G-PRIVACY 2023

2023 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

ZDR(Zero-day intrusion Detection & Response)

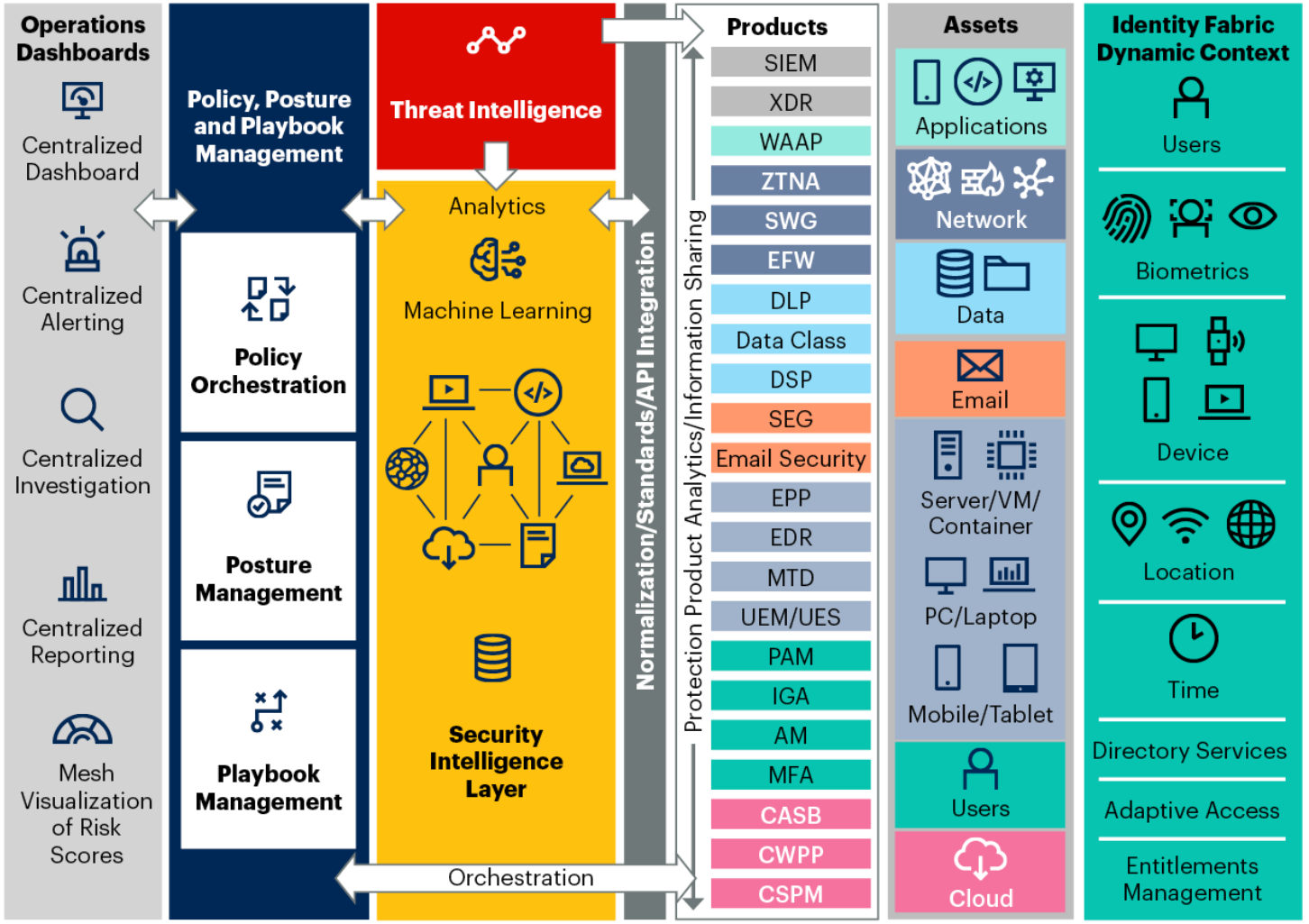
Threat Hunting의 새로운 표준

ABYSS

1. 보안 패러다임 진화의 필요성
2. 제로데이 공격 대응 : Threat Hunting
3. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술
4. 기존 기술과의 비교 분석
5. 제로데이 공격 침투의 실제 사례 분석

01. 보안 패러다임 진화의 필요성 : Many but not Enough

Cybersecurity Mesh Architecture Reference



Source: Gartner

01. 보안 패러다임 진화의 필요성

아직도 답을 하지 못하는 질문이 존재 : 보안사각(NSBS, Network Security Blind Spot)

매일 신규 탐지 정보의 추가를 결재 받을 때

이미 침투해 있지는 않을까요?

새로운 보안 취약점을 발견했을 때

이미 이곳으로 공격을 당하지는 않았을까?

이상한 통신 행위를 발견했을 때

언제, 어디로, 어떻게 들어왔지?

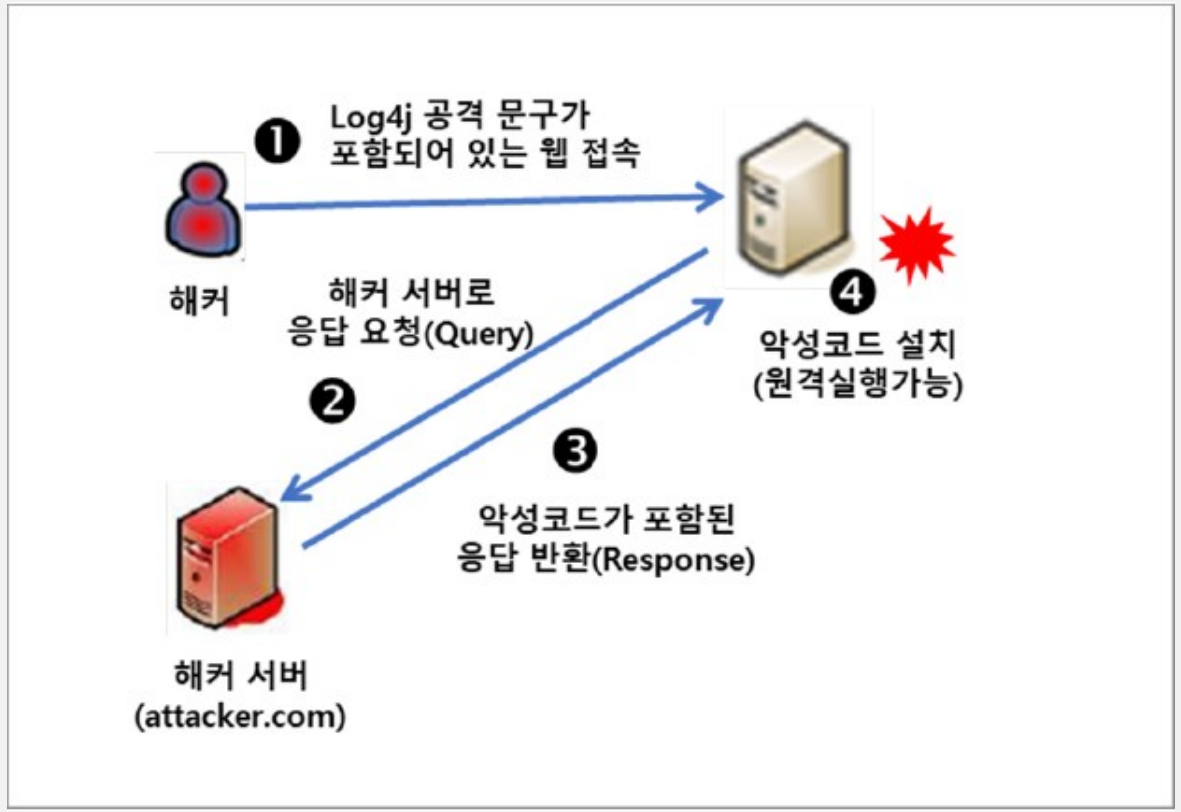
제로데이 문제(공격)

