

침해평가 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 위협대응 활동

”



=



+



목적 (3S)

Secure

공격 대상이 될수 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 』

MITRE ATT&CK 기반 침해 평가

공격자의 TTP (전술, 기법, 절차)를 기반으로 알려진 공격부터 잠재적인 위협 행위까지 체계적으로 평가
- 초기침투, 거점확보, 실행/지속, 내부이동, 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 **나루씨큐리티**와 **플레인비트**가 여러분의 사이버 방어력을 한층 강화해드립니다.

네트워크 기반 침해평가서비스 (진단형)

NCA, Network Based Compromise Assessment

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



필요성

01

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

02

보안체계를 우회한 공격이
 내부망에서 탐지되지
 않은 채 활동하고 있을
 가능성 상존

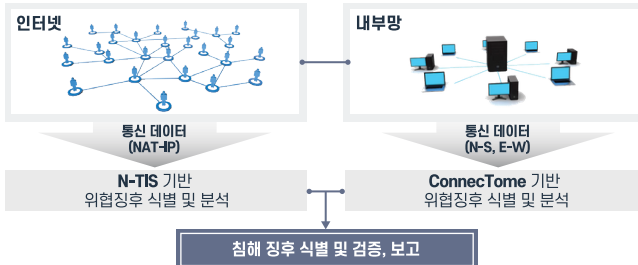
03

(공격활동 진행
 (자료유출 등), 공격자
 인프라로 악용, 차후
 공격 고도화 확보 등)

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



운용개념



수행시기

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



특장점

- | | | | |
|---|--|--|---|
| <p>✓ 01.</p> <p>“증가하는 침해사고, 탐지되지 않은 침해 문제”의 적극적 대응을 위해 국내 최초(‘24.5.) 서비스 출시</p> | <p>✓ 02.</p> <p>(주)나루씨큐리티는 NCA 3대 요건 (위협/침해사고분석 전문가, 분석도구, 위협 인텔)을 모두 갖추고 있음</p> | <p>✓ 03.</p> <p>N-TIS 기반의 원격진단 정보와 ConnectTome 도구를 활용한 효율적인 NCA 수행</p> | <p>✓ 04.</p> <p>HCA 전문기업 “플레인비트” 와 전략적 제휴를 통해 필요시 CA (침해평가) 공동 수행</p> |
|---|--|--|---|

