|  |
| --- |
| **Detection Rules Development Framework** |

# [Rule Name]

|  |  |  |
| --- | --- | --- |
| **Detection Engineer: <Insert-Name>** | | * Development Date: * Validation Date: * Deployment Date: |
|  |  | |

|  |  |
| --- | --- |
| Rule Objective | <Insert Objective> |
| Source | * Threat Intelligence/Red Team/Incident |
| Categorization | |  |  |  |  | | --- | --- | --- | --- | | Tactic | Technique | Procedure | MITRE ID | | <Tactic-Name> | <Technique-Name> | <Procedure-Name> | <MITRE-ID> | |
| Detection Strategy | |  |  |  | | --- | --- | --- | | MITRE ID – Technique Name | | | | Data Sources | Data Components | | | Command Line | <Insert Tool> | <Insert Tool> | | <Insert Command> | <Insert Command> | | API’s | <Insert API Call> | | | Process | <Insert Process Name> | | | Windows Registry | <Insert Registry Key> | | | Log Sources | <Insert Windows Event ID’s> | | | RPC | <Insert RPC Call> | | | Network Protocol | <Insert Network Protocol> | | |
| Rule Development | * Log Source: * Rule Type: Signature/Behavioral/Anomaly * Deployment Date: |
| Priority | * **Critical**/**High**/**Medium**/**Low** |
| Validation | * Rule Validation Date: * True Positive: Yes/No  |  |  |  | | --- | --- | --- | | No | Red Team Methodology | Alert Status | | 1 |  | Trigger/Evasion | |
| Deficiencies | |  |  |  |  | | --- | --- | --- | --- | | No | Deficiency | Status | Comment | | 1 |  | Yes/No | <Insert Comment> | |
| Deployment | * Deployment Date: * Automation: Yes/No * Interval: Daily/Weekly/Monthly |
| Maintenance | |  |  |  | | --- | --- | --- | | Rule Efficiency Ratio | Rule Review Date | Technique Evolution | | <Insert % Ratio> | <Insert Date> | * <Update> | |
| Confidence Level | * Strong/Fair/Low |
| Response Procedures | 1. <Insert Procedure 1> 2. <Insert Procedure 2> |
| Resources | * <Public Disclosed Resource> |