tenable eGISEC 2025

Exposure Management
공격 경로 분석과 리스크 대응

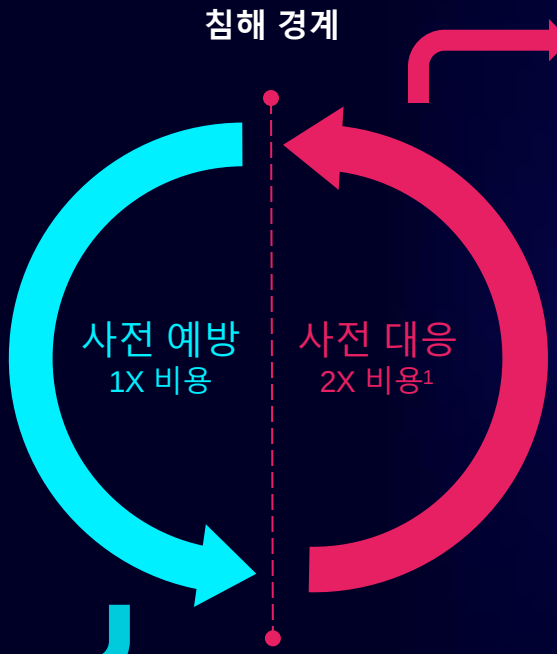
이준희
Tenable Sales Engineer

목차

- 위험 노출 관리 (Exposure Management)
- 위험 관리 방안
- AI를 활용한 공격 경로 분석

tenable

보안의 두가지 축



위험 노출 관리(Exposure Management)

공격표면 제거 및
위험 노출에 사전 예방적으로
대응할수 있는 컨텍스트 제공

$ 4.88 Million / 침해[2]

Brand / Revenue / Clients / Penalties / Lawsuits

침해 관리(Breach Management)

실제 공격을 확인 및
영향을 최소화하기 위한 사고 관리

- CISA: 72 시간
- NIS2: 72 시간
- GDPR: 72 시간
- SEC: 96 시간

3X 위험 감소

침해 발생 가능성[3]

출처: 1: Gartner Market Share - Sec Soft WW, 2: IBM - Cost of a data breach 2024, 3: Gartner - Implement a CTEM Program

tenable

위험 노출관리 정의

위험 노출관리(Exposure management)는 기업에서 비즈니스를 위해 사용되는 시스템, 어플리케이션, 장치 및 계정과 같은 전체 자산에 대해 접근성, 악용가능성 및 주요도를 지속적으로 평가하고 관리하는 프로세스와 기술의 집합입니다.

VISIBILITY

위험 노출 관리는 취약점 관리에서 발전한 것으로 공격 가능성, 인증 관련 권한 문제, 공격 가능 경로 확인, 비즈니스 중요도를 고려하여 실제 위험 노출 우선순위를 정하고 가장 높은 위험에 먼저 대응할수 있도록 지원 합니다.

CONTEXT

가트너에서 위험노출 관리를 프로그램으로 설명

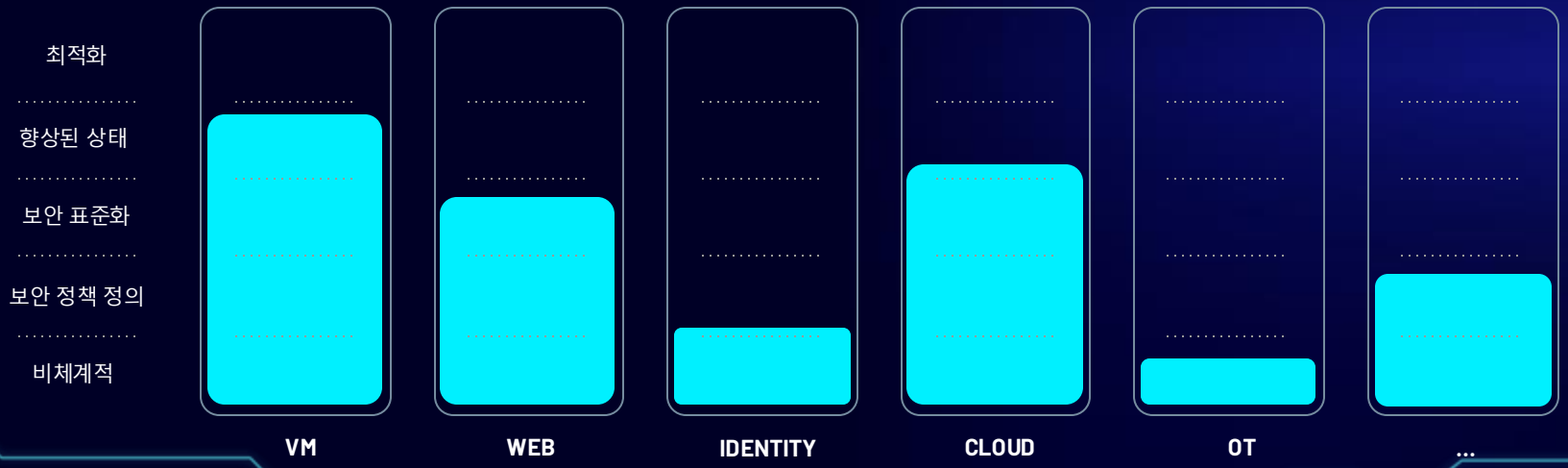
Continuous Threat Exposure Management (CTEM)

기업의 디지털 및 물리적 자산에 대한 접근성, 악용가능성, 위험노출 사항을 지속적이고 일관된 기준으로 평가할 수 있는 프로세스 및 기능의 집합.

