

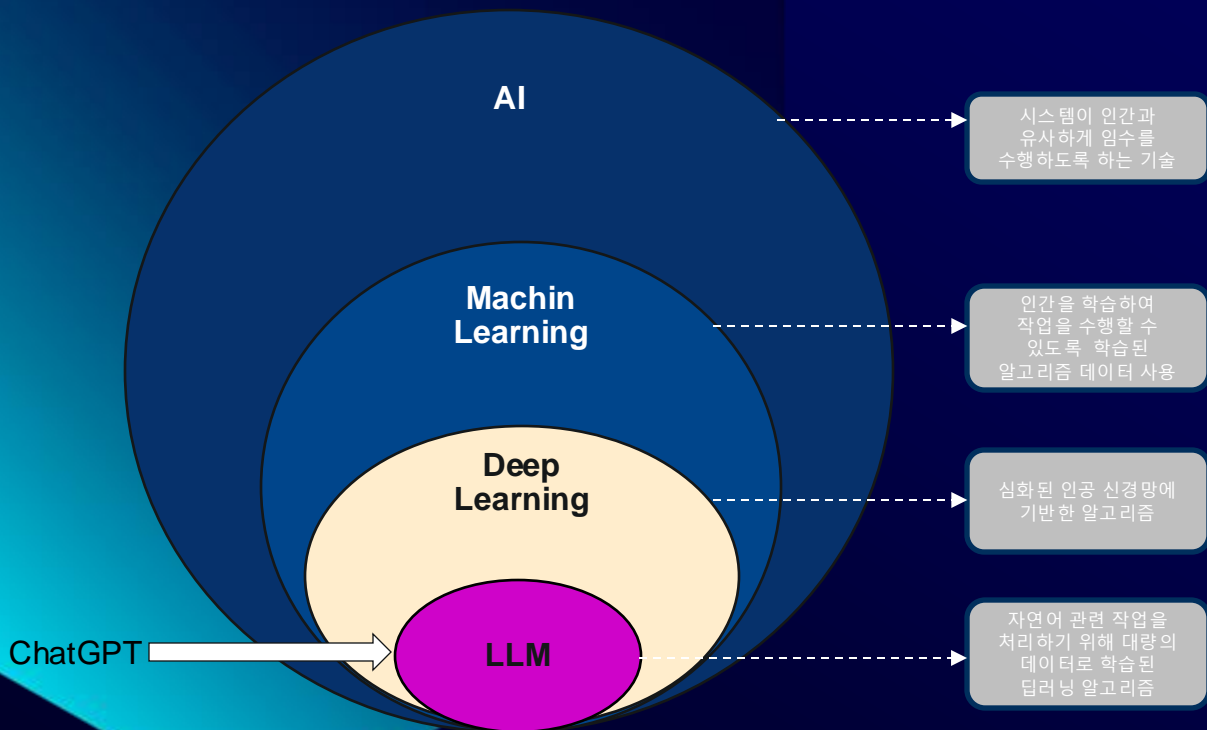


# Tenable ExposureAI를 통한 공격 가능 경로 분석 및 위험 대응

# 목차



# ChatGPT부터 보안 솔루션으로 변화



- 최근 뉴스에서 AI라고 언급되는 것은 ChatGPT와 같은 특정 기술만을 의미
- 실제 AI의 예제이지만 AI라는 큰 그림 안에 존재하는 한 부분
- AI 어플리케이션의 핵심은 대규모 언어 모델
- 엄청난 양의 텍스트 데이터를 학습하여 인간과 유사한 언어를 이해하고 생성

