Microsoft Professional Program Cybersecurity Guidebook

Microsoft

Squarenet™

목차

Cyber Security 코스 정보

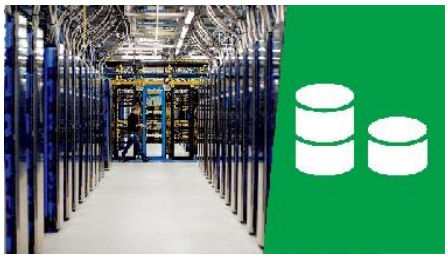
* 코스가 진행되는 동안 어떤 순서로 수강해도 상관 없지만 아래의 순서에 따라 진행하는 것을 권고 드립니다. 코스가 여러 코스 옵션으로 나열될 경우(6. Secure and Protect Data -3 개 옵션) 과정 이수 요건을 충족시키기 위해 하나만 완료해도 됩니다.

1. Introduction To Cybersecurity(사이버 보안 소개)

Enterprise Security Fundamentals
(엔터프라이즈 보안 기초)

현재 엔터프라이즈 보안 환경을 설명하고, 타협적 접근 방식(Assume Compromise)을 정의하고, 레드팀 대 블루팀으로 나눠 연습하고, 기업의 보안을 준비(preparation), 진행(processes), 대응하는(responses)개발 방법을 학습하십시오.

2. Detect Security Breaches Early(조기에 보안 위반 탐지)



Threat Detection: Planning for a Secure Enterprise
(위협 탐지: 보안 엔터프라이즈 계획)

이 과정에서는 심층 방어 전략의 일부로 위협 탐지에 대한 개요를 제공합니다. 위협 탐지 및 완화 도구(mitigation tools)의 기능을 탐색하면서 사이버 범죄를 보호, 탐지 및 대응하는 방법을 배우게 됩니다.

3. Respond to Security Incidents(보안 사고 대응)

Planning a Security Incident Response
(보안 사고 대응 계획)

일반적인 오류(Common errors)를 피하면서 엔터프라이즈 보안 사고를 관리하는 방법과 사고 대응 노력의 효과와 효율성을 높이는 방법에 대해 배웁니다.

4. Enhance Security Using Code(코드를 사용하여 보안 강화)

PowerShell Security Best Practices
(PowerShell 보안 모범 사례)

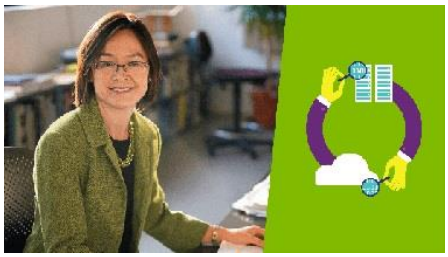
PowerShell 을 사용하여 보안을 향상시키고 새로운 위협 및 악용에 대비하십시오. 서버 구성 및 보안을 위한 DSC (Desired State Configuration) 및 JEA (Just Enough Administration)와 같은 관리 도구의 기능을 살펴보십시오.

5. Manage Identity(계정 관리)

Managing Identity
(계정 관리)

Microsoft 사건 대응 팀의 실제 경험을 토대로 이 과정에서는 실습 방식으로 코스가 진행됩니다. 호스트를 만들고, 권한이 있는 액세스 관리를 구성하고, Microsoft Identity Manager 를 설정하는 등의 작업을 수행합니다.

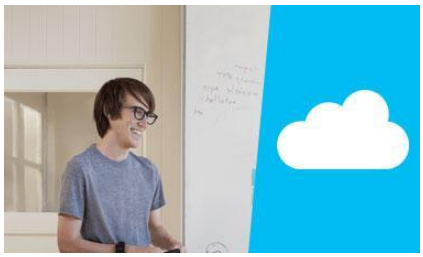
6. Secure and Protect Data [3 TRAINING OPTIONS AVAILABLE]



Option 1

Security in Office 365
(Office 365 의 보안)

기업을 대상으로 겪을 수 있는 다양한 유형의 위협을 검토하고 고급 위협 방지, 위협 정보 및 고급 보안 관리와 같은 Office 365 보안 기능을 구현 및 관리하는 방법을 알아보십시오.



Option 2

Securing Data in Azure and SQL Server
(Azure 및 SQL Server 에서 데이터 보안)

SQL Server 2016, Linux 의 SQL Server v. Next(SQL Server 용 Linux) 및 Azure SQL 데이터베이스에서 데이터를 보호하는 방법을 익히십시오. 전문가와 함께 사용자 인증, 사용자의 위치, 권한 및 수행할 수 있는 작업을 살펴보십시오. 항목에는 사용자 인증 및 연결(Connections), 사용자가 리소스에 액세스하도록 권한 부여, 데이터 액세스 감사(Auditing) 및 데이터 암호화가 포함됩니다.

Option 3

Microsoft SharePoint 2016: Authentication and Security
(Microsoft SharePoint 2016: 인증 및 보안)

환경을 보호하기 위해 SharePoint 사내(On – Premises)솔루션을 계획 및 구성하는 방법에 대해 알아보십시오. 이 과정에서는 필요한 하드웨어 및 소프트웨어 요구 사항과 SharePoint 보안에 대한 전반적인 방법을 검사합니다.

7. Secure Operating Systems(안전한 운영 체제)

Windows 10 Security Features
(Windows 10 보안 기능)

남들보다 보안을 더 빠르게 배울 수 있습니다 - 지속적으로 발전하고 있는 Windows 10 운영 체제의 보안 기능에 대해 알아보십시오. Microsoft 보안 엔지니어 팀이 고급 기능을 배포하는 방법을 알아보십시오.

8. Secure Servers(보안 서버)

Windows Server 2016 Security Features
(Windows Server 2016 보안 기능)

Windows Server 2016 은 알려진 위협 및 새로운 위협을 모두 해결할 수 있는 보호 계층을 제공합니다. 인프라 보안을 하는 방법에 대해 알아보고 보안 침해(Security breaches)에 대한 보호를 강화하십시오.

9. Secure Cloud-Enabled Services and Data (클라우드 기반 서비스 및 데이터 보안)

Microsoft Azure Security Services (Microsoft Azure 보안 서비스)

Azure 보안 모범 사례를 배우고 매우 안전하고 탄력적인(resilient) 클라우드 서비스를 만들기 위한 용어, 도구 및 기술을 이해하십시오. 또한, Azure 및 Intune 에서 제공되는 추가 보안 서비스에 대해 배우고 사용할 수 있습니다.

01. Enterprise Security Fundamentals

주당 2–4 시간, 총 4주

이 과정은 기업의 보안 상태를 개선하기 위한 보안 실행에 대한 통찰력을 제공합니다.

레드팀 대 블루팀 연습은 조직의 정보 시스템에 대한 공격 시뮬레이션을 포함합니다. 레드팀은 조직의 IT 시스템에 대한 공격을 시뮬레이트 하고, 경우에 따라 PoC(proof of concept) 컨셉 증명 단계를 수행합니다. 블루팀은 그 공격에 대한 반응을 시뮬레이션 합니다.

이러한 적대적인 접근 방식은 조직의 IT 시스템이 구성되는 방식에서의 보안 취약점을 식별할 수 있을 뿐만 아니라 조직의 정보 시스템 담당자가 공격을 감지하고 대응하는 방법을 학습할 수 있도록 합니다.

1. Before you start(시작하기 전)

사전 요구 사항

- 현재 사이버 보안 생태계에 대한 이해

2. What you will learn(배우게 될 것)

이 과정을 이수한 학생들은 다음을 할 수 있습니다.

