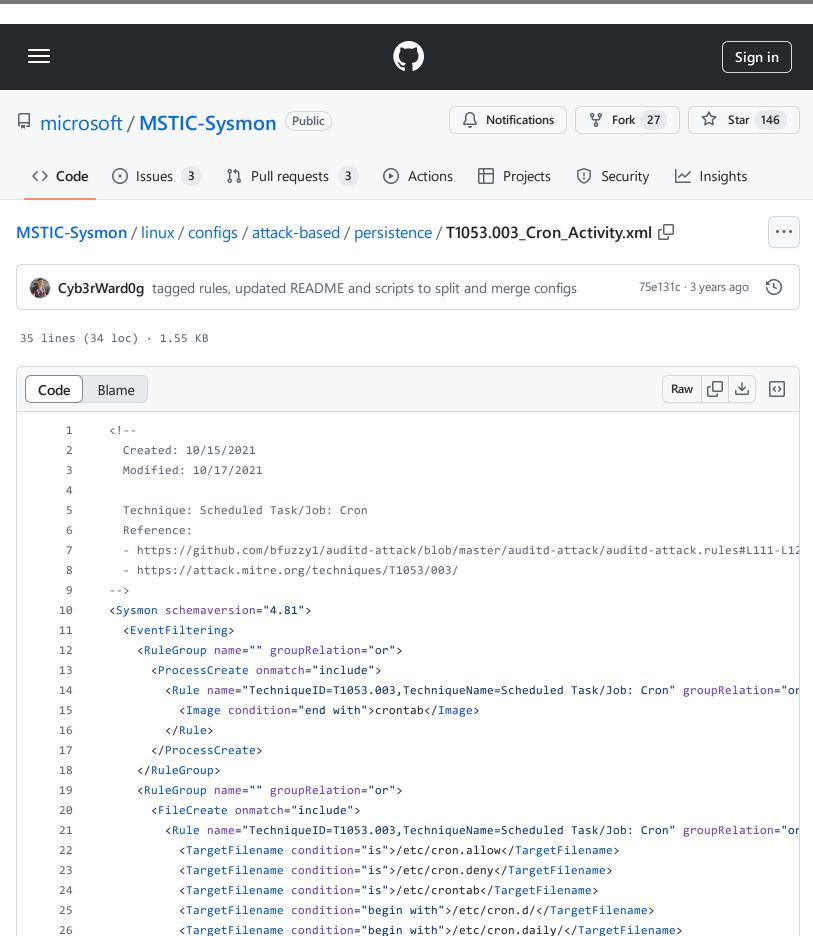
MSTIC-Sysmon/linux/configs/attack-based/persistence/T1053.003\_Cron\_Activity.xml at f1477c0512b0747c1455283069c21faec758e29d · microsoft/MSTIC-Sysmon · GitHub - 31/10/2024 14:49 https://github.com/microsoft/MSTIC-Sysmon/blob/f1477c0512b0747c1455283069c21faec758e29d/linux/configs/attack-based/persistence/T1053.003\_Cron\_Activity.xml



MSTIC-Sysmon/linux/configs/attack-based/persistence/T1053.003\_Cron\_Activity.xml at f1477c0512b0747c1455283069c21faec758e29d · microsoft/MSTIC-Sysmon · GitHub - 31/10/2024 14:49 https://github.com/microsoft/MSTIC-Sysmon/blob/f1477c0512b0747c1455283069c21faec758e29d/linux/configs/attack-based/persistence/T1053.003\_Cron\_Activity.xml

```
27
                 <TargetFilename condition="begin with">/etc/cron.hourly/</TargetFilename>
28
                 <TargetFilename condition="begin with">/etc/cron.monthly/</TargetFilename>
                 <TargetFilename condition="begin with">/etc/cron.weekly/</TargetFilename>
29
30
                 <TargetFilename condition="begin with">/var/spool/cron/crontabs/</TargetFilename>
31
             </FileCreate>
32
33
           </RuleGroup>
34
         </EventFiltering>
35
       </Sysmon>
```