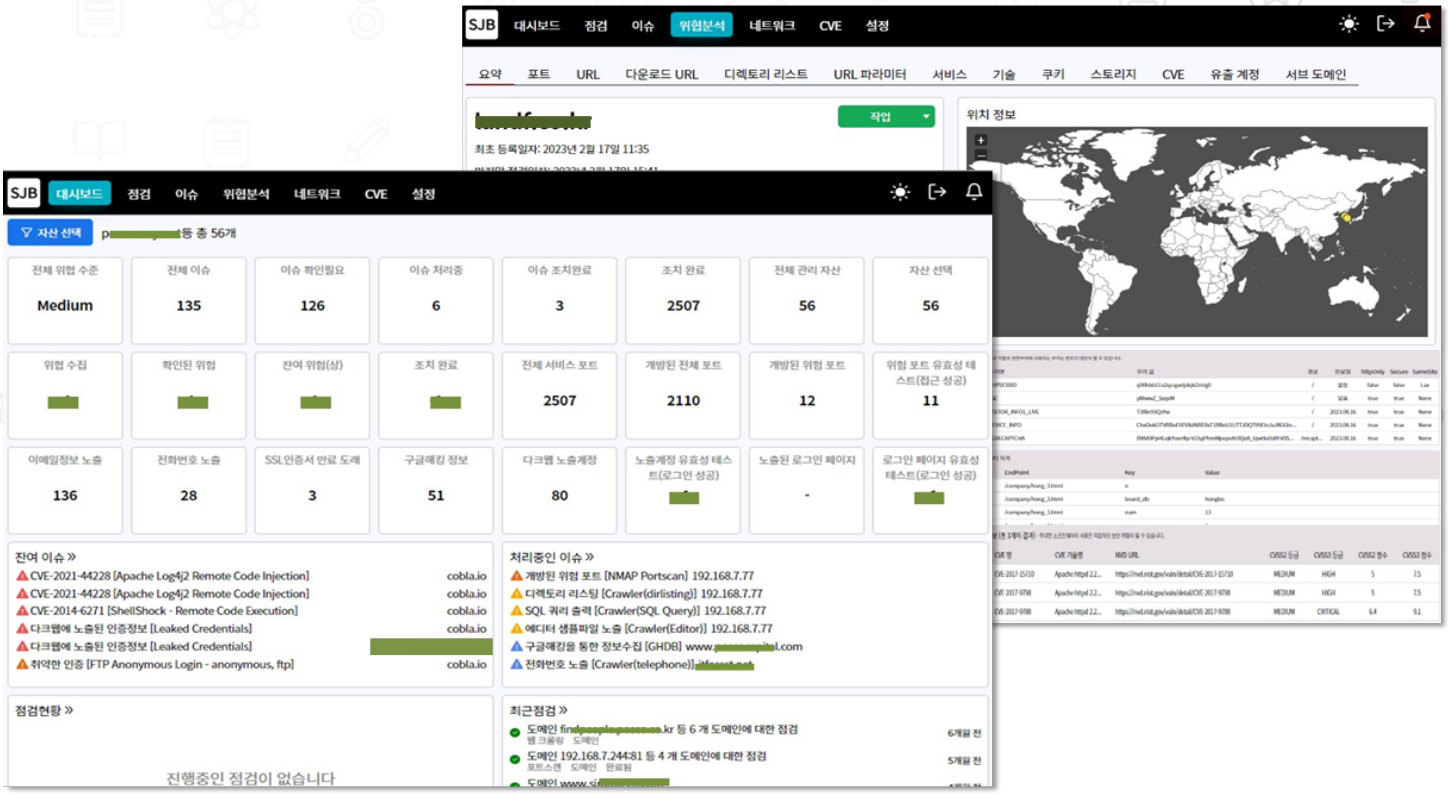
지속적 보안위협 노출 관리 및 PenTesting 자동화를 위한

공격 표면 관리(ASM) 솔루션

SooJi.Bee

Attack Surface Management by ITF



공격자 관점

약 1,800개 자동 취약점 테스트

공격자의 관점에서 접근가능한 다양한 공격표면을 자동 진단!