- 현재 엔터프라이즈 보안 환경 설명
- 타협적 접근 방식(Assume Compromise approach) 정의
- 레드 팀(공격) 대 블루 팀(수비) 연습
- 조직의 보안 준비, 프로세스 및 대응 능력 개발

Module 1 사이버 보안 환경에 대한 이해

- 현재 사이버 보안 환경
- 공격의 진화
- "타협(Assume Compromise)"의 이해
- 타협의 예

Module 2 레드 팀: 침투(Penetration), 측면 이동(lateral movement), 에스컬레이션(escalation) 및 확대(exfiltration)

- 레드 팀 대 블루 팀
- 레드 팀 킬 체인
- 비치헤드(Beachhead)
- 횡 방향 움직임
- 권한 상승(Privileged escalation)
- 공격자의 임무 수행

Module 3 블루 팀: 탐지(Detection), 조사(investigation), 대응(response) 및 완화(mitigation)

- 블루 팀 킬 체인
- 권한 상승 제한
- 온-프레미스(On-premises: 사내) 네트워크 보안
- 측면 움직임(lateral movement) 제한
- 공격 감지

Module 4

- 조직 준비
- 프로세스
- CIA 트라이어드(Triad)
- 전략적 로드맵 개발
- 마이크로소프트 보안센터 악용 가능성 지표(Exploitability Index)

3. Overview(개요)

이 과정은 마이크로소프트 프로페셔널 프로그램의 일부분인 사이버보안 과정입니다.

월 스트리트저널(WSJ)에 따르면 "모든 IT 일자리는 사이버보안 일자리"라고 합니다.

이 과정에서는 레드 팀-블루 팀 보안 전문가의 개념을 살펴봅니다. 여러분은 레드 팀 대 블루 팀 훈련을 연습할 것입니다. 레드 팀은 회사의 보안 인프라의 일부를 공격하고 상대 그룹인 블루 팀은 공격에 대항합니다. 두 팀 모두 회사의 방어를 강화하기 위해 노력합니다.

여러분은 레드 팀과 블루 팀 모두가 어떻게 비즈니스가 더 높은 수준의 보안을 갖도록 돕는지 알게 될 것이며, 보안 업계가 현재 퍼플 팀이라고 부르는 것을 알게 될 것입니다.

4. Meet your instructors(강사 소개)

Orin Thomas

Microsoft 클라우드/데이터 센터 전문가. 저자, 마이크로소프트 MVP & 리전 책임자. 테크니컬 라콘테어

Orin Thomas 는 MCT(Microsoft 공인 강사)의 Microsoft Regional Director 의 MVP(지난 10 년간 디렉터리 서비스의 Microsoft MVP)이며 Microsoft MCSE 및 MCITP 인증을 받았습니다. 그는 Windows Server, Windows 클라이언트, Azure, System Center, Exchange Server, 보안 및 SQL Server 와 같은 주제로 Microsoft Press 에 3 권 이상의 책을 저술했습니다. 그는 Plural Sight 의 저자이며 Charles Sturt University 의 정보 기술 의사(Doctor of Information Technology) 프로그램의 후보(candidate)입니다.

02. Threat Detection: Planning for a Secure Enterprise

주당 2–4 시간, 총 4주

사이버 범죄를 보호, 탐지 및 대응하기 위한 심층 방어 전략의 일환으로 위협 탐지에 대해 알아보십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- 현재의 사이버 보안 환경
- 컴퓨터 및 네트워크의 해킹 분석
- 기본 리스크 관리

2. What you will learn(배우게 될 것)

이 과정을 이수한 학생들은 다음을 할 수 있습니다.

- 서명 기반 및 behavioral/heuristic 탐지 방법을 설명할 수 있습니다.
- 사내(On-premise) 위협 탐지 및 완화 도구(mitigation tools)의 기능을 나열할 수 있습니다.
- 하이브리드 및 클라우드 위협 탐지 및 완화 도구(mitigation tools)의 기능에 이름을 지정할 수 있습니다.
- 엔터프라이즈 위협 탐지 모니터링의 중요성을 인식하게 됩니다.

Module 1 심층 방어 전략의 일환으로 위협 탐지 소개

- 현대적인 사이버 위협 경관(landscape)에 대한 개요
- 사이버 위협을 완화(mitigation)하기 위해 사전 위반 및 사후 위반 방법 통합
- 서명 기반 및 behavioral/heuristic 탐지 방법 비교
- 위협 지속성 방지

Module 2 사내(On – premises) 환경에서 위협 감지

- Windows Defender 고급 위협 요소 방지
- Microsoft 고급 위협 분석
- Microsoft 엔터프라이즈 위협 검색
- Microsoft 보안 위험 요소 탐지
- 맬웨어 방지 프로그램 검색 인터페이스
- 로깅(Logging) 및 감사(Auditing)

- 위협 탐지 도구

Module 3 하이브리드 및 클라우드 환경의 위협 탐지

- Office 365 고급 위협 방지
- Office 365 클라우드 App 보안 및 Microsoft 클라우드 App 보안
- Azure 고급 위협 탐지
- Azure Active Directory 계정 보호
- Azure Active Directory 계정 위협 탐지
- Microsoft OMS (운영 관리 제품 군)
- Azure 보안 센터
- 고급 위협 탐지 기능 - 기타 Azure 서비스
- Azure Marketplace 를 통한 타사 ATD 기능
- Azure Logging(로깅) and Auditing(감사)
- Microsoft 365

Module 4 실제 위협 탐지 솔루션 분석

- Windows Defender 를 사용하여 지속적인 위협 감지, 고급 위협 요소 방지 및 고급 위협 분석
- 엔터프라이즈 위협 탐지 행동 모니터링

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity의 일부입니다.

2021년 전세계 사이버 범죄 피해는 기업이 6조 달러를 부담해야 될 것으로 예상됩니다. 승인되지 않은 응용 프로그램, 관리되지 않는 장치, 암호 보호 취약성 및 기타 보안 문제는 공격에 취약한 부분을 너무 많이 남겨두고 있습니다. 기업이 디지털로 변하는 것을 수용함에 따라 IT 인프라에 대한 통제력을 높이고 보안 위험을 줄이는 것이 점점 더 시급한 과제로 대두되고 있습니다.

이 과정은 심층 방어 전략의 일환으로 위협 탐지에 대한 개요입니다. 위협 탐지 및 완화 도구(mitigation tools)의 기능을 탐색하면서 사이버 범죄를 보호, 탐지 및 대응하는 방법을 배우게 됩니다.

4. Meet your instructors(강사 소개)

Marcin Policht

Marcin 은 IT 분야에서 20 년 이상의 경력을 쌓은 시스템 엔지니어입니다.

MVP: 지난 10 년간 디렉터리 서비스의 Microsoft MVP

MCT: Microsoft 공인 강사

03. Planning a Security Incident Response

주당 2–4 시간, 총 4주

이 과정에서는 기업 보안 침입에 대응할 때 사용할 계획 프로세스 및 절차에 대해 자세히 설명합니다.

1. Before you start(시작하기 전)

사전 요구 사항

- 현재의 사이버 보안 환경에 대한 이해.

2. What you will learn(배우게 될 것)

이 과정을 이수한 학생들은 다음을 할 수 있습니다.

- 보안 사고에 대한 우선순위를 효과적으로 설정할 수 있습니다.
- 컴퓨터 보안 사고 대응 팀(CSIRT)을 구축할 수 있습니다.
- 사고 대응 행동 계획을 수립할 수 있습니다.
- 사고 후 조치해야 할 활동을 나열할 수 있습니다.

