

AZ-104. Challenge Lab 08

LAB 03. Defender for Cloud를 사용하여 보안 모니터링 및 해결

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

저작권에 관련된 법률을 준수하는 것은 고객의 역할이며, 이 문서를 마이크로소프트의 사전 동의 없이 어떤 형태(전자 문서, 물리적인 형태 막론하고) 어떠한 목적으로 재 생산, 저장 및 다시 전달하는 것은 허용되지 않습니다.

마이크로소프트는 이 문서에 들어있는 특허권, 상표, 저작권, 지적 재산권을 가집니다. 문서를 통해 명시적으로 허가된 경우가 아니면, 어떠한 경우에도 특허권, 상표, 저작권 및 지적 재산권은 다른 사용자에게 허용되지 않습니다.

© 2023 Microsoft Corporation All right reserved.

Microsoft®는 미합중국 및 여러 나라에 등록된 상표입니다.

이 문서에 기재된 실제 회사 이름 및 제품 이름은 각 소유자의 상표일 수 있습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.29	1.0.0	우진환	LAB 03 내용 작성

목차

도전 과제	5
STEP 01. DEVSYSTEM1 가상 머신에 RDP로 연결	5
STEP 02. AZURE 보안 경고 검토 및 해결.....	5
STEP 03. DEVSYSTEM1의 MICROSOFT ANTIMALWARE 설치 확인.....	5
TASK 01. DEVSYSTEM1 가상 머신에 RDP로 연결	6
TASK 02. AZURE 보안 경고 검토 및 해결	7
TASK 03. DEVSYSTEM1의 MICROSOFT ANTIMALWARE 설치 확인	8

도전 과제

이 실습에서는 가상 머신의 Defender for Cloud를 사용하여 문제를 검토하고 해결합니다.

STEP 01. DevSystem1 가상 머신에 RDP로 연결

1. DevSystem1 가상 머신에 사용자 이름(student)과 암호(Pa\$\$w0rd123456)를 사용하여 RDP로 로그인합니다.
2. DevSystem1 가상 머신에서 IE 보안 강화 설정을 해제합니다.

STEP 02. Azure 보안 경고 검토 및 해결

1. Azure 포털에서 DevSystem1 가상 머신의 [클라우드용 Microsoft Defender]로 이동하여 권장 사항을 검토합니다. 권장 사항이 표시될 때까지 최대 24시간이 소요될 수 있으니 권장 사항이 표시되지 않는다면 다음 단계로 진행합니다.
2. DevSystem1 가상 머신에 "Microsoft Antimalware" 확장을 다음 구성으로 설치합니다.

설정	값
Excluded files and locations	C:\Windows
Scan type	Quick
Scan day	Sunday
Scan time	180

STEP 03. DevSystem1의 Microsoft Antimalware 설치 확인

1. 다음 속성으로 [Cloud Shell]의 PowerShell 세션을 시작합니다.

속성	값
Cloud Shell 지역	미국 동부
리소스 그룹	VMRG1od<xxxxxxxxxx>
스토리지 계정	"기존 항목 사용"을 선택하고 기존에 만들어져 있는 스토리지 계정 선택
파일 공유	"새로 만들기"를 선택한 후 "cloud-shell"을 입력

2. [Cloud Shell]의 PowerShell 세션에서 Get-AzVMExtension 명령을 사용하여 antimalware가 설치되었는지 확인합니다.
3. DevSystem1 가상 머신에서 [Task Manager]를 열고 Windows Process 섹션에 "Antimalware Service Executable" 프로세스가 표시되는 것을 확인합니다.

