

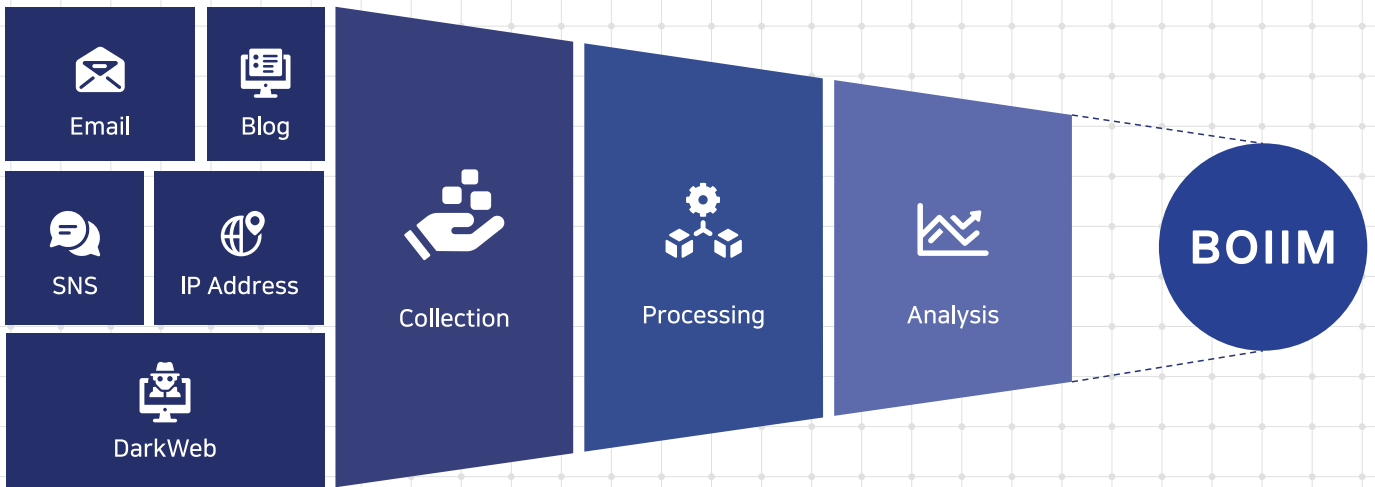
성공적인 비즈니스 운영을 위한 위협 인텔리전스 관리 서비스
Business Operational Information Intelligence Management

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

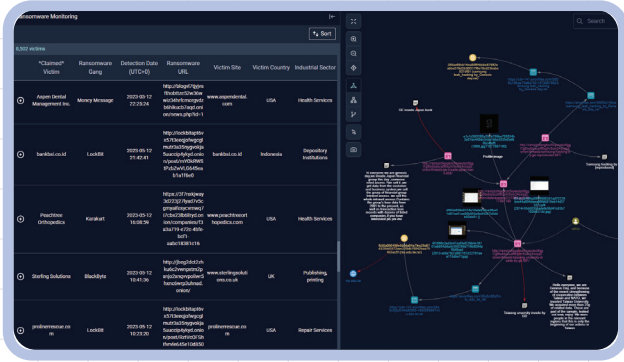
다크웹&공개출처 위협 정보

- + 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)



+ 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 위험 관리를 위한 대시보드 제공
- 노출된 보안 위험을 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(loC)를 활용한 위협정보 분석
- ID/PW 유출 상황과 감염된 디바이스 데이터 분석

deep.insight
고객사 명
Open-Source Intelligence 조사 리포트

NSHC
NSHC
작성일 : 2022-07

조사대상 도메인 / 키워드
- xxxxxx.com
- xxxxxx.co.kr
- ns-xxxxx.com
- 고객사 [비밀감염]

외부평가 및 SNS 평판조사

최근 1개월 간 외부 평가
평판 관련 대역역 키워드
의역 키워드

총합이전

이번 OSINT 기반 정보 수집 및 분석 결과가 따라 다음과 같은 확인 및 조치를 권장합니다.

1. 특정 사이트 및 악성 프로그램 설치 시도 확인
IP 및 도메인 확인 결과 DNS Replication을 ns-xxxxx.com 도메인을 통해 악성 프로그램(트로이안 등)의 배포가 시도된 것을 확인하였습니다.
(악트스 환경에서 악성 프로그램의 사용 및 배포를 차단)
DNS Replication에 대한 지속적인 감시를 통해 도메인 도용을 통한 피싱 등 악성행위를 예방할 수 있는 조치가 필요합니다.
2. 부가 관련 문서 공유 확인
대부분 유출된 문서는 OOOO에서 배포된 공개 문서이므로 확인 및 있지만, 기사에서 전달되는 추가 관련 문서에 대한 유출을 확인하였습니다. 문서 보안에 대한 점검 및 업데이트를 권장합니다.
3. 보안 상황에 대한 리포트가 포함된 Onion 사이트 확인
OOOO 서버에 대한 취약점 진단 관련 Onion 사이트를 확인하였습니다.
SSL 정보 및 기타 공개된 취약점(CVE)에 대한 체크리스트가 Onion 사이트에 존재하는 것을 확인하였습니다.
공공은 보안 업데이트와 보안 관제, 그리고 보안 솔루션을 통해 기사의 유출사고 방지를 권장합니다.

