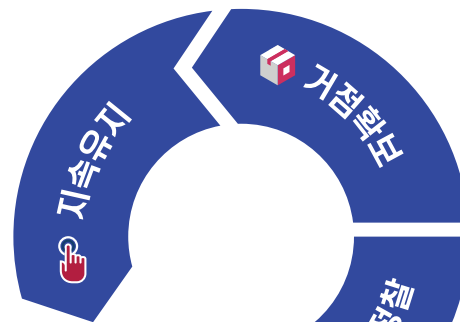


여러분의 중요한 IT 자산이

해킹 위협에 노출되어 있거나, **이미 해킹**되었을 수 있습니다.

Cyber Kill Chain 초기 침투 이후
침해 과정에서 발생하는
공격자의 움직임(통신 사실)을 포착하라!!!



정찰

초기침투

권한상승

측면이동

내부정찰

목표달성

(주)나루씨큐리티가 제공하는 보안 서비스는 네트워크 **통신 데이터의 특성 및 변화**를
침해 관점에서 관리하고 **악성 여부**를 **ZeroTrust 관점**에서 지속적으로 **검증**합니다.



CONNECTOME® ZeroTiCA

네트워크 통신 데이터를 기반으로 **사이버 위협을 식별**하고 **분석**하는
국내 최고의 전문 기업 **(주)나루씨큐리티**가 여러분과 함께하겠습니다.

사이버 위협 현황 및 대응 전망



위협 현황

SBS NEWS
전날 대 PC에 깔린 '이것' 북한 해커조직이 노렸나?

이슈
방산업체 10여곳, 탈탈 털렸다 북한 해킹 조직, 전방위 공격 확인

뉴스A
아는가? 뺑뚨린 사법부 어떤 정보 샀나?

해커
제국어웹

의성코드
신한은행·농협·제주은행

KT 직원들, 고객 PC 해킹 의혹

삼성·LG, 내부 영업비밀·개인정보 등 유출

SK telecom
SKT, 고객 유실 정보 유출 정황

중소기업 랜섬웨어 피해 '속수무책'

8 NEWS
"공공기관, 방산·바이오업체 60여 곳 피해"

과거 수법 안 쓰면 특정 어려워...10%는 불특정

북 해커들, 대기업보다는 주변 '악한 고리' 겨냥

북한 해킹조직 특정 어려워...공동 목표 해킹 늘어

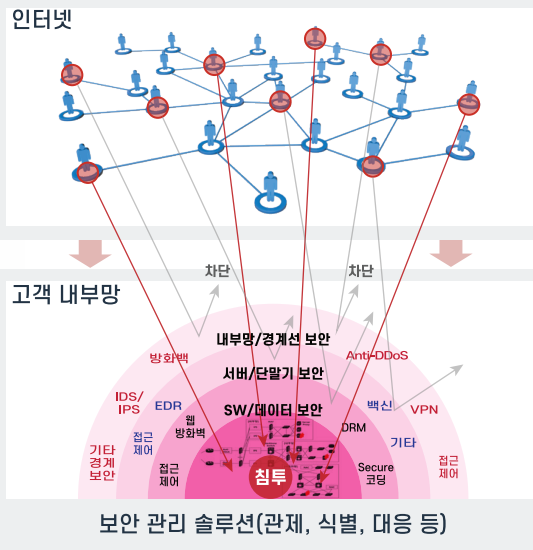
건설·기계분야도 '기술 탈취 주의' 합동권고문 발표

북, 60여개 기관 200여 PC해킹 피해...

사이버 공격은

발생건수, 규모, 피해 심각성, 파급 영향 측면에서 **계속 진화 중** ...

사이버 공격이 갈수록 고도화, 지능화, 정교화되고 있으며 위협의 양상도 빠르게 변화하고 있음



사이버 공격 TTPs (탐지 / 방어 한계)

- 방어 회피, 원점 추적 차단, 표적 공격 등 기술 사용
- AI 기술 및 공급망 악용, IoT 기기 악용 등 전술 사용



대응 전망

IT 환경 복잡

IT 환경의 보안 영역 다양성

보안환경 복잡

데이터/Application/물리/인프라/계정보안, 운영보안, 서비스, 사기/거래보안, 거버넌스/규제 등

변화 촉진

Zero Trust 보안 모델 기반의 방어 체계 가속화

"절대 신뢰하지 말고 **항상 검증**하라."