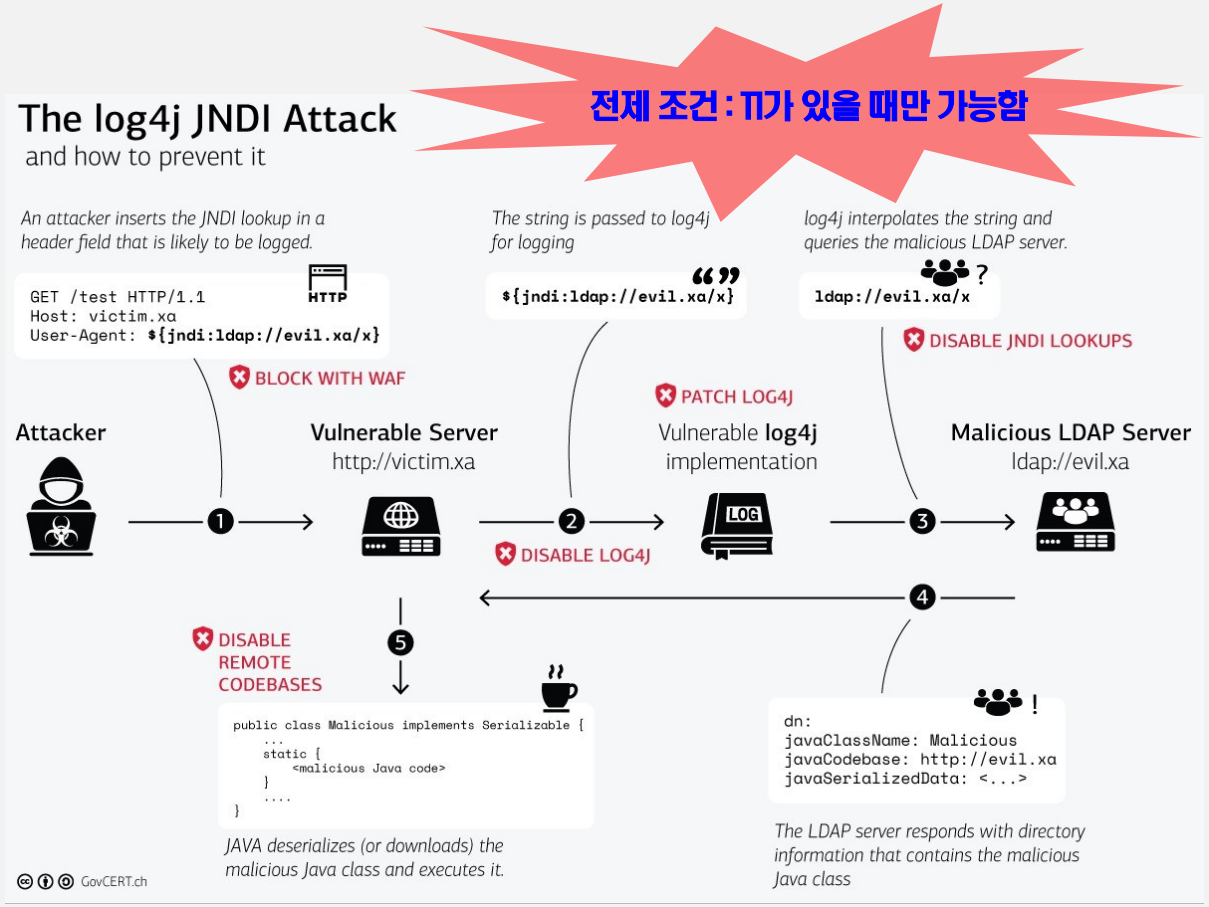
제로데이란 신규 사이버보안 위협이 생성되고 난 후, 해당 위협을 탐지하거나 대응할 수 있는 정보가 나올 때까지의 보안 공백 기간 말합니다. 제로데이 공격은 제로데이 특성을 이용하여 대응 기술이나 보안 패치가 제공되기 전에 이루어지는 공격을 말하며, 이는 아직 미해결 분야로 남아있는 사이버 보안의 마지막 문제점입니다.

제로데이 공격으로 인한 시간/운용상의 보안사각은 탐지 규칙이 제공되기 전에 이루어지기 때문에, 침투에 대한 대처 방법이 없고 이로 인한 데이터 유출 등에 대응이 불가하여 피해 최소화가 유일한 대응 방법임.

