CLOUDSEC 2023

ENVISION IT

운영의 완벽을 완성하는 Tanium의 위력

Tanium 강두원 부장

Hosted by

TREND MICRO

소프트웨어 공급망 위협 대응

TREND MICRO

소프트웨어 공급망 위협 대응

solarwinds

2020년 공격자는 소프트웨어 빌드 서버에 백도어 삽입하였고, 일상적인 소프트웨어 업데이트를 통해 다수의 사용자에게 확산된 사례

미국 연방정부
국가의 사이버보안 향상에 관한 행정명령(EO 14028) 발표

행정명령 4절. 소프트웨어 공급망 보안 강화

Gartner®

2025년에는 전 세계 조직의 약 45%가 소프트웨어 공급망 공격을 경험할 것으로 예상 (21년 대비 3배 증가)

TREND MICRO™

소프트웨어 공급망 위협 대응

70+%

오픈 소스
구성 비율

40+%

취약점
보유 현황

2,800+

오픈 소스
사용 현황

1. Linux Foundation | 2. Linux Foundation | 3. Olive Platform

소프트웨어 공급망 위협 대응

Nutrition Facts

1 serving per container
Serving size **1 Sandwich (264g)**

Amount per serving
Calories **470**

	% Daily Value*
Total Fat 18g	**23%**
Saturated Fat 1.5g	**8%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 1390mg	**60%**
Total Carbohydrate 62g	**23%**
Dietary Fiber 3g	**11%**
Total Sugars 3g	
Includes 0g Added Sugars	**0%**
Protein 17g	
Vitamin D 0mcg	0%
Calcium 113mg	8%
Iron 5mg	30%
Potassium 258mg	6%

Honey White Bread Mix (no leavening)

INGREDIENTS: Bleached flour (wheat flour, niacin, reduced iron, thiamin mononitrate, riboflavin, folic acid, enzyme [improves yeast baking]), sugar, baking powder, nonfat dry milk, vinegar powder (IP maltodextrin, white distilled vinegar), non-iodized salt, soybean oil, honey powder (cane sugar, honey), whole eggs, soy lecithin, dough conditioner (enriched wheat flour [wheat flour, niacin, reduced iron, thiamine mononitrate, riboflavin, folic acid], ascorbic acid, wheat gluten, enzymes).
CONTAINS: Egg, milk, soy, wheat.

High Temperature Cheddar Cheese

Directions:
Add cheese at 10% ratio (1 lb. cheese to 10 lbs. of meat).
This cheese will stay in chunks up to 400°F.

Storage:
Recommended temperature 33-72°F for up to 180 days.
Refrigerate to retain freshness.
Store in air-tight container.

INGREDIENTS:
SHELF STABLE CHEDDAR (CULTURED PASTEURIZED MILK, WATER, SALT, SODIUM PHOSPHATE, NATURAL FLAVORING, SORBIC ACID (PRESERVATIVE), ADDED COLOR, ENZYMES), CORN STARCH AND/OR CELLULOSE (TO PREVENT CAKING), NATAMYCIN (PRESERVATIVE).

CONTAINS: MILK

DISTRIBUTED BY:
LEM PRODUCTS
WEST CHESTER,OH 45011
TOLL FREE | 877.536.7763
LEMPRODUCTS.COM
SKU #8075 LP ITEM #3101

Nutrition Facts

About 300 servings per container
Serving size 1/4 cup (30g)