1. *범위 산정: 기업의 비즈니스 중요도를 기준으로 조정*
2. *발견 : 공격 표면 전반에 대한 자산과 관련 위험을 확인*
3. *우선순위: 악용시 기업에 영향을 미칠수 있는 위험을 확인*
4. *검증: 공격자가 기존의 관리 환경을 악용할 수 있는지 검증*
5. *대응: 위험 사항에 대한 협력 및 대응*

tenable

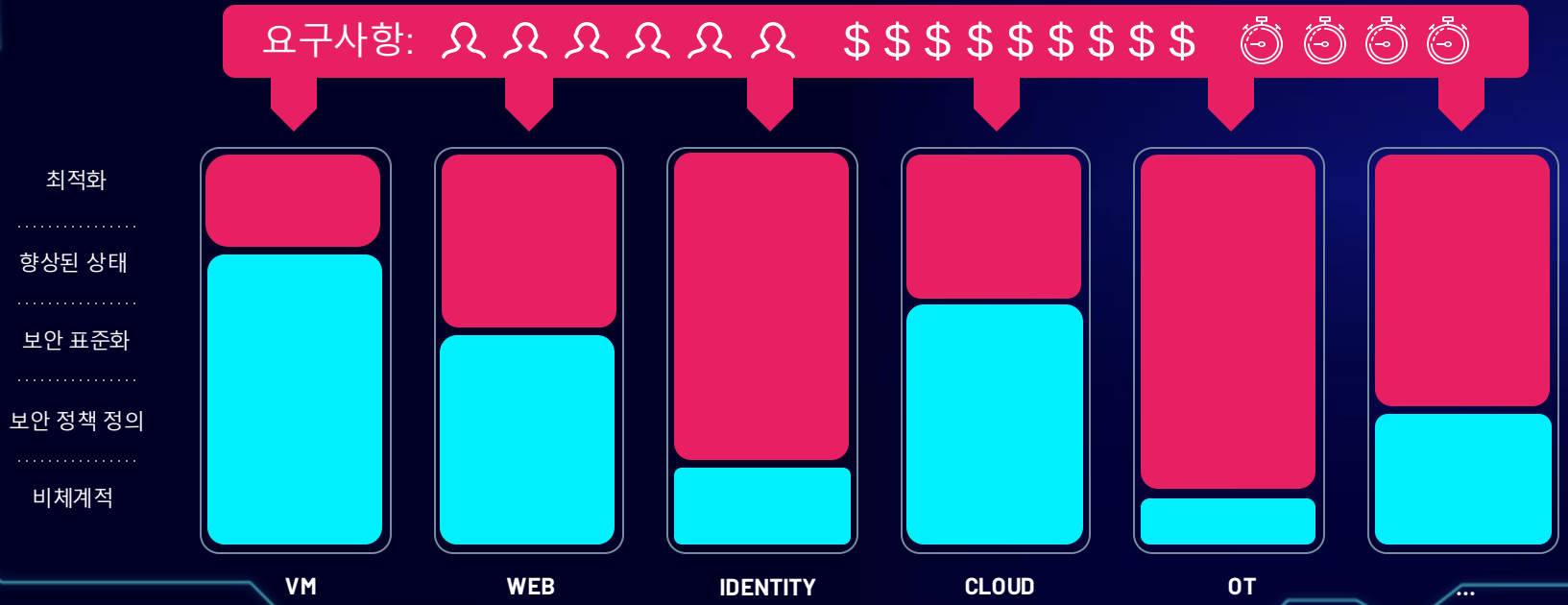
현재: 사전 예방 보안 현황- 보안 성숙도 차이



tenable

과제: 한정적 자원으로 인한 보안 성숙도 향상 어려움

활용 가능: $ $ $

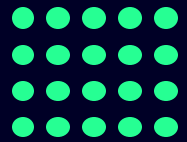


tenable

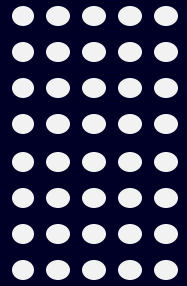
위험평가 기준 및 방안이 필요

위험 발견
공격 표면들
1

Identities



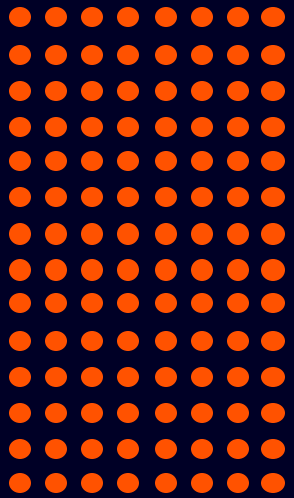
Assets



내외부 접점의 자산과 계정 관련 사항을 확인

위험 확인
방어 가능한 위험
2

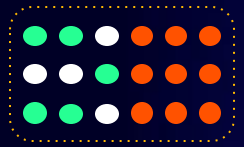
취약점 | 잘못된 설정 | 과도한 권한