"공격자가 내부 **침입**했다고 **가정**하라."

"**신뢰** 수준을 **명시적**으로 **확인**하라."

변화 촉진

공격기술 진화

공격과 방어의 비대칭성

보호/방어 한계

공격자는 IT인프라 및 서비스 환경의 단 한 가지 약점만 이용하여 침투하면 성공하지만, 방어자는 모든 환경 요소에 대한 보안조치 필요 (보호/방어의 한계)

그럼에도 불구하고

100% 방어 불가!!!

단순 방어전략 (예방, 탐지, 대응)

능동적인 방어전략 (적극적인 내외부 공격자 식별)

- 기존 보안체계 무력화를 통해 내부망에 침투 후 탐지되지 않고 활동하는 공격을 식별하여 차단 (내부망 침해 여부 확인)
- 내부망 초기 침투 이후 목적 달성 이전에 공격을 식별하여 차단
- 내부망 침투 공격에 대한 인터넷 공격 경로 및 원점 추적, 대응

(주)나루씨큐리티 전문성

2010년 회사 설립 초기부터 국가기관을 지원하여 **사이버 위협 및 범죄 행위에 대응**하여 왔으며
혁신적인 위협 분석 및 침해 사고 조사 노하우를 기반으로 보안 서비스를 제공하고 있습니다.



네트워크 위협 분석 전문 기업

침해 평가 및 사고분석 전문 기업

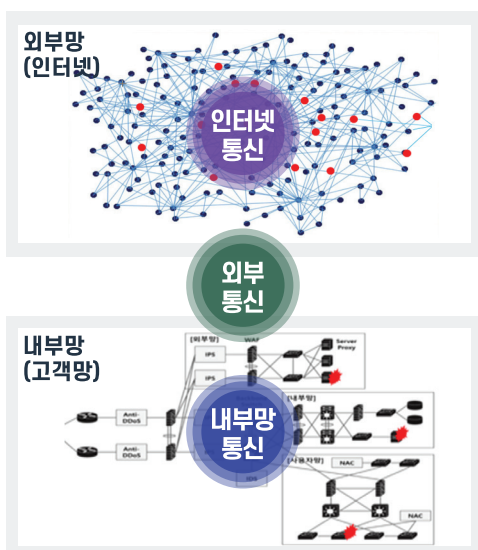
Cyber BattleField 전문기업

15년 이상 사고조사 및 대응 경험

50건 이상 대규모 사고조사 경험

상시 유관기관 침해 사고 대응 협력

공급 제품 및 서비스



공급 솔루션		제공형태	용도
ConnecTome NDR		제품	내부망 통신 데이터 기반 공격 징후 식별/추적/분석, 위협 헌팅
N-TIS		제품/서비스	외부 인터넷 통신 데이터 기반 공격 징후 식별 및 공격 원점 추적
침해 평가 (CA)	NCA (진단형)	서비스	ConnecTome + N-TIS 기반 침해 사고 분석 및 위협 평가
	ZeroTiCA (구독형)		
Cyber BattleField (사이버 배틀필드)		제품/서비스	가상화 기술 기반 사이버 훈련체계 및 테스트 베드 구축