- 선제적인 보안위협에 능동적으로 대응가능
- 지속적이고 변화하는 보안 위협 노출 관리

딥웹& 다크웹

약 1천 억 개 딥/다크웹 데이터 기반

기술적 취약점 활용이 아닌 유출정보 기반 접근은 가장 큰 위협!

- 유출된 내부 인증정보(크레덴셜) 확인 가능
- 멀웨어에 감염된 기기를 통한 유출상황 확인

방어 관점 보안수동관리에서 **제로 트러스트** 자동대응으로

ASM은 공격자의 관점에서 직간접적으로 활용될 수 있는 외부에 노출된 보안 위협 요인, 즉 "공격 표면"으로 불리는 잠재적 취약점을 지속적으로 관리하는 대응 솔루션입니다. 방어 관점의 보안관제 활동보다 더 빠르게 선제적 보안 위협에 능동적으로 대응할 수 있는 보안 위협 노출 관리가 가능합니다.

NSHC SECURITY

ba.sales@nshc.net 02-6951-3999

(주)NSHC 서울시 금천구 가산디지털1로 186 제이플라츠 806호

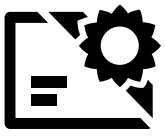
ASM?
왜 필요한가요?

IT환경의 변화로 해커가 공격가능한 표면(루트), 방법(수단), 기회가 급증!

재택 근무 + 네이티브 클라우드 + IoT 기기 + 모바일 / PC + 시스템 취약점 + 부족한 보안의식

예상 가능한 모든 공격표면과 공격방법에 대응해야 합니다

진보된 공격표면관리의 시작, 정보수집부터 검증까지 원스톱으로!



노출된 보안 위협 확인 (공격 시나리오에 활용되는 정보)

불필요한 Open Port 정기적 확인공개된
서비스 및 로그인 관리자 페이지 확인
취약한 SSL인증 정보, 만료일 여부 알림

공개/유출된 보안 위협 확인 (직접 공격에 활용되는 정보)

공개된 정보 기반의 취약점 즉시 확인
정기적인 다크웹 내 고객사 유출정보 확인
유출된 인증정보(Credential) 정보 제공

자동 검증(Validation) 수집된 정보 유효성 여부 검증

확인된 취약점 기반 테스트 자동화
이슈 상태 관리, 조치여부 확인
CVE 자동 공격 테스트 시, 관제/모니터링 활용

다양한 Pen-Test 결과를 바탕으로 한 공격자 행위 시나리오 및 정보 제공!

지속적인 Black-Box형 침투 테스트(Pen-Test)를 실제 환경에서 수행한 결과를 토대로
공격자의 관점에서 가장 필요한 정보가 무엇이며, 어떻게 수집할 수 있는가를 시나리오화하고
수집된 정보가 Risk인지, Issue인지 확인하기 위한 자동 검증결과 데이터를 전문가가 검수하여
타겟의 보안 위협과 관련된 직접적인 공격 표면 정보 결과만을 제공해 드리고 있습니다.

