openbase

FireEye™

where the intelligence works 오픈베이스

APT 공격 차단 솔루션

www.openbase.co.kr

FireEye™

제로데이 공격, 랜섬웨어 그리고 다양한 전달/우회 기법을 이용하는 멀티 벡터 기반 고도화된 APT 공격 증가

외부 영역 | 대응 기준 | 내부 영역

1 정찰
- 정보 수집 및 프로파일링
- 네트워크 애플리케이션 정보 수집
- 원격 접속 식별

2 초기침투
- 스피어 피싱 이메일
- 멀티플로우 잇스플로잇

3 거점확보
- 악성코드 다운로드 C&C

4 권한상승
- Mimikatz 바이너리 전송
- Mimikatz 사용 흔적
- Windows Credential Editor 바이너리 전송

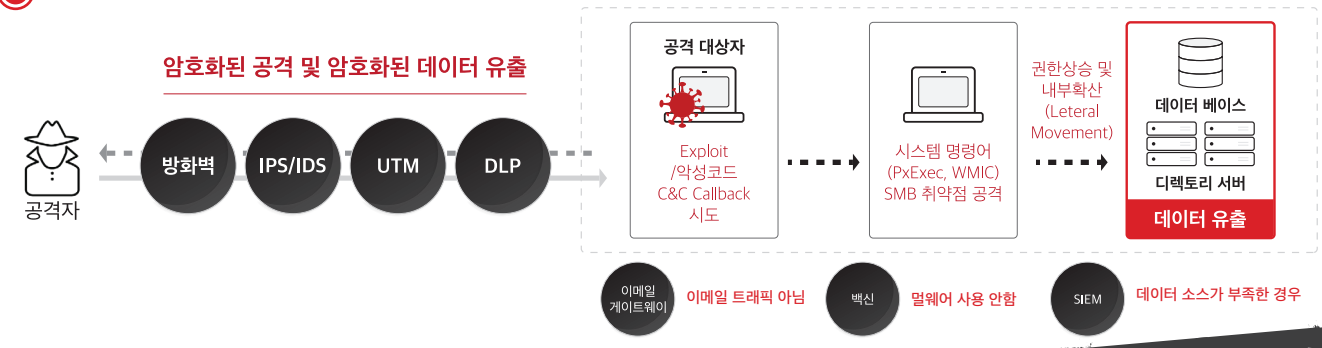
5 내부정찰
- DNS Zone 트랜스퍼
- 사용자 디렉터리 목록화
- 원격 사용자/공유 폴더 확인

6 내부확산
- AT 원격 스케줄러 서비스
- PsExec 사용
- Windows WMI 원격 쉘 실행

7 연결유지
- SMB 포트를 이용한 악성코드 업로드
- 원격으로 파일 전송
- 휴지통 폴더 이용

8 목적달성
- ADMIN$ 또는 C$에서 일반적이지 않은 파일의 전송

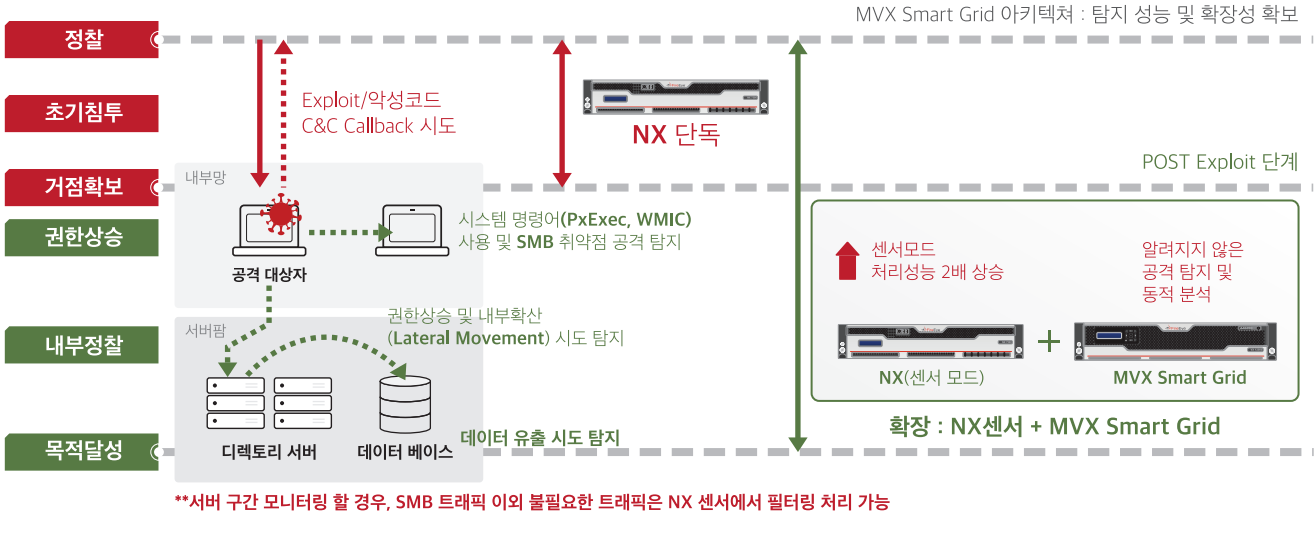
54% 기업은 1번 이상 해킹 피해로 데이터 유출 또는 내부 시스템 피해 경험



더 나은 보안 가시성 확보와 효율적인 대응 방안 필요 !