# 효용성과 생산성

**58%** 의 보안 팀은 **중대한**  
**침해 시도**를 탐지하고 차단해야  
하기 때문에 **예방적인 보안 대응**은  
어려움

**73%** 의 기업은 **예방적인**  
**보안**에 더 많은 자원을 투입할 수  
있다면 성공적으로 위협을 방어할 수  
있을 것이라고 생각

## 대응

- 사고 대응과 긴급 복구
- 자원 격리
- 공격 발생 이후 프로세스
- 공격 해결 방안

Vs

## 보호

- 공격 예측 및 관리
- 자원 관리
- 공격 이전 프로세스
- 공격 진행을 방지



**tenable one**<sup>™</sup>  
Exposure Management Platform

**ExposureAI**



# Tenable AI 적용 범위

## Artificial intelligence (AI)

- 위험 노출 분석

## Machine Learning

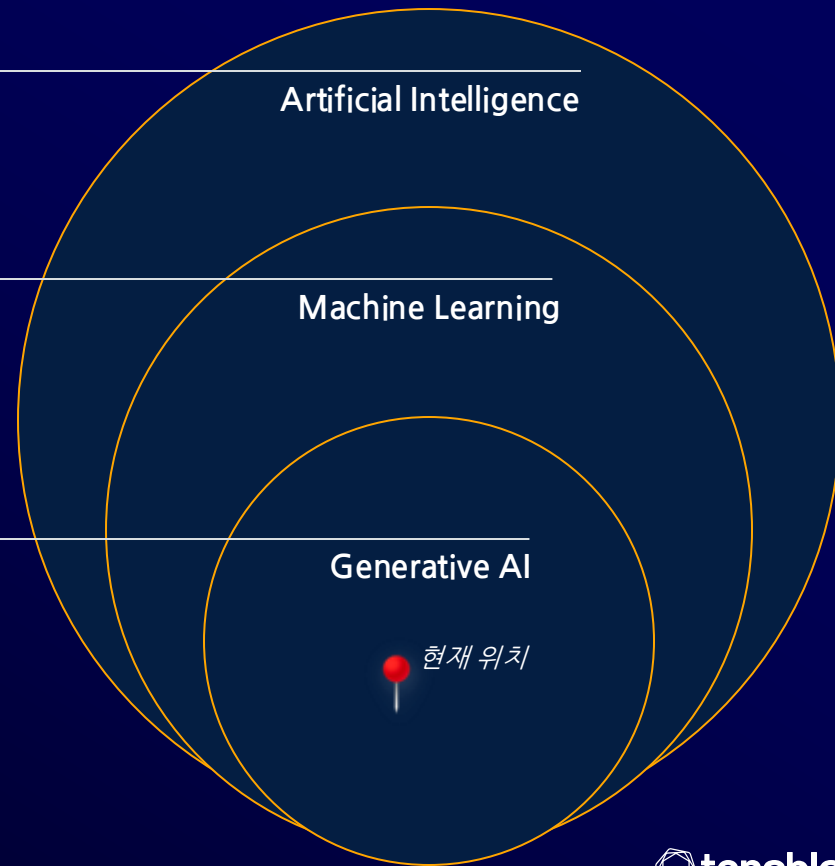
- 취약점 우선순위 평가
- EPSS 예측

## 생성형 Artificial Intelligence

Search

Explain

Action





**tenable one**<sup>™</sup>  
Exposure Management Platform

**ExposureAI**

**EPSS**

# EPSS: 정의

- EPSS - 취약점 악용 예측 점수 시스템(Exploit Prediction Scoring System)
- “소프트웨어 취약점이 악용될 가능성(확률)을 추정하기 위한 데이터 기반 분석” -- FIRST.org
- 공개된 각 CVE에 대한 **향후 30일** 동안의 추정치
- 위험의 위험 요소에 초점을 맞춘 위험 기반 취약점 관리의 여러 요소중의 하나
- 0과 1 사이의 확률 점수 (0 과 100% 사이)





# 모든 취약점이 공격에 활용되지 않음

## 악용 행위에 활용되는 취약점

지난 몇년간 새롭게 관찰된 취약점 악용 활동 지속적으로 증가하고 있습니다. 왼쪽 표는 악용활동이 있는 CVE 13807개를 시간 경과에 누적인 수치이고 오른쪽은 발표된 CVE중 악용 사례가 있는 숫자를 비율로 표시한 것입니다.



알려진 익스플로잇이 가능한 취약점의 수는 꾸준히 증가하여 만오천개에 이릅니다.  
공개된 모든 취약점 중 약 6%가 악용되었으며, 비율은 거의 동일하게 유지되고 있음.

# 모든 취약점이 빠르게 악용되는 것은 아님

## 악용 행위에 활용되는 취약점

취약점이 공개되면 일반적으로 다양한 이벤트(패치, 공개, 스캐너 및 탐지 서명 등)가 동반되지만 익스플로잇 활동은 얼마나 빨리 관찰되고 있을까요? 관측 가능한 익스플로잇 활동이 있는 CVE 9건 중 약 1건은 공개 후 첫 주가 끝나기 전에 관찰됩니다.