Module 1

- 소개
- 위협 모델링이란?
- 사고 대응 계획의 필요성
- 환경의 취약성 평가
- 네트워크 트래픽 및 시스템 성능에 대한 모니터링 및 검토 수립
- 로그 분석

Module 2

- 사고 대응 정책, 계획 및 절차 생성
- CSIRT 생성
- CSIRT 팀 역할 수립
- Governing 정책 수립

Module 3

- 사건의 초기 평가

- 공격 벡터
- False positives 와 False negatives 는 무엇입니까?
- 공격의 본질(nature of the attack)을 결정합니다.
- 훼손된 시스템 식별
- Containment 전략 선택하기

Module 4

- 사고 후 활동
- 기능을 복원하는 동안 증거를 보호하십시오. (Protect the evidence while restoring functionality)
- 학습한 권장 사항 및 교훈
- 보안 사고 보고서

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity의 일부입니다.

이 과정은 일반적인 보안 문제를 피하면서 기업 보안 사고를 관리하고 사고 대응 노력의 효과와 효율성을 높이는 데 도움을 주기 위해 제작되었습니다.

4. Meet your instructors(강사 소개)

Philip E. Helsel

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Philip Helsel 은 Microsoft Learning 팀의 수석 콘텐츠 개발자로 현재 Windows 10, Hyper-V 및 Configuration Manager 용 IT Professional 코스를 만드는 데 중점을 두고 있습니다. 그는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 계획 담당자이기도 합니다.

Microsoft 에 입사하기 전에는 Fast Search(빠른 검색) 및 Pre-Sales Engineer (사전 판매 엔지니어) 및 강사를 했으며, Oracle Corporation 의 Pre-Sales Engineer (사전 판매 엔지니어) 및 Sun Micro systems 에 있었습니다. 그는 또한 미 육군 대위로도 일했습니다.

Phil Helsel 은 수학 및 물리학에서 학사 학위를, Computer Science 에서 석사 학위를 취득했습니다. 그는 또한 Microsoft Certified Trainer(MCT), MCITP, CCNA, VCP5, CISM, Security +, Network + 및 기타 여러 인증을 보유하고 있습니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Kimberly 는 Microsoft Learning 팀의 수석 콘텐츠 개발자입니다.

Kimberly는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

04. PowerShell Security Best Practices

주당 2–4 시간, 총 4주

PowerShell 을 안전하게 사용하는 방법과 PowerShell 을 사용하여 보안을 강화하는 방법에 관한 모범 사례를 학습하십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- Windows 네트워킹 경험이 있어야 합니다.
- Windows Server 관리 경험이 있어야 합니다.
- Windows PowerShell 사용 경험이 있어야 합니다.

2. About this course(이 과정에 대하여)

이 과정은 Microsoft Professional Program in Cybersecurity 의 일부입니다.

이 과정에서는 학생들에게 Windows PowerShell 5.x 를 사용하여 관리 작업을 안전하게 수행하는 방법을 가르칩니다. 학생들은 PowerShell 기본 사항을 검토하고 PowerShell 운영 보안 및 구성 관리에 대해 배웁니다.

학생들은 DSC (Desired State Configuration) 및 JEA (Just Enough Administration)와 같은 관리 도구를 사용하여 서버를 구성하고 보안하는 방법을 배우게 됩니다. 이 과정에서는 새로운 위협, 새로운 공격, 끊임없이 변화하는 공격을 막는 방법에 대해 살펴봅니다.

Module 1 – PowerShell Fundamentals(기초)

- Windows PowerShell Architecture(구조)
- Windows PowerShell editions and versions
- Windows PowerShell 실행

Module 2 – PowerShell 운영 보안

- Windows PowerShell 실행 정책(Policy)을 사용하여 로컬 스크립트 실행 관리
- Windows PowerShell의 원격 실행 기능 관리
- 제한된 종단점(endpoints)
- 언어 모드(Language Mode)

- 안티-멀웨어 스캔 인터페이스 (AMSI)

Module 3 – Windows PowerShell 기반 보안 구현

- Widows PowerShell DSC
- Just Enough Administration (JEA)
- Windows PowerShell 감사(Auditing) 및 로깅(Logging)

Module 4 – Windows PowerShell 기반 공격(Exploits) 및 완화(Mitigation)

- Windows PowerShell 기반 공격
- Windows PowerShell 기반 보안 도구
- Windows PowerShell 기반 보안 관련 기술 요약

Module 5 - 과정 수료

- Graded Lab
- 최종 시험
- Post Course 설문 조사

3. What you'll learn(배우게 될 것)

이 과정을 이수한 학생들은 다음을 할 수 있습니다.

- PowerShell 의 Architectures 를 이해할 수 있습니다.
- PowerShell 운영 보안 배포(Deploy)를 할 수 있습니다.
- PowerShell Auditing(감사) and Logging(로깅) 분석을 할 수 있습니다.
- Desired State Configuration, Just Enough Administration 을 사용하여 서버 관리 기능을 향상시킬 수 있습니다.
- 스크립트 분석 및 디버그를 할 수 있습니다.
- PowerShell 기반 악용 및 보호 방법을 이해할 수 있습니다.

4. Meet the instructor(강사 소개)

Marcin Policht

시스템 엔지니어, SR Tech

Marcin 은 IT 분야에서 20 년 이상의 경력을 쌓은 시스템 엔지니어입니다.

MVP: 지난 10 년간 디렉터리 서비스의 Microsoft MVP

MCT: Microsoft 공인 강사

05. Managing Identity

사이버 보안 방어 계획을 수립할 때 Active Directory, Azure Active Directory 및 계정 관리에 관한 모범 사례를 학습하십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- Windows 클라이언트 관리, 유지 관리 및 문제 해결 경험이 있어야 합니다.
- Active Directory 의 기본 지식이 있어야 합니다.
- 간단한 Windows PowerShell 명령어를 사용해본 적이 있으면 좋습니다.

2. What you will learn(배우게 될 것)

- 계정은 방화벽을 대체하는 경계(perimeter)인 새로운 Control plane 입니다.
- Active Directory 를 보호하는 방법에 대해 배웁니다.
- Azure Architectures 및 Azure Architectures 에서 지원하는 Identity Federation 및 액세스 솔루션에 대해 배우게 됩니다.
- Kerberos 및 Privilege Attribute Certification 을 작동하는 방법에 대해 배우게 됩니다

Module 1: 계정 관리, 새로운 제어 평면(new control plane)

Module 2: Active Directory 보안

Module 3: Azure Active Directory

Module 4: Active Directory의 인증 및 권한 부여

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity의 일부입니다.

오늘날의 보안 환경에서 계정을 새로운 보안으로 정할 때는 최신 보안 관리 방법을 따라가는 것이 중요합니다. 지난 몇 년 동안 사용하도록 허용된 프로토콜, 상호 작용할 수 있는 사람 및 수행할 수 있는 대상을 정의하는 계정은 지난 몇 년 동안 크게 발전했습니다.

이 보안 과정에서는 방화벽 및 포트를 넘어서고 Microsoft Incident Response 팀의 검증된 실제 경험을 토대로 계정 관리에 대한 실용적인 단계(learn practical steps)와 규범적 지침(prescriptive guidance)을 학습합니다.

계정을 개념적으로 살펴보고, Active Directory 모범 사례를 탐색하고 Azure Active Directory를 보호하는 방법을 찾은 다음 비디오, 텍스트 및 호스팅 된 랩을 조합하여 직접 체험하십시오.

기존 도메인에 대한 보호하는 호스트를 만들고 PAM (Privilege Access Management) 및 JIT (Just in Time Administration)를 구성하고 JRE를 설치하며 Microsoft Identity Manager를 설정합니다. 과정을 성공적으로 마치면 환경의 보안 상태를 개선하는 방법을 이해하고 사이버 보안 방어 계획의 계정을 구현하고 관리할 수 있습니다.

