LG CNS

침해사고 선제적 대응을 위한

위협 사냥 (Threat Hunting) 방법론

2021. 5.
LG CNS 스마트보안관제팀 조용섭 책임

LG CNS

Contents

침해사고 선제적 대응을 위한
위협 사냥 (Threat Hunting) 방법론

1/ 위협 사냥이란?

2/ 위협 사냥 방식

3/ 서비스 내역

4/ 서비스 특장점

5/ 서비스 방식

1. 위협 사냥(Threat Hunting)이란?

배경

고도화된 해킹 공격에 의한 랜섬웨어 사고 등 기업 피해가 지속적으로 증대되고 있음

- 20.01 미국 전선생산기업(사우스와이어) 800여대 생산장비 랜섬웨어 감염 및 데이터 유출
- 20.04 유럽 전력회사(EDP) 해킹 및 데이터 유출
- 20.05 영국 전기기업(Elexon) 데이터 유출 및 인터넷 협박
- 20.06 일본 자동차 기업(혼다) 랜섬웨어로 인한 가동 중단

발생 원인

1/ 악성 e-Mail 등으로 **최초 거점 확보 후 조용한 내부 전파**
2/ 파일리스 공격으로 **기존 보안장비 우회**
3/ 기업 내 인지하지 못한 **취약점으로 통한 공격**

Threat Hunting 이란?

- 내부에 숨겨져 있는 위협을 찾는 좋은 방법
- Alert 전에 위협을 감지하여 사고 손실을 줄이거나 제거
- 취약점 발견 및 제거로 공격 가능성이 있는 부분을 줄임
- Alert이 없지만 위협 행위자가 이미 들어와 있지 않은지 확인
- Threat Hunting은 최후의 방어선

※ Gartner 2020, Using Threat Hunting for Proactive Threat Detection

1. 위협 사냥(Threat Hunting)이란?

위협 사냥으로
찾을 수 있는
보안 위협은
무엇일까요?

1 내부 위협 탐지

- 실제 해커가 사내로 침투하여 해킹 시도를 하고 있는가?
- 사내 서버/PC는 악성코드에 감염되어 있지 않은가? 감염되었다면 얼마나 감염 되었나?
- 중앙관리서버(AD, PC보안, 자산관리, 패치관리) 등 주요 서버는 안전한가?

2 보안 취약점 파악

- 외부에서 내부로 접근 가능한 경로가 있는가? RDP, SSH 등
- 정보유출 차단솔루션을 우회하는 통신이 있는가?
- 내부에서 외부로 보안정책을 우회하는 트래픽이 있는가?

3 이상행위 탐지

- 기업 내부에서 외부로 비정상적인 트래픽이 있는가? 과도한 트래픽, 비정상 서비스 접근 등
- 비정상적인 S/W설치로 인한 트래픽은 없는가?

2. 위협 사냥 방식

침해대응 Know-How와 국내외 동향, 내부 사례를 MITRE ATT&CK* 기반에 녹여 점검 기준을 만들고, 이를 통해 기업 내 악성코드/해킹 징후를 탐지함