TASK 01. DevSystem1 가상 머신에 RDP로 연결

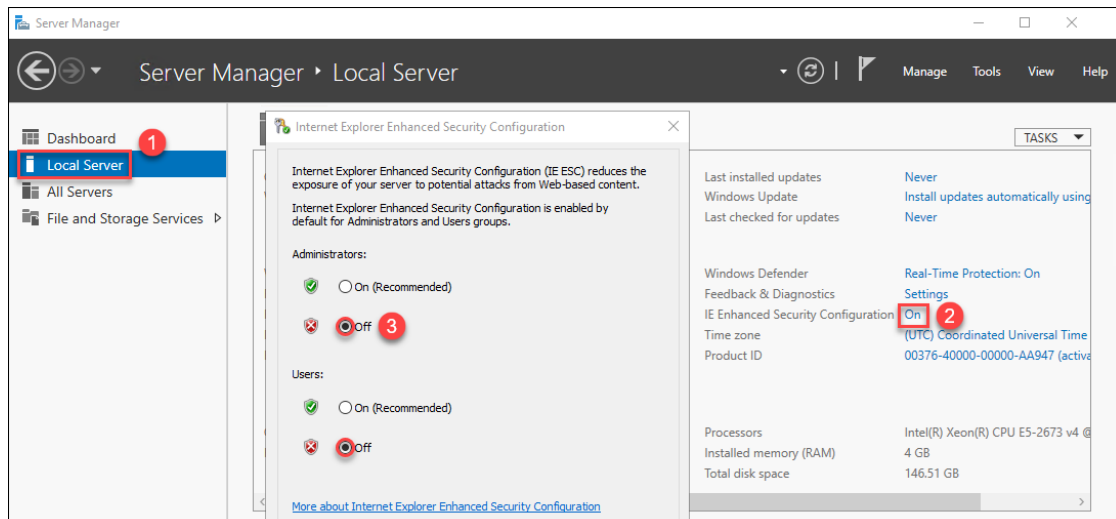
1. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 DevSystem1 가상 머신을 클릭합니다.



2. [DevSystem1 가상 머신] 블레이드의 [설정 - 연결]로 이동한 후 원시 RDP 타일에서 [선택]을 클릭합니다. [원시 RDP] 창에서 [RDP 파일 다운로드]를 클릭합니다. 다운로드한 파일을 실행한 후 사용자 이름(student)과 암호(Pa\$\$w0rd123456)를 사용하여 로그인합니다.



3. [Server Manager]에서 [Local Server]로 이동한 후 "IE Enhanced Security Configuration"의 "On" 링크를 클릭합니다. [Internet Explorer Enhanced Security Configuration] 창에서 모든 설정을 "Off"로 모두 변경한 후 [OK]를 클릭합니다.



TASK 02. Azure 보안 경고 검토 및 해결

1. Azure 포털에서 [DevSystem1 가상 머신] 블레이드의 [설정 - 클라우드용 Microsoft Defender]로 이동한 후 보안 권장 사항이 표시되는지 확인합니다. 권장 사항이 자동으로 표시될 때까지 최대 24시간이 소요될 수 있으므로 권장 사항이 표시되지 않는다면 다음 단계로 이동합니다.

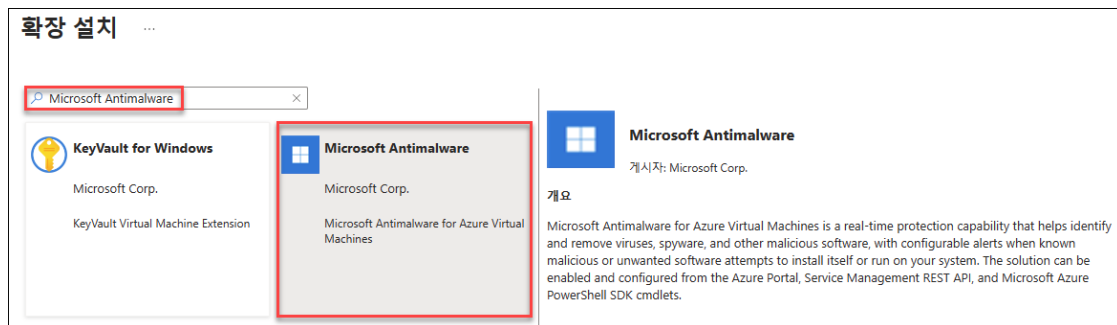


2. [DevSystem1 가상 머신] 블레이드의 [설정 - 확장 프로그램 + 애플리케이션]으로 이동한 후 [확장] 탭에서 [추가]를 클릭합니다.



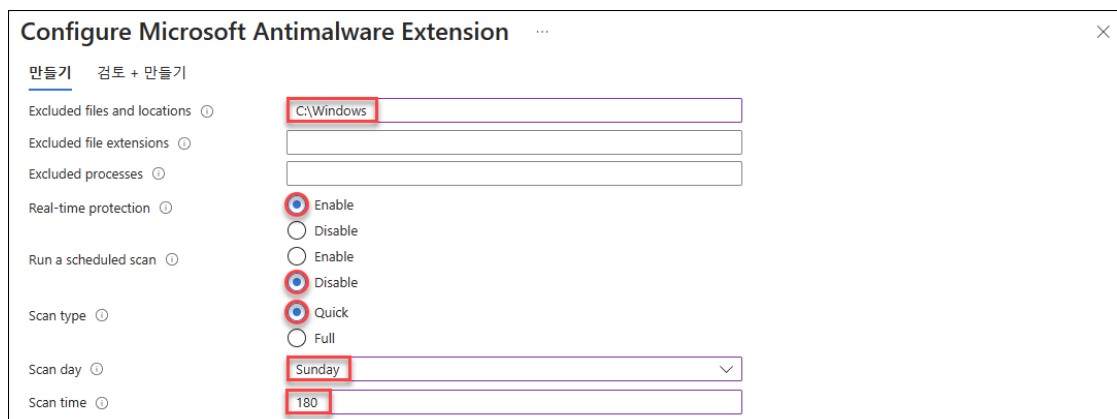
3. [확장 설치] 블레이드에서 "Microsoft Antimalware"를 검색한 후 [추가 로드]를 클릭합니다.