4. Audience(대상)

이 교육을 받는 학생들은 전문적인 경험 외에도 다음과 같은 기술적 지식을 갖추어야 합니다.

- Windows 클라이언트 관리, 유지 관리 및 문제 해결 경험이 있어야 합니다.
- Windows 방화벽 네트워크 설정, DNS, DHCP, WiFi 및 클라우드 서비스 개념을 포함하여 Windows 네트워킹 기술에 대한 기본적인 경험과 이해가 있어야 합니다.
- 도메인 제어 기능, 사인 온 서비스 및 그룹 정책 이해를 포함하여 Active Directory에 대한 기초 지식을 습득한 상태여야 합니다.
- Windows Server 2012 R2 및 2016을 사용하여 시스템 관리에 대한 지식과 관련 경험이 있어야 합니다.
- 코스 전제 조건(Prerequisites):
- 이 교육을 받는 학습자는 보안 관리자, 시스템 관리자 또는 네트워크 관리자로서 실질적인 경험을 통해 지식과 기술을 습득함으로써 전제 조건을 충족시킬 수 있습니다.
- Windows PowerShell은 이 과정에서 기능을 구현할 때 선택할 수 있는 도구입니다. 학습자는 간단한 Windows PowerShell 명령에 액세스하고 사용하는 데 필요한 기초가 있어야 합니다. 이 지식은 INF210x, Windows PowerShell 기본에서 얻을 수 있습니다.

5. Meet your instructors(강사 소개)

Philip E. Helsel

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Philip Helsel 은 Microsoft Learning 팀의 수석 콘텐츠 개발자로 현재 Windows 10, Hyper-V 및 Configuration Manager 용 IT Professional 코스를 만드는 데 중점을 두고 있습니다. 그는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 계획 담당자이기도 합니다.

Microsoft 에 입사하기 전에는 Fast Search(빠른 검색) 및 Pre-Sales Engineer (사전 판매 엔지니어) 및 강사를 했으며, Oracle Corporation 의 Pre-Sales Engineer (사전 판매 엔지니어) 및 Sun Micro systems 에 있었습니다. 그는 또한 미 육군 대위로도 일했습니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Kimberly 는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

06-1. Security in Office 365

주당 2–4 시간, 총 5주

Office 365 에서 보안을 계획, 구현 및 관리하는 방법에 대해 알아보십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- 클라우드 기반 서비스 개념, Office 365 및 해당 구성 요소 서비스에 대해 이해를 하고 있어야 합니다.
- IT 통신의 보안 요구 사항 및 일반적인 위협에 대한 배경 지식이 있어야 합니다.

2. What you will learn(배우게 될 것)

- 데이터를 대상으로 하는 위협 및 데이터 침해에 대한 이해
- Office 365 고급 위협 방지를 구현할 수 있습니다.
- Office 365 위협 Intelligence를 사용하여 구현할 수 있습니다.
- Office 365에서 감사(auditing), 경고(alerting) 및 보고(reporting)를 구성할 수 있습니다.
- Office 365의 고급 보안 관리를 사용할 수 있습니다.

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity의 일부입니다.

Office 365®의 보안에서 기업의 Office 365 보안 기능을 계획, 구현 및 관리하는 방법을 학습합니다. Office 365의 보안 및 규정 준수 센터는 Office 365에서 사용자와 데이터를 보호할 수 있는 다양한 보안 기능을 제공합니다. 기업을 대상으로 할 수 있는 다양한 유형의 위협 및 고급 위협 방지, 위협 정보, 감사(auditing) 및 고급 보안 관리와 같은 보안 기능에 대해 Office 365에서 기업의 데이터를 보호하는 방법에 대해 알아봅니다.

Module 1 – Office 365의 보안 소개

- 위협(Threat) 벡터 및 데이터 유출(breaches)
- Office 365의 보안 솔루션
- Secure Score 소개

Module 2 - Office 365 ATP 구현 및 관리

- Exchange Online Protection 소개
- Office 365 고급 위협 방지 개요
- 안전한 첨부 파일 관리
- 안전한 링크 관리
- 모니터링 및 보고

Module 3 – Office 365 위협 Intelligence사용

- Office 365 위협 Intelligence개요
- 위협(Threat) 대시 보드 사용
- 위협(Threat) 탐색기(Explorer) 사용

Module 4 – 감사(auditing), 통찰력(insights) 및 경고(alerts) 구현(Implementing)

- 보안 및 규제 준수 센터의 감사(auditing) 개요
- Exchange Online에서 사서함 감사(auditing) 사용
- 감사(audit) 로그 검색
- SharePoint 및 OneDrive에 대한 공유(sharing) 감사(auditing) 활성화
- 보안 & 규제 준수 센터(Compliance Center)에서 통찰력(insights) 및 경고 관리

Module 5 – 고급 보안 관리

- 고급 보안 관리 개요
- 정책 및 경고 구현
- App 검색 구현
- App 권한 구현

4. Meet your instructors(강사 소개)

Martin Coetzer

선임 컨텐츠 개발자, Learning experiences Team Microsoft Corporation

Martin Coetzer 는 Microsoft Learning eXperiences 팀의 수석 콘텐츠 개발자입니다. Martin Coetzer 는 Office 365, Exchange, Lync, SharePoint, Office 및 Dynamics 인증 포트폴리오를 관리합니다. 그전에는 전 세계 중소 규모 고객에게 Microsoft 기술을 설계하고 배포하는 MCS (Microsoft Consulting Services) 컨설턴트를 했습니다.

Ankur Kothari

President, Olive + Goose

Ankur Kothari 는 eDiscovery 비즈니스 분야의 베테랑으로서 Microsoft 에서 처음으로 eDiscovery 를 시작할 때 큰 도움이 되었습니다. 그는 현재 Office 365 및 규정 준수 기술 전문 컨설팅 회사인 Olive + Goose 의 사장입니다. 그전에는 Microsoft 내에서 다양한 직책을 맡았습니다.

Joe Turick

수석 컨설턴트, Olive + Goose

Joe Turick 은 Olive + Goose 의 수석 컨설턴트로 Office 365 및 Exchange 의 기술 콘텐츠 제작의 전문 지식을 보유하고 있습니다. 그는 Microsoft Office 서버 환경에 대한 방대한 지식을 가지고 있으며, 이전에는 Microsoft 의 기술 서비스 책임자로 근무했습니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Kimberly 는 Microsoft Learning 팀의 수석 콘텐츠 개발자입니다.

Kimberly 는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

06-2. Securing Data in Azure and SQL Server

주당 2–3 시간, 총 4주

Azure 및 SQL Server 에서 데이터를 안전하게 유지하기 위한 최신 프로세스에 대해 알아보십시오.

1. Before you start(시작하기 전)

사전 요구 사항

이 과정의 실습 요소를 완료하려면 Azure 구독이 필요합니다. 무료 Azure 평가 판 가입을 신청할 수 있습니다. (확인을 위해서는 사용 가능한 신용 카드가 필요하지만 Azure 서비스에 대해서는 요금이 부과되지 않습니다) 모든 지역에서 무료 평가판을 사용할 수 있는 것은 아닙니다. 또한, 과정을 마치고 실습을 끝내지 않고도 인증서를 얻을 수 있습니다. 데이터베이스 개념 및 기본 SQL 쿼리 구문을 잘 알고 있어야 합니다. 기술 문제를 해결할 때 적극적으로 배우고 자발적으로 공부해야 합니다.