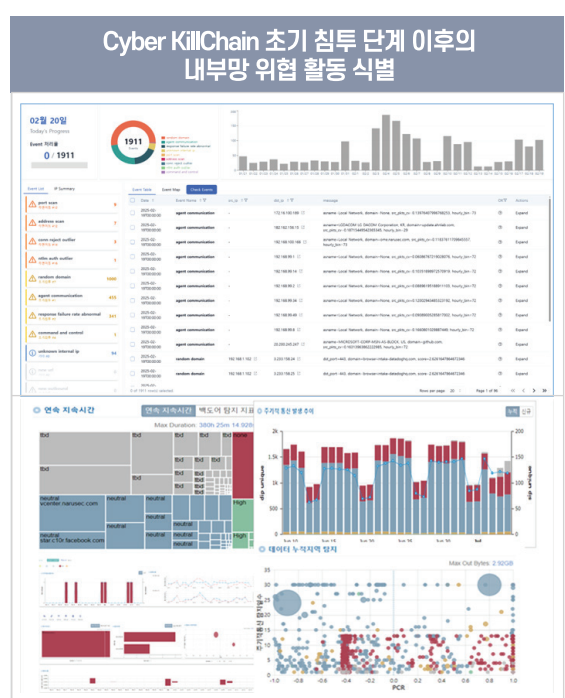
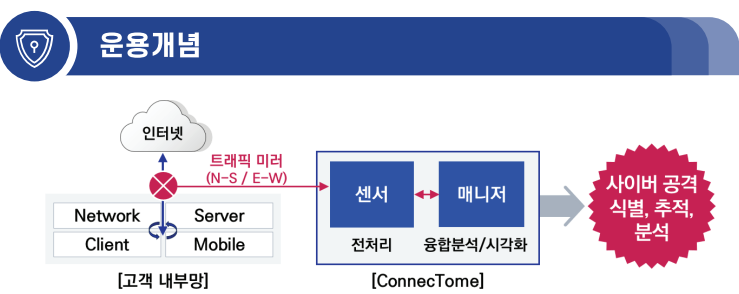
내부망 위협 징후 탐지체계 (ConnecTome NDR)

APT 공격 등 고도화·지능화된 방식으로 경계선 방어 체계를 우회 침투하여 탐지되지 않은 채 내부망에서 은밀히 활동 중인 위협을 탐지하는 솔루션입니다.

필요성

“사이버 공격을 위해서는 네트워크 통신이 반드시 필요하며 이러한 통신 데이터에는 공격자의 움직임(통신 사실)이 숨어 있습니다.”

- 01**
내부망이 해킹된 상태로 침해가 진행되고 있는지 알 수 없다.(침해를 전제로 한 위협 대응 방식 필요)
- 02**
방화벽, IDS/IPS, 백신, APT 대응체계 등을 우회한 고도화·지능화된 공격 행위 (악성 호스트) 식별 필요
- 03**
내부망 통신 데이터 분석을 통해 보안 관점의 IT 자산 운용 및 위협 상황의 실시간 인식 및 대응 필요
- 04**
식별된 침해 지표 또는 위협 인텔을 기반으로 내부망 위협 탐지 및 침해 사고 분석 체계 필요



-
- 주요기능**
- 1**

실시간 상황 이벤트 발생 및 분석 기능 제공

• 센서/매니저, 네트워크/자산운용 변화
• IoT 기반 위협 탐지, 통신 행위 기반 이상 징후 등
- 2**

실시간 운용 상황 및 위협 상황 인식 시각화 제공

• 센서/매니저/네트워크/로그/자산운용 변화, 통신 현황 등 종합적인 운용 상황 파악 가능
• 탐지 위협 등 대한 종합적인 위협 상황 파악 가능
- 3**

내부망 위협 추적(헌팅) 및 침해 분석 기능 제공
- 4**

내부망 위협의 인터넷 추적·분석(N-TIS 연계) 등

- 기존 보안체계를 우회 침투하여 내부망에서 은밀히 활동하는 **지능형 지속 위협(APT) 공격 식별**
- 목표 네트워크를 표적으로 특수 목적을 수행하도록 정밀하게 설계된 **맞춤형 표적 공격 식별**
- 조직 내부자의 악용/실수 또는 HW/SW 공급(유지 보수) 업체를 통한 **공급망 위협 식별** 등

네트워크 트래픽과 활동을 실시간 모니터링하고 분석하여 내부망 위협 징후를 식별하여 대응하세요.

“네트워크 통신 데이터를 신뢰하지 말고 검증하라!”

네트워크 통신 데이터에 대한 ZeroTrust 원칙을 적용한 솔루션



특장점



01.

On-Premise 또는 Cloud 환경을

기반으로 위협 및 이상 징후 식별에 특화된

독창적인 통신 데이터 수집

- IP 주소, 포트, 연결 상태, 전송된 바이트 수, 프로토콜 정보 등 네트워크 연결에 대한 정보
- HTTP, DNS, FTP, Kerberos, SMB, SSH, SSL/TLS 등 다양한 프로토콜 트래픽 정보
- 응용 계층 프로토콜 헤더 값 분석/ 처리 후 저장
- 네트워크를 통해 전송되는 파일에 대한 정보 (파일의 해시값, 파일 이름, MIME 타입 등)
- ARP, ICMP, IP, TCP/UDP 기반의 세션 추적에 필요한 정보
- 네트워크 연결에서 발생하는 IP 주소의 지리적 위치 정보

내부망 통신 및 독창적인 메타데이터 생성



02.