ba.sales@nshc.net

NSHC SECURITY

StealthMole
다크웹 위협 인텔리전스

THREAT RECON
사이버 위협 인텔리전스

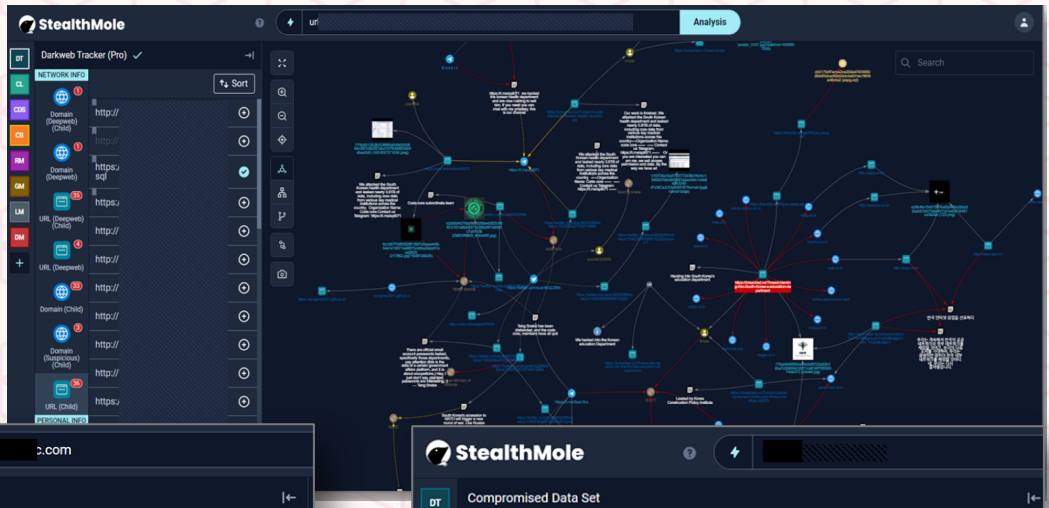
SooJi.Bee
Attack Surface Management by ITF
공격 표면 관리 (ASM)

