



Microsoft Defender External Attack Surface Management (EASM)

지속적인 글로벌 공격 표면 인사이트 확보

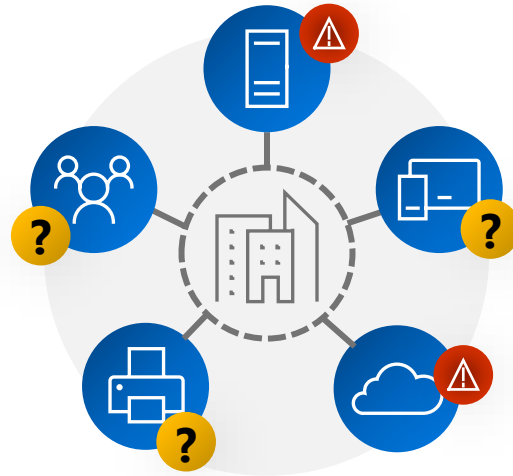
Microsoft Korea



외부 공격 표면 관리 과제



지금과 같은 하이브리드 워크 시대에
새도우 IT는 점점 더 심각한 보안
위험을 초래하고 있습니다.



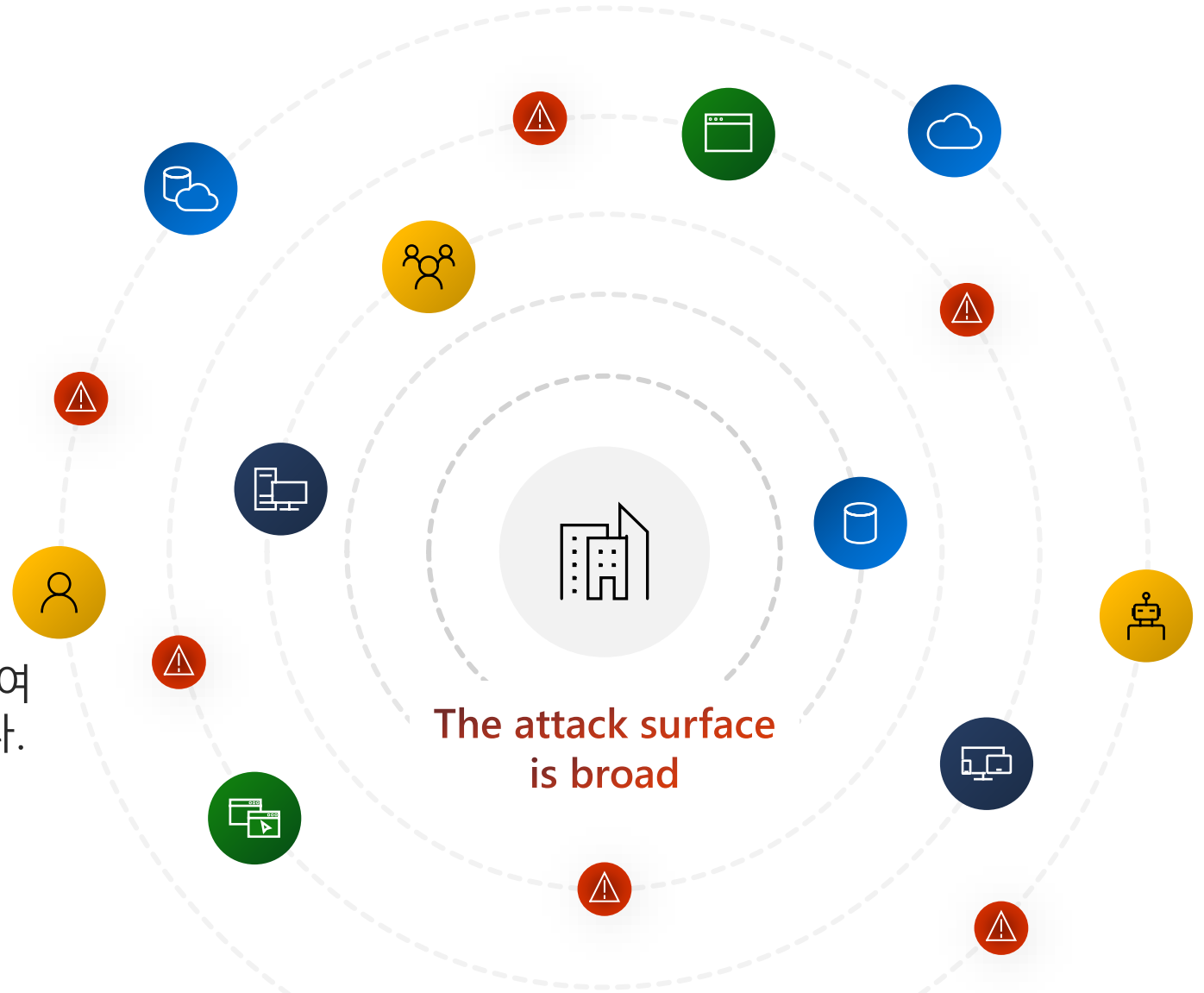
인터넷에 노출된 자산은 알 수 없고
관리되지 않는 리소스인 경우가 많아
조직에 보안 위험을 초래합니다.