공격자 통신 행위 탐지를 위한 통신 특성
변화관리 기반의 **지능형 이상 징후 탐지 모델 및
명령제어 채널 자동 탐지 엔진(미국 특허)을 적용**

- ▶ 최초침투 단계
C2통신, 웹 셸 통신 탐지 등(00개)
- ▶ 측면이동 단계
스캔행위, 내부이동 탐지 등(00개)
- ▶ 거점장악 단계
원격연결, 관리자PC 장악 등(00개)
- ▶ 정보유출 단계
DB서버 장악, 유출징후 등(00개)

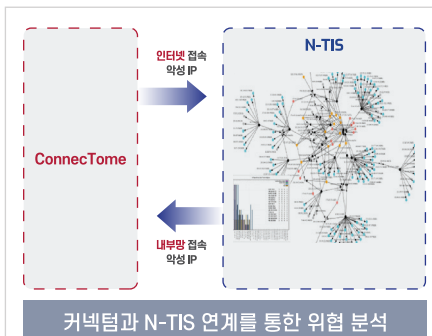
총 00개의 위협 탐지 모델 기반 이상 징후 분석



03.

ConnecTome에서 식별한 위협에 대한
N-TIS 기반의 **인터넷 위협 경로 분석** 지원

* N-TIS : (주)나루씨큐리티(위협대응센터)에서 추적을 통해 관리하고
있는 위협 인텔리전스를 기반으로 위협 분석을 지원하는 서비스

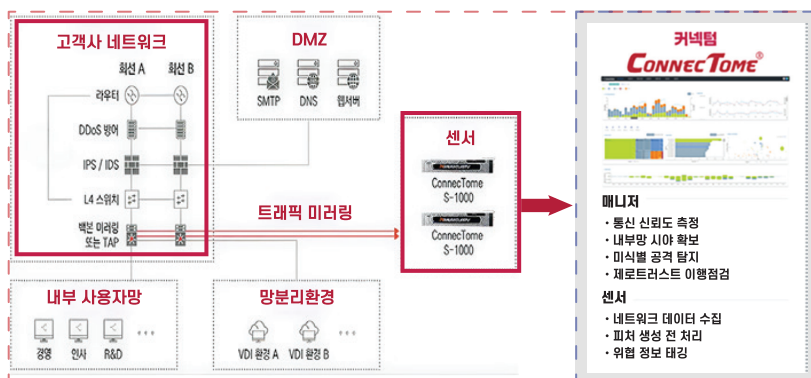


커넥톰과 N-TIS 연계를 통한 위협 분석

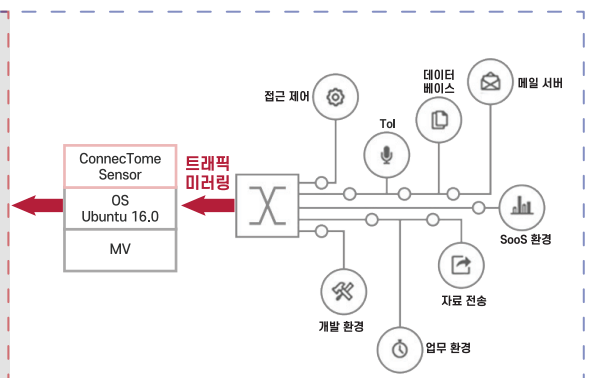


ConnecTome 구성 환경

01. On-Premise 환경



02. Cloud 환경



“

ConnecTome(커넥톰)은 내부망에서 공격자의 통신 행위 탐지 모델을 기반으로
알려지지 않은 위협을 식별하는데 특화된 **NDR** 솔루션입니다.

”

01.

조직 내부망에서 탐지되지
않은 채 은밀히 활동하는
위협을 탐지할 수 있습니다.

02.

위협 식별(탐지) 시
공격 경로 추적 및 피해 자산
식별이 가능합니다.

03.