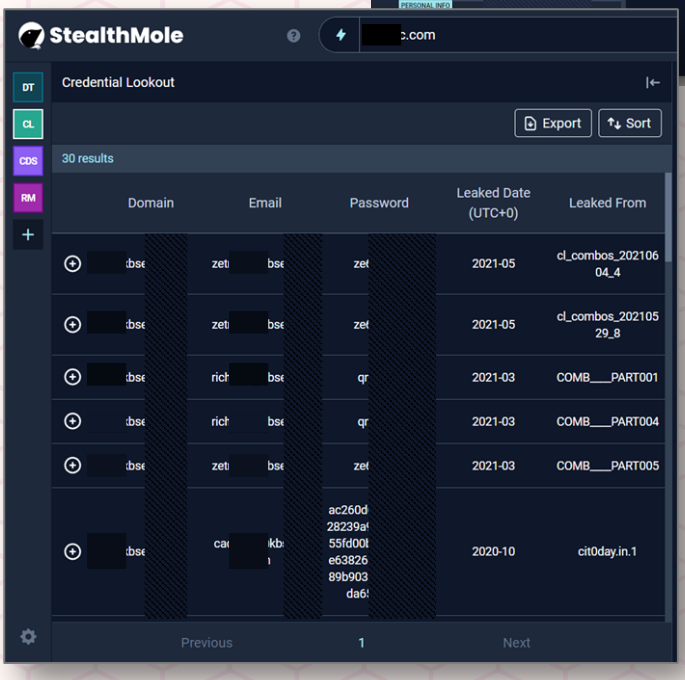
유출된 정보 및 사이버 범죄 위협 정보 조사를 위한 다크웹/딥웹

빅데이터 모니터링 플랫폼

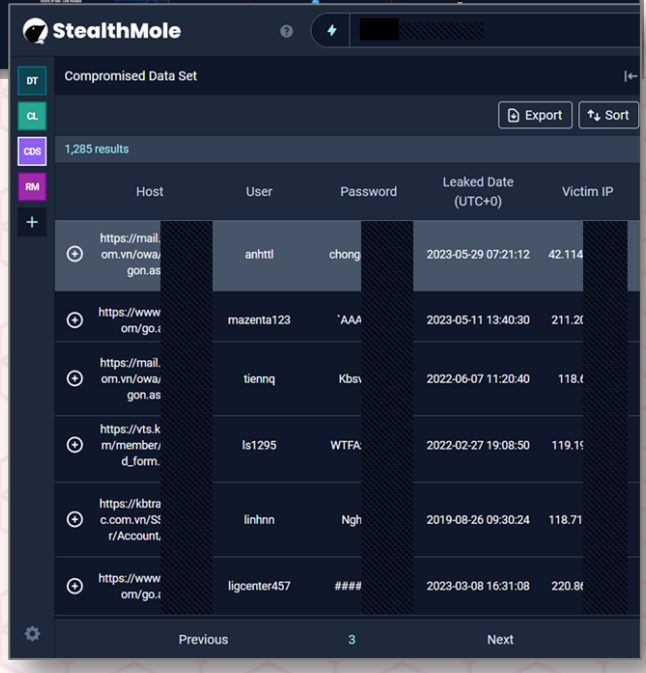
검색 인텔리전스 (프로파일링 캔버스) DT

StealthMole Intelligence





계정 유출정보 조회 CL



침해기기 유출정보 조회 CDS

다크웹, 텔레그램 등 약 2천억 건 이상 분석된 빅데이터를 활용한
위협 인텔리전스와 보안리스크 관리, StealthMole로 시작하세요

- 다양한 검색 지시자 지원
- 타입별 검색 결과 출력 가능
- 최신 해킹 사고 분석 사례 제공
- 다크웹 사이트 히스토리 스냅샷 제공

NSHC SECURITY

ba.sales@nshc.net 02-6951-3999

(주)NSHC 서울시 금천구 가산디지털1로 186 제이플라츠 806호

CTI?
왜 필요한가요?

'제로 트러스트' 시대, 방어형 보안보다 위협에 대한 **선제적 조치**가 시급합니다.

다크웹 Darkweb + 다크웹 Deepweb + 텔레그램 + 메시징 어플 + 블랙마켓 + 블록체인 데이터

웹에 공개된 정보들을 파악하고 계정정보, 내부자료, 기밀문서 등
외부로 유출된 정황이 확인된 정보자산을 모니터링할 수 있습니다.

주요 기능 (Key Feature)

유출 데이터 검색

- 천억개 이상의 데이터 레코드
- 다양한 검색 지시자
  - 데이터 유형 지정 검색
- 유형별 검색 결과 출력
  - URL, 이미지, 문서, 실행파일 등

추적 프로파일링

- 해킹 그룹 및 해커 추적 특화
- 가시성 높은 프로파일링 캔버스
- 다양한 관계 구조도 지원
  - 트리형 / 방사형 / 고정형
- 최신 해킹 사고 분석 사례 제공
- 검색,분석,데이터 저장 기능 지원

다양한 모니터링

- 다크웹 사이트 히스토리 스냅샷
- 랜섬웨어 공격 모니터링
- 유출계정 / 침해기기 모니터링
- 관심 키워드 등록 및 검색

글로벌 레퍼런스를 통한 검증된 플랫폼과 서비스

글로벌 유저들이 사용하는 플랫폼과 위협 데이터 제공 레퍼런스 보유

- 전세계 20개국 + 이상의 정부 사용자
- 100 + 이상의 기업 사용자
- 4,000 + 이상의 개인 사용자

Austria, Czech Republic, Denmark, France, Germany, Hong Kong, India, Indonesialtaly, Jamaica, Japan, Poland, Portugal, Saudi Arabia, Spain, Taiwan, USA, UAE

ba.sales@nshc.net

NSHC SECURITY

StealthMole
다크웹 위협 인텔리전스

THREAT RECON
사이버 위협 인텔리전스

SooJi.Bee
Attack Surface Management by ITF
공격 표면 관리 (ASM)