Network 시리즈 솔루션

SmartVision 엔진 - Full Attack Life Cycle 기반 지능형 APT 공격 대응 위한 고급 상관관계 분석 엔진



**서버 구간 모니터링 할 경우, SMB 트래픽 이외 불필요한 트래픽은 NX 센서에서 필터링 처리 가능

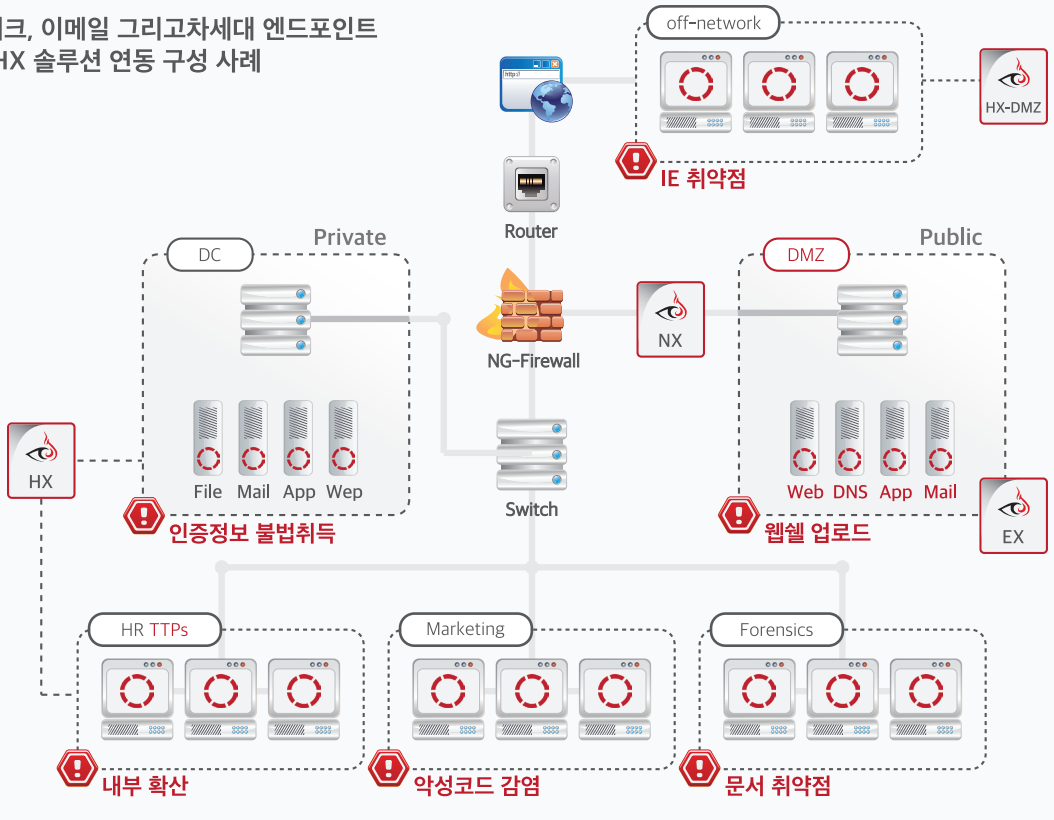
Email 시리즈 솔루션

이메일 기반 알려진/알려지지 않은 APT 위협, 지능형 타켓형 공격 그리고 랜섬웨어 위협 증가

Attack Life Cycle 기반 이메일 APT 공격 대응



네트워크, 이메일 그리고차세대 엔드포인트 APT HX 솔루션 연동 구성 사례



❶ 탐지

Av엔진, Exploit 엔진, Intel룰 기반 IOC 룰

- NX, EX 연동을 통한 탐지 IOC 룰 자동 생성
- 맨디언트 IOC 룰 업데이트 제공
- 알려진 위협 대응 AV엔진
- 이상 행위 기반 Exploit 차단 엔진

❷ 검증 및 조사

Triage Summary, 전수 검사(Enterprise Search)

- 자동화된 Triage 정보 수집
- 사용자 중심 타임라인 기반 검증 및 조사 (Triage 뷰어)

❸ 호스트 격리 및 조치

호스트 격리, Live Response 데이터 수집

- 원-클릭 호스트 격리 조치
- Live Response를 통한 추가 데이터 수집
- 침해 호스트 심층 분석
- 대응 IOC 룰 생성 및 대응 전략 수립

차세대 엔드포인트 시큐리티 기반 대응 복잡성 제거 및 보안 가시성 개선을 통한 지능형 위협 대응 체계 구축



침해 대응 자동화 플랫폼 (Helix)

통합된 침해대응 전용 플랫폼을 통해 보안의 자동화 적용x



어떠한 위협이라도 발견에서 조치까지 수분 이내 완료 가능한 플랫폼



Helix를 이용할 경우, 침해대응과 조치를 불과 수십분만에 완료 가능



여러 경로로 집요하게 침투하는 APT 공격,

이제 실시간 차단으로 빈틈없이 방어하세요!



서울특별시 서초구 매헌로 16 하이브랜드빌딩 4층 (우)06771
TEL 02.3404.5700 FAX 02.3452.3654 E-Mail systemsales@openbase.co.kr