조직 내부 네트워크에서
데이터 유출 징후를
식별할 수 있습니다.

04.

침해 지표를 기반으로
내부 네트워크에 대한 위협
현황(정찰)이 가능합니다.

05.

네트워크 트래픽 데이터를
기반으로 위협 분석 및 침해 사고
조사 분석이 가능합니다.

표적형 위협 인텔리전스 서비스

N-TIS, Network based Targeted Intelligence Service

인터넷 통신 데이터의 위협 분석을 통해 식별된 위협 인프라 정보를 기반으로 추적 대상 표적(IP/대역)에 대한 위협 분석 서비스를 제공하는 시스템입니다.



필요성

01

사이버 공격자는 글로벌 인터넷 공간에서 공격에 악용할 인프라를 구축하고 필요시 공격에 활용 중

02

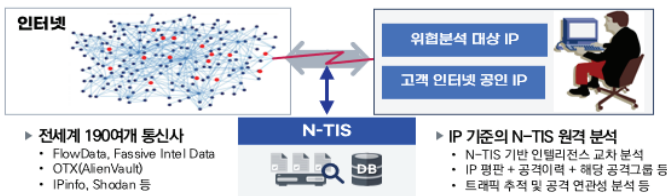
방어자는 네트워크 경계선 기반 대응으로 인터넷 공간의 위협을 분석하고 추적하는 데 한계가 있음

03

침해 사고 예방 및 위협 대응을 위해 탐지된 위협에 대한 인터넷 경로 및 원점 추적·분석 필요성 절실



운영개념



주요기능

- 1 내부망에서 탐지한 위협 징후 또는 침해에 대한 인터넷 공간의 공격 경로 및 원점 등 추적·분석 지원
- 2 내부망에 대한 위협 징후 분석 및 진단 서비스 제공
- 3 공격자 표적 등 특정 표적에 대한 다양한 분석 지원
- 4 N-TIS 인텔을 활용한 내부망 방어 수준 강화 등



특장점



01.

인터넷 악성 인프라 추적 및 연관분석, 변화관리 등을 통해 표적형 위협 인텔리전스 관리



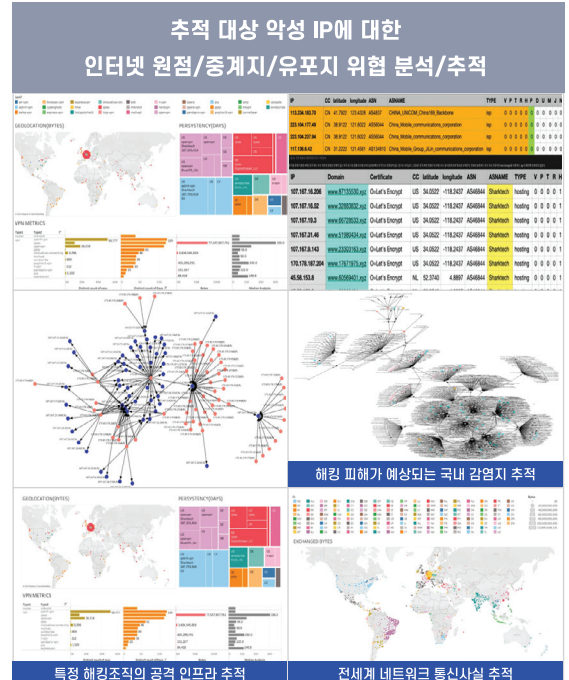
02.

관심 네트워크(IP/대역)에 대한 장기 추적성 관리



03.

내부망 탐지 위협에 대한 인터넷 추적 가시성 제공 등



침해 평가 서비스

CA, Compromise Assessment

고객 IT 인프라 환경을 네트워크부터 호스트까지 침해 관점으로 평가해
“우리 기업이 이미 **해킹**되어 있는 것은 아닌가?”라는 의문에 답을 드리는 서비스입니다.



침해평가란?