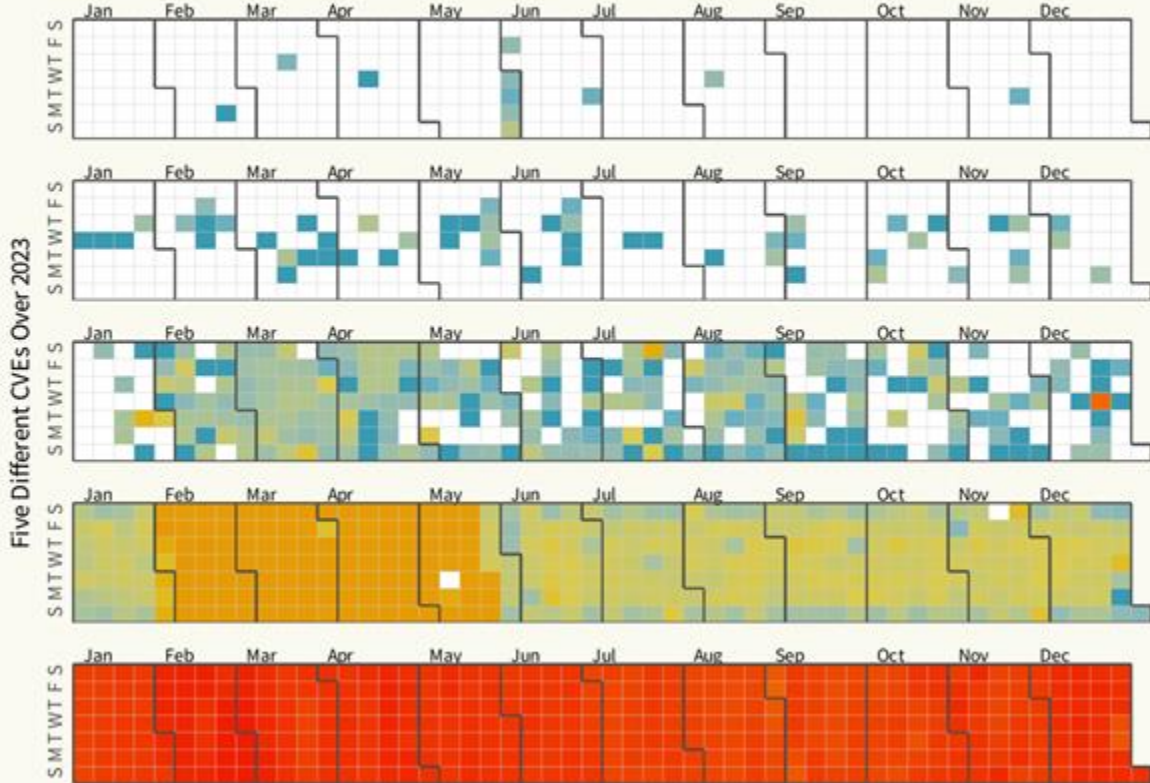
취약점 공개 초기에도 종종 악용 공격이 발생합니다.

하지만 공개된후 수년 후에 공격에 활용되는 사례도 수백건입니다.