기사들 중 기사
기사에 대한
기사에 대한

기밀정보 유출조사

고객사에서 제공받은 키워드 정보로 다양한 정보 출처 DB 내에서 정보유출을 분석하였습니다.

기밀정보 조사
이해 5가지 키워드

다크웹 조사

다크웹 상에 고객사 정보가 유출된 흔적이 있는지 조사했습니다.
다크웹 조사결과
아래 키워드에 대한 다크웹 검색결과입니다.

Leaked E-mail

1. www.xxxxx.co.kr
2. www.xxxxx.co.kr
3. www.xxxxx.co.kr

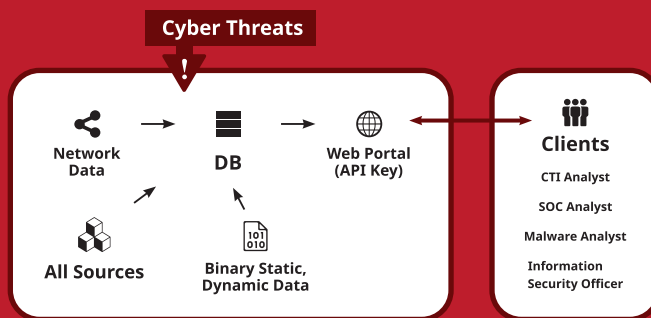
사이버 위협 인텔리전스 플랫폼

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

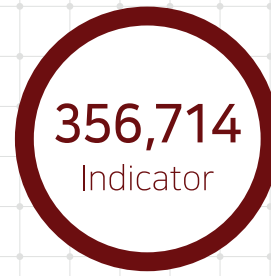
NSHC ThreatRecon Team 자체 플랫폼에 의한 위협 데이터 및 상관 정보 추출

04

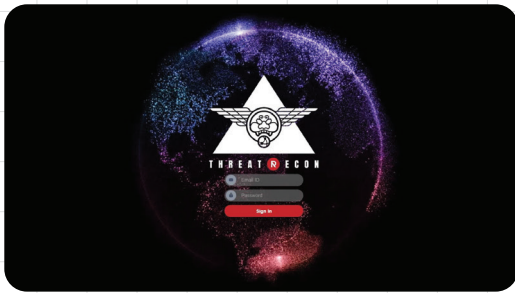
특정 이슈 확인

특정 이슈 관련 위협 정보의 확인 가능

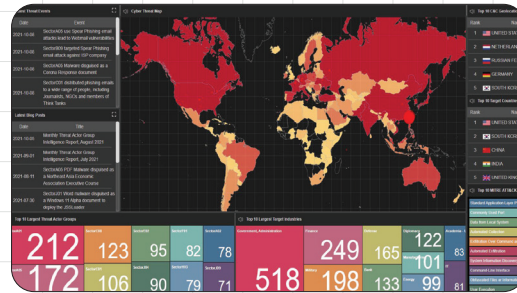
▶ ThreatRecon CTI 플랫폼 (2022년 11월 기준)