01. 보안 패러다임 진화의 필요성 : Log4j 사례 분석

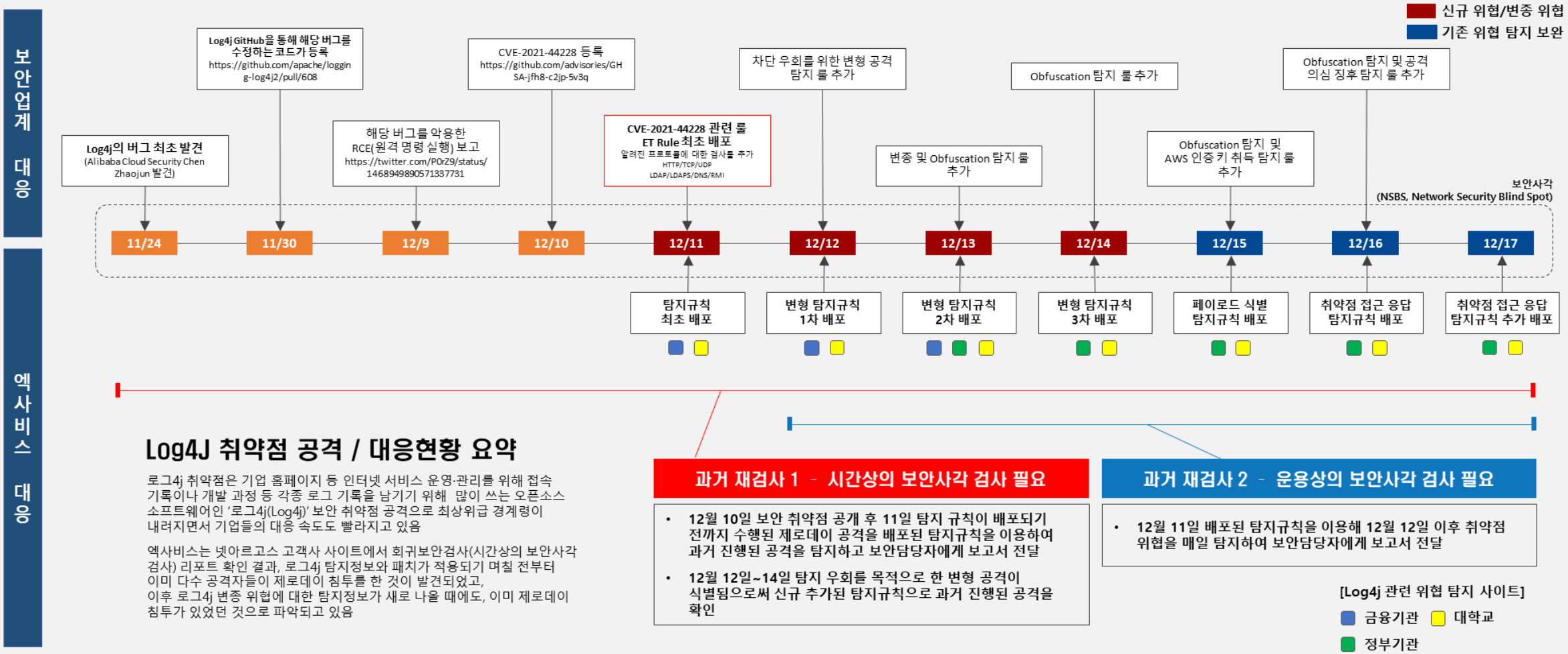
2021년 12월에 발생한 **Log4j 취약점**은 보안 역사상 최악의 취약점, 해결에 수년이 걸릴 것으로 예상





01. 보안 패러다임 진화의 필요성 : Log4j 사례 분석

신속한 TI의 설정과 패치의 적용이 더 이상 안전하지 않음 : 잠재적인 위험에 대한 대응이 전무



Log4J 취약점 공격 / 대응현황 요약

로그4j 취약점은 기업 홈페이지 등 인터넷 서비스 운영·관리를 위해 접속 기록이나 개발 과정 등 각종 로그 기록을 남기기 위해 많이 쓰는 오픈소스 소프트웨어인 '로그4j(Log4j)' 보안 취약점 공격으로 최상위급 경계령이 내려지면서 기업들의 대응 속도도 빨라지고 있음

엑사비스는 넷아르고스 고객사 사이트에서 회귀보안검사(시간상의 보안사각 검사) 리포트 확인 결과, 로그4j 탐지정보와 패치가 적용되기 며칠 전부터 이미 다수 공격자들이 제로데이 침투를 한 것이 발견되었고, 이후 로그4j 변종 위협에 대한 탐지정보가 새로 나올 때에도, 이미 제로데이 침투가 있었던 것으로 파악되고 있음

과거 재검사 1 - 시간상의 보안사각 검사 필요

- 12월 10일 보안 취약점 공개 후 11일 탐지 규칙이 배포되기 전까지 수행된 제로데이 공격을 배포된 탐지규칙을 이용하여 과거 진행된 공격을 탐지하고 보안담당자에게 보고서 전달
- 12월 12일~14일 탐지 우회를 목적으로 한 변형 공격이 식별됨으로써 신규 추가된 탐지규칙으로 과거 진행된 공격을 확인

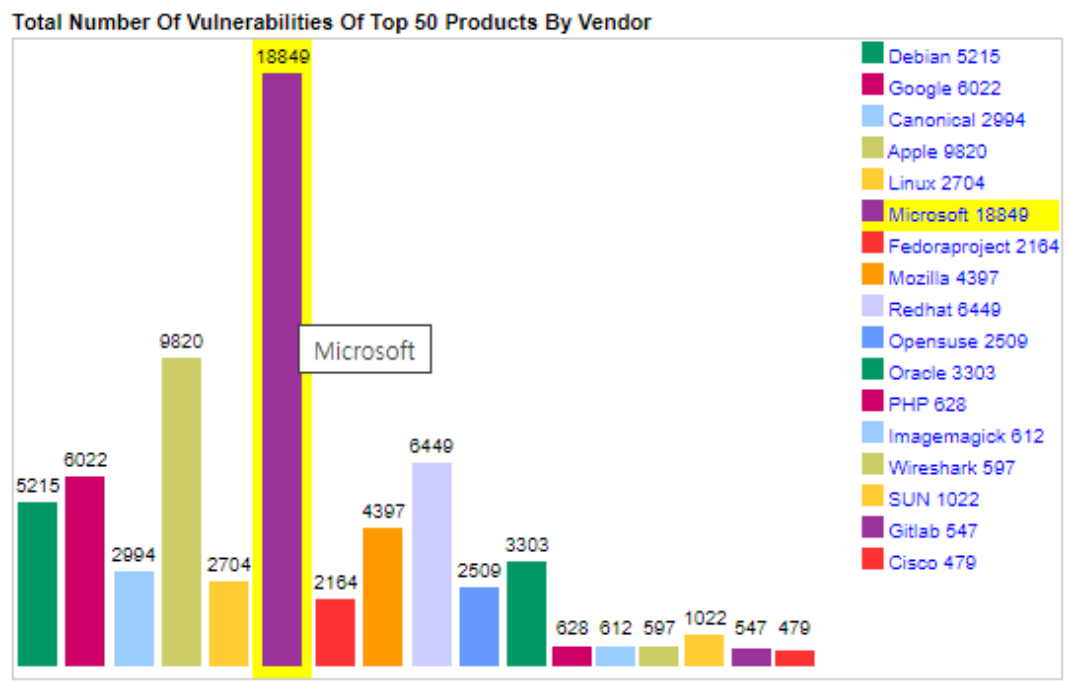
과거 재검사 2 - 운용상의 보안사각 검사 필요

- 12월 11일 배포된 탐지규칙을 이용해 12월 12일 이후 취약점 위협을 매일 탐지하여 보안담당자에게 보고서 전달

[Log4j 관련 위협 탐지 사이트]
금융기관 대학교
정부기관

01. 보안 패러다임 진화의 필요성

2021년 현재까지 발견된 CVE 카운트는 68,311건, 하루에 약 253건의 취약점이 보고



68,311 건 매년 증가 추세

253건/Day 발표 즉시 공격 시작

02. 제로데이 공격 대응 (Threat Hunting)