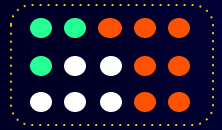
접속 및 측면 이동에 사용되는 세가지 형태의 위험을 확인

위험 조정
비즈니스 연관성
3

비즈니스 서비스 A

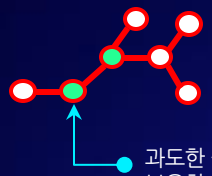


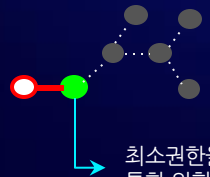
비즈니스 프로세스 B



자산, 계정, 위험을 사업측면과 연결하고 우선 순위를 선정

위험 개선
실제 위험 노출 확인
4





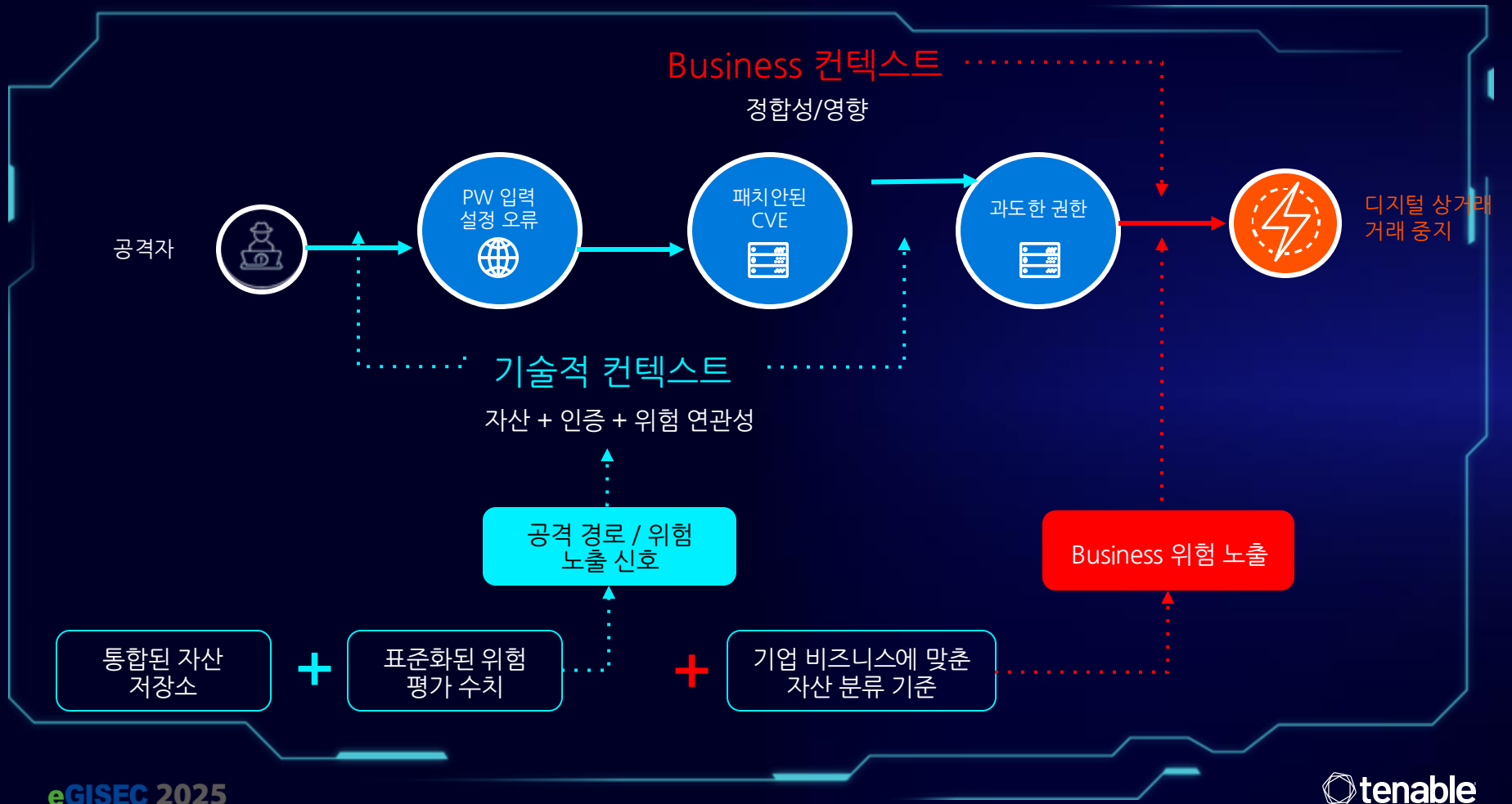
공격 경로를 분석하고 최적의 위치에 조치 가능 사항을 적용

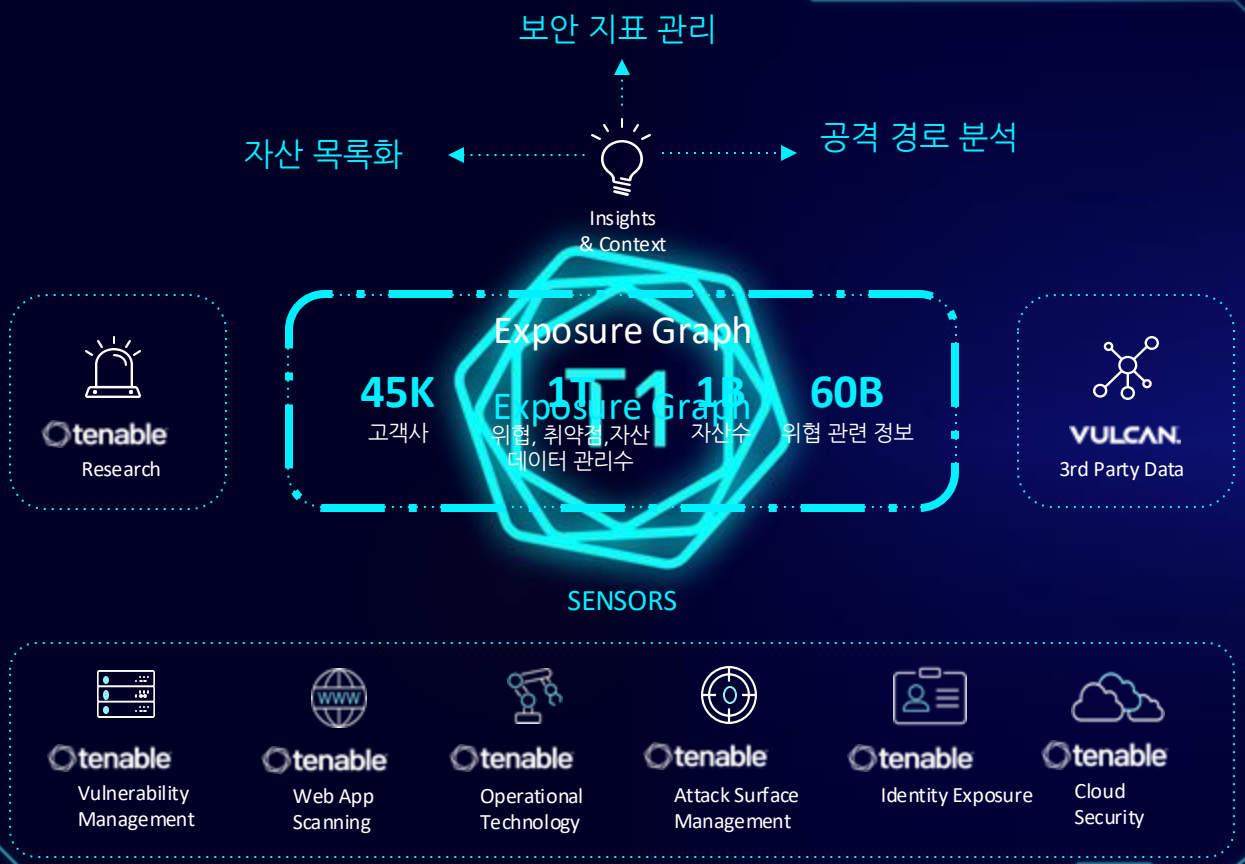
지속적인 위험 개성
투자 최적화
5

최적의 보안 결과가 나올수 있는 위치를 파악하고 투자 및 관리

tenable


자산
위험
솔루션
위험도평가
위험 점수
웹 어플리케이션
인증 방법의 잘못된 설정
WAS
L M H C
HIGH
윈도우즈 서버
조치되지 않은 CVE
VM
CVSS 0-10
8.2
시스템 계정
과도한 권한 설정
AD
PASS FAIL
FAIL
통합 자산 저장소
악용 가능성
영향도
위험 노출 지표
VPR = 7.5
ACR = 10
AES = 901
VPR = 9.2
ACR = 7
AES = 827
VPR = 9.5
ACR = 3
AES = 750
어떤 자산이 운영되고 있는지?
어떤 자산의 가장 위험한 것으로 평가되는지?
표준화된 위험 점수


Business 컨텍스트
정합성/영향
공격자
PW 입력
설정 오류
패치안된
CVE
과도한 권한
디지털 상거래
거래 중지
기술적 컨텍스트
자산 + 인증 + 위험 연관성
공격 경로 / 위험
노출 신호
Business 위험 노출
통합된 자산
저장소
+
표준화된 위험
평가 수치
+
기업 비즈니스에 맞춘
자산 분류 기준


보안 지표 관리
자산 목록화
공격 경로 분석
Insights
& Context
Exposure Graph
45K
고객사
1T
위협, 취약점,자산
데이터 관리수
1B
자산수
60B
위협 관련 정보
Exposure Graph
tenable
Research
VULCAN.
3rd Party Data
SENSORS
tenable
Vulnerability
Management
tenable
Web App
Scanning
tenable
Operational
Technology
tenable
Attack Surface
Management
tenable
Identity Exposure
tenable
Cloud
Security