조직은 빠른 속도로 클라우드로
전환하고 있으며,
외부 공격 표면을 구성하는 방식이 넓어지고
복잡성이 증가하고 있습니다.

공격표면은 계속 변화하며 증가하고 있습니다.


클라우드와 디지털 트랜스포메이션은
보안 체계를 혼란에 빠뜨렸고,
공격자들은 내부를 들여다보는 기법을 사용하여
방어자에 대한 우위를 점할 수 있게 되었습니다.



Defender EASM은 방화벽 외부의, 인지하지 못한 리소스와
관리되지 않는 리소스를 보안팀이 확인 할 수 있도록 도와줍니다.

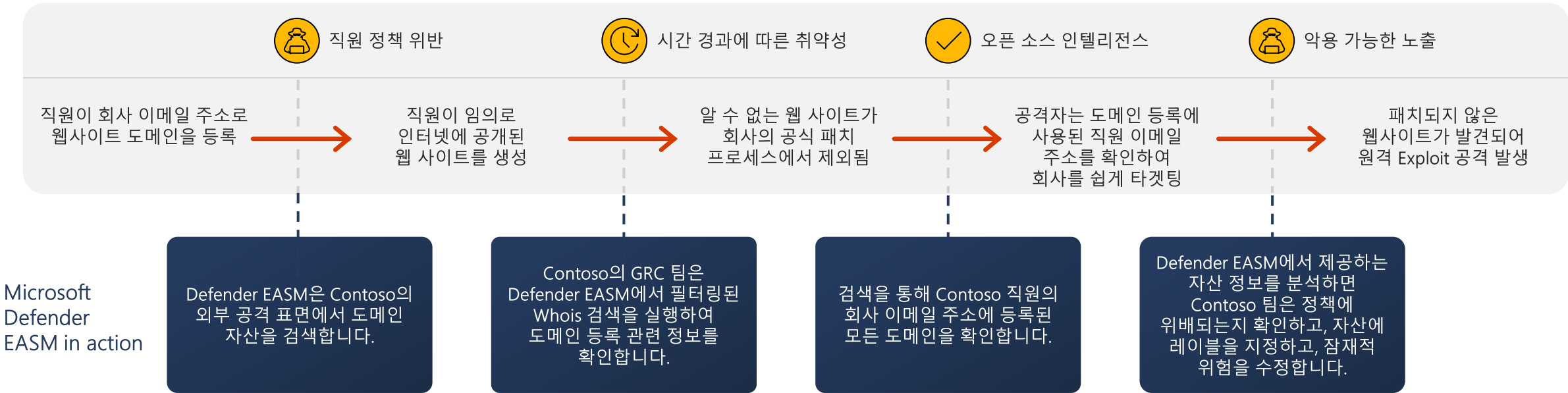
Microsoft Defender EASM이 Shadow IT를 찾는 방법:

Contoso의 실제 이야기



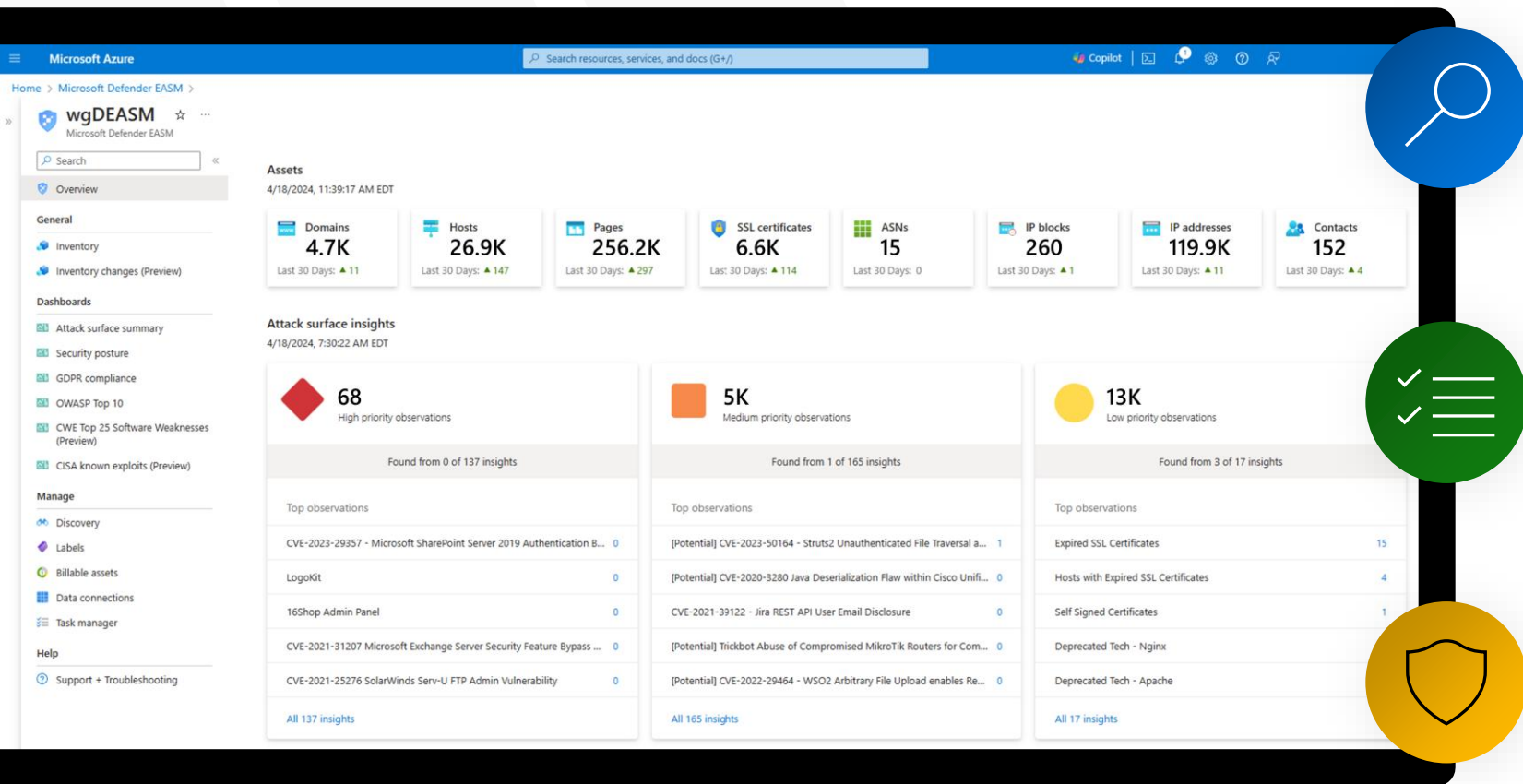
Contoso GRC(Governance, Risk, and Compliance) 팀의 구성원으로서 저는 도메인 등록(domain-admin@constoso.com)을 위해 예약된 공식 이메일 주소 대신 직원 회사 이메일 주소로 도메인을 등록 합니다. 이렇게 등록된 이메일 주소는 외부 공격 표면에서 식별 되고, 이는 회사 정책에 위배되면서 굉장히 큰 위험을 초래합니다.