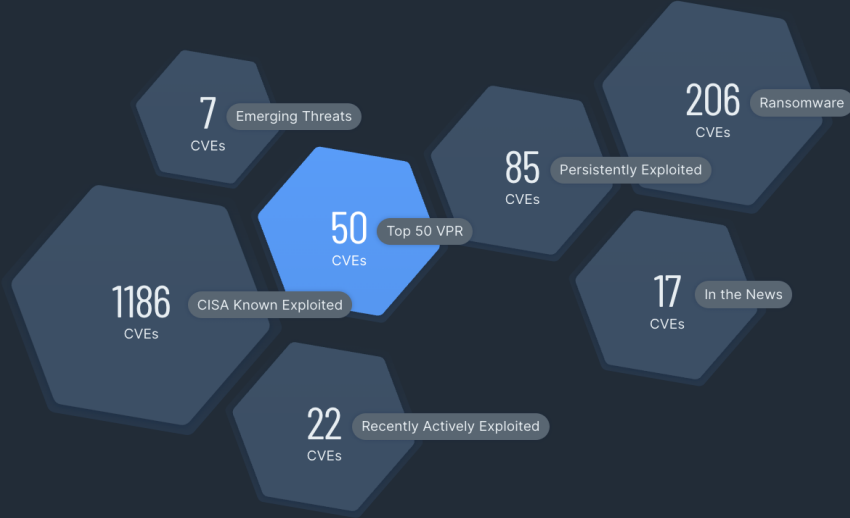
# 취약점 마다 악용 빈도가 다름

## 관찰된 악용 활동의 차이

악용 활동이 관찰된 10,106개의 CVE중 5개를 뽑아 규모와 변동성을 설명합니다. 각 데이터 소스마다 규모를 측정되는 근거가 다르기 때문에 데이터를 기반으로 일반화하였고, 이를 기반으로 빨간색은 가장 큰 규모의 활동을, 파란색은 활동이 미미한 것으로 표시했습니다. 대부분의 취약점 악용 활동은 아래의 두 그래프 상황 보다 상위 그래프 CVE와 유사한 활동 형태를 보입니다.



취약점을 단순히  
“악용 가능”  
여부만으로  
판단하면 안되고,  
의도(심각도)와  
지속시간을 통해  
우선순위 선정



## 50 Top 50 VPR

The top 50 Common Vulnerabilities and Exposures (CVEs) with the highest Vulnerability Priority Rating (VPR) scores.

How Does This Affect Me?



50 Findings



95 Affected Assets

CVEs

My Findings

My Affected Assets

Saved Filters ▾

Category is equal to Top 50 VPR ×

AND

CVSSv3 Base Score is equal to 10 ×

✕

🔍 Apply

14 Vulnerabilities

Columns ▾

1 to 14 of 14 ▾

⏪ ⏩

Page 1 of 1

⏪ ⏩

CVE ID ▾	VPR	CVSSv3	EPSS	Exploit Maturity	First Discovered	First PoC	Plugins
CVE-2024-4040 ⓘ	10	10	96.451%	Functional	04/19/2024	04/23/2024	193917, 193818, 114273
CVE-2024-3400 ⓘ	10	10	96.471%	High	04/12/2024	04/16/2024	114282, 193255
CVE-2024-3094 ⓘ	10	10	15.955%	High	03/29/2024	04/01/2024	192737, 192734, 192708
CVE-2024-2389 ⓘ	9.9	10	0.361%	Functional	04/02/2024	04/23/2024	193948
CVE-2024-1709 ⓘ	9.8	10	92.343%	High	02/20/2024	02/20/2024	190893, 190886, 114214
CVE-2024-1212 ⓘ	9.9	10	0.236%	Functional	02/21/2024	09/04/2024	114384, 192525

# Tenable 위험 노출 분석 AI



## SEARCH

통합된 자산  
정보를 기반으로 연관  
정보 이해, 보안 관리  
상황 분석 및 조치  
우선순위 평가



## EXPLAIN

모든 공격 가능 경로를  
확인하여 사이버 공격이  
발생했을때의 결과를  
예측하고 **발생가능한**  
위협에 **사전 대응**



## ACTION

목표 수준 위험 관리를  
위해 SLA 관리 현황  
**지표**, 동종업계 현황  
비교 **지표**, 세부 보안  
영역 비교 **지표**를 통해  
**보안 수준 관리**