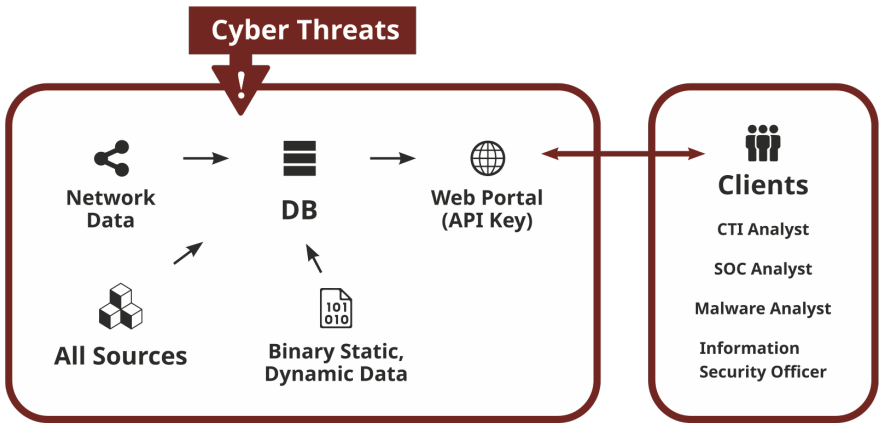
Cyber Threat Intelligence Platform

사이버 위협 인텔리전스 플랫폼

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

THREAT RECON

THREAT RECON



1

집중 및 차별화

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

2

정보보안 활동 체계 수립

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

3

특화된 플랫폼

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

4

특정 이슈 확인

특정 이슈 관련 위협 정보의 확인 가능

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

NSHC SECURITY

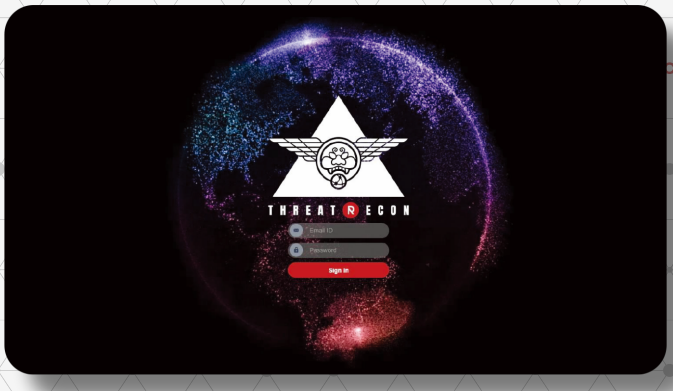
ba.sales@nshc.net 02-6951-3999
(주)NSHC 서울시 금천구 가산디지털1로 186 제이플라츠 806호

특화된 CTI 서비스

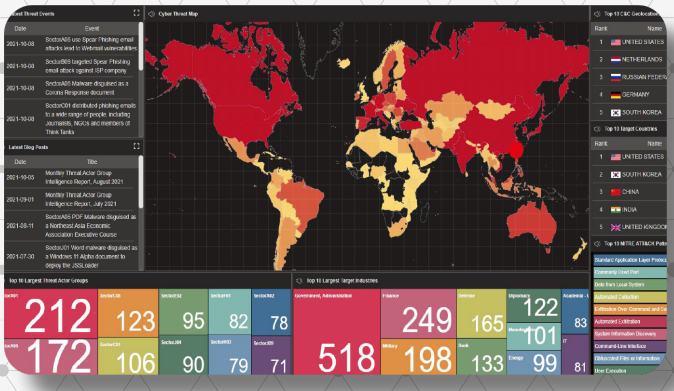
ThreatRecon팀이 축적해 온 위협 탐지 체계 기술력으로 위협 정보를 수집 및 분석합니다. 이를 바탕으로 기업 내 활용 가능하고 **특화된 CTI (Cyber Threat Intelligence) 서비스**를 제공합니다.