“

고객 IT 인프라 환경에 과거 또는 현재 진행 중인 침해 흔적이 있는지 여부와 보안 취약성 등을 분석·평가 및 보고를 통해 “**침해가 사고로 이어지지 않도록**” 대응하는 새로운 개념의 위협 대응 활동

”



목적 (3S)

Secure

공격 대상이 될 수 있는 표면,
공격에 취약한 구조적인 문제점 식별

Safe

해킹 공격을 조기에 식별해
공격이 완성되기 이전에 무력화

Success

비즈니스 연속성 보장

『 NCA가 숲을 본다면

HCA는 나무를 보는 것 』

Making Sense of the Unknown
NARUSECURITY

PLAINBIT

MITRE ATT&CK 기반 침해 평가

공격자의 TTP (전술, 기법, 절차)를 기반으로 알려진 공격부터 잠재적인 위협 행위까지 체계적으로 평가
- 초기 침투, 거점 확보, 실행/지속, 내부 이동, 유출/파괴 행위 식별

제로트러스트 기반 침해 평가

네트워크와 호스트에서 일어나는 모든 연결 행위를 모니터링해 평가
- 원격제어, 터널링, 프록시, 비정상 DNS 질의 등 통신 식별

위협 지표 기반 침해 평가

최근 3년 동안 발생한 침해사고에서 활용된 위협 지표를 기반으로 평가
- 봇넷/해킹 공유지/명령제어 인프라 연결 통신, 공격 도구

10년 이상, 4,000건 이상의 사고조사/대응 경험과 노하우를 기반으로 국내 침해대응 분야를
선도하는 나루씨큐리티와 플레인비트가 여러분의 사이버 방어력을 한층 강화해드립니다.

네트워크 기반 침해 평가 서비스 (진단형)

NCA, Network Based Compromise Assessment

고객 인터넷 또는 내부망 네트워크 환경에서 발생하는 **통신 데이터를 수집·분석하여**
내부망 침해 징후 및 취약성 여부를 평가하여 대응 방안을 제시하는 서비스입니다.

필요성

01

지능적인 사이버 공격
 기술의 진화로 100%
 네트워크 방어 한계 발생
 (보안체계 우회 침투)

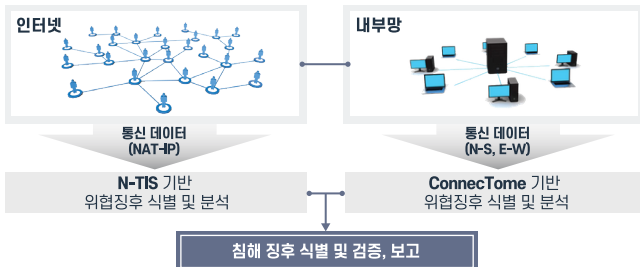
02

보안체계를 우회한 공격이 내부망에서 탐지되지
 않은 채 활동하고 있을 가능성 상존
 (공격 활동 진행 (자료 유출 등), 공격자
 인프라로 악용, 차후 공격 교두보 확보 등)