기존 기술(Network Forensic 등)으로는 현실적으로 대응이 불가능

3%

신규 발생

매일 3% ~ 5%의
위협정보가 업데이트

30%

보안 위협

악성코드 공격의
30% 이상이
제로데이 공격

76%

성공한 공격

성공한 침투의 76%는
제로데이 공격

3M

제로데이 기간

제로데이 기간은 평균
3개월

잠재적 보안사고의 최소화를 위해 **보안 책임자에게 일일 보안 업무 보고 및 결재** 시에
신규 TI의 제공과 적용 뿐만이 아니라 **제로데이 침투 여부**도 보고할 수 있어야 함

02. 제로데이 공격 대응(Threat Hunting)

미탐지 된 보안 위협 침투는 Threat Hunting을 통해 능동적으로 대응해야 함

정의 (from Wikipedia)

" 기존의 보안 체계를 우회하는 위협을 탐지하고 격리하기 위하여 네트워크를 능동적이고 반복적으로 검색하는 프로세스"

- 잠재적인 위협이나 침해사고가 발생한 후에 조사/분석을 하는 기존 위협 관리 시스템(방화벽, IDS, SIEM 등)과 차별화

기존 위협 관리 시스템		사이버 위협 헌팅(Cyber Threat Hunting)
모든 위협을 막을 수 있다.	VS	모든 위협을 차단할 수는 없다.
알려진 위협에 대한 관리		차단되지 않은 위협에 대한 관리
방어 & 사후 분석		탐지/ 분석 / 추적 후 대응
위협 차단 (Prevention)		**피해 최소화 (Detection & Response)**

- 기존의 도구에 의한 탐색을 회피한 위협을 탐색하는 적극적인 보안 탐색으로 수동적인 접근을 하는 Cyber detection과 다르다.

- 아직 탐지되지 않은 것을 찾는 것, 이미 위협은 침투되었을 것을 가정하고 이를 찾아내는 Aggressive Detection

- 포렌식 분석과 위협 추적(hunting)을 위한 과거 이벤트 분석을 위해 몇 주 이상의 저장된 패킷을 검사/분석

02. 제로데이 공격 대응 (Threat Hunting) : AS-IS(Problem Remains)

지금까지는 **제로데이 문제를 하나의 보안사각으로만 인식했기에 정확한 대응에 한계가 존재**

현재의 보안 대응 절차	대응 영역	현재의 대응 체계
알려진 TI를 기반으로 실시간 침투를 방어	경계 보안 체계를 통한 실시간 침투 대응	**Firewall, IPS, WAF, Vaccine EMS, SIEM, SOAR**
아직 TI가 없는 보안 위협을 **이상행위탐지를 통해 모니터링**	Threat Hunting 이상행위의 검출을 통한 제로데이 침투 대응 ▪ 보안사각지대 ▪ 제로데이 공격	ATP / EDR / NDR ▪ 정확도에 대한 보장이 안됨 (Best Effort) ▪ 제로데이 침투의 검출, 분석, 추적이 안됨

대응 절차

02. 제로데이 공격 대응 (Threat Hunting) : TO-BE(Divide and Conquer)

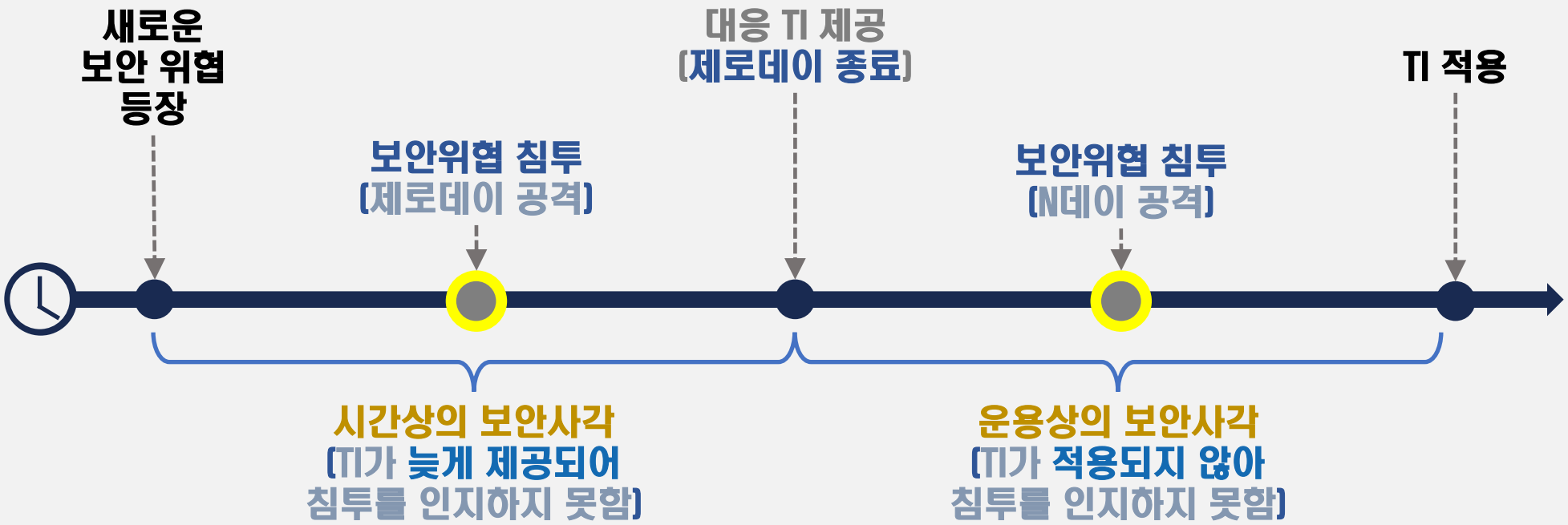
정확한 보안사각 문제 영역의 구분과 적합한 기술 적용을 통한 보안의 사각지대를 최소화하는 것이 중요

이상적인 보안 대응 절차	대응 영역	이상적인 대응 체계
알려진 TI를 기반으로 실시간 침투를 방어	경계 보안 체계를 통한 실시간 침투 대응	Firewall, IPS, WAF, Vaccine EMS, SIEM, SOAR
신규 TI 나오면 빨리 적용하여 침투 방어의 공백 최소화	Threat Hunting: 운용상의 보안사각	제로데이 침투의 확인과 추적 및 검증을 위한 솔루션이 부재
과거 트래픽의 재검사를 통해 제로데이 침투를 검출하여 대응	Threat Hunting: 시간상의 보안사각	제로데이 침투의 확인과 추적 및 검증을 위한 솔루션이 부재
아직 TI가 없는 보안 위협을 이상행위탐지를 통해 모니터링	Threat Hunting: 언노운 보안사각	ATP / EDR / NDR