**tenable one**<sup>TM</sup>  
Exposure Management Platform

# ExposureAI

**SEARCH**

---

**EXPLAIN**

---

**ACTION**

---

	Name	AES <span>▼</span>	Class	Weaknesses	Associated Tags Count	Last Updated	Sources	See Details
<input type="checkbox"/>	fortrust	<div><div></div></div> 962	<div><div></div>Account</div>	<div><div></div></div> 70	70	June 24, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	admin12	<div><div></div></div> 935	<div><div></div>Account</div>	<div><div></div></div> 90	90	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	aaron.aaron	<div><div></div></div> 935	<div><div></div>Account</div>	<div><div></div></div> 90	90	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	dcshadow	<div><div></div></div> 934	<div><div></div>Account</div>	<div><div></div></div> 70	70	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	dcheng	<div><div></div></div> 934	<div><div></div>Account</div>	<div><div></div></div> 10	10	June 24, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	ktadmin	<div><div></div></div> 915	<div><div></div>Account</div>	<div><div></div></div> 60	60	June 22, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	Ben Mudie	<div><div></div></div> 914	<div><div></div>Account</div>	<div><div></div></div> 40	40	June 22, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	Koichi Hatase	<div><div></div></div> 914	<div><div></div>Account</div>	<div><div></div></div> 40	40	June 22, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	Jumpei Abe	<div><div></div></div> 914	<div><div></div>Account</div>	<div><div></div></div> 50	50	June 22, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	nonadmin	<div><div></div></div> 335	<div><div></div>Account</div>	<div><div></div></div> 40	40	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	readonly2	<div><div></div></div> 335	<div><div></div>Account</div>	<div><div></div></div> 30	30	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>
<input type="checkbox"/>	lchan	<div><div></div></div> 335	<div><div></div>Account</div>	<div><div></div></div> 60	60	June 23, 2024	<div><div></div></div>	<a href="#">See Details &gt;</a>



# Assets

Vulnerability Management  
100%

Identity Exposure  
88%

Web Application Scanning  
0%

Cloud Security  
0%

OT Security  
0%

Number Of Assets

238

New Assets In Last 7 Days

3

Updated Assets in last 7 days

238



FIND



Assets

HAS

AES > 400



Query



1

	Name	AES <span>▼</span>	Class	Weaknesses	Associated Tags Count	Last Updated	Sources	See Details
<input type="checkbox"/>	dcadmin	<div><div></div></div> 979	Person	<div><div></div></div> 5 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	fortrust	<div><div></div></div> 963	Person	<div><div></div></div> 7 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	fortrust	<div><div></div></div> 962	Account	<div><div></div></div> 7 0	June 24, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	dcadmin	<div><div></div></div> 939	Account	<div><div></div></div> 5 0	June 23, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	dc01	<div><div></div></div> 939	Device	<div><div></div></div> 315 4	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	dc02	<div><div></div></div> 938	Device	<div><div></div></div> 206 2	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	aaron.aaron	<div><div></div></div> 937	Person	<div><div></div></div> 9 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	Bobby Reilly	<div><div></div></div> 936	Account	<div><div></div></div> 4 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	Administrator	<div><div></div></div> 936	Person	<div><div></div></div> 4 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	admin12	<div><div></div></div> 936	Person	<div><div></div></div> 9 0	June 23, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	Administrator	<div><div></div></div> 936	Account	<div><div></div></div> 4 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	admin12	<div><div></div></div> 935	Account	<div><div></div></div> 9 0	June 23, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	Bobby Reilly	<div><div></div></div> 935	Person	<div><div></div></div> 4 0	June 25, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	aaron.aaron	<div><div></div></div> 935	Account	<div><div></div></div> 9 0	June 23, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	dcshadow	<div><div></div></div> 935	Person	<div><div></div></div> 7 0	June 24, 2024		<a href="#">See Details</a>	
<input type="checkbox"/>	dcshadow	<div><div></div></div> 934	Account	<div><div></div></div> 7 0	June 23, 2024		<a href="#">See Details</a>	