tenable

Tenable One

위험 노출 관리 플랫폼

통합 가시성

공격 표면에 존재하는 모든 자산과 위험을 확인

통합 인사이트

중요 연관정보를 활용하여 실제 위험 노출의 중요도를 판정

통합 조치

위험을 제거하기 조직들간의 대응 태세 구축

멀티 클라우드

연결 계정

하이브리드 어플리케이션

관리되지 않는 자산

OT 및 IoT

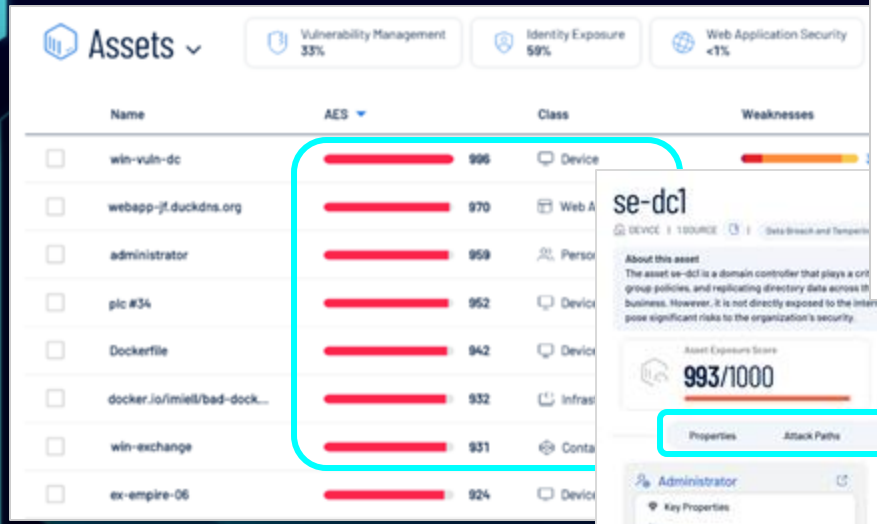
프라이빗 클라우드 와 IT

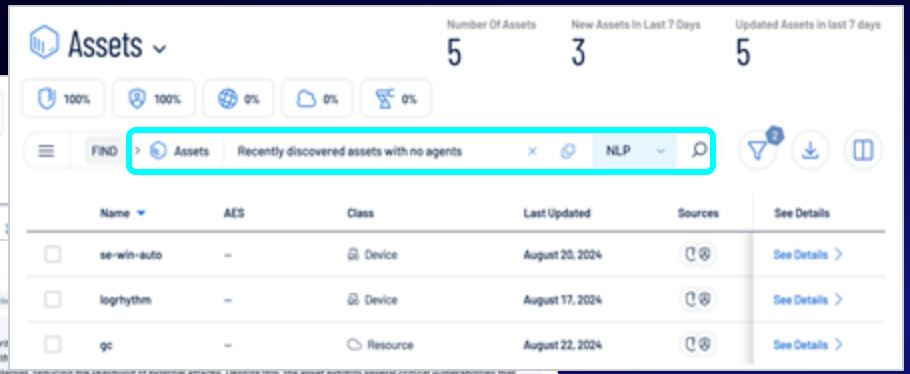
tenable

통합 가시성- 자산 분석 및 조사 간소화

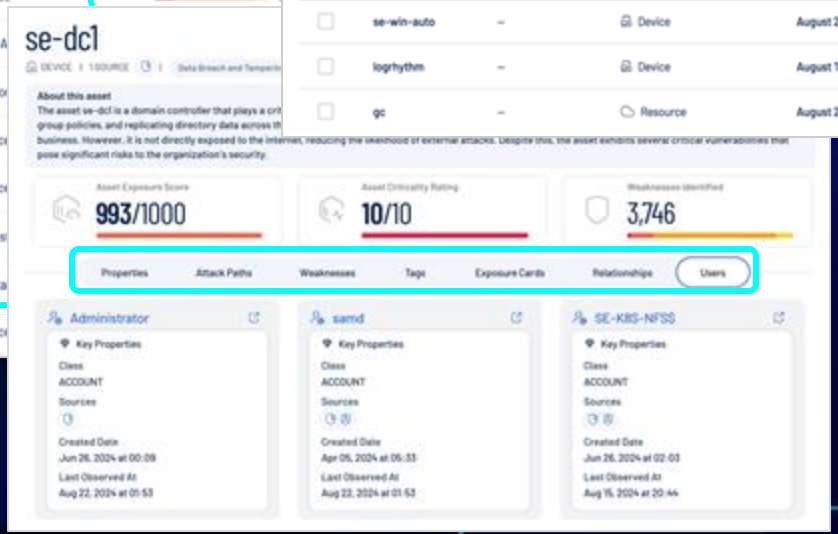
AI - 기반 검색 기능

전체 도메인 자산 목록화+ 위험 표준화





Agent 없이 최근에 확인된 자산 목록



자산 상세 정보, 계정 및 관계분석

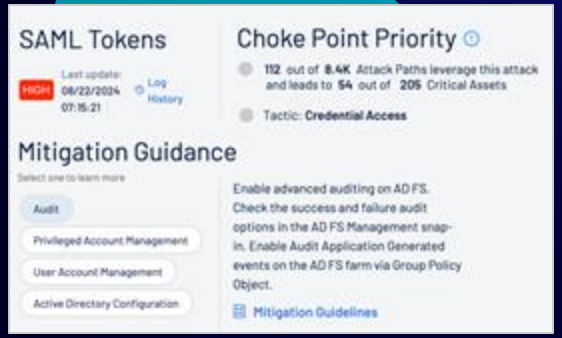
tenable

통합 인사이트- 연관정보 공유 및 실제 위험 노출 우선순위 분석

X-도메인 공격 경로

Solarwinds: On Prem to Identity to Cloud

AI - 공격 경로 관련 분석 정보



Choke Point 관련 정보 제공

Back to Attack Paths

- ExternalAsset reaches into Windows Server through RDP
- Public Internet can reach into dc01 from the internet
- 3.84.5.178 compromises LN-DEMO through RDP
- External asset 3.84.5.178 reaches to prod-bigfix by exploiting CVE-2023-28231
- External asset 3.84.5.178 reaches to win-2019 by exploiting CVE-2022-27776
- External asset 3.84.5.178 reaches to win-sql2012 by exploiting CVE-2022-30136
- External asset 3.84.5.178 reaches to win-2019 by exploiting CVE-2023-23403
- External asset 3.84.5.178 reaches to workstation ex-empire-05 by exploiting CVE-2023-28247
- External asset 3.84.5.178 reaches to workstation ex-empire-05 by exploiting CVE-2022-30145
- External asset 3.84.5.178 reaches into ex-empire-05 by exploiting CVE-2020-0809

View Findings (1)

Attacker exploits CVE-2024-21440 to gain access to srv1 AI

An attacker starts by exploiting a vulnerability in apaws, CVE-2024-21440. This vulnerability allows the attacker to gain access to APADC, the domain controller. Once the attacker has access to the domain controller, they can use the NTDS technique to access the Active Directory database. The attacker can then use the Domain Accounts technique to create a new user account with administrative privileges. Finally, the attacker can use the Services Registry Permissions Weakness technique to gain access to srv1.

