**Rule migration checklist**

Before embarking on the journey to migrate rules from your current SIEM to Azure Sentinel, there are some preliminary steps that should be taken to increase your chances of success with the undertaking. The following checklist is recommended:

|  |  |  |
| --- | --- | --- |
| **No** | **Item** | **Check Box** |
| 1 | Select use cases. The selection of use cases for the migration should answer the question: what problems are we trying to solve? Consider use cases in terms of business priority |  |
| 2 | Review the detection efficacy of existing rules and alerts before electing to migrate them into Azure Sentinel |  |
| 3 | Eliminate some of the low-level alerts you routinely ignore. The more you can weed our alerts you don’t act upon; the more higher value alerts will be more likely to be acted upon |  |
| 4 | Drive value and visibility by mapping Analytics to the [MITRE ATTACK framework](https://attack.mitre.org/#:~:text=MITRE%20ATT&CK%C2%AE.%20MITRE%20ATT&CK%20%C2%AE%20is%20a%20globally-accessible,and%20in%20the%20cybersecurity%20product%20and%20service%20community.) |  |
| 5 | Review the “Built-in Azure Sentinel rules” to identify out-of-the-box rules that can address your use-cases |  |
| 6 | Review your SOC metrics and consult your SOC team to identify alerts they routinely ignore without negative consequence. Drop these from your alert feeds |  |
| 7 | Review rules that haven’t triggered any alerts in the last 6 to 12 months to determine whether they are still relevant. |  |
| 8 | Build a candidate list of rules that have a high true positive rate and ignore the rest |  |
| 9 | Confirm the existence of the data and their collection mechanism in Azure Sentinel to support the inbound rules: [Azure Sentinel: The connectors grand (CEF, Syslog, Direct, Agent, Custom and more) - Microsoft Tech Community](https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-the-connectors-grand-cef-syslog-direct-agent/ba-p/803891) |  |
| 10 | Define test scenarios and build a test script to be used for rule validation |  |