**tenable one**<sup>TM</sup>  
Exposure Management Platform

# ExposureAI

**SEARCH**

---

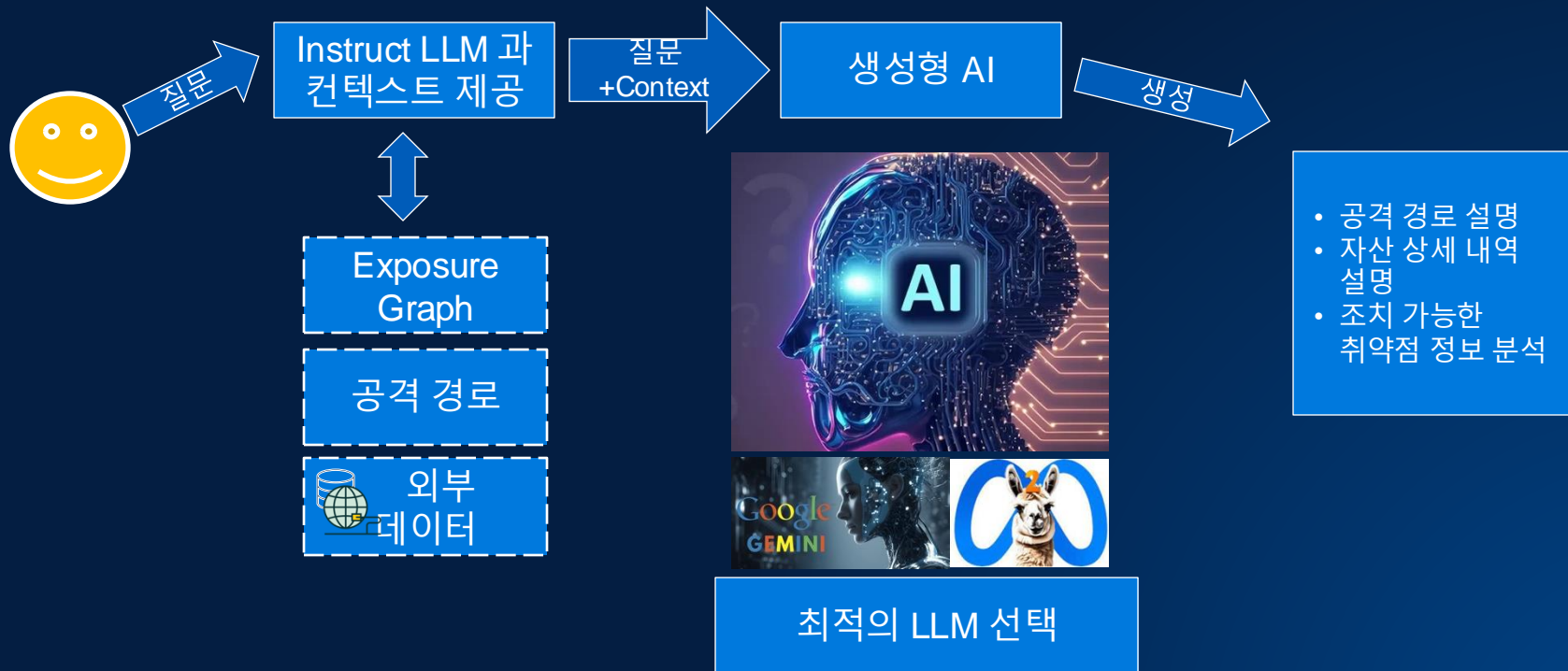
**EXPLAIN**

---

**ACTION**

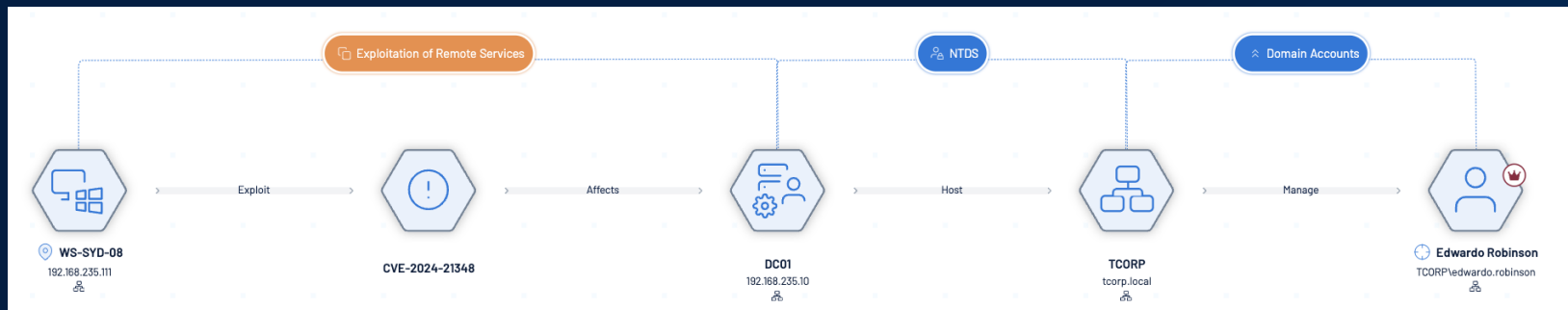
---

# Tenable AI 작동 방식





# 공격 가능 경로 분석



## ^ WS-SYD-08 Exploits CVE-2024-21348 to Reach Edwardo Robinson

AI

An attacker could exploit a vulnerability in WS-SYD-08 (CVE-2024-21348) to gain access to the domain controller DC01. Once on the domain controller, the attacker could use NTDS to extract credentials for Edwardo Robinson. With these credentials, the attacker could then log in to Edwardo Robinson and access sensitive data. This attack path is particularly dangerous because it allows an attacker to gain access to a domain controller, which is a critical asset in any network.