Related Products, Assets, and Findings

- Tenable Identity Exposure (AD)
- Tenable Vulnerability Management (44401, 64582, 167250, 167251, 191947)

Exposed Asset | Critical Asset

AI Assistant

Open Findings
9002
0 Critical
0 High
5 Medium
9K Low

Archived Findings
53700
0 Critical
0 High
26 Medium
53.7K Low

Total Findings
62702
0 Critical
0 High
31 Medium
62.7K Low

Back to Findings

Exploitation of Remote Services

MED Last update: 11/25/2024 14:48:06 | Log History

From Windows Workstations 2 +4 more
To apaeng.apadomain.internal

View Attack Paths
Share

Details

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine ...

Choke Point Priority

MED

- 2 out of 8.3K Attack Paths leverage this attack and leads to 1 out of 146 Critical Assets
- Tactic: **Lateral Movement**

Mitigation Guidance

Select one to learn more

- Privileged Account Management
- Disable or Remove Feature or Program
- Threat Intelligence Program
- Application Isolation and Sandboxing

Minimize permissions and access for service accounts to limit impact of exploitation.

Mitigation Guidelines

Related Products, ndings

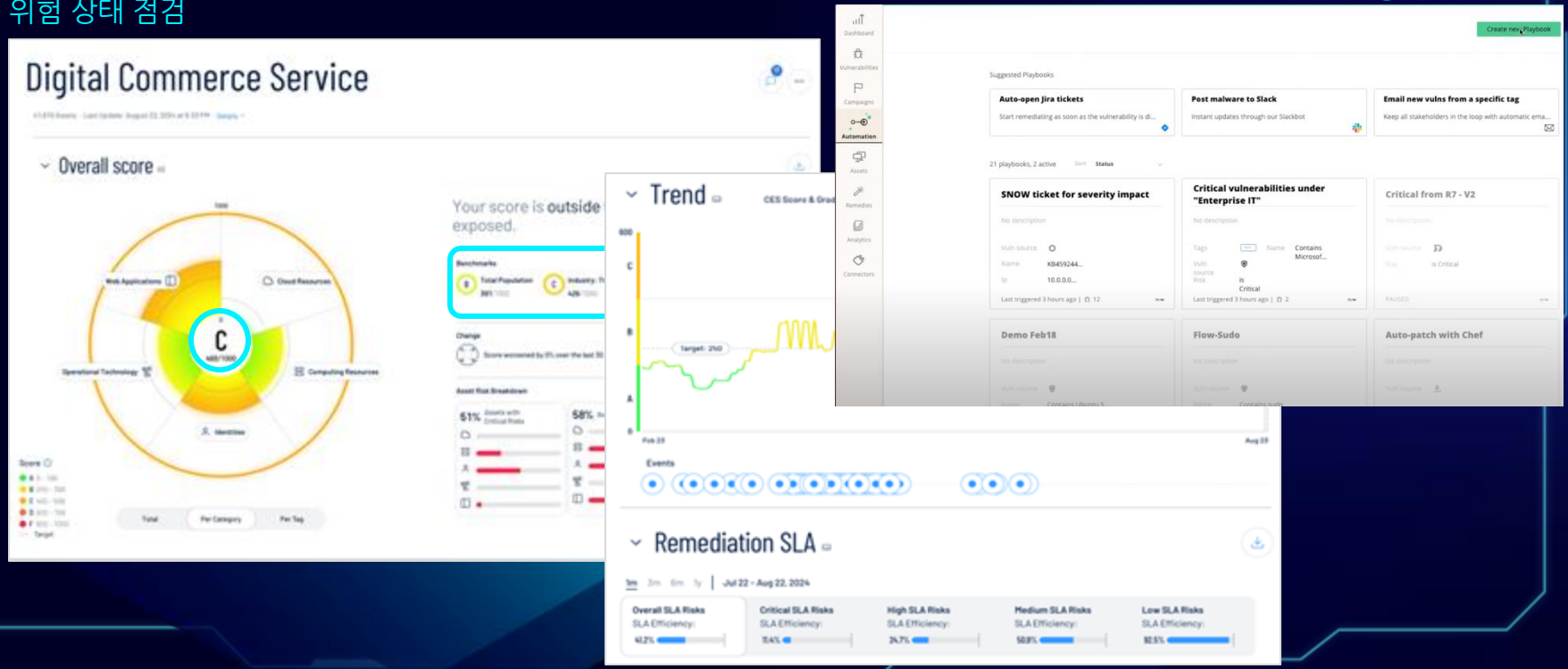
KB5035885: Windows Server 2012 R2 Security Update (March 2024)

- Tenable Vulnerability Management (64582, 191942)

통합 조치- 위험 현황을 점검하고 자동화를 통한 조치

위험 상태 점검

자동화



조치 현황 관리

tenable

New Custom Card

Custom Cards 30 Total

C Direct Sales Portal
$10.3 Million
472 471 459
Categories Tags SLA

C Digital Commerce Portal
$51 Million
586 551 470
Categories Tags SLA

A Retail: Point of Sale
$3.7 Million
162 152 148
Categories Tags SLA

B Non-Revenue Impacting
320 314 310
Categories Tags SLA

76 Assets · Last Update: October 31, 2024 at 10:41 AM · Details

Remediation SLA

X

SLA Efficiency | Overall SLA risks

1 Month 3 Months 6 Months 1 Year | Jan 12 - Feb 12, 2025

Overall SLA Risks	Critical SLA Risks	High SLA Risks	Medium SLA Risks	Low SLA Risks
34.9% 2,486/7,130 SLA Efficiency	6.4% 40/621 SLA Efficiency	17.1% 650/3,809 SLA Efficiency	61.1% 1,382/2,263 SLA Efficiency	94.7% 414/437 SLA Efficiency