대응 절차

02. 제로데이 공격 대응 (Threat Hunting) : 시간 및 운용상의 보안사각

보안사각을 통한 제로데이 공격의 침투와 데이터 유출은 100% 성공하며, 침투 여부가 인지되지 않음



03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술

보안사각으로 인한 **제로데이 침투**를 해결하기 위해서,
제로데이 기간 동안의 과거 트래픽을 저장한 후, **새로운 탐지정보가 제공될 때마다 자동으로 회귀보안검사 와 분석을 실시**

03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술

ZDR은 지금까지 통제선 밖에 있었던 **시간/운용상의 보안사각**을 통제선 안으로 인양

Z

- 시간/운용상의 보안사각에 대응하기 위해 제로데이 기간 동안의 과거 트래픽을 저장

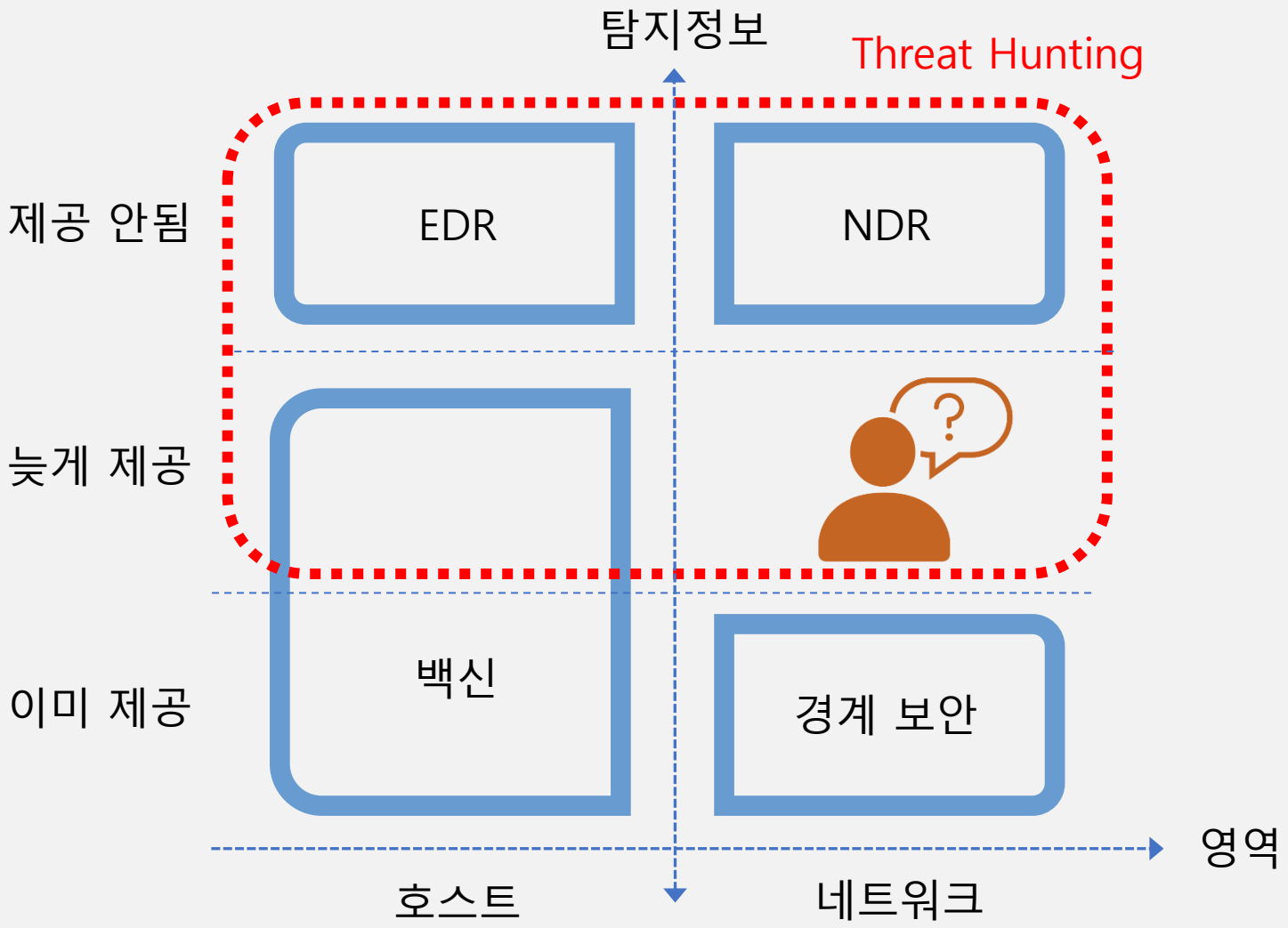
D

- TI(Threat Information)의 업데이트 시마다 자동 회귀보안검사 및 분석을 통해 제로데이 침투와 관련된 행위를 검출

R

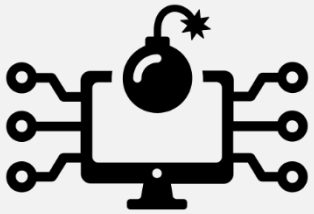
- 자동 분석 리포트와 보안 장비와 연동 대응을 통해 운용자의 부담을 최소화

03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술



03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술

실세계의 CCTV와 DVR을 Cybersecurity에 도입한 효과

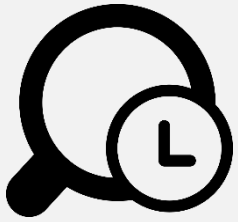


제로데이 침투 검출

- 신규로 알려진 TI에 대한 과거의 제로데이 침투 여부 확인
- 제로데이 침투 검출 결과의 검증 및 분석

제로데이 통신 검출

- 신규로 알려진 Blacklist IP에 대한 제로데이 데이터 통신 여부 확인
- 신규로 알려진 C&C IP에 대한 제로데이 제어 통신 여부 확인



제로데이 가시성 확보

- 제로데이 침투 이후의 유관 행위 추적 및 피해 상황 분석
- 제로데이 통신 전후에 대한 유관 행위 추적 및 피해 상황 분석
- 장기간에 걸친 과거 트래픽의 재검사 및 분석 데이터 추출