03

침해 사고 예방 및 위협
 대응을 위해 탐지된 위협에
 대한 인터넷 경로 및 원점
 추적·분석 필요성 절실

운용개념

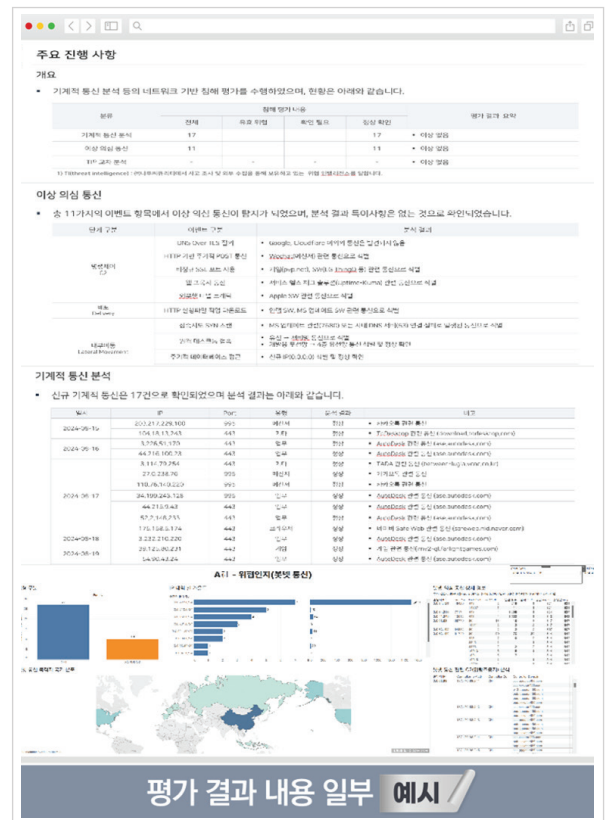


수행 시기

- ✓ 내부망이 침해 상태인지 확인이 필요한 경우
- ✓ 침해 사고 이후 잔존 위협 확인이 필요한 경우
- ✓ 침해로 의심되는 위협 및 이상 징후 감지 시
- ✓ 침해 사고 예방 차원의 주기적 진단 필요 시
- ✓ 동종 업계 또는 협력사 등 침해 사고 발생 시

특장점

- ✓ **01.** “증가하는 침해 사고, 탐지되지 않은 침해 문제”의 적극적 대응을 위해 국내 최초(‘24.5.) 서비스 출시
- ✓ **02.** ㈜나루씨큐리티는 NCA 3대 요건 (위협/침해 사고분석 전문가, 분석 도구, 위협 인텔)을 모두 갖추고 있음
- ✓ **03.** N-TIS 기반의 원격진단 정보와 ConnectTome 도구를 활용한 효율적인 NCA 수행
- ✓ **04.** HCA 전문 기업 “플레인비트”와 전략적 제휴를 통해 필요시 CA (침해 평가) 공동 수행



ZeroTiCA (구독형)

ZeroTrust with Targeted Intelligence & Compromise Assessment

고객 내부망에 대한 실시간 위협 탐지 및 침해 여부를 평가하여 대응 방안을 제공하는 **ZeroTrust 기반의 구독형 침해 평가 서비스**입니다.

“ 내부망에 변화가 발생하면 신뢰하지 말고 검증하라!!! ”



서비스 배경

01

정보보호 수준 저조로 사이버 공격에 취약한 기업을 대상으로 내부망 위협을 탐지하는 원격 서비스 제공

02

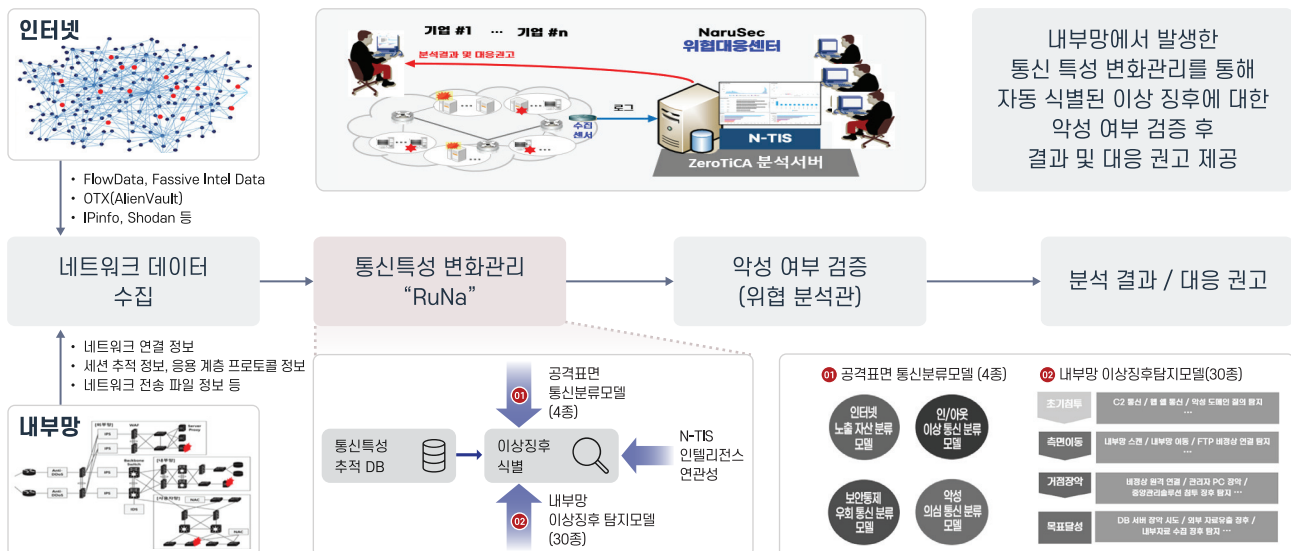
Cyber Kill Chain 초기 침투 후 내부망에서 활동하는 표적형 공격을 탐지하는 원격 서비스 제공