Shadow IT attack path example



Microsoft Defender EASM

단일 메뉴를 통해 조직의 외부 디지털 자산을 관리할 수 있습니다.



자산의 발견

알려진 인터넷 연결 자산과 알려지지 않고 모니터링되지 않는 자산을 지속적으로 검색하여 인터넷에 노출된 공격 표면의 변화를 확인합니다.

우선 순위 설정

관찰을 통해 확인된 리소스를 보호하고 위험의 우선 순위를 지정하여 더 강력한 보안 태세를 보장합니다.

보호 조치

검색된 장치를 지속적으로 모니터링하여 조직을 보호하고 자격 증명이 없는 장치와 새로운 취약성을 검색합니다.

Discover your external attack surface

공격자와 동일한 방식으로 외부에서 내부로 조직을 바라봅니다.



Discover



Prioritize



Secure

- > 지속적인 인터넷 스캔을 통해 외부 인터넷 연결 자산에 대한 가시성 확보
- > 알려지지 않은 자산, Shadow IT 및 여전히 온라인에서 운영되고 있는 레거시 서비스를 확인
- > 조직의 자원과 자산에 대한 정확한 최신 목록을 갱신

Add discovery group ...

Group Information **Seeds** Review + Create

Tell us what you know
Enter what you know about your organization using the seed fields below.

Quick Start (optional)

Seeds

Domains (4)
Seed Domains for asset discovery ⓘ
contoso.com
adatum.com
adventure-works.com
Example: office.com | One per line.

IP Blocks (2)
Seed IP Blocks for asset discovery ⓘ
10.255.255.255
172.16.0.0
Example: 20.64.0.0/10 | One per line.

Hosts (1)
Seed Hosts for asset discovery ⓘ
host.contoso.com

IP Blocks to exclude from asset discovery ⓘ

Hosts to exclude from asset discovery ⓘ

- 대표도메인을 입력하는 것만으로 Scan 설정 완료
- Agent 설치, 추가 정보 확인 등을 위한 기업 보안담당자의 도움 없이 모든 작업 수행 가능

Prioritize any vulnerabilities

노출된 자산의 특성을 이해하고 수정하는 방법을 확인합니다.



Discover



Prioritize



Secure

- > 방화벽 내부 및 외부에서 운영되는 자산 및 리소스의 전체 목록을 확인
- > 가장 심각한 위험과 노출을 식별하여 완화하거나 제거
- > Microsoft 연구원의 심층적인 인사이트를 통해 위험에 대한 이해도 확장

Attack surface insights

12/11/2023, 1:22:56 AM EST



29

High priority observations

Found from 8 of 131 insights

Top observations

CVE-2022-41082 & CVE-2022-41040 - Microsoft Exchange Server Authenti... 4

CVE-2022-21980 - Microsoft Exchange Server Authenticated Privilege Escal... 4

CVE-2023-28310 & CVE-2023-32031 - Microsoft Exchange Server Authenti... 4

CVE-2023-21529 - Microsoft Exchange Server Authenticated Remote Code ... 4

CVE-2023-21745 - Microsoft Exchange Server Authenticated Privilege Escal... 4

[All 131 insights](#)



194

Medium priority observations

Found from 11 of 150 insights

Top observations

Hosts with Expired SSL Certificates 42

[Potential] US-CERT Issues Alert On Critical Vulnerabilities Exploited By Ru... 38

[Potential] CVE-2020-8243 Pulse Secure Custom Templates May Lead to C... 24

Multiple Vulnerabilities in Pulse Connect Secure 24

CVE-2020-1938 - AJP File Read/Inclusion Vulnerability in Apache Tomcat 19

[All 150 insights](#)



173

Low priority observations

Found from 6 of 16 insights

Top observations

Expired SSL Certificates 141

Deprecated Tech - Nginx 14

Deprecated Tech - Apache 10

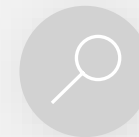
Self Signed Certificates 5

Deprecated Tech - JQuery 2

[All 16 insights](#)

Secure your infrastructure

악용되기 전에 위험을 제거합니다.



