 점검 및 멀웨어 감염 상태 확인



IAM/AAD 시각화 및 정책권한 관리

- 클라우드 내 모든 인증정보의 구조를 시각화
- 계정에 할당된 정책, 권한 관리 기능을 통해 과도한 권한 및 위협에 대한 대응이 가능