18	252	4,222	356,714
Sector	Group	Event	Indicator

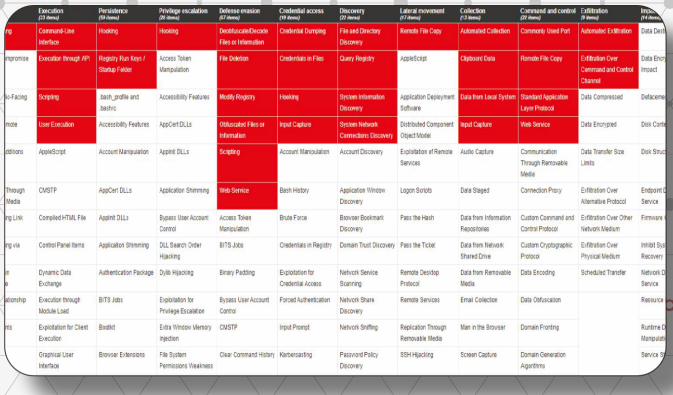
ThreatRecon 특장점



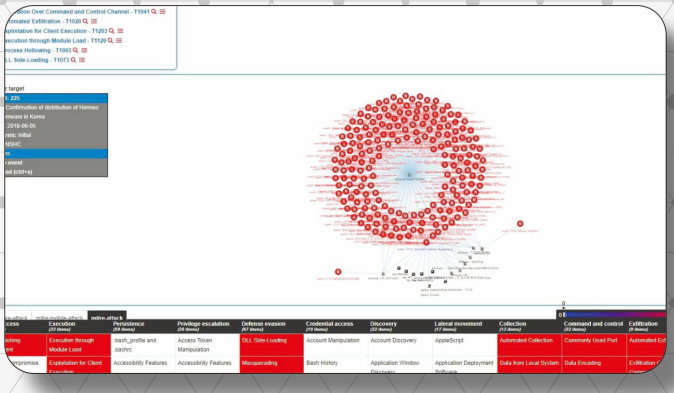
웹 기반 포탈 접속



대시보드



MITRE ATT & CK Framework 기반 공격 단계 정의



수집된 이벤트와의 상관 정보

ba.sales@nshc.net

NSHC SECURITY

StealthMole
다크웹 위협 인텔리전스

THREAT RECON
사이버 위협 인텔리전스

SooJi.Bee
Attack Surface Management by ITF
공격 표면 관리 (ASM)

THE BOIM 안전한 비즈니스 운영을 위한

사이버 위협 인텔리전스 서비스

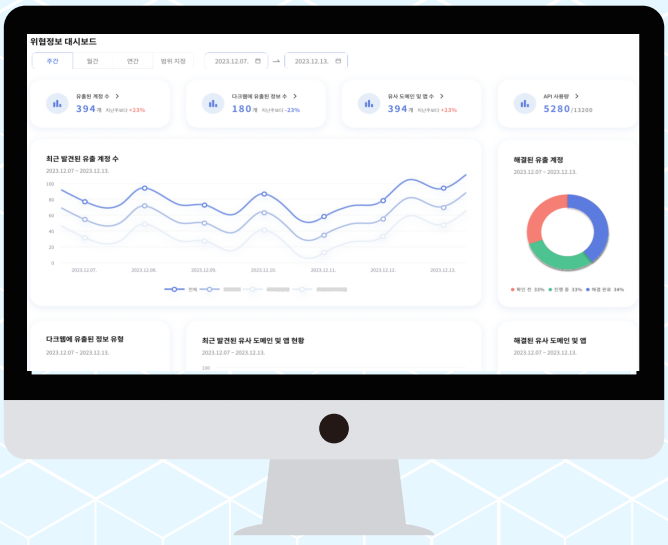
Threat Hunting Expert -Business Operational Intelligence Management

외부위협정보 인식&대응 자동화 서비스

THE BOIM

외부위협정보 조사 리포트 (구독형)

deep.insight



실시간 위협대응

전문가 솔루션을 사용하지 않고도 자사의 외부위협정보와 유출정보의 실시간 모니터링 가능

- 저렴한 비용으로 리스크에 대응
- 웹 상 유출정보 확인시 실시간 알람

D.A.R.T 모델

사이버 보안 리스크 관리 4단계 모델 제시

- Dashboard : 손쉬운 위협 모니터링
- Alarm : 실시간 신규 유출정보 알람
- Report : 정기 위협정보 조사 리포
- Treatment : 외부 노출 IT자산 관리

누구나 사이버 보안 리스크를 전문적으로 관리할 수 있는 세상!
합리적인 **Cyber Risk Management의 자동화**가 가능한
THE BOIM 서비스를 지금 만나보세요!

NSHC SECURITY

ba.sales@nshc.net 02-6951-3999

(주)NSHC 서울시 금천구 가산디지털1로 186 제이플라츠 806호

CRM?
Cyber Risk Management

비즈니스 운영을 위한 **유출정보 모니터링 서비스**로서,
IT인프라를 사용하는 **모든 기업들이 관리 대상**입니다.

유출정보 DB + IP/DNS 진단 + SNS 공개정보 + 기밀정보 유출조사 + ASM 공격표면

매년 난이도가 높아지는 IT자산 관리와 사내 정보보안 리스크,
THE BOIM의 정기 리포팅과 자동화 모니터링 서비스로 대응하세요!