Overall SLA Risks

Total Risks 7,130 106.1%

Avg remediation days 108.0 Days -45.1%

Filter trend graph: Overall Critical High Medium Low

SLA Breakdown | Overall SLA risks

All Risks | Remediated Risks | Non-Remediated Risks

Risk Distribution

Inside SLA

Risk Distribution in days

In time Overdue

3rd Party 데이터 통합

어플리케이션 보안 제품군

Acunetix by Invicti
Micro Focus Fortify
BITSIGHT
Netsparker by Invicti
CYCOGNITO
Security Scorecard

ENDPOINT 보안 제품군

CROWDSTRIKE
Microsoft
SentinelOne
paloalto NETWORKS
TANIUM

클라우드

aws
WIZ
aqua
Google
Microsoft
orca security

자산 INV.

AXONIUS
jamf

BUG BOUNTY

bugcrowd
hackerone

IOT

ARMIS

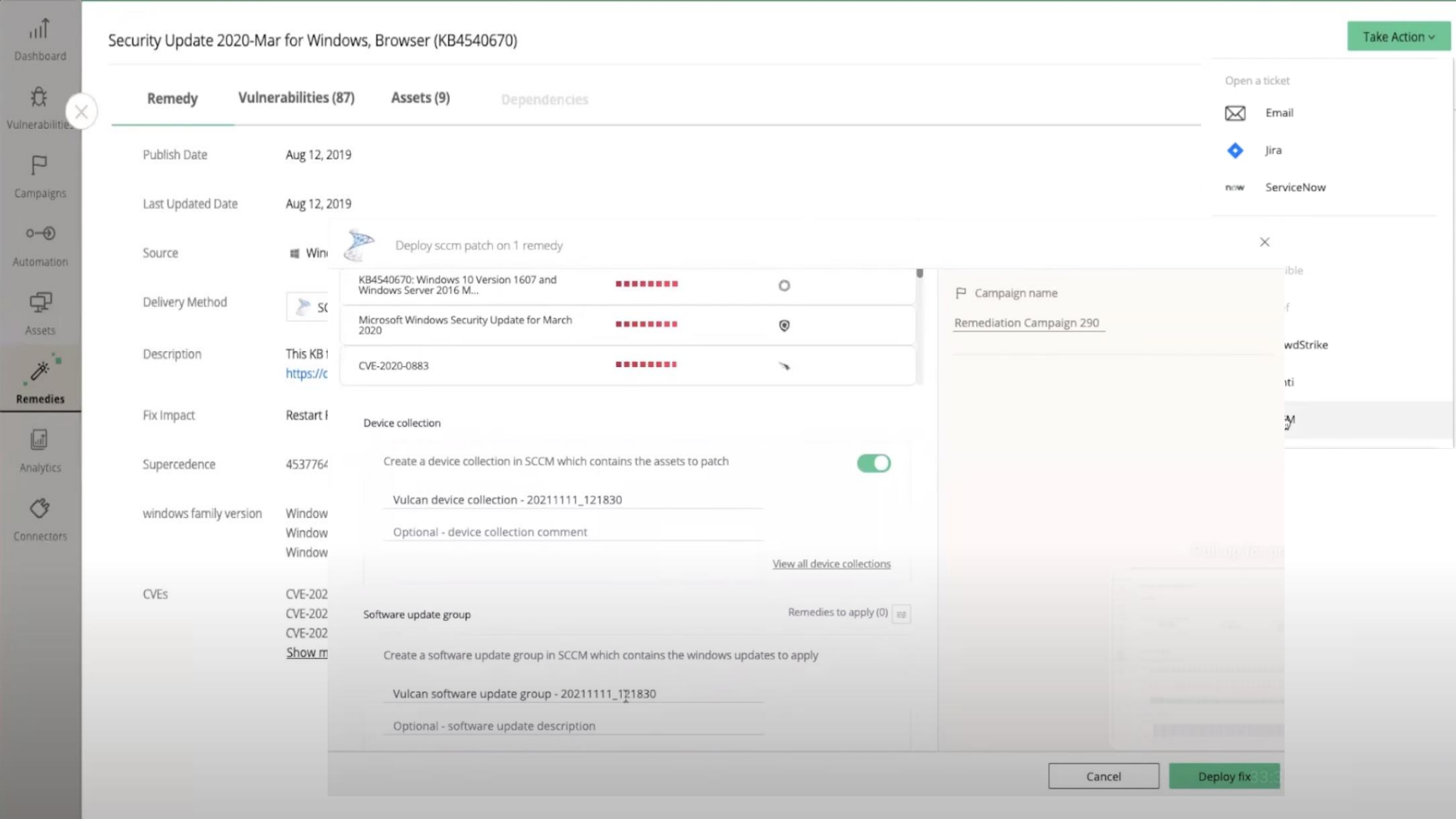
CMDB

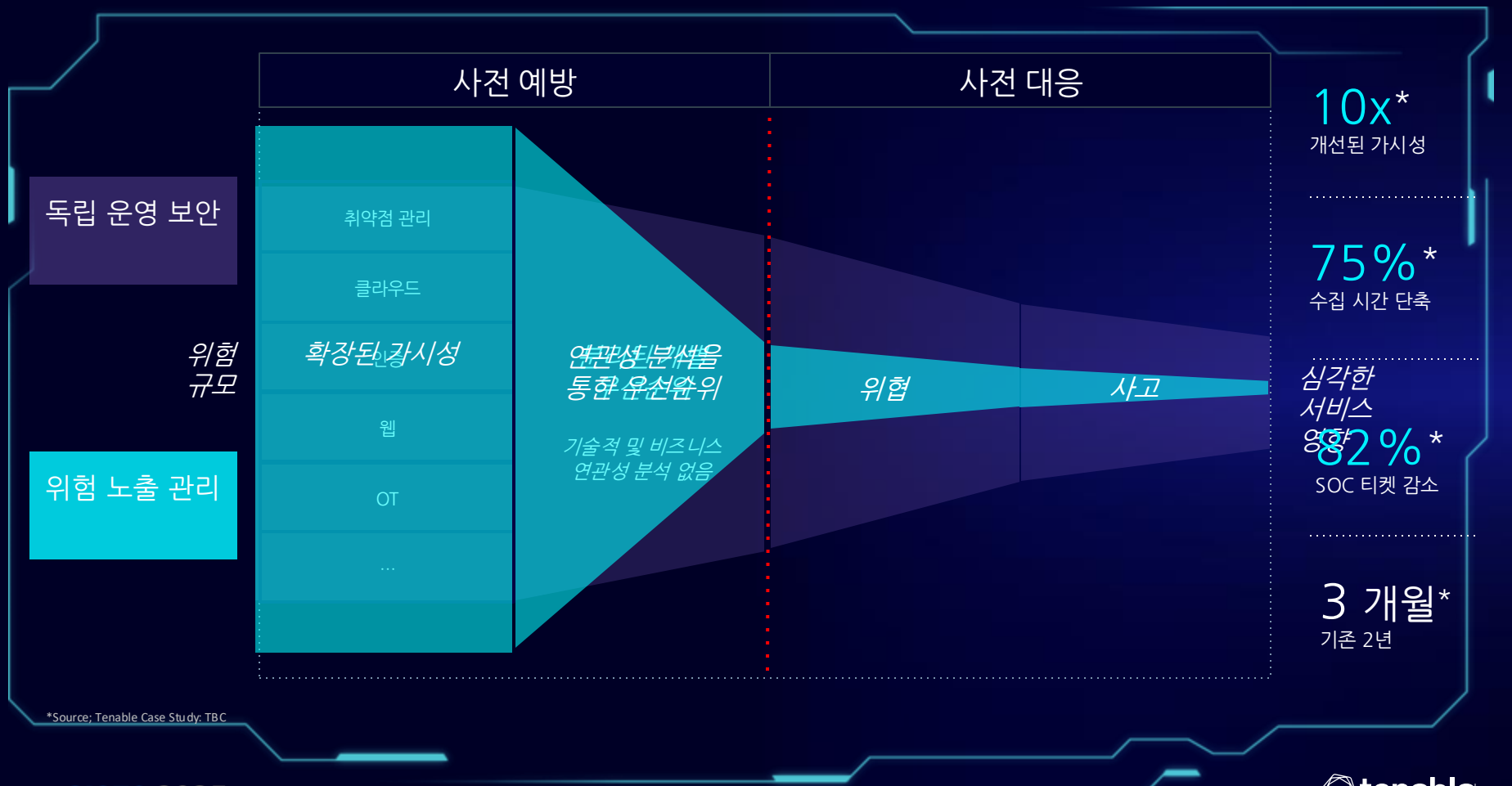
ATLASSIAN
servicenow

취약점 점검

CLONE SYSTEMS.
PRISMA BY PALO ALTO NETWORKS
Intune
Qualys.
LACEWORK
RAPID7
Outpost24
Red Hat

tenable


Dashboard
Vulnerabilities
Campaigns
Automation
Assets
Remedies
Analytics
Connectors
Security Update 2020-Mar for Windows, Browser (KB4540670)
Take Action
Remedy
Vulnerabilities (87)
Assets (9)