03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술

제로데이 가시성과 제어 환경을 제공함으로써 제로데이 보안사각에 대한 대응 능력을 제공

제로데이 침투 및 통신 정보
검증 및 분석을 위한 트래픽 정보

SIEM SOAR

언노운 보안사각 검증 및 분석을 위한
트래픽 정보

APT NDR EDR

ZDR

Packet / Network Meta data / Zero-day Event

Firewall IPS WAF

제로데이 침투 및 데이터 유출 위협의 차단
정책 생성 및 전달

03. ZDR : NSBS 대응을 위한 새로운 Threat Hunting 기술

Zero Trust Security Service : 기존 보안 관제 체계가 통제하지 못하는 시간/운용상의 보안사각에 대한 대응 능력을 제공

ZDR

Packet
0101010101
0011001100
1001110011

네트워크 메타 데이터
/ 패킷 정보 추출

주기적 회귀보안검사로
제로데이 침투 검출

회귀보안검사를 통한 TI 최적화

TI에 대한 회귀보안검사로 Zero-day 침투 확인

제로데이 경보
추적 및 분석 정보

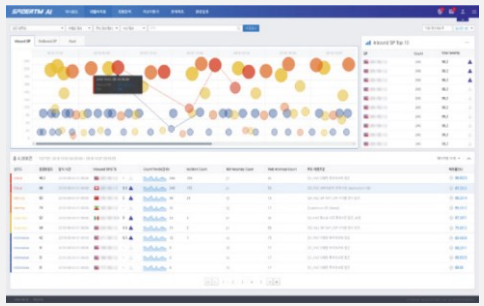
신규 학습 TI

제로데이 정보

SIEM/SOAR

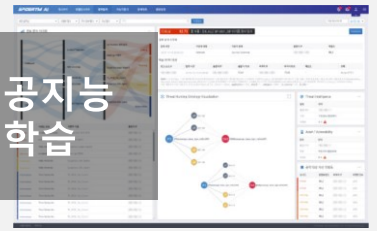
이미 침투한 위협 이벤트 수집/분석

- 회귀보안검사로 탐지된 위협 및 가시성 확보
- EDR/NDR 연동 분석을 통한 Threat Hunting



Threat Hunting
위협 모델링(TI) 생성

인공지능
학습



04. 기존 기술과의 비교 분석 : ZDR Vs Forensic

1대의 ZDR은 50대의 Network Forensic 효과

ZDR	FORENSIC
▪ **장기간 First-N Packet 저장 후 검사** ▪ 2% 패킷 저장 ▪ 99.6% 검출	▪ **짧은 기간 Full Packet 저장 후 검사** ▪ 100% 패킷 저장 ▪ 100% 검출
▪ **매일 보안사각에 대한 자동 회귀보안검사 : 사전 대응** ▪ **보안 사고 인지 후 원인 분석 : 사후 대응**	▪ **보안 사고 인지 후 원인 분석 : 사후 대응**
▪ **시간/운용상의 보안사각 대응 가능** ▪ **OPTION : 병행 Full Packet 저장 지원**	▪ **시간/운용상의 보안사각 대응에 과다한 비용 소모**

04. 기존 기술과의 비교 분석 : ZDR Vs Forensic

Forensic ANALYTICS SOLUTION

막대한 디스크 공간 소요
10G 1회선 기준 3개월간의 트래픽 저장을 위해 4.5PB의 저장 공간이 필요하며, 64TB 스토리지 기준 서버 75대 소요

고가의 컴퓨팅 하드웨어
저장된 데이터의 1회/1일 재검사를 위해 2.4GHz/8코어 서버 50여대 소요

분석 전문 인력 필요
저장된 데이터에 대한 분석을 위해 전문 인력 별도 요구

기존 솔루션을 이용한 시간/운용상의 보안사각 탐지는
너무 많은 비용이 소모되어 **현실적으로 도입 불가**

ZDR SOLUTION

특수 패킷 저장기법
FPC 이외의 특수한 패킷 저장기법을 통해 1대의 시스템으로 3개월 이상 데이터 저장

50배 수준의 하드웨어 비용 절감

매일 1회 이상 주기적 자동 보안 재검사
매일 1회 이상 자동으로 새로 업데이트된 공격탐지방법으로 회귀보안 검사를 수행하고, 분석 후 리포팅

자동 분석으로 전문 인력 불필요
AI 기반의 전문가 시스템으로 별도의 전문인력 불필요.

정해진 시간동안 자동으로 분석이 이루어지며 운영자에게 자동 리포트 전송

최소의 비용으로 시간/운용상의 보안사각 제거

04. 기존 기술과의 비교 분석 : ZDR Vs NDR

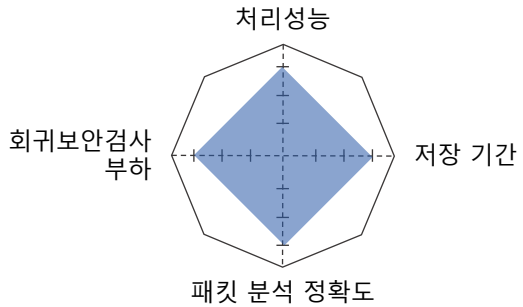
시간 및 운용상의 보안사각 vs 언노운 보안사각

ZDR		NDR
▪ 매일 보안사각에 대한 자동 회귀보안검사(조기 대응) ▪ 제로데이 침투 보고 및 대응을 위한 자동 리포팅 및 검증을 위한 과거 트래픽 제공(장기간)	역할 분석	▪ 네트워크 상에서 발생하는 이상행위 모니터링 ▪ 검출된 이상행위 검증을 위한 과거 트래픽 제공(단기간)
▪ 시간/운용상 보안사각에 대한 새로운 Threat Hunting 능력 제공 ▪ 타 보안 솔루션이 커버할 수 없는 신규 영역(보안사각)	적합성 분석	▪ 언노운 보안사각에 대한 Threat Hunting 능력 제공
▪ 일일 보안사각 보고 및 대응을 통해 보안 강화 ▪ 연동 검증이 완료된 기존 NAC, SIEM, EDR과의 연계를 통한 보안 위협 대응 능력 강화	기대효과 분석	▪ 탐지 결과의 오탐 및 분석을 위한 전문 인력이 필요

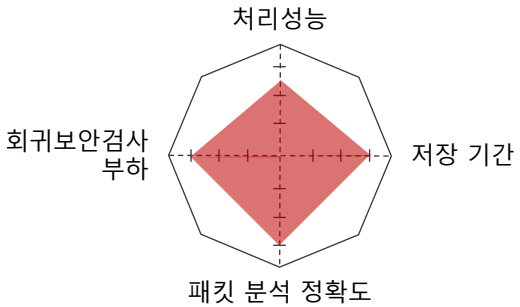
04. 기존 기술과의 비교 분석 : Packet 저장 및 회귀보안분석 기술