주요 기능 (Key Feature)

CTI + DarkWeb + ASM + MTI	1	다양한 모듈
인텔리전스 전문 연구 조직 보유	2	전문가 진단
유출정보 모니터링/실시간 알람	3	실시간 대응

여러 보안전문가용 플랫폼 중 필요한 모듈만 추려서 서비스의 형태로 제공!

THE BOIM의 유출정보 모니터링 서비스는 타겟 비즈니스와 업계에 맞춘 최적의 플랫폼을 선택, 사이버 보안 전문 분석가가 직접 도출한 결과를 Dashboard, Alarm, Report 등의 제공 형태로 **실시간에 가까운 모니터링 및 분석 서비스**를 가장 **최적화된 가격**으로 제공하고 있습니다.

ba.sales@nshc.net

NSHC SECURITY

THE BOIM
사이버 위협 관리 서비스

FRIIM
클라우드 보안 및 자원관리

THE NEXUS
가상자산 보안 및 위험관리

Cloud Native Application Protector Platform

클라우드 보안 및 자원관리 통합 솔루션

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

FRIIM

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 기준에 따른 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

“ 클라우드 보안도 제로 트러스트!

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

NSHC SECURITY

ba.sales@nshc.net 02-6951-3999
(주)NSHC 서울시 금천구 가산디지털1로 186 제이플라츠 806호

FRIIM
도입효과

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

운영 비용
최대 50% 절감

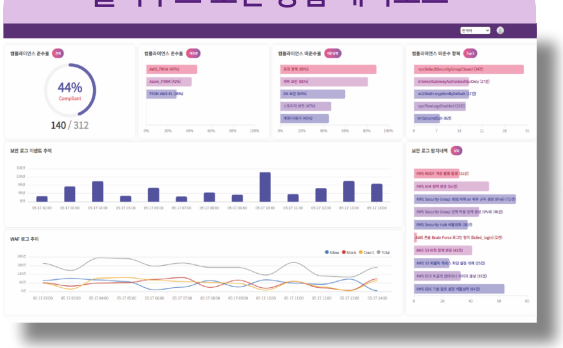
관리 체계
최대 40% 개선

서비스 점검시간
최대 2시간 단축

클라우드 보안준수율
최대 100% 달성

FRIIM 특장점

클라우드 보안 통합 대시보드

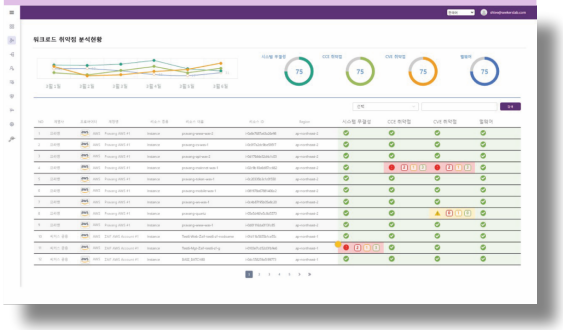


- 컴플라이언스 준수율 및 미준수 항목 확인
- 보안 이벤트 및 WAF 로그 추이, 탐지 내역 확인
- 고객맞춤형 대시보드 커스터마이징 서비스

클라우드 네트워크 토폴로지

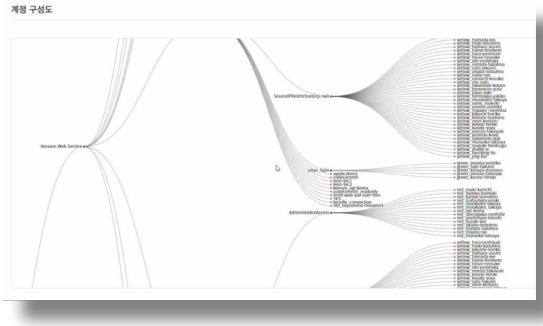
- 네트워크 자산 배치 상황 및 리소스 점유율 확인
- 미사용 VPC 등의 불필요 자산 검출 기능
- On-Demend 서버와 하이브리드 네트워크도 인식

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 대응 가능

ba.sales@nshc.net

NSHC SECURITY

THE BOIM
사이버 위협 관리 서비스

FRIIM
클라우드 보안 및 자원관리

THE NEXUS
가상자산 보안 및 위험관리