Dependencies
Publish Date
Aug 12, 2019
Last Updated Date
Aug 12, 2019
Source
Delivery Method
Description
Fix Impact
Supercedence
windows family version
CVEs
Open a ticket
Email
Jira
ServiceNow
Deploy sccm patch on 1 remedy
KB4540670: Windows 10 Version 1607 and Windows Server 2016 M...
Microsoft Windows Security Update for March 2020
CVE-2020-0883
Campaign name
Remediation Campaign 290
Device collection
Create a device collection in SCCM which contains the assets to patch
Vulcan device collection - 20211111_121830
Optional - device collection comment
View all device collections
Software update group
Remedies to apply (0)
Create a software update group in SCCM which contains the windows updates to apply
Vulcan software update group - 20211111_121830
Optional - software update description
Cancel
Deploy fix


사전 예방
사전 대응
독립 운영 보안
위험 노출 관리
위험
규모
취약점 관리
클라우드
확장된 감시성
웹
OT
…
연관성 분석을
통한 우선순위
기술적 및 비즈니스
연관성 분석 없음
위협
사고
10x*
개선된 가시성
75%*
수집 시간 단축
심각한
서비스
영향
82%*
SOC 티켓 감소
3 개월*
기존 2년
*Source; Tenable Case Study: TBC
eGISEC 2025
tenable

Thank you