점검 기준

침해대응 Know-How

\+

국내외 침해동향

\+

내부 관제사례

MITRE ATT&CK Framework*

MITRE ATT&CK Framework*
실제 사고사례를 기반으로 한 민간/정부의 사이버 보안 제품 및 서비스의 위협모델/방법론

점검 방식

시스템 정보 및 로그

- System Info.
- N/W Traffic
- System Logs
- Endpoint behavioral
- VPN Log

보안 Risk 식별

- 악성코드
- 보안정책 우회
- 해킹 징후
- 취약한 설정
- 침해 흔적
- C2 통신

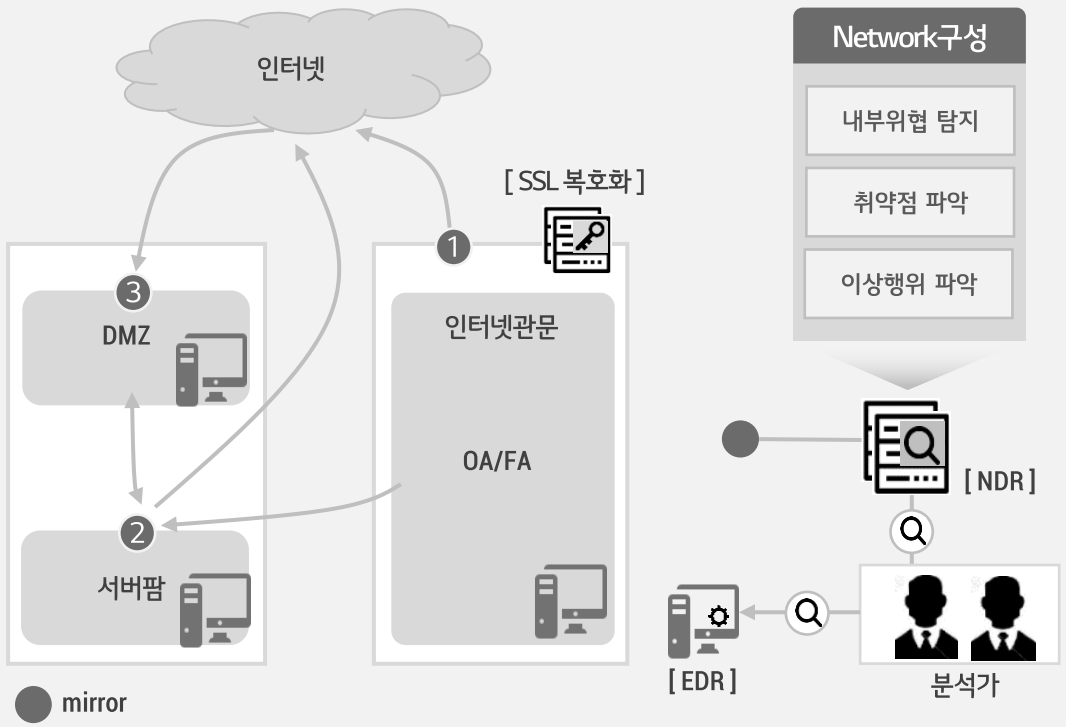
2. 위협 사냥 방식

응용, 네트워, Endpoint단에서 4단계의 위협 헌팅 사이클을 수행함으로써 기존 보안시스템에서 탐지하기 어려운 잠재위협을 식별하고, 위험을 선제적으로 제거할 수 있음

2. 위협 사냥 방식

네트워크 트래픽 분석 전용솔루션, Endpoint 행위기반 분석 솔루션 및 로그 수집기 등을 활용하여 다양한 로그를 수집하고 이를 보안 전문가가 분석함

구성 방식



주요 내용

Network	• NDR(Network Detection & Response)을 활용한 네트웍 이상징후 분석 • Full Packet 기반 트래픽 분석을 통해 보안 장비에서 탐지되지 않는 이상징후 탐지
Endpoint	• EDR(Endpoint Detection & Response)을 활용한 이상징후 분석 • 다양한 OS의 PC/Server에 설치하여 설치 시점 이후의 Endpoint에서 발생하는 위협을 탐지함 • PC/서버에서 수집한 이벤트로그 등으로 과거 및 현존하는 위협을 식별
APP	• AD, VPN, WEB Access, WEB Proxy, DNS 등의 App. 로그 분석을 통해 과거에 존재했던 위협을 식별함

3. 서비스 내역

현재 진행중인 위협과 과거 위협 이력, 그리고 기업내에 존재하는 보안 취약점을 도출하여, 기업내 침투 위협을 가시화함

서비스 01

실시간 위협 탐지

- 실시간 네트워 패킷 분석을 통한 위협 경보 탐지 및 후속 분석
- Endpoint 행위 분석을 통한 위협 경보 탐지 및 후속 분석
- 이기종 장비간 상관 분석을 통한 이상행위 탐지 분석
- 위협 사냥 Cycle (가설 > 수집 > 분석 > 증명) 수행에 따른 선제적 보안 위협 탐지