2. What you will learn(배우게 될 것)

- Connections 및 사용자 로그인을 인증하는 방법에 대해 배웁니다.
- 사용자가 자원에 액세스하도록 권한을 부여하는 방법에 대해 배웁니다.
- 데이터 액세스 감사(audit) 방법에 대해 배웁니다.
- Over the wire 를 통해 데이터를 암호화하는 방법에 대해 배웁니다.

Module 1: 사용자 및 연결 인증
이 모듈에서는 SQL Server 및 Azure SQL 데이터베이스의 배포를 준비하기 위한 계획 프로세스를 소개합니다. 하드웨어, 소프트웨어, 보안 및 가용성에 대한 고려 사항을 다룹니다.

Module 2: 사용자가 리소스에 액세스하도록 권한 부여
이 모듈은 Windows, Linux 및 Azure SQL 데이터베이스에 SQL Server를 배포하는데 필요한 작업과 단계를 설명합니다.

Module 3: 데이터 액세스 감사(Auditing)
이 모듈은 DML (데이터 조작 언어) 트리거, 서버 감사(audits) 및 데이터베이스 감사(audits)로 데이터에 대한 감사(auditing) 액세스를 다루고 있습니다.

Module 4: 데이터 암호화
이 모듈은 Transparent Data Encryption, Always Encrypted, Dynamic Data Masking을 사용하여 데이터를 암호화합니다.

Final Exam(최종 시험)
마지막 모듈을 이수한 후 최종 시험을 보면 최종 시험의 성적이 70% 비율이며 각 모듈의 숙제는 30%의 비율로 점수를 결정합니다. 이 과정을 통과하고 인증서를 취득하려면 총 70% 이상의 점수를 받아야 합니다.

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity 의 일부입니다.

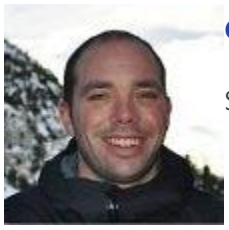
오늘날의 보안 환경에서 SQL Server 데이터베이스 관리자의 역할이 지속적으로 확대됨에 따라 데이터 보안 유지 방법을 파악하는 것이 중요합니다.

이 과정에서 전문가와 함께 사용자 인증 및 권한 부여에 대해 알아보십시오. 또한, 시스템 액세스 및 데이터 암호화 감사(audits)를 통해 데이터가 올바르게 보호되는지 확인하십시오.

SQL Server 2016, Linux 의 SQL Server v. Next(SQL Server 용 Linux)Azure SQL 데이터베이스에서의 모습을 비교하면서 다양한 플랫폼의 lenses 를 통해 주제를 살펴보겠습니다.

이 Computer Science 과정에서는 데이터베이스 보안을 위한 기능과 기술을 소개합니다. 항목에는 Authenticating Users and Connections, 사용자가 리소스에 액세스하도록 권한 부여, 데이터 액세스 Auditing 및 데이터 암호화 과정이 포함됩니다. SQL Server 2016, Linux 의 SQL Server v. Next(SQL Server 용 Linux) 및 Azure SQL 데이터베이스에서 데이터를 보호하는 방법을 학습합니다.

4. Meet your instructors(강사 소개)



Geoff Allix

SQL Server 담당 Microsoft 공인 IT 전문가, Content Master

Geoff Allix 는 CM Group Ltd.의 한 부서인 Content Master 의 Microsoft SQL Server 분야의 전문가이자 전문 컨텐츠 개발자입니다. Geoff 는 SQL Server 기술에 대한 데이터베이스 및 BI 솔루션 설계 및 구현에 대한 풍부한 경험을 갖춘 SQL Server 전문 Microsoft 공인 IT 전문가입니다. 그는 데이터베이스 솔루션을 구현 및 최적화하려는 기업에 컨설팅 서비스를 제공하고 SQL Server 2014 Microsoft 공식 커리큘럼 과정을 비롯한 다양한 SQL Server 과정에 전문가로 공헌했습니다.

Chris Randall

선임 컨텐츠 개발자, Microsoft Learning Experiences Microsoft

Chris 는 SQL Server 및 Microsoft 데이터 플랫폼이 전문이며, 25 년의 업계 경력을 보유한 트레이너, 컨설턴트 및 저자입니다. 그는 SQL Server 데이터 플랫폼 및 비즈니스 인텔리전스에 대한 Microsoft 공인 솔루션 전문가이며 Microsoft Learning Experiences 팀에서 수석 콘텐츠 개발자로 일하면서 최고의 개발자를 위한 개발자 및 데이터 전문가용 콘텐츠를 계획하고 있습니다.

06-3. Microsoft SharePoint 2016: Authentication and Security

주당 3-5시간, 총 9주

기업의 환경을 보다 잘 보호하기 위해 SharePoint Server 2016 의 인증 및 보안 요구 사항을 계획 및 구성하는 방법에 대해 알아보십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- Windows Server 2012 R2 역할 및 기능에 대한 지식이 있어야 합니다.
- SQL Server 에 대한 기본 지식이 있어야 합니다.

2. About this course(이 과정에 대하여)

이 과정은 Microsoft Professional Program in Cybersecurity 입니다.

Microsoft SharePoint 2016 인증 및 보안에서는 환경을 보호하는데 도움이 되는 다양한 인증 수준(level) 및 보안 요구 사항에 맞게 SharePoint 사내(On-premise) 솔루션을 계획 및 구성하는 방법을 학습합니다. 또한 SharePoint 보안에 필요한 하드웨어 및 소프트웨어 요구 사항과 전체 방법론에 대해 알아봅니다.

이 과정은 Microsoft SharePoint Server 2016 X Series 의 일부입니다.

3. What you'll learn(배우게 될 것)

- 인프라, 프로세스 및 방법에 따라 인증을 계획하고 구성하는 방법에 대해 배웁니다.
- 권한 설정 관리에 대해 배웁니다.
- 플랫폼 및 팜 보안 계획 및 구성에 대해 배웁니다.
- 사용자 프로파일 관리에 대해 배웁니다.
- 웹 어플리케이션 제공 및 구성에 대해 배웁니다.

4. Meet the instructor(강사 소개)

Christina Singletary

선임 컨텐츠 개발자, **Self Employed**

Christina 는 SharePoint 제품 및 서비스를 전문으로 하는 선임 콘텐츠 개발자였습니다. 그녀는 창립 이래 SharePoint 의 힘을 십분 활용했으며 제품과 관련된 모든 역할을 수행해 왔습니다. 현재 프로젝트 관리 및 마케팅 분야에서 석사 학위를 취득했으며 현재 협업 도구 및 Machine Learning 에 초점을 맞춰 정보 기술 박사 과정을 마쳤습니다.

Ankur Kothari

President, **Olive + Goose**

Ankur Kothari 는 eDiscovery 비즈니스 분야의 베테랑으로서 Microsoft 에서 처음으로 eDiscovery 를 시작할 때 큰 도움이 되었습니다. 그는 현재 Office 365 및 규정 준수 기술 전문 컨설팅 회사인 Olive + Goose 의 사장입니다. 그전에는 Microsoft 내에서 다양한 직책을 맡았습니다.

Joe Turick

수석 컨설턴트, **Olive + Goose**

Joe Turick 은 Olive + Goose 의 수석 컨설턴트로 Office 365 및 Exchange 의 기술 콘텐츠 제작의 전문 지식을 보유하고 있습니다. 그는 Microsoft Office 서버 환경에 대한 방대한 지식을 가지고 있으며, 이전에는 Microsoft 의 기술 서비스 책임자로 근무했습니다.

Elisabeth Jones

컨설턴트, **Olive + Goose**

Elisabeth Jones 는 Olive + Goose 의 컨설턴트로 정보 과학 부분에서 7 년의 경력을 쌓았습니다. 그녀는 정보 과학 박사 학위를 갖고 있으며 University of Washington 과 University of Michigan 에서 온라인 및 개인 교육 과정을 가르쳤습니다.