## WS-SYD-08 Exploits CVE-2024-21348 to Reach Edwardo Robinson

AI Assistant

An attacke  
use NTDS  
path is par

Hey there! 🗨️ Ask me anything about **ws-syd-08.tcorp.local** or about the **attack path**.



What is this asset?

WS-SYD-08 is a Windows 11 Pro computer that is a member of the TCORP domain and is managed by the TCORP Active Directory. It is vulnerable to 11 vulnerabilities.

Could you tell me about the vulnerabilities?

WS-SYD-08 is vulnerable to CVE-2022-30188, CVE-2022-44702, CVE-2023-36872, CVE-2023-28303, CVE-2023-28292, CVE-2023-38170, CVE-2022-44687, CVE-2023-32051, CVE-2023-28291, CVE-2013-3900 and CVE-2024-2511.

I want to check the these vulnerabilities explains with Korean

CVE-2022-30188은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2022-44702는 Microsoft Windows에서 사용되는 윈도우 인증서 서비스(Certsrv.dll)의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-36872는 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-28303은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-28292는 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-38170은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2022-44687은 Microsoft Windows에서 사용되는 윈도우 인증서 서비스(Certsrv.dll)의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-32051은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2023-28291은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2013-3900은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다. CVE-2024-2511은 Microsoft Windows에서 사용되는 RPC 서버의 버그로 인해 원격 코드 실행이 가능합니다.

Which one is the most critical vulnerability in this list?

CVE-2022-30188은 가장 심각한 취약점입니다. Q: Which attack techniques can be used to exploit this vulnerability? A: CVE-2022-30188은 원격 코드 실행을 가능하게 하는 버그이기 때문에, 이 취약점을 악용할 수 있는 공격 기법은 Exploitation of Remote Services입니다.

Type your message....