[Microsoft Antimalware] 타일을 선택한 후 [다음]을 클릭합니다.



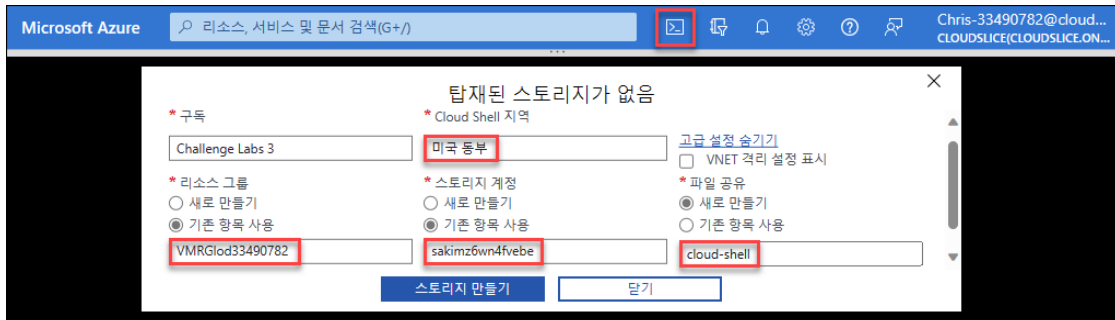
4. [Configure Microsoft Antimalware Extension] 블레이드의 [만들기] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.

- Excluded files and locations: C:\Windows
- Scan type: Quick
- Scan day: Sunday
- Scan time: 180
- 다른 설정은 기본값을 유지합니다.