07. Windows 10 Security Features

주당 2-4시간, 총 4주

Windows 10 의 새로운 보안 Architectures 와 기능에 대해 배우고 현재의 보안 위협 환경을 탐구하면서 Windows 10 의 활성화 방법을 익히십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- Windows 클라이언트 관리, 유지 보수 및 문제 해결할 수 있어야 합니다.
- Windows 네트워킹 기술을 알고 있어야 합니다.
- Active Directory
- Windows Server 관리에 대해 알고 있어야 합니다.

2. About this course(이 과정에 대하여)

이 과정은 Microsoft Professional Program in Cybersecurity 의 일부입니다.

남들보다 보안을 더 빠르게 배우고 계신가요? Windows 10 의 새로운 보안 Architectures 와 기능에 대해 알아보고 이를 배포하는 방법을 배우면 미래에 필요한 통찰력(insight)과 지식을 습득할 수 있습니다.

Microsoft 보안 엔지니어는 stack 의 모든 layer 에서 운영 체제를 강화하여 다양한 위협으로 보호하는 새로운 보안 기능을 개발하여 공격 대상을 줄였습니다. 전문가 팀에 가입하여 Windows 10 에서 계속 증가하는 보안 수준(level)을 탐색하십시오.

bundle 된 보안 기능을 포함하여 Windows 10 방어 스택부터 시작합니다.

Endpoint 보안을 구성하고 Windows 정보 보호 및 Windows Defender Exploit Guard 와 같은 추가 보안 도구를 검토하십시오. 이 코스에서는 ISV 및 OEM 파트너로 구성된 대규모 에코 시스템에 대한 기본 제공, 포괄적인 보호 및 지원에 대한 세부 정보를 얻을 수 있습니다.

실습 가상화, 데모, 퀴즈 및 최종 시험을 통해 오늘날의 보안 위협에 대처할 수 있는 기술을 습득하십시오. Andrew Warren, Lesley Kipling, Erdal Ozkaya, Neil Carpenter, Sami Laiho, Raymond Comvalius, Seth Moore, Michiko Short, Mike Terrill, Amitai Rottem, Randy Treit 등의 공인 전문가가 이 과정에 참여했습니다.

3. What you'll learn(배우게 될 것)

- 보안 위협 환경의 현재 특성에 대해 배웁니다.
- 위협을 완화시키는 새로운 보안 Architectures 및 Windows 10 의 기능에 대해 배웁니다.
- Windows 10 최신판에 bundle 된 보안 서비스에 대한 통찰력(insight)을 키우게 됩니다.
- 보안 외부 인프라 지원에 대한 지식을 쌓게 됩니다.
- 그룹 정책 개체 (GPO)를 사용하여 구성할 수 있는 새로운 보안 기준선을 알게 됩니다.

Module 1 – 내장된 Windows 10 방어(defenses)

- 소개.
- 공격의 진화.

Module 2 – WIndows 10이 보안을 위해 최신 하드웨어 기능을 사용하는 방법

- UEFU Secure Boot의 배경 이해.
- TPM (Trusted Platform Module) 개요.
- 신뢰할 수 있는 보안 부팅.
- 측정된(Measured) 부팅.
- 초기 출시 맬웨어 방지 프로그램(ELAM)
- 데이터 실행 방지(Prevention).
- 주소 공간 레이아웃 무작위 화(Randomization).
- 보호된 프로세스.
- 힙(Heap) 보호 또는 malloc () 및 free ().
- 커널(Kernel) 풀(pool) 보호.

Module 3 – Windows 10 소프트웨어 보안 기능 - 1

- 고급 보안이 설정된 Windows 방화벽.
- 가상 보안 모드 (VSM).
- 자격(Credential) 인증(Guard) (CC).
- BitLocker.
- Windows Defender Antivirus (WDAV).

- Windows 정보 보호 (WIP).
- PowerShell 네트워크 cmdlet

Module 4 – Windows 10 소프트웨어 보안 기능 -2

- 원격(Remote) 신원(Credential) 확인(Guard).
- Device Guard.
- Device Guard가있는 AppLocker.
- Windows Defender SmartScreen (WDSS).
- Windows 10 수준의 원격 측정(telemetry)

Module 5 – Windows 10 Creator 업데이트의 보안 기능

- 엔터프라이즈 인증서(Certificate) 고정(Pinning).
- Windows Hello 및 Windows Hello for Business.
- Windows 및 Windows Server에 대한 새로운 그룹 정책 설정 참조.
- Windows Defender 보안 센터 (WDSC).
- Windows Defender Exploit Guard (WDEG).
- WDAG (Windows Defender Application Guard).
- Windows Defender 사전 위협 방지 (ATP).
- Ransomware를 서비스로 사용합니다.
- 사례 연구: Petya ransomware 공격에 대한 Windows 10의 저항(resistance).

Module 6 - 과정 수료

- Graded Lab
- 최종 시험
- Post Course 설문 조사

4. Meet the instructor(강사 소개)

Philip E. Helsel

선임 컨텐츠 개발자, Learning experiences Team **Microsoft**

Philip Helsel 은 Microsoft Learning 팀의 수석 콘텐츠 개발자로 현재 Windows 10, Hyper-V 및 Configuration Manager 용 IT Professional 코스를 만드는 데 중점을 두고 있습니다. 그는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 계획 담당자이기도 합니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team **Microsoft**

Kimberly 는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

08. Windows Server 2016 Security Features

주당 2–4 시간, **총 5주**

1. Before you start(시작하기 전)

사전 요구 사항

- 전제 조건 없음.

2. What you will learn(배우게 될 것)

- 보안 위협 환경의 현재 특성에 대해 배우게 됩니다.
- 위협을 완화하는 새로운 보안 Architectures 및 Windows Server 2016 의 기능에 대해 배웁니다.
- Windows Server 2016 최신 버전과 함께 제공되는 보안 서비스에 대한 통찰력(insight)을 키우게 됩니다.
- 보안 외부 인프라 지원에 대한 지식을 쌓게 됩니다.
- Hyper-V 의 새로운 보안 기능에 대한 이해
- DSC (Desired State Configuration)에 대해 배웁니다.

- Windows Server 2016 의 강화(Hardening)
    - 보안 부팅을 위한 하드웨어 요구 사항
    - BitLocker
    - 자격(Credential) 인증(Guard)
    - Device Guard - 코드 무결성 - App Locker
    - Windows Defender 맬웨어 방지 프로그램
    - 패치/WSUS
    - Windows Server 2016 에서 시스템 서비스 비활성화에 대한 지침
- 네트워크 보안 구성
    - 호스트 방화벽
    - 분산형 방화벽
    - 3.1.1 의 SMB 보안
- 안전한 가상화
    - 차폐된 VM
    - 암호화가 지원되는 VM
    - 보호된 구조
    - vTPM
- 위협 탐지
    - 그룹 정책

    - 향상된 Windows 로그
    - 고급 위협 분석(ATA)
- 권한 있는 사용자
    - Privilege 액세스 관리
    - JEA
    - 원격(Remote) 자격(Credential) 인증(Guard)

Module 1 – 공격 표면(Surface) 감소

- Server Core 배포로 공간(footprint) 최소화
- 공격 면(surface) 감소에 대한 이해
- 서비스 계정 관리
- 그룹 관리 서비스 계정 구성
- 보안 부팅을 위해 Windows Server 2016 구성
- 장치 가드를 사용하여 신뢰할 수 없는 코드의 실행을 제한하십시오.