Discover



Prioritize



Secure

- 외부에 노출되어 있지만, 관리되지 않는 리소스 목록을 확인
- 특정 위험을 완화하기 위해 권장되는 조치 가이드
- 공격자와의 정보 격차를 해소하고 보안 태세를 개선

Attack surface composition

12/7/2023, 12:01:36 PM EST

Visibility is key to operating a business on the internet today. Knowing about all your assets allows you to better inform your internal security practices and mitigate your overall risk.

Total
17.0K

Domains
264

ASNs
1

Hosts
5.2K

IP blocks
13

Pages
6.7K

IP addresses
4.5K

SSL certificates
351

Contacts
15

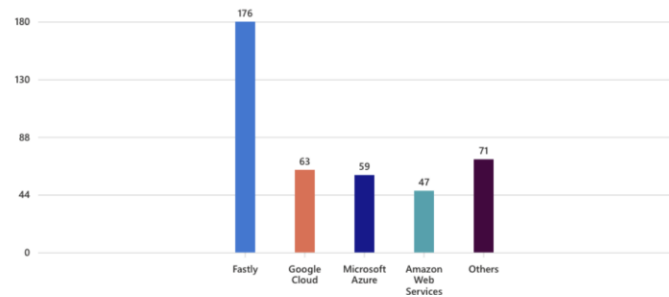
Securing the cloud

12/7/2023, 12:01:36 PM EST

Many organizations adopt the cloud gradually, creating a hybrid environment that can be difficult to manage. Defender EASM is able to understand the usage of specific hosting providers and CDNs (content delivery networks) that can inform your cloud adoption program and ensure it's compliant with your organization's process.

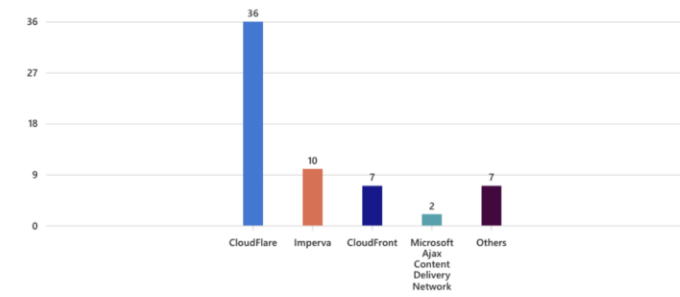
Hosting providers

12/7/2023, 12:01:36 PM EST



CDNs

12/7/2023, 12:01:36 PM EST



The Defender EASM advantage

동적 외부 공격 표면 검색

- ▶ 독점적인 검색 메커니즘을 활용하여 Shadow IT를 포함한 외부 공격 표면을 식별
- ▶ 지속적인 자동 모니터링을 통해 인터넷 변경 사항에서 새로운 자산을 식별
- ▶ 디스커버리 체인 기능으로 투명성 보장
- ▶ 사용자 지정 검색 기능을 통해 더 심층적인 인프라 통찰력 확보



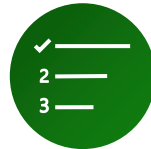
확장된 보안 태세 가시성

- ▶ 외부 위험 태세에 대한 조감도 확보
- ▶ Microsoft Security 솔루션 전반의 보안 태세를 통합
- ▶ 모든 클라우드에서 알려진 자산과 알려지지 않은 자산을 찾는 다음, 이를 프로파일링 하여 글로벌 공격 표면 전반에서 취약성을 발견
- ▶ Azure 플랫폼을 통한 지역별 가용성



상황에 맞는 취약성 우선 순위 지정

- ▶ 관찰 인사이트를 확인하여 잠재적으로 영향을 받을 수 있는 자산에 대한 높은, 중간, 낮은 우선순위를 파악
- ▶ 데이터를 조합하고 여러 대시보드 보기를 통해 취약성, 위험 및 규정 준수 문제의 우선 순위를 지정
- ▶ Microsoft Defender 위험 인텔리전스 데이터와 유기적으로 통합되어 자산 정보를 심층적으로 분석
- ▶ EASM 취약성 데이터를 다른 보안 도구로 내보내 새로운 통찰력 확보