이상적인 ZDR의 조건을 만족시킬 수 있는 새로운 적합한 저장 및 분석 기술이 필요

Theoretical

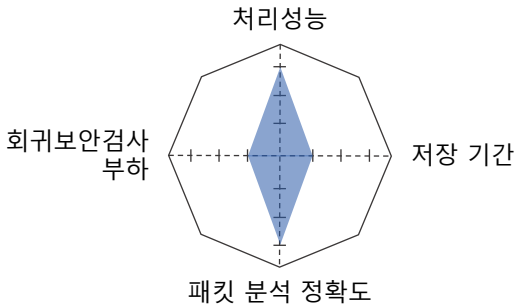


First-N

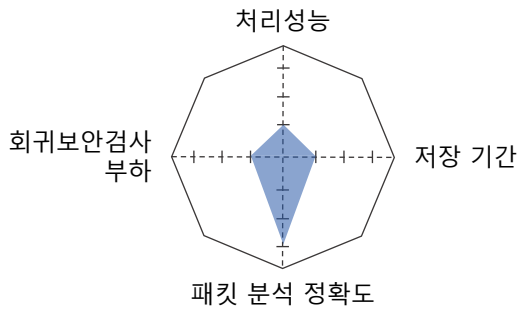


FPC

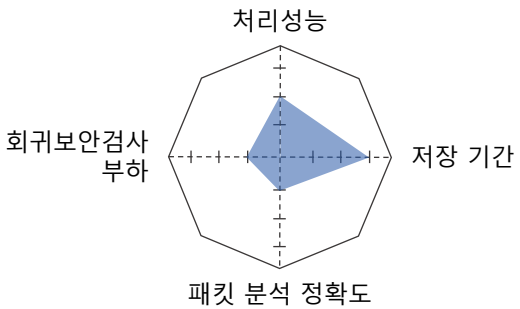
[Full Packet Capture]



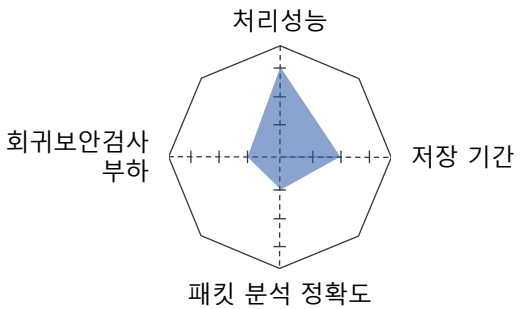
Packet Compression



Event-Driven



Packet Slicing



05. 제로데이 공격 침투의 실제 사례 분석

새로운 보안 취약점의 발표 후 탐지 정보의 제공 이전에 제로데이 공격과 침투가 지속적으로 발견

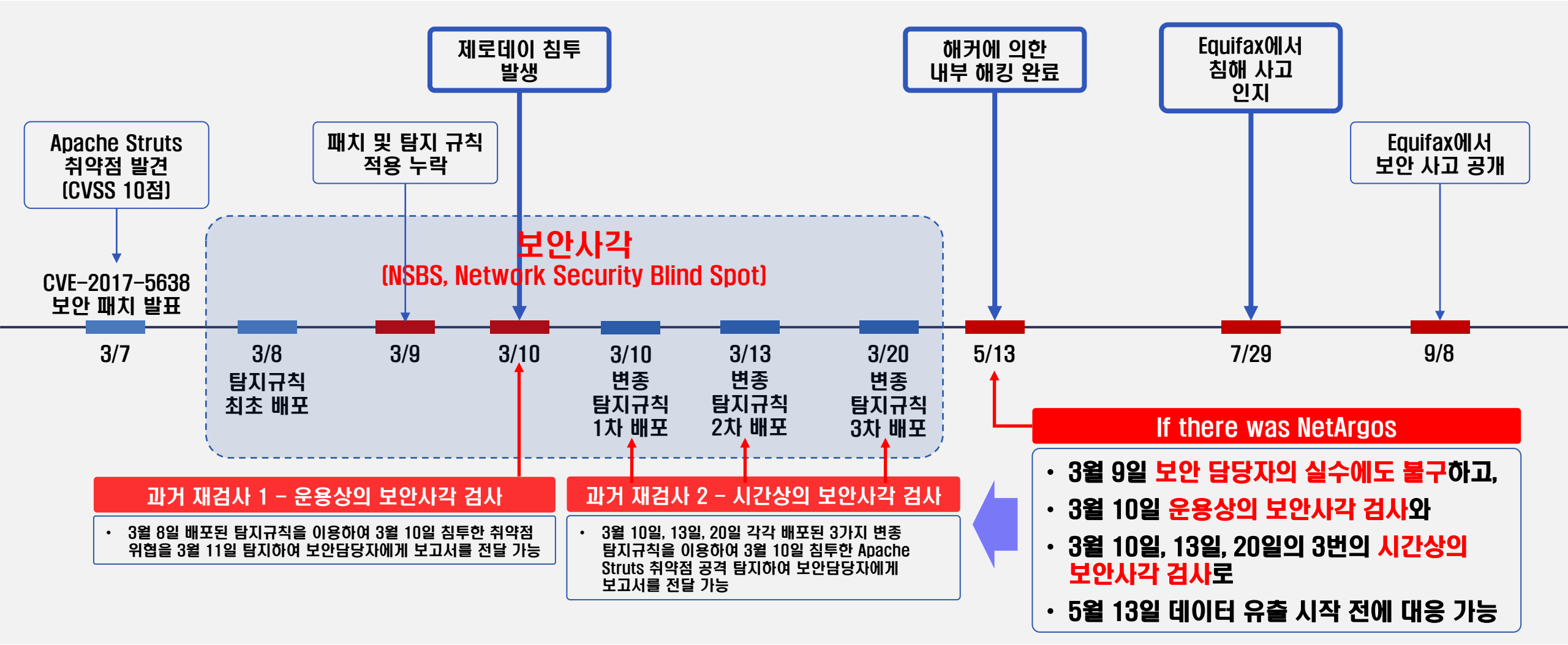
.....

- **CVE-2022-26186 : TOTOlink, 4월 7일 수행된 시간상의 보안사각 검사에서 4월 1일 totolol.sh 다운로드 발견**
- **CVE-2022-25075 : TOTOlink, 4월 7일 수행된 시간상의 보안사각 검사에서 4월 2일 명령어 실행 시도 발견**
- **CVE-2022-22965(CVSS 9.8) : Spring4Shell, 4월 8일 수행된 시간상의 보안사각 검사에서 3월 30일 원격 코드 실행 시도 발견**
- **CVE-2022-22965(CVSS 9.8) : Spring4Shell, 4월 13일 수행된 시간상의 보안사각 검사에서 4월 3일 침투 검출**
- **CVE-2020-17456 : SEOWON INTECH, 4월 16일 수행된 시간상의 보안사각 검사에서 3월 31일 원격 코드 실행 시도 발견**
- **CVE-2022-1388(CVSS 9.8) : BIG-IP iControl, 5월 14일 수행된 시간상의 보안사각 검사에서 5월 11일 공격 검출**

.....