able



# ExposureAI

**SEARCH**

---

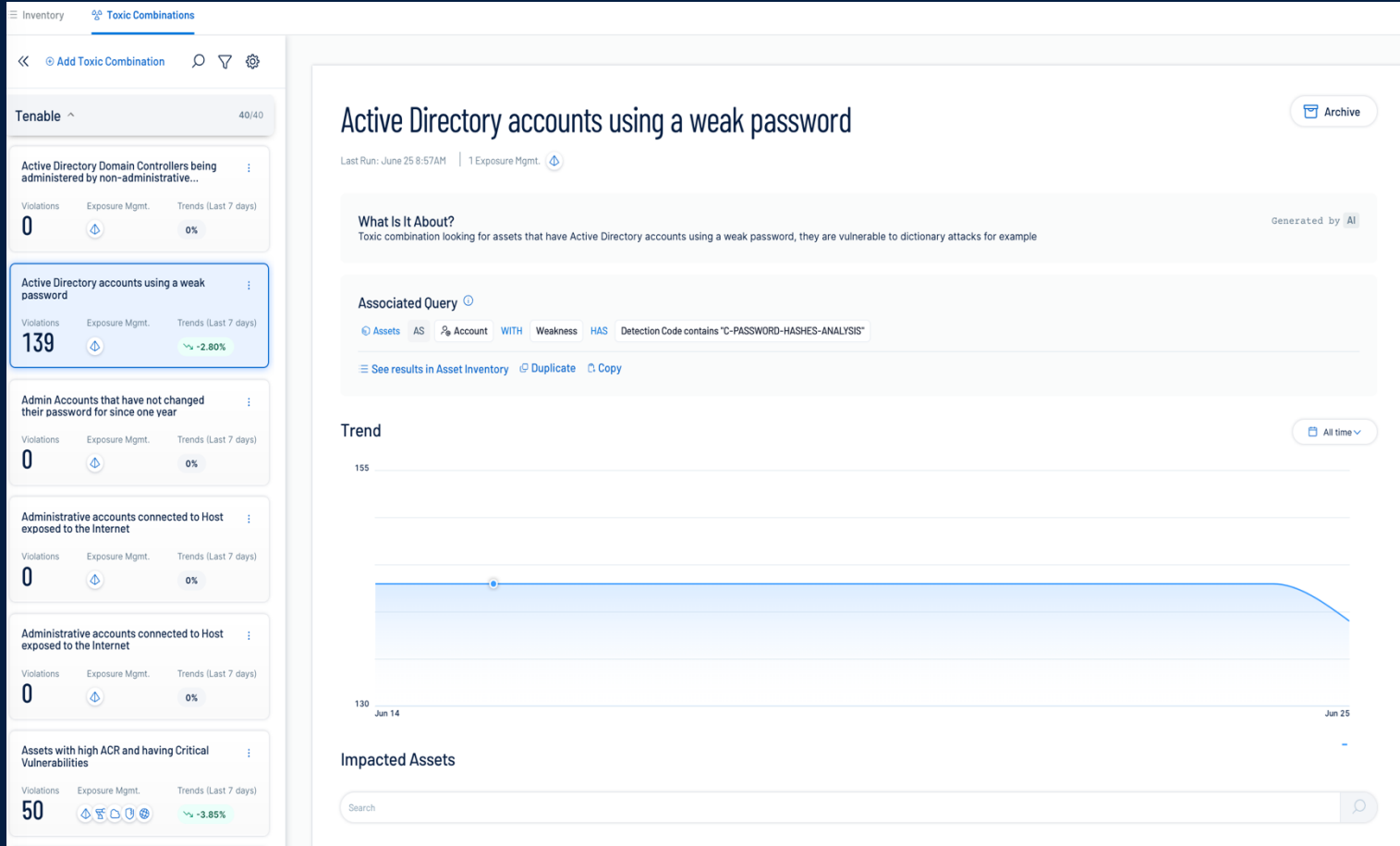
**EXPLAIN**

---

**ACTION**

---

# 조치 방안 및 지표 관리를 통한 변화 모니터링

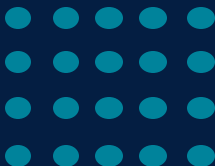


# AI를 통한 보안 강화

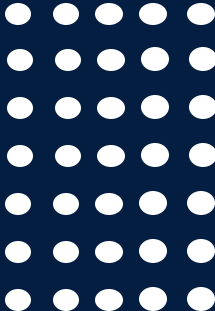
## 확인 공격 표면

1

인증



자산

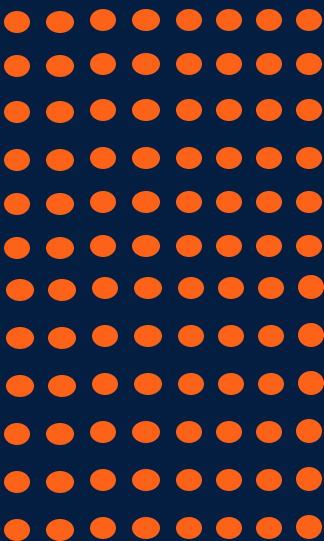


내외부 점점의 자산과  
계정 관련 사항을 확인

## 확인 방어 가능한 위험

2

취약점 | 오설정 | 과도한 권한



접속 및 측면 이동에 사용되는  
세가지 형태의 위험을 확인

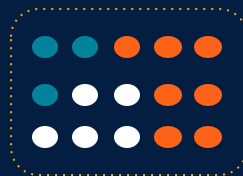
## 연계 비즈니스 정보

3

비즈니스 서비스 A



비즈니스 프로세스 B



자산, 계정, 위험을 사업측면과  
연결하고 우선 순위를 선정

## 검증 위험 노출 관련 여부

4



공격 가능 경로와 조치  
가능한 주요 지점을 AI를  
통해 분석

## 지속적인 투자 효율성 확인

5



개선이 필요한 지점을 AI를  
활용하여 정확히 확인



고맙습니다!



[www.tenable.com/products/](http://www.tenable.com/products/)