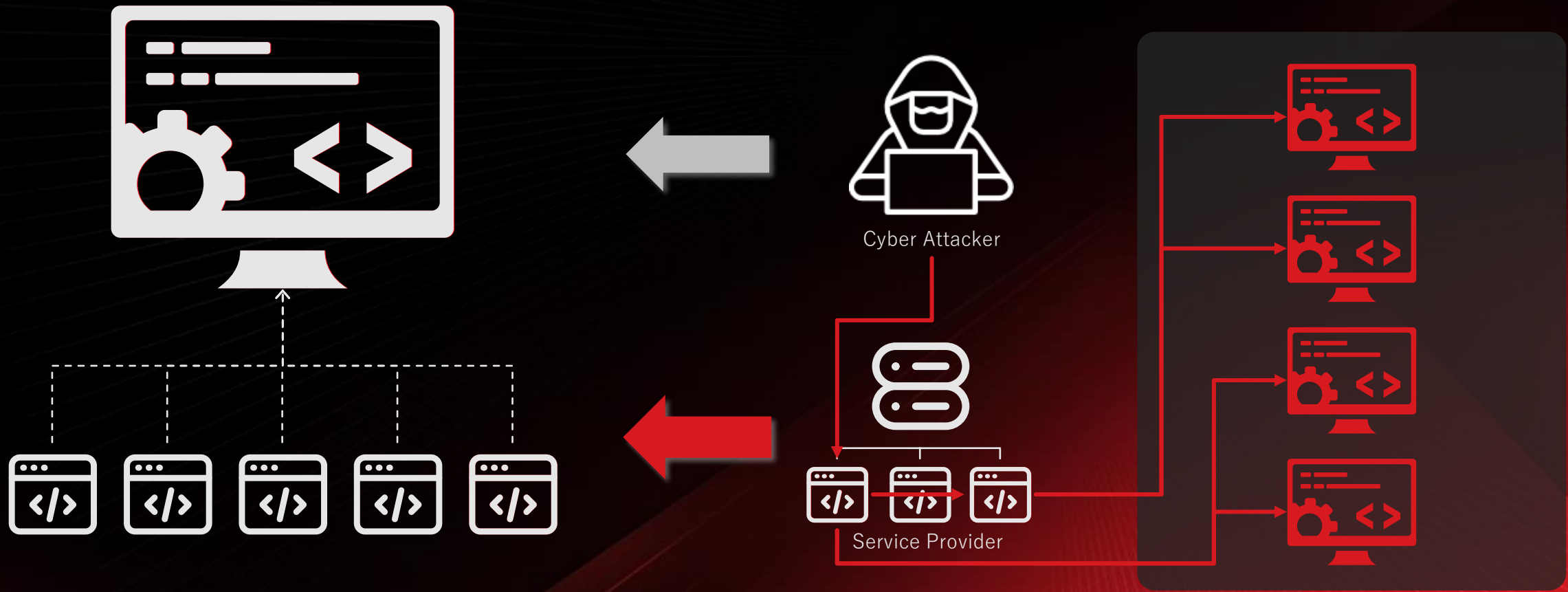
Amount per serving
Calories **110**

	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 6g	**30%**
Trans Fat 0g	
Cholesterol 25mg	**8%**
Sodium 390mg	**17%**
Total Carbohydrate 1g	**0%**
Dietary Fiber 0g	**0%**
Total Sugars 0g	
Includes 0g Added Sugars	**0%**
Protein 6g	**12%**
Vit. D 0mcg 0% • Calcium 200mg 15%	
Iron 0mg 0% • Potassium 25mg 1%	

*The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

INGREDIENTS:
PORK HAM, WATER, CONTAINS 2% OR LESS: HONEY, SEA SALT, EVAPORATED CANE SUGAR, ROSEMARY, CELERY POWDER, SODIUM LACTATE.