- **CVE-2022-36804 (CVSS 9.8) : Atlassian Bitbucket Exploit Attempt, 9월 22일 수행된 시간상의 보안사각 검사에서 9월 21일 공격 검출**

05. 제로데이 공격 침투의 실제 사례 분석 : Equifax 2017



05. 제로데이 공격 침투의 실제 사례 분석 : SUNBURST 2020

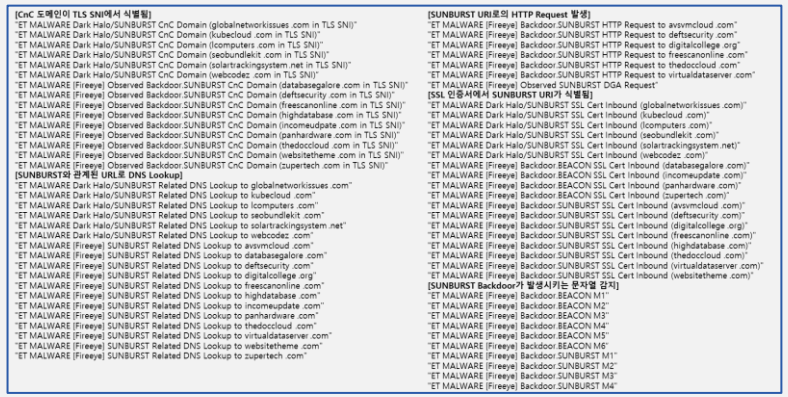
당면 문제 : 사고와 인지 사이의 장기간의 시간 차

1. 침투 여부 파악? : 회귀보안검사가 필요
2. 피해 여부 및 피해 범위 파악? : 회귀보안검사 결과 분석이 필요
3. 대응 방안? : 회귀보안검사 결과 분석에 따른 맞춤 대응이 필요

시간상의 보안사각
(NSBS, Network Security Blind Spot)

회귀보안검사 및 분석을 통한 대응 및 피해 최소화

2020.03 — 2020.12.13 — 2020.12.14 — 2020.12.16 — 2020.12.21



<SUNBURST Detection Rules in ET Pro Rule set>

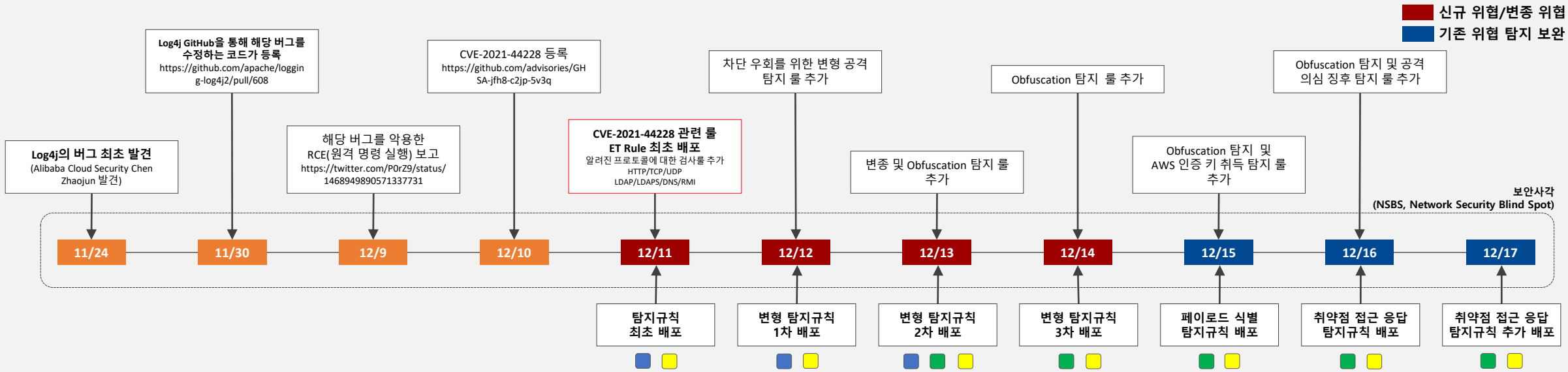
해결책 : ZDR(Zero-day intrusion Detection and Response)

1. 침투 여부 및 피해 여부/범위 파악
   1. 회귀보안검사 : SUNBURST 탐지 룰 → 2020년 3월부터 현재까지 저장된 패킷 재검사
   2. 회귀보안분석
      - C&C 서버와의 통신 기록 및 추가 Malware 침투 여부 파악
      - 데이터 유출 여부 검색 및 검증
2. 대응 방안
   1. FireEye와 MS가 배포한 KillSwitch 실행
   2. 실시간 네트워크 보안 제품에 차단를 적용
   3. ZDR Solution을 이용한 주기적 회귀보안검사 실시

05. 제로데이 공격 침투의 실제 사례 분석 : Log4j 2021

보안업계 대응

엑사비스 대응



Log4J 취약점 공격 / 대응현황 요약

로그4j 취약점은 기업 홈페이지 등 인터넷 서비스 운영·관리를 위해 접속 기록이나 개발 과정 등 각종 로그 기록을 남기기 위해 많이 쓰는 오픈소스 소프트웨어인 '로그4j(Log4j)' 보안 취약점 공격으로 최상위급 경계령이 내려지면서 기업들의 대응 속도도 빨라지고 있음

엑사비스는 넷아르고스 고객사 사이트에서 회귀보안검사(시간상의 보안사각 검사) 리포트 확인 결과, 로그4j 탐지정보와 패치가 적용되기 며칠 전부터 이미 다수 공격자들이 제로데이 침투를 한 것이 발견되었고, 이후 로그4j 변종 위협에 대한 탐지정보가 새로 나올 때에도, 이미 제로데이 침투가 있었던 것으로 파악되고 있음

과거 재검사 1 – 시간상의 보안사각 검사 필요

- 12월 10일 보안 취약점 공개 후 11일 탐지 규칙이 배포되기 전까지 수행된 제로데이 공격을 배포된 탐지규칙을 이용하여 과거 진행된 공격을 탐지하고 보안담당자에게 보고서 전달
- 12월 12일~14일 탐지 우회를 목적으로 한 변형 공격이 식별됨으로써 신규 추가된 탐지규칙으로 과거 진행된 공격을 확인

과거 재검사 2 – 운용상의 보안사각 검사 필요

- 12월 11일 배포된 탐지규칙을 이용해 12월 12일 이후 취약점 위협을 매일 탐지하여 보안담당자에게 보고서 전달

[Log4j 관련 위협 탐지 사이트]
금융기관 대학교
정부기관

Detect the Knife of Assassin

www.xabyss.com

경기도 수원시 영통구 영통로 237, 305호/306호
(영통 에이스하이엔드타워)
Tel: +82-70-7510-8200
Fax: +82-70-8673-8200