사용자 지정 인벤토리 구성

- ▶ 고객 정의 라벨링을 통해 비즈니스 컨텍스트 적용
- ▶ 자산을 대량으로 업데이트하고 작업 추적을 활용하여 업데이트의 정합성을 보장
- ▶ 대시보드에서 새로 검색된 자산을 쉽게 확인
- ▶ 자산 특성에 기반한 유연한 인벤토리 검색 기능



Defender EASM use cases

Demo



MDEASM resources

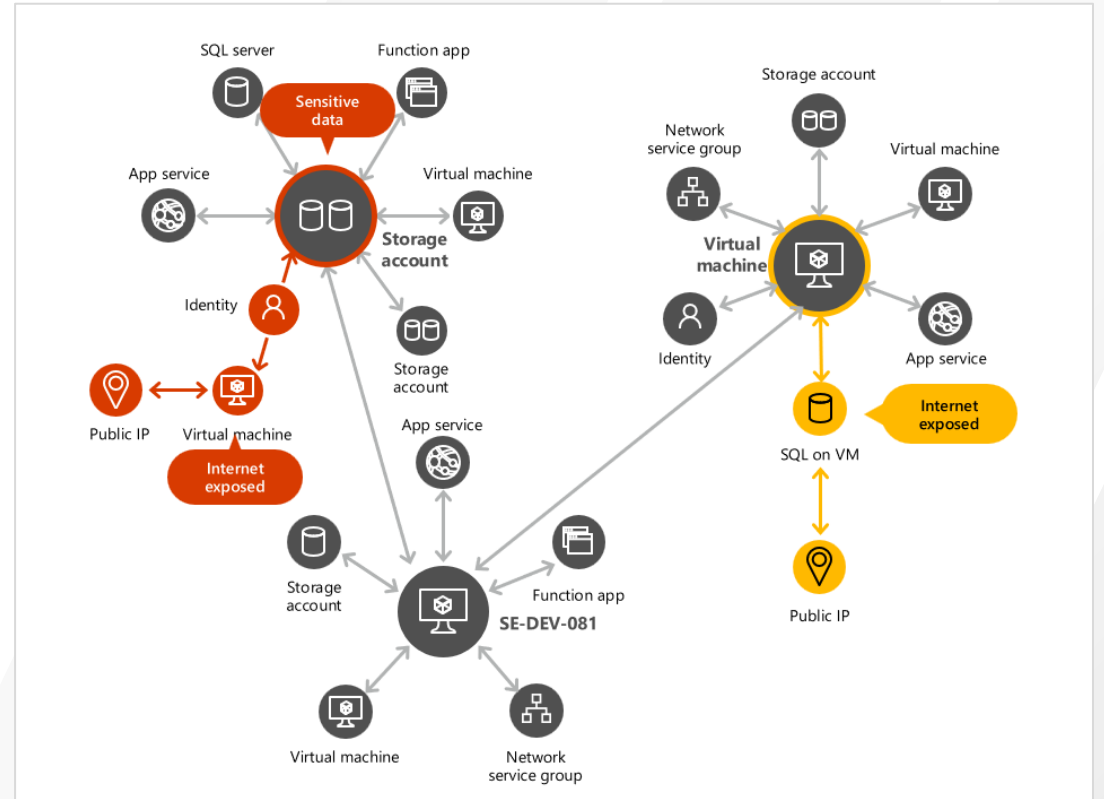


»» Learn more: aka.ms/mdeasm

»» Try it today: azure.microsoft.com/free

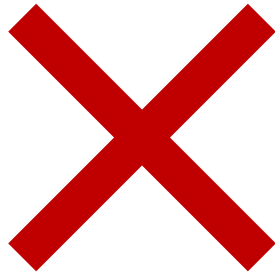
Defender EASM with CSPM

- > 인터넷망에 노출된 자산 정보와 CSPM을 통해 확인된 실제 Attack Path 매칭
- > 가장 심각한 위험과 노출을 식별하여 완화하거나 제거