Module 2 - 안전한 관리

- 권한 있는 계정을 보호해야 할 필요성을 이해합니다.
- 자격(Credential) 인증(Guard)
- 원격(Remote) 자격(Credential) 인증(Guard)
- 관리자 액세스 제한
- Just In Time Administration
- Just Enough Administration

Module 3 – 컨테이너(Containers) 작업 부하(Workloads) 격리

- 컨테이너(Containers) 작업 부하(Workloads) 격리
- 컨테이너(Containers) 유형 이해
- Docker로 컨테이너(Containers) 관리
- Hyper-V 컨테이너(Containers) 이해
- Windows Server 컨테이너(Containers) 이해

Module 4 – 안전한 가상화 인프라(Infrastructure)

- 보호된 패브릭(fabric) 및 위협을 이해합니다.
- Admin-trusted 및 tpm-trusted 증명(attestation)
- 호스트 보호자 서비스
- 암호화 및 보호된 VM

Module 5 - 과정 수료

- 최종 시험
- Post Course 설문 조사

3. Overview(개요)

이 과정은 Microsoft Professional Program in Cybersecurity의 일부입니다.

Windows Server 2016의 새롭고 강화된 보안 기능을 탐색할 기회가 있었습니까? 오린 토마스(Orin Thomas)는 새로운 코스인 Windows Server에 대해 책을 썼습니다! – 책을 단계별로 읽으며 보안 침해(breaches)로부터 보호하는 법을 배웁니다.

Windows Server 2016은 알려진 위협 및 새로운 위협을 모두 해결할 수 있는 보호 계층을 제공합니다. 인프라 보호에 적극적으로 기여하는 방법을 배우게 됩니다. 다양한 공격 방식을 완화하고 데이터 센터 내부에서 진행되는 공격의 전반적인 위협을 처리하기 위해 보호 기능이 어떻게 구축되었는지 확인하십시오.

Secure Boot에 대한 하드웨어 요구 사항 및 시스템 서비스 비활성화에 대한 지침을 포함하여 Windows Server 2016의 보안 강화에 대해 살펴보겠습니다. 방화벽을 포함한 네트워크 보안을 구성하고 암호화가 지원되는 가상 시스템과 같은 안전한 가상화를 찾는 방법을 살펴보십시오. 여기에서 보안 가상화, 위협 탐지, 권한 있는 계정, 원하는 상태 구성 등의 정보를 얻을 수 있습니다. 진행중인 보안 관리 기술을 습득하면서 데모를 보거나 실습 랩에 참여하고 최종 시험에 합격하십시오.

4. Meet your instructors(강사 소개)

Philip E. Helsel

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Philip Helsel 은 Microsoft Learning 팀의 수석 콘텐츠 개발자로 현재 Windows 10, Hyper-V 및 Configuration Manager 용 IT Professional 코스를 만드는 데 중점을 두고 있습니다. 그는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 계획 담당자이기도 합니다.

Microsoft 에 입사하기 전에는 Fast Search(빠른 검색) 및 Pre-Sales Engineer (사전 판매 엔지니어) 및 강사를 했으며, Oracle Corporation 의 Pre-Sales Engineer (사전 판매 엔지니어) 및 Sun Micro systems 에 있었습니다. 그는 또한 미 육군 대위로도 일했습니다.

Phil Helsel 은 수학 및 물리학에서 학사 학위를, Computer Science 에서 석사 학위를 취득했습니다. 그는 또한 Microsoft Certified Trainer(MCT), MCITP, CCNA, VCP5, CISM, Security +, Network + 및 기타 여러 인증을 보유하고 있습니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Kimberly 는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

Orin Thomas

Microsoft 클라우드/데이터 센터 전문가. 저자, 마이크로소프트 MVP & 리전 책임자. 테크니컬 라콘테어

Orin Thomas 는 MCT(Microsoft 공인 강사)의 Microsoft Regional Director 의 MVP(지난 10 년간 디렉터리 서비스의 Microsoft MVP)이며 Microsoft MCSE 및 MCITP 인증을 받았습니다. 그는 Windows Server, Windows 클라이언트, Azure, System Center, Exchange Server, 보안 및 SQL Server 와 같은 주제로 Microsoft Press 에 3 권 이상의 책을 저술했습니다. 그는 Plural Sight 의 저자이며 Charles Sturt University 의 정보 기술 의사(Doctor of Information Technology) 프로그램의 후보(candidate)입니다.

09. Microsoft Azure Security Services

주당 2–4 시간, 총 4주

보안 위협 환경의 현재 특성을 이해하고 Microsoft Azure 의 새로운 보안 Architectures 와 기능을 연구하십시오.

1. Before you start(시작하기 전)

사전 요구 사항

- On premises TCP/IP 네트워킹
- 모바일 장치 관리에 익숙해야 합니다.
- 일반적인 클라우드 원칙을 알고 있어야 합니다.

2. What you will learn(배우게 될 것)

Azure 및 Intune에서 제공하는 추가 보안 서비스를 이해하고 사용합니다.

- Azure 보안 Architectures 개요에 대해 배웁니다.
- Azure 네트워킹 보안에 대해 배웁니다.
- 네트워크 보안 그룹에 대해 배웁니다.
- 보안 원격 액세스에 대해 배웁니다.
- 모니터링 및 위협 탐지에 대해 배웁니다.
- Reference Architectures 에 대해 배웁니다.
- IaaS workload 보안에 대해 알아봅니다.
- Azure Security Center 의 기능 이해
- Azure 가 DDoS (Distributed Denial of Services) 공격을 방어하는 방법에 대해 배웁니다.
- Azure 안티 맬웨어 검사에 대해 배웁니다.
- Windows, iOS 및 Android 장치 용 Microsoft Intune 이해에 대해 배웁니다.
    - MDM
    - MAM
    - GDPR 을 통한 Data governance
    - Auto Pilot

Module 1

- Azure 보안 architecture 개요
- Azure Networking Security
- 네트워크 보안 그룹

- Azure IaaS Workload Security (누가 무엇을 유지하는지)

Module 2

- Azure Security Center
- Azure Security Center 사례 연구
- 클라우드 서비스 모델
- Azure 백업
- Azure 로그 분석

Module 3

- Azure 응용 프로그램 게이트웨이
- Azure 웹 응용 프로그램 방화벽
- DDoS 대응
- Azure 디스크 및 저장소 암호화

Module 4

- Windows, iOS 및 Android 장치 용 Microsoft Intune
- MDM, MAM
- GDPR 을 통한 Data Governance
- Overview of Auto Pilot

3. Overview(개요)

이 과정은 사이버 보안 전문가 프로그램의 일부입니다.

이 과정에서는 Azure 내에서 서비스와 데이터를 안전하게 보호하기 위해 Azure Security 서비스에 대한 통찰력(insight)을 얻을 수 있습니다.

Azure 보안 모범 사례를 배우고 탄력적인 클라우드 서비스를 만들기 위한 용어, 도구 및 기술을 이해합니다. Azure와 Intune에서 제공되는 추가 보안 서비스에 대해서도 배우고 사용할 것입니다.

4. Meet your instructors(강사 소개)

Philip E. Helsel

선임 컨텐츠 개발자, Learning experiences Team Microsoft

Philip Helsel 은 Microsoft Learning 팀의 수석 콘텐츠 개발자로 현재 Windows 10, Hyper-V 및 Configuration Manager 용 IT Professional 코스를 만드는 데 중점을 두고 있습니다. 그는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 계획 담당자이기도 합니다.

Microsoft 에 입사하기 전에는 Fast Search(빠른 검색) 및 Pre-Sales Engineer (사전 판매 엔지니어) 및 강사를 했으며, Oracle Corporation 의 Pre-Sales Engineer (사전 판매 엔지니어) 및 Sun Micro systems 에 있었습니다. 그는 또한 미 육군 대위로도 일했습니다.