소프트웨어 공급망 위협 대응

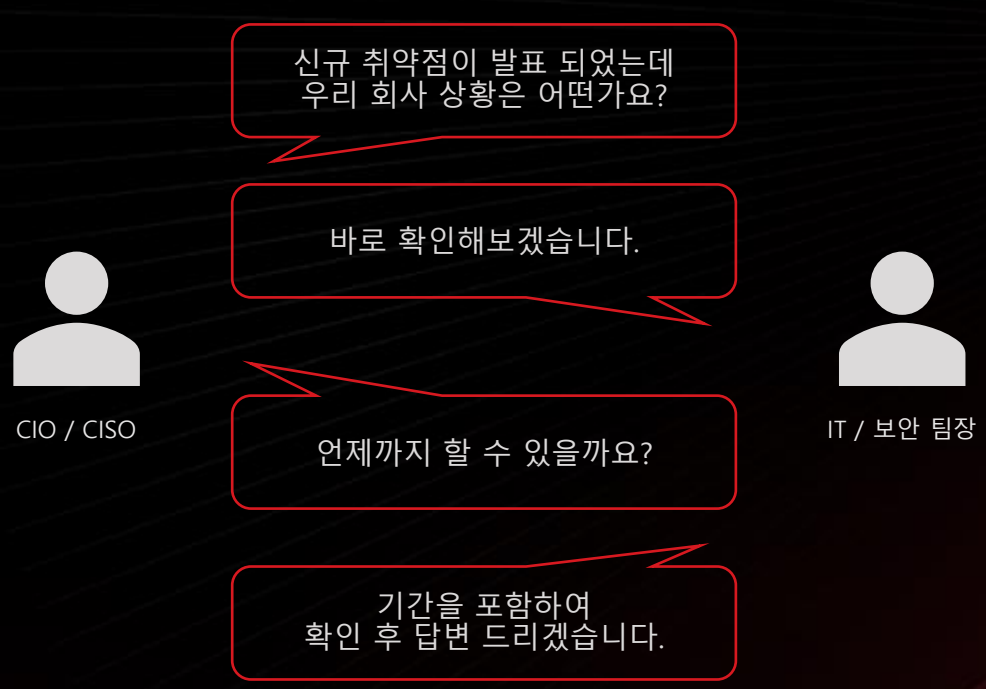


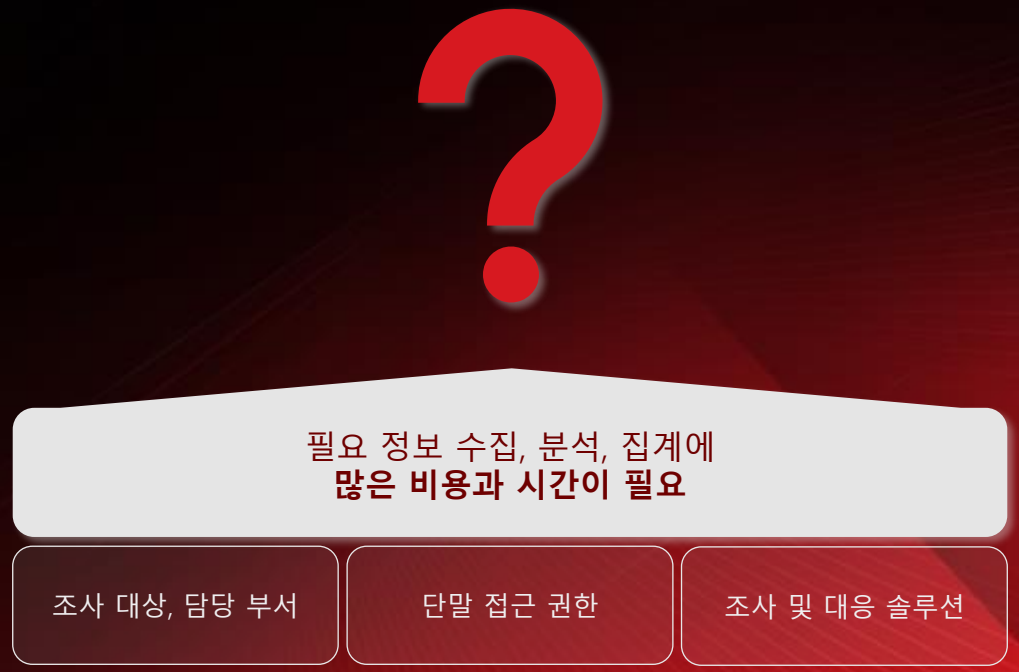
소프트웨어 공급망 위협 대응

Build time

Runtime

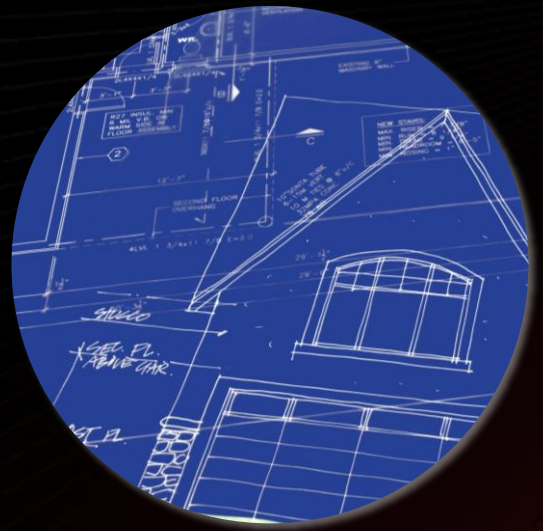
소프트웨어 공급망 위협 대응





소프트웨어 공급망 위협 대응

수집 유무



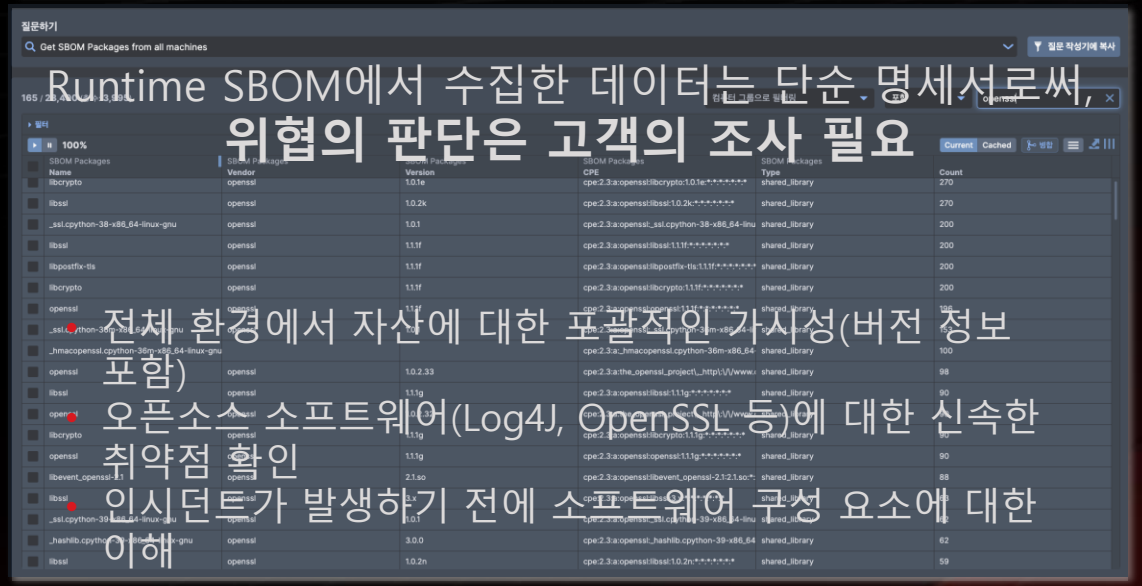