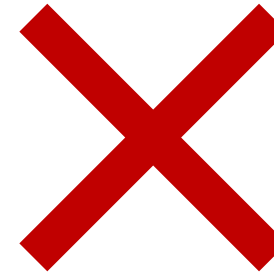


Free Trial 신청 절차

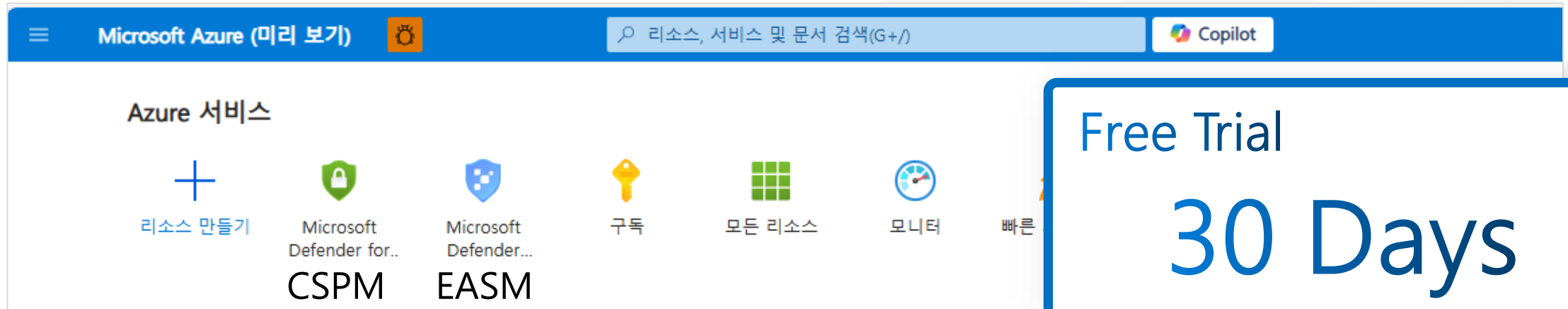
Defender EASM



Defender CSPM



<https://portal.azure.com/>





Thank you!

보안담당자 FAQ

Q. 우리회사의 자산을 임의로 스캔하는 것은 불법이 아닌가요?

A. IP 포트 스캔과 웹 사이트 캡처는 대부분의 경우 불법이 아닙니다. 매우 범용적으로 활용되는 일반 기술입니다.

Q. 어찌 되었든, 우리 회사의 자산을 스캔하는 것은 불쾌합니다. 그만뒀 주세요.

A. 특정 자산을 스캔 예외 처리하는 절차가 있는지는 확인 해보겠습니다. 하지만 해킹그룹에서도 이러한 방법으로 타겟 기업을 스캔 완료하고 변화사항을 모니터링 하고 있습니다. 내 눈을 가린다고 해서 우리 조직의 약점이 사라지지는 않습니다.

Q. 이 솔루션을 도입하면, 우리 시스템에 스캐닝 부하가 증가하지 않나요?

A. 스캐닝의 부하는 우리회사의 웹 사이트를 1회 방문한 부하와 같습니다. 그리고 이미 전세계의 모든 IP와 도메인에 대한 스캔이 완료되어 있기 때문에 추가적인 부하 증가는 없습니다. EASM을 Enable 시키면, 전세계의 모든 데이터 중 우리 조직의 자산을 엮어주는 작업만 진행하게 됩니다.

Q. 나도 이런 취약점 이미 다 알고 있어요. 하고 싶어도 포트를 막거나 패치를 할 수 없는데 어떻게 하라구요?

A. 담당자 분의 사정은 충분히 이해가 갑니다. 그래서 EASM 대시보드에서는 위험성이 더 높은 취약점에 대해 우선순위를 지정해 주고, 왜 위험한지를 상세히 알려주고 있습니다. 이 화면을 업무시스템 운영 담당자와 함께 보시면, 훨씬 의사소통이 용이할 수 있습니다. 그리고 Defender CSPM을 활성화 시키면, 인터넷망에 오픈 된 특정 IP를 통해 어떻게 공격이 이루어 지는지, 공격 경로를 직접 확인하시면서 위험도에 따라 조치하실 수 있습니다.