- ▶ 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



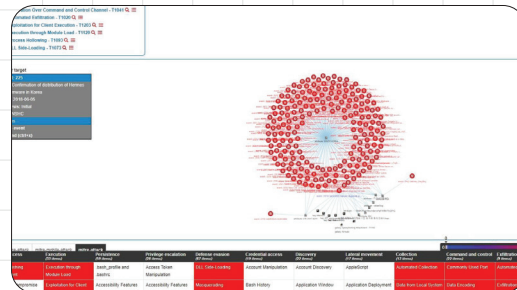
웹 기반 포탈 접속



대시보드

Category	Prevention	Detection	Response	Recovery	Reporting	Communication	Collaboration	Continuity	Leadership	Compliance	Validation	Improvement
Account Security	Account Lockout	Account Suspense	Account Deletion	Account Recovery	Account Transfer	Account Migration	Account Provisioning	Account Archiving	Account Archival	Account Audit	Account Review	Account Improvement
Application Security	Application Hardening	Application Monitoring	Application Patching	Application Backup	Application Update	Application Migration	Application Provisioning	Application Archiving	Application Archival	Application Audit	Application Review	Application Improvement
Asset Security	Asset Discovery	Asset Classification	Asset Protection	Asset Disposal	Asset Migration	Asset Provisioning	Asset Archiving	Asset Archival	Asset Audit	Asset Review	Asset Improvement	Asset Improvement
Business Process Security	Business Process Hardening	Business Process Monitoring	Business Process Patching	Business Process Backup	Business Process Update	Business Process Migration	Business Process Provisioning	Business Process Archiving	Business Process Archival	Business Process Audit	Business Process Review	Business Process Improvement
Cloud Security	Cloud Hardening	Cloud Monitoring	Cloud Patching	Cloud Backup	Cloud Update	Cloud Migration	Cloud Provisioning	Cloud Archiving	Cloud Archival	Cloud Audit	Cloud Review	Cloud Improvement
Container Security	Container Hardening	Container Monitoring	Container Patching	Container Backup	Container Update	Container Migration	Container Provisioning	Container Archiving	Container Archival	Container Audit	Container Review	Container Improvement
Device Security	Device Hardening	Device Monitoring	Device Patching	Device Backup	Device Update	Device Migration	Device Provisioning	Device Archiving	Device Archival	Device Audit	Device Review	Device Improvement
Endpoint Security	Endpoint Hardening	Endpoint Monitoring	Endpoint Patching	Endpoint Backup	Endpoint Update	Endpoint Migration	Endpoint Provisioning	Endpoint Archiving	Endpoint Archival	Endpoint Audit	Endpoint Review	Endpoint Improvement
Identity Security	Identity Hardening	Identity Monitoring	Identity Patching	Identity Backup	Identity Update	Identity Migration	Identity Provisioning	Identity Archiving	Identity Archival	Identity Audit	Identity Review	Identity Improvement
Infrastructure Security	Infrastructure Hardening	Infrastructure Monitoring	Infrastructure Patching	Infrastructure Backup	Infrastructure Update	Infrastructure Migration	Infrastructure Provisioning	Infrastructure Archiving	Infrastructure Archival	Infrastructure Audit	Infrastructure Review	Infrastructure Improvement
Network Security	Network Hardening	Network Monitoring	Network Patching	Network Backup	Network Update	Network Migration	Network Provisioning	Network Archiving	Network Archival	Network Audit	Network Review	Network Improvement
Physical Security	Physical Hardening	Physical Monitoring	Physical Patching	Physical Backup	Physical Update	Physical Migration	Physical Provisioning	Physical Archiving	Physical Archival	Physical Audit	Physical Review	Physical Improvement
Platform Security	Platform Hardening	Platform Monitoring	Platform Patching	Platform Backup	Platform Update	Platform Migration	Platform Provisioning	Platform Archiving	Platform Archival	Platform Audit	Platform Review	Platform Improvement
System Security	System Hardening	System Monitoring	System Patching	System Backup	System Update	System Migration	System Provisioning	System Archiving	System Archival	System Audit	System Review	System Improvement
Third Party Security	Third Party Hardening	Third Party Monitoring	Third Party Patching	Third Party Backup	Third Party Update	Third Party Migration	Third Party Provisioning	Third Party Archiving	Third Party Archival	Third Party Audit	Third Party Review	Third Party Improvement
Vendor Security	Vendor Hardening	Vendor Monitoring	Vendor Patching	Vendor Backup	Vendor Update	Vendor Migration	Vendor Provisioning	Vendor Archiving	Vendor Archival	Vendor Audit	Vendor Review	Vendor Improvement

MITRE ATT & CK Framework
기반 공격 단계 정의



수집된 이벤트와의 상관 정보

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 요구사항에 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!

국내의 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 토폴로지
- + 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

> 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

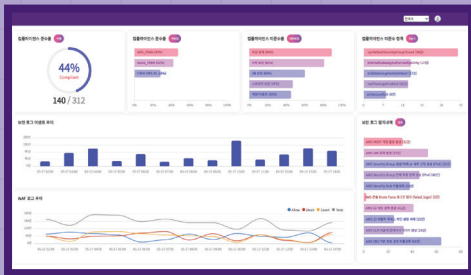
최대 2시간 단축



클라우드 보안준수율

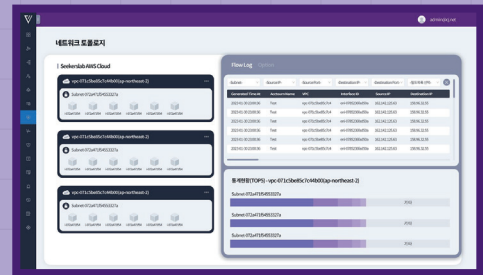
최대 100% 달성

> FRIIM 특징점



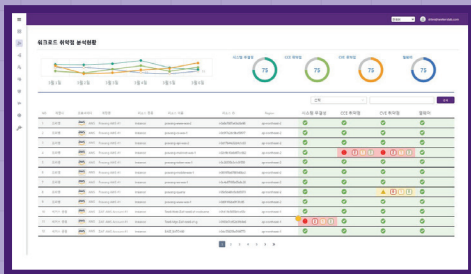
클라우드 보안 통합 대시보드

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



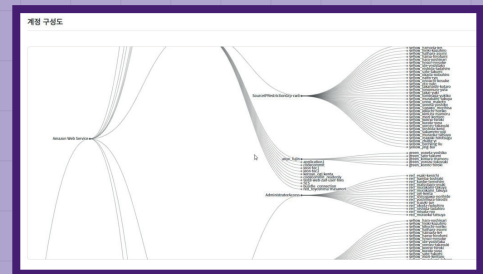
클라우드 네트워크 토폴로지

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



워크로드 현황 대시보드 & 클라우드 로그

- 클라우드 로그(Flow Log, WAF Log 등)를 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