수집 방식

정확도

대응 시간

소프트웨어 공급망 위협 대응

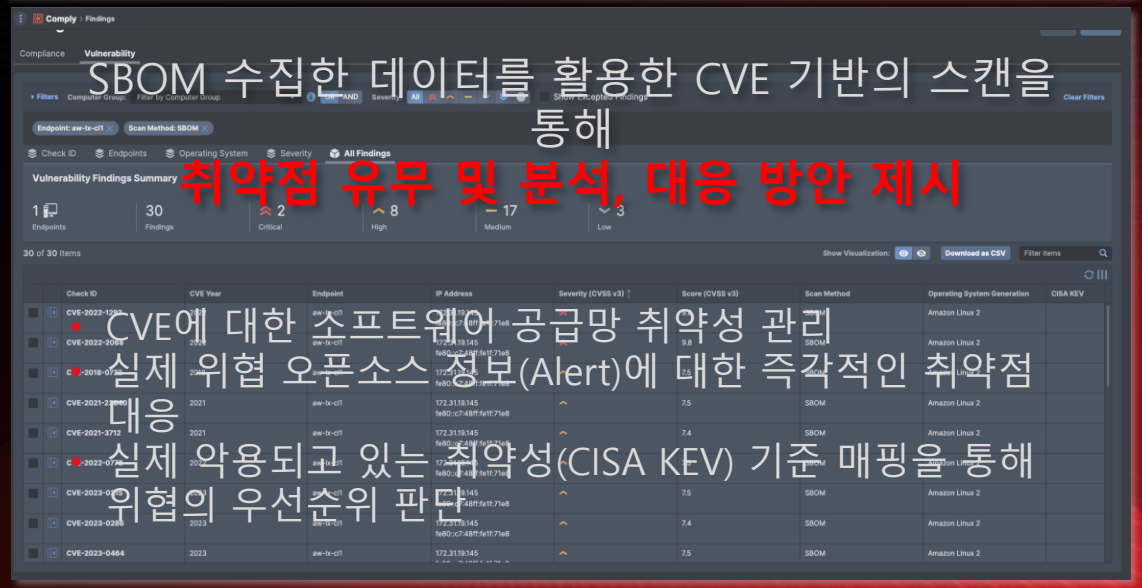
SBOM



Runtime SBOM에서 수집한 데이터는 단순 명세서로써, **위협의 판단은 고객의 조사 필요**

- 전체 환경에서 자산에 대한 포괄적인 가시성(버전 정보 포함)
- 오픈소스 소프트웨어(Log4J, OpenSSL 등)에 대한 신속한 취약점 확인
- 인시던트가 발생하기 전에 소프트웨어 구성 요소에 대한 이해