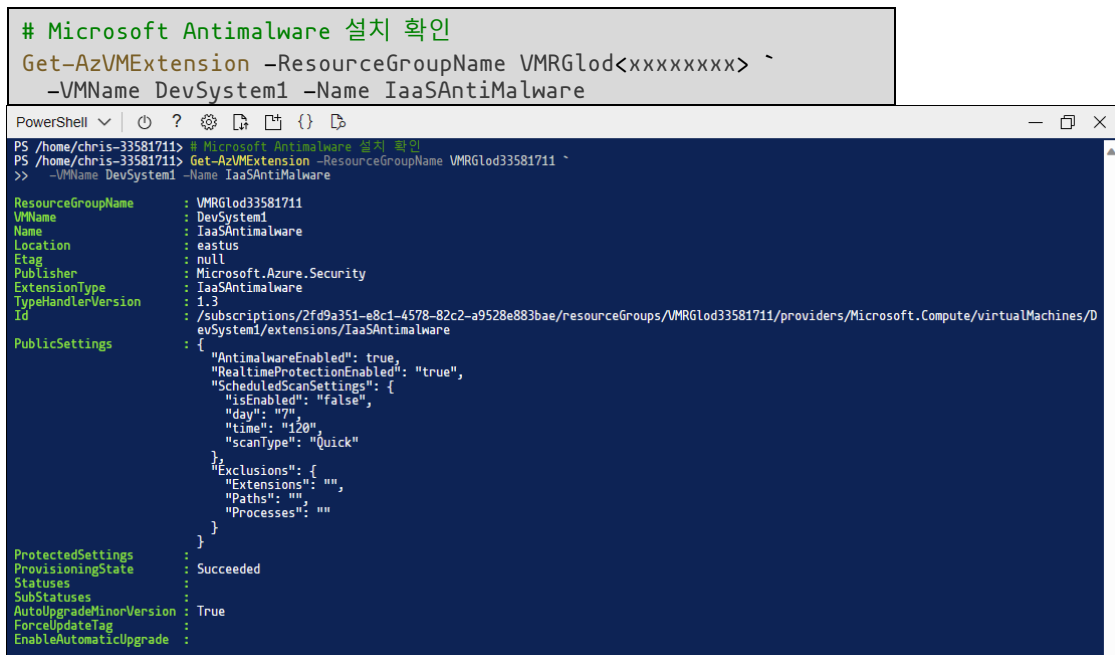


TASK 03. DevSystem1의 Microsoft Antimalware 설치 확인

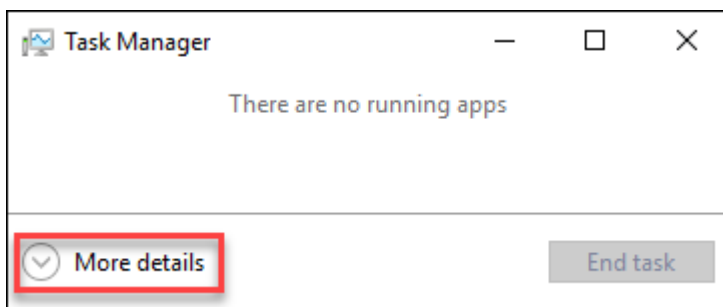
1. Azure 포털에서 [Cloud Shell] 아이콘을 클릭한 후 "PowerShell"을 클릭합니다. [탑재된 스토리지가 없음] 창에서 "고급 설정 표시" 링크를 클릭합니다. [탑재된 스토리지가 없음] 페이지에서 아래와 같이 구성한 후 [스토리지 만들기]를 클릭합니다.
 - Cloud Shell 지역: 미국 동부
 - 리소스 그룹: "기존 항목 사용"을 선택한 후 VMRGlod<xxxxxxxx> 리소스 그룹을 선택합니다.
 - 스토리지 계정: "기존 항목 사용"을 선택한 후 표시되는 스토리지 계정을 선택합니다.
 - 파일 공유: "새로 만들기"를 선택한 후 "cloud-shell"을 입력합니다.



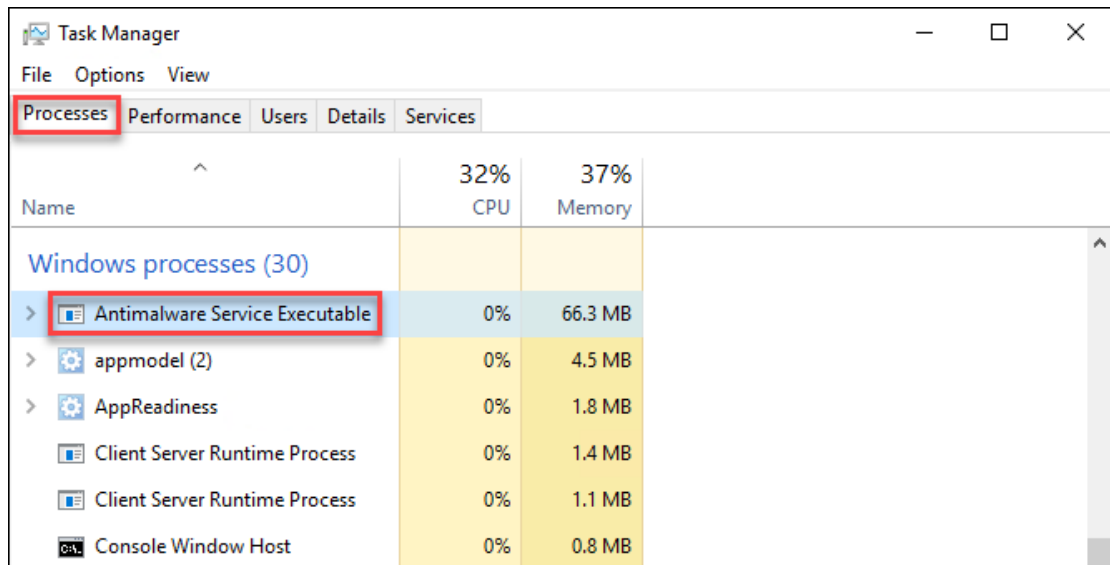
- [Cloud Shell]의 PowerShell 세션에서 다음 명령을 실행하여 Microsoft Antimalware가 **DevSystem1** 가상 머신에 설치되었는지 확인합니다.



- DevSystem1** 가상 머신에 RDP로 로그인한 후 [Task Manager]를 엽니다. [More details]를 클릭합니다.



- [Task Manager] 창의 [Processes] 탭에서 "Windows processes" 섹션에 "Antimalware Service Executable" 프로세스가 표시되는지 확인합니다.



Task Manager		
File Options View		
Processes Performance Users Details Services		
Name	32% CPU	37% Memory
Windows processes (30)		
> Antimalware Service Executable	0%	66.3 MB
> appmodel (2)	0%	4.5 MB
> AppReadiness	0%	1.8 MB
Client Server Runtime Process	0%	1.4 MB
Client Server Runtime Process	0%	1.1 MB
Console Window Host	0%	0.8 MB