Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

olafhartong / sysmon-modular Public

Notifications Fork 589 Star 2.7k

Code Issues 32 Pull requests 20 Discussions Actions Projects Wiki Security Insights

Files

fa1ae53

Go to file

- .github
- 0_custom_configuration
- 10_process_access
- 11_file_create
  - exclude_dell_process.xml
  - exclude_elastic_logs.xml
  - exclude_intel_gfx_service.xml
  - exclude_ivanti_res.xml
  - exclude_microsoft_click2run.xml
  - exclude_microsoft_services.xml
  - exclude_microsoft_windows_rec...
  - exclude_microsoft_windows_upd...
  - exclude_msdatp.xml
  - exclude_outlook_profile.xml
  - exclude_provtool.xml
  - exclude_psscriptpolicytest.xml
  - exclude_sccm.xml
  - exclude_scheduled_task_noise.xml
  - include_appc_shim.xml
  - include_batch_files.xml
  - include_chm_files.xml
  - include_cloud_credendials.xml
  - include_credendials.xml
  - include_default_profile_changes....
  - include_desktop.xml
  - include_dotnet.xml
  - include_downloaded_files.xml
  - include_drivers_added.xml
  - include_electron_app_injection.x...
  - include_executables.xml
  - include_group_policy_changes.xml
  - include_hta_scripts.xml
  - include_iso.xml
  - include_javascript.xml
  - include_kirbi.xml
  - include_links.xml

sysmon-modular / 11_file_create / include_dotnet.xml

olafhartong Proper XML formatting 05ba7a6 · 3 years ago History

Code Blame 16 lines (16 loc) · 1.51 KB Raw

```
<Sysmon schemaversion="4.30">
        <EventFiltering>
                <RuleGroup name="" groupRelation="or">
                        <FileCreate onmatch="include">
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                                <TargetFilename name="technique_id=T1218,technique_name
                        </FileCreate>
                </RuleGroup>
        </EventFiltering>
</Sysmon>
```

- include_microsoft_clickonce.xml
- include_microsoft_msbuild_scrip...
- include_microsoft_settingconten...
- include_ms_office_documents_w...
- include_ms_office_excel_iqy_slk.x...
- include_outlook_attachments.xml