Section 4: Lower Cost in Azure for Security Operations

Video 4.2: Mastering Microsoft Sentinel Pricing

* <https://azure.microsoft.com/en-us/pricing/calculator/>
* <https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers#free-data-sources>
* <https://azure.microsoft.com/en-us/pricing/offers/sentinel-microsoft-365-offer/>
* <https://azure.microsoft.com/en-us/pricing/details/monitor/>
* <https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/>

Video 4.3: Exceptions to Microsoft Sentinel Pricing

* <https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers#free-data-sources>
* <https://azure.microsoft.com/en-us/pricing/offers/sentinel-microsoft-365-offer/>
* <https://azure.microsoft.com/en-us/pricing/calculator/>

Video 4.4: Demo: Microsoft Sentinel Pricing Calculator

* <https://azure.microsoft.com/en-us/pricing/calculator/>

Video 4.8: Demo: Optimization Strategies for Significant Cost Savings

* <https://learn.microsoft.com/en-us/azure/sentinel/windows-security-event-id-reference>
* <https://koosg.medium.com/unlimited-advanced-hunting-for-microsoft-365-defender-with-azure-data-explorer-4fc30574cf29>
* <https://azure.microsoft.com/en-us/pricing/details/storage/data-lake/>
* <https://github.com/seyed-nouraie/Azure-Security-Data-Lake/tree/main>
* <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-table-plans?msclkid=3c629183cfef11ecbd520ceb6ff77849&tabs=portal-1>
* <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-query?tabs=portal-1#limitations>
* <https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/>

Video 4.9: Understanding Basics Logs

* <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-query?tabs=portal-1#limitations>
* <https://learn.microsoft.com/en-us/azure/sentinel/basic-logs-use-cases>
* <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/logs-table-plans?tabs=portal-1#supported-tables>

Video 4.14: Exploring Azure Data Explorer

* <https://github.com/seyed-nouraie/Azure-Security-Data-Lake>
* <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-azure-sentinel-hunting-supports-adx-cross-resource/ba-p/2530678>
* <https://learn.microsoft.com/en-us/azure/data-explorer/solution-architectures>
* <https://learn.microsoft.com/en-us/kusto/query/schema-entities/external-tables?view=azure-data-explorer&preserve-view=true>
* <https://koosg.medium.com/unlimited-advanced-hunting-for-microsoft-365-defender-with-azure-data-explorer-646b08307b75>

Video 4.15: Demo: Ingesting Logs into Azure Data Explorer from Azure Storage

* <https://dataexplorer.azure.com/freecluster>
* <https://learn.microsoft.com/en-us/azure/data-explorer/lightingest>

Video 4.16: Cross Resource Query in Microsoft Sentinel

* <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/azure-monitor-data-explorer-proxy#cross-query-your-log-analytics-or-application-insights-resources-and-azure-data-explorer>
* <https://dataexplorer.azure.com/publicfreecluster>