취약성 스캔 with SBOM



SBOM 수집한 데이터를 활용한 CVE 기반의 스캔을 통해 **취약점 유무 및 분석, 대응 방안 제시**

- CVE에 대한 소프트웨어 공급망 취약성 관리
- 실제 위협 오픈소스 정보(Alert)에 대한 즉각적인 취약점 대응
- 실제 악용되고 있는 취약성(CISA KEV) 기준 매핑을 통해 위협의 우선순위 판단

소프트웨어 공급망 위협 대응

기존 솔루션 접근 방식의 문제점은
이미 배포된 모든 애플리케이션의 현황 파악 불가
+
신규 취약 발생 시 즉각적인 대응의 어려움

Tanium에서 제공하는 소프트웨어 공급망 관리 방안

단말 내 애플리케이션
구성 요소 조사

조사된 데이터 기반
취약점 유무 판단

급격하게 변하는 환경의 엔드포인트 관리 방안

TREND MICRO

급격하게 변하는 환경의 엔드포인트 관리 방안

WORK FROM OFFICE

WORK FROM HOME

HYBRID WORK

TREND MICRO™

급격하게 변하는 환경의 엔드포인트 관리 방안

01 모든 데이터 소스 및 컴퓨팅 서비스는 리소스로 간주된다.

02 네트워크 위치에 관계없이 모든 통신을 보호해야 한다

03 모든 조직 리소스에 대한 액세스 권한은 세션별로 부여한다.

04 자원에 대한 접근은 여러 정보를 포함한 **동적 정책에 의해 결정**된다.

05 **조직의 모든 자산의 무결성 및 보안 상태를 모니터링하고 측정한다.**

06 모든 자원에 대한 **인증 및 권한 부여는 접근이 허용되기 전에 엄격하게 시행**한다.

