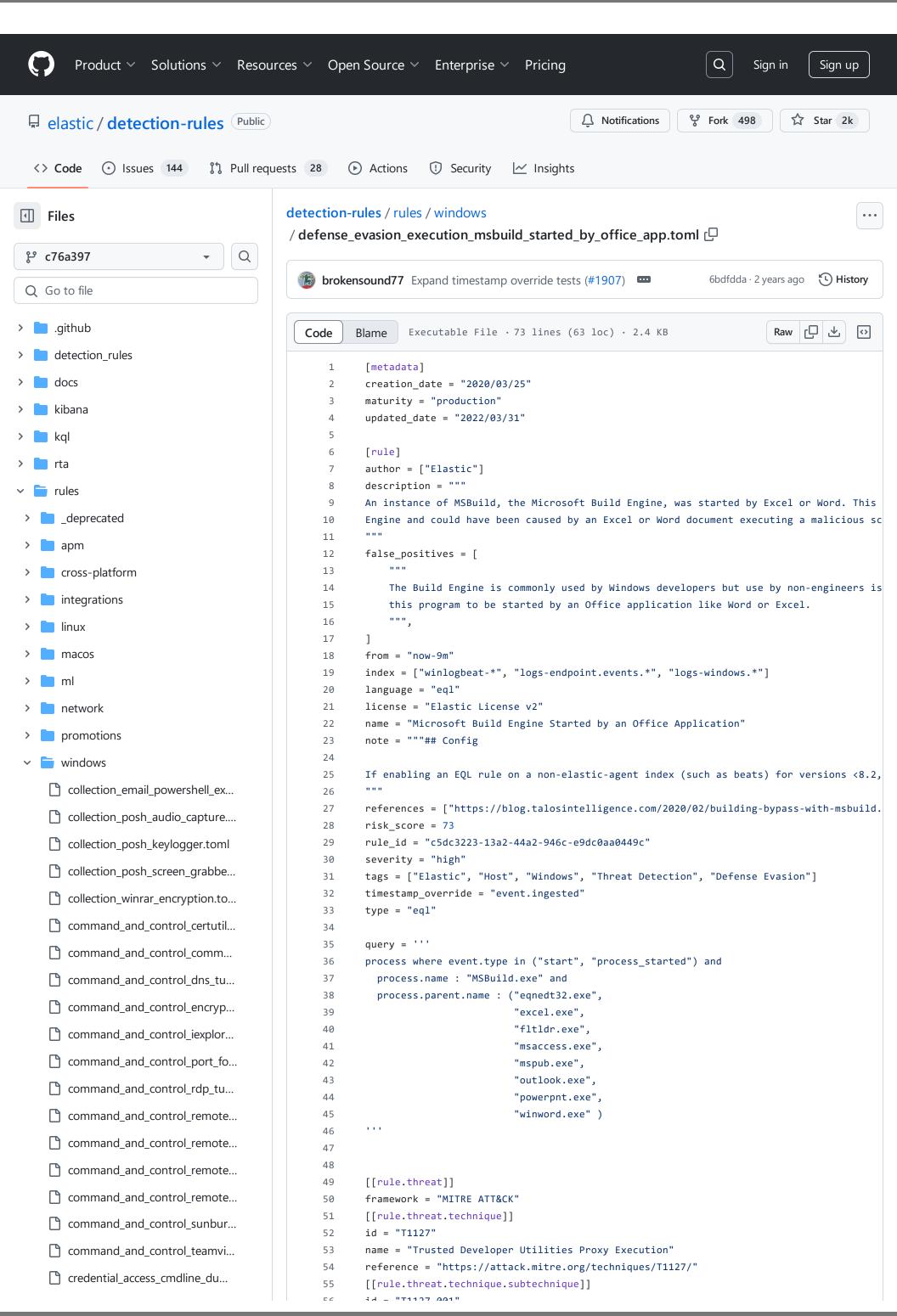
rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/defense_evasion_execution_msbuild_started_by_office_app.toml



rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/windows/defense_evasion_execution_msbuild_started_by_office_app.toml

```
credential_access_copy_ntds_s...
credential_access_credential_d...
credential_access_dcsync_replic...
credential_access_disable_kerb...
credential_access_domain_back...
credential_access_dump_regist...
```

```
TU = 1117/ . AAT
סכ
57
       name = "MSBuild"
58
       reference = "https://attack.mitre.org/techniques/T1127/001/"
59
60
61
62
       [rule.threat.tactic]
63
       id = "TA0005"
64
       name = "Defense Evasion"
65
       reference = "https://attack.mitre.org/tactics/TA0005/"
66
       [[rule.threat]]
67
       framework = "MITRE ATT&CK"
68
69
       [rule.threat.tactic]
70
       id = "TA0002"
71
       name = "Execution"
72
       reference = "https://attack.mitre.org/tactics/TA0002/"
```