03

ZeroTiCA 서비스를 통해 고객 네트워크 침해 사고 예방을 위한 최고의 보안 파트너로서 역할 수행



운영개념



특장점

✓	01.	✓	02.	✓	03.	✓	04.
	웹 기반의 서비스로 내부망 위협 식별 및 분석을 원격에서 지원하도록 설계		위협 분석 전문가 경험 및 노하우를 반영한 통신 특성 변화관리 엔진 기반의 공격자 통신 행위 식별		위협 분석 전문가의 모니터링을 통한 이상 징후 분석 및 악성 여부 검증		(주)나루씨큐리티의 위협 분석 및 사고조사 역량 100% 활용 (내부망 위협에 대한 모니터링 및 대응)

사이버 배틀필드 (Cyber Battlefield)



① 침해대응 및 공방 훈련체계

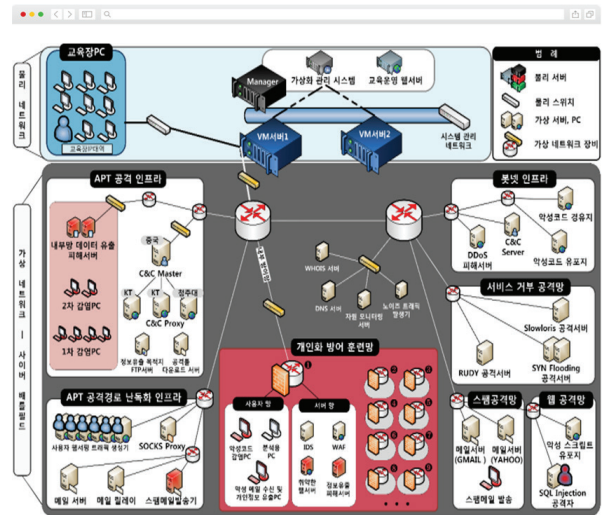
네트워크 및 호스트 가상화 기술 기반의 인터넷 및 기업 내부 네트워크 환경을 구성하여 침해 사고 대응 및 사이버 공방 훈련을 지원하는 시스템입니다.

주요 기능

1	침해대응 및 공방 훈련을 위한 가상 네트워크 환경 구성	• 가상 네트워크와 및 실제 물리 장비 연동 환경 포함
2	침해대응 및 공방 훈련 시나리오 기반 운용 콘텐츠 구성	• APT 공격, DDoS 공격 웹 해킹 사례 등
3	개인별 훈련 환경 구성, 교육과정 관리, 훈련 모니터링	

특장점

✓ 01.	자체 개발한 가상 네트워크 맵 구성 자동화 도구를 기반으로 복잡·다양한 교육훈련 환경 구축 및 자체 변경 관리 가능
✓ 02.	실제 물리 장비와 가상 네트워크 커넥터 기술 적용 및 훈련 상황 모니터링을 위한 시각화 기능 제공



사이버 배틀필드 구성 예시



② 사이버 테스트 베드(Cyber Testbed)

사이버 기술 시험평가, 사이버 공방 훈련, 체계 성능 평가 등 시험환경 구성에 최적화된 가상화 기반의 테스트 베드 구축 서비스입니다.

주요 기능

1	다양한 유형의 가상화 네트워크 구축 기능 제공 (웹 기반의 네트워크 구성 및 관리, 효과적인 VM 제어 등)
2	가상머신(VM) 설정 기능 제공 (도메인명, CPU, Memory, vNIC, DNS 서버 설정 등)
3	실제 물리 장비 연동 설정 기능 제공 등

특장점

✓ 01.	자체 개발한 가상 네트워크 구성 자동화 도구를 활용하여 다양한 시험환경을 신속히 구축 가능
✓ 02.	고객 자체적으로 자동화 도구를 활용하여 시험환경 변경 가능



테스트베드 구성 예시



Naru Security, Inc.

www.narusec.com

서울시 강남구 영동대로 621, 8~9층 (삼성동 621빌딩) 06087

P. 02-522-7912 | F. 02-522-5765
E. sales@narusec.com