07 **자산, 네트워크 및 통신 상태에 대해 가능한 한 많은 정보를 수집합니다.**

급격하게 변하는 환경의 엔드포인트 관리 방안

과제

원격근무, 커뮤니케이션 활성화 등으로
'새로운' 일하는 방식 도입 필요

전 지역에 산재된 다양한 구성 및 OS 환경 단말에 대해
실시간 조사의 어려움

인증 단계의 유저에 대한 식별은 가능하나
단말 기기의 검증 방안 부재

업무 중인 단말에 대한
지속적인 상태 점검 및 미비점 조치 방안 없음

해결방안

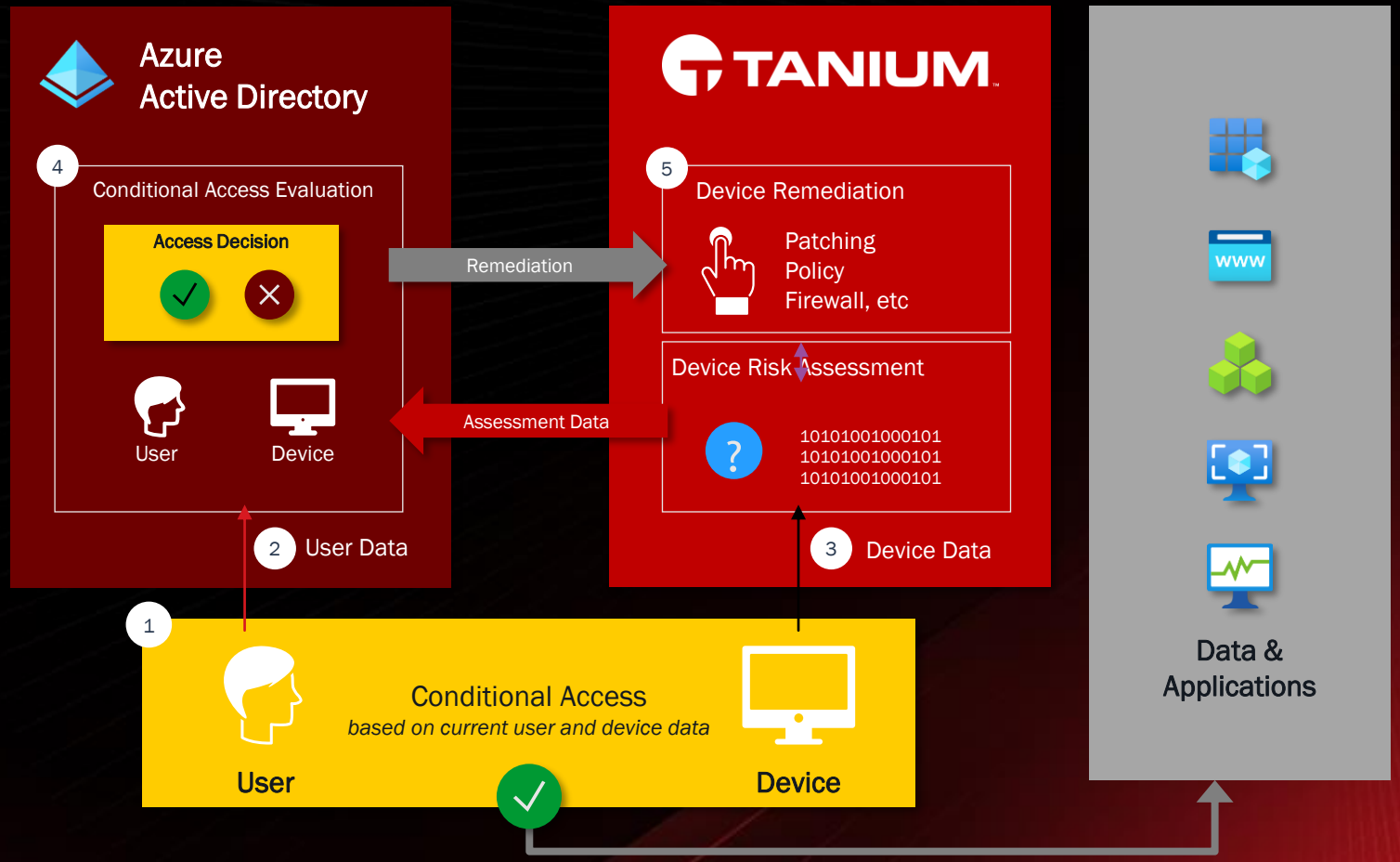
식별/인증 단계에서 단말의 최소 수준은 보안 정책 이행

- 사내 보안 규정
- CVE 기반 취약점 보유 현황
- OS/어플리케이션 최신 패치/배포 현황
- 운영, 보안 필수 어플리케이션 설치 및 동작 유무

업무 중 지속적인 단말 모니터링

- OS/어플리케이션 최신 패치/배포 적용
- 주기적인 취약성 검사 및 일괄 조치
- 접근 방식(Lan, VPN, Internet)에 따른 단말 정책 적용
- 위협 발생 시, 전수 조사를 기본으로 헌팅 및 긴급 조치

급격하게 변하는 환경의 엔드포인트 관리 방안



1. 유저/단말 상태를 실시간 조사할 수 있는 확장 기능의 부재

   ↓

   다양한 조건으로 유저/단말 상태 판단
   - Defender 동작 상태
   - 정책 적용 상태
   - 패치 적용 유무
   - 취약점 진단 결과 등

2. 비즈니스 생산성과의 직결되는 접근 거부 상태

   ↓

   조건을 충족한 단말은 즉각적인 허용 조치 (접근 권한 획득)

급격하게 변하는 환경의 엔드포인트 관리 방안

제로트러스트 구현을 위해 필수 요건

실시간 조회 및 조치

- 자산 관리
- 취약성 검사
- 구성 관리

지속적인 관리체계

- 증적 확보
- 패치 및 배포
- 정책 배포

즉각적인 대응체계

일본 제조업체 사이버 공격 사례를 통해 살펴본 통찰

사건 발생 일지

날짜	이벤트
x월 8일	사내 시스템 장애 발생
	시스템 장애로 인한 출하 및 생산 중단
	전 직원 대상 PC 사용 제한 실시 실시
x월 9일	본사, 공장 관계부서 직원에게 유급휴가 사용 촉구
	원인은 사이버 공격으로 인한 것으로 발표
x월 10일	사이버 공격 피해를 입은 사내 서버에 대한 대응이 완료 본사 직원 PC 사용 제한 해제
x월 12일	사이버 공격으로 시스템 장애가 발생한 전 공장 복구 지원

전사 대상으로 시도하는 사이버 공격으로부터 비즈니스와 데이터를 보호하기 위해 무엇을 준비해야 하는가?

대내외 환경 변화에 대응하면서

'지금 어디에', '어떤 리스크가', '얼마나 존재하는가'

글로벌 전 거점, 전 자산의 리스크 현황을 실시간으로 정확하게 파악하여 경영 리스크 최소화 가능

모든 엔드포인트 대상으로 수행하는 IT/보안 관련 업무를

“One Platform”으로 “실시간 조회 및 조치”

TREND MICRO™ | Global Leader in Cybersecurity

+82 02-6007-2040

doowon.kang@tanium.com