How to Work with Threat Indicators with Microsoft Sentinel

This How to Work with Threat Indicators with Microsoft Sentinel training covers how to stay on top of the threats and risks to your network with intelligent threat indicators that reveal vulnerabilities and key information.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Getting To Know Microsoft Sentinel — 157 min.

SIEMs and SOARs	11
Microsoft Sentinel Workspaces	11
Setting Up Microsoft Sentinel	6
Microsoft Sentinel Roles	7
Microsoft Sentinel Data Storage	15

Microsoft Sentinel Data Connectors

Overview	1
Data Sources and Prerequisites	15
Configuring Data Connectors Via Policies	5
Syslog and CEF Event Collectors	18
Threat Intelligence Connectors	9
Ingesting Custom Logs	12

Microsoft Sentinel Analytics Rules

Overview	1
Intro to Sentinel Analytics Rules	1
Design and Configure Analytics Rules	9
Activate Microsoft Security Analytics Rules	4
Custom Analytics Rules	5
Connector Provided Queries and Workflow	4
Incident Creation Logic with KQL	14
KQL Exercise	7

WEEK 2

139 min.

Manage and Use Watchlists	18

SOAR and Incident Response

Overview	1
Creating Playbooks	8
Automation Rules	6
Defender Playbooks	5
Incidents Within Sentinel	15
Multi-Workspace Incidents	6
User and Entity Behavior Analytics (UEBA)	6

Sentinel Workbooks, Notebooks and Hunting

Overview	1
Sentinel Workbooks	10
Custom Workbooks	10
Security Operations Efficiency Workbook	5
Threat Hunting Queries	6
Hunting With Livestreams	4
Sentinel Bookmarks	5
Hunting With Notebooks	13
Configure and Use MSTICPy in Notebooks	17

Last updated 12.3.2024