서비스 02

과거 침투 이력 식별

- 보안장비 및 OS 로그 분석을 통한 과거 침투 이력 후속 분석
- 실시간 위협 탐지와 연계한 침해사고 발생 이력 가시화

서비스 03

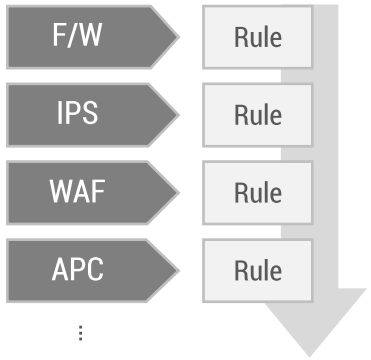
보안 취약점, 보안정책 우회 경로 파악

- 공격 추이 분석에 따른 노출된 보안 취약점 파악
- 보안 정책에 위배되는 이상 트래픽 식별을 통한 보안 정책 Hole, 취약점 식별
- 보안 장비 운영상의 개선 사항 도출

4. 서비스 특장점

LG CNS에서 제공하는 Threat Hunting 서비스는 기존 보안관제서비스의 한계점을 개선을 한 차원 높은 신개념 보안관제서비스로 보안 위협에 대해 수동적인 방어가 아닌 선제적인 방어 기법임

기존 보안관제서비스

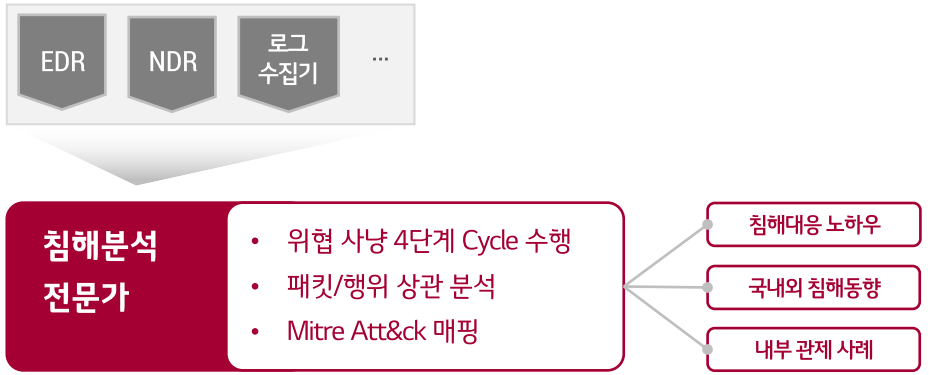


- 알려진 공격 위주 탐지
- 수직적 모니터링 체계
- 장비 로그 의존

수동적인 방어 중심의 보안관제

- 관제 장비 수집 로그 기반 이벤트 모니터링
- 임계치 기반 이상행위 탐지
- 보안 로그에 한정된 침해 공격 파악

Threat Hunting 서비스



선제적 공격 탐지 중심의 보안관제

- 모든 통신 내역 및 실행 행위 모니터링
- 다각화된 정보를 기반으로한 이상행위 탐지
- 보안장비외 다양한 로그 기반 침해 공격 파악

LG CNS의
Threat Hunting 서비스 방식

유형	주요내용
서비스 방식 01 **컨설팅 서비스**	• 특정기간 기업 내 위협을 진단하는 서비스 • 서비스 기간 내 임대 장비 제공되며, EDR/NDR 장비 구매 불필요 • EDR/NDR 장비설치 전 과거의 위협 분석에 제약이 있음
서비스 방식 02 **상시 서비스**	• 서비스에 필요한 EDR/NDR 장비를 제공하여 상시적으로 제공하는 서비스 • 1회성 검증이 아닌 지속 검증으로 다양한 위협에 대해 더 빠른 식별 • EDR/NDR 장비는 고객구매 또는 임대서비스 가능

맺음말

- 위협 사냥은 기업내 숨겨진 위협을 적극적으로 찾아내는 선제적 예방 활동
- 기존 보안 솔루션에서 탐지하지 못하는 영역을 커버 할 수 있어야 함
- 초기에는 일회성으로 실시해보고, 장기적으로는 상시 적용하여 실시간 모니터링하는 것이 중요
- 위협 사냥은 고도화된 전문역량을 보유한 전문업체가 수행해야 효과적

Digital Innovation Enabler

Thank You

LG CNS