Phil Helsel 은 수학 및 물리학에서 학사 학위를, Computer Science 에서 석사 학위를 취득했습니다. 그는 또한 Microsoft Certified Trainer(MCT), MCITP, CCNA, VCP5, CISM, Security +, Network + 및 기타 여러 인증을 보유하고 있습니다.

Kimberly Rasmusson-Anderson

선임 컨텐츠 개발자, Learning experiences Team Microsoft

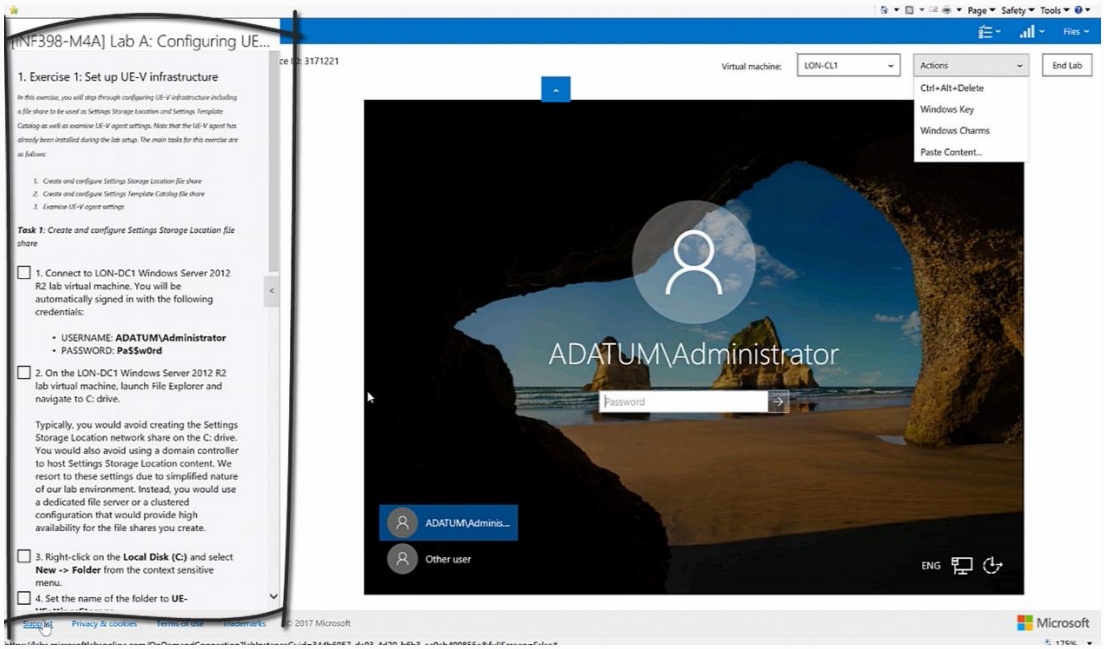
Kimberly 는 IT 전문가 과정에 책임을 맡고 있습니다. 그녀는 또한, 새로운 Microsoft Virtual Academy 엔터프라이즈 Security 채널의 프로젝트 관리자이기도 합니다. 그전에는 그녀는 Microsoft 고객 서비스 및 지원 부서의 기술 책임자였습니다.

온라인 랩 사용 방법

1) 준비 되셨나요? 랩 사용 방법에 대해 알려드리겠습니다.

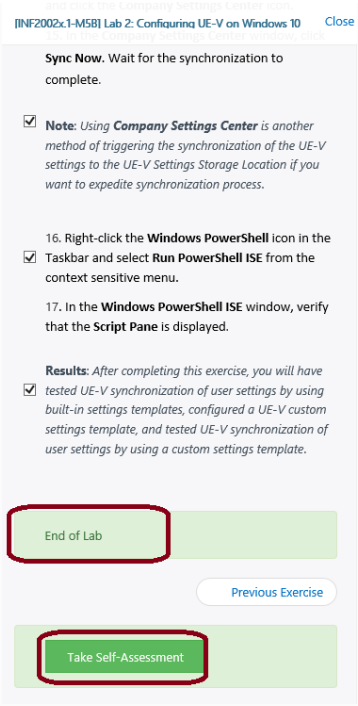
2) Scored 온라인 랩 항목에서 아래 그림과 유사한 "Launch Scored Lab"을 클릭하십시오.

3) 진행 과정에서 체크 박스를 클릭하여 랩을 진행합니다.



주의할 점: Scored 온라인 랩을 시작할 때마다 ("Launch Scored Lab"버튼 클릭) 해당 랩에 대한 채점 프로세스가 시작됩니다. 이전에 테스트를 한번 응시 했어도 점수를 향상시키기 위해 다시 시험에 응시할 수 있습니다. 그렇게 될 경우 이전 시험 점수는 사라지며, 현재 시험 점수로 기록이 됩니다.

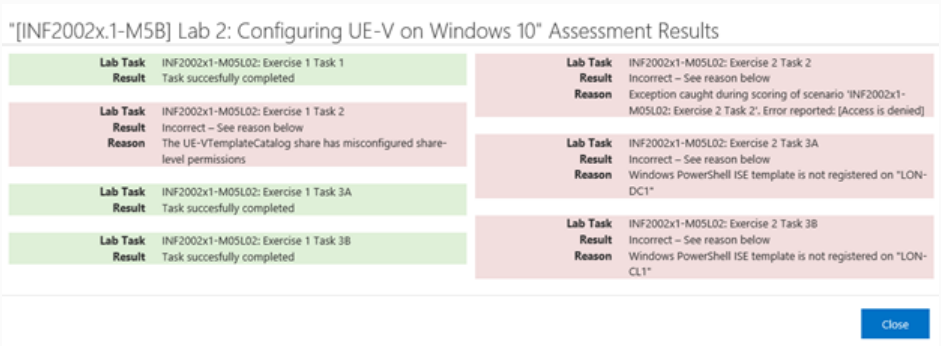
4) 온라인 랩 단계에서 MLO 환경에서 랩을 진행하고 완료한 단계의 체크 박스를 선택하십시오.



참고: 랩 단계 텍스트 링크는 실습 모듈에 실습 단계가 포함된 경우에만 나타납니다.

5) 모든 랩 단계가 완료되고 모든 체크 박스가 선택되면 Take Self-Assessment 를 클릭하여 수행한 작업을 확인합니다.

6) 결과를 확인하고 다시 수강할 필요가 있는 지 판단하십시오.



사이버 보안 트랙 FAQ

각 과정을 완료하는 데 얼마나 많은 시간이 필요합니까?

이것은 물론 사람마다 다릅니다. 전체 코스를 완료하는데 필요한 예상 시간은 78-181시간입니다. 시간은 학생에 따라 다릅니다. 이미 주제에 익숙한 학생들이나 주당 시간을 많이 쓰는 학생들은 코스를 더 빨리 마칠 수 있고, 아니면 기술 습득에 더 많은 시간이 필요할 수 있습니다.

Cybersecurity 코스를 시작하기 전에 필요한 것은?

학생들은 Windows 네트워킹, Windows Server 관리 및 Windows PowerShell에 대한 경험이 있어야 합니다.

Cybersecurity 코스를 완성하기 위해 특별한 소프트웨어 또는 클라우드 서비스가 필요합니까?

아닙니다. 학생들은 코스를 완성하기 위해 특별한 소프트웨어 나 클라우드 서비스가 필요하지 않습니다.

사이버 보안 Capstone 프로젝트는 무엇입니까?

Capstone 프로젝트는 사이버 위협을 탐지, 보호 및 대응해야 하는 모의 환경을 제공합니다.