Data recorded on Dec 22, 2023 by https://github.com/rowham/WinSigmaRuleAnalyzer
Roham Diba

Windows Sigma Rules Overview

Sigma rules contain either a **service** field or a **category** within the logsource field. (Refer to the official Sigma Rule documentation.)	This column has been enriched by the script, aiding in the identification of entries related to Sysmon or Powershell.	This column displays the number of rules per 'Service or Category' at each **level**. In theory, higher level triggers more critical alert. For more information about levels in Sigma rules, refer to the documentation. https://github.com/SigmaHQ/sigma/tree/master/documentation/logsource-guides/windows					This column shows the quantity of rules per '**Service** or **Category**'. It would be beneficial to understand the number of Sigma rules that can be implemented for a given log source or a win channel.	This column contains either EventIDs used in the rules or is enriched by the script. Though not perfect, it provides an overview. (see the official sigma log source conf. doc for full list) https://github.com/SigmaHQ/sigma/tree/master/documentation/logsource-guides/windows
Type	**Service or Category (Log Source)**	**Channel / Provider**	**Informational**	**Low**	**Medium**	**High**	**Critical**	**Total Rules in Log Source**	**Event IDs**
Category	process_creation	Microsoft-Windows-Sysmon	2	51	457	524	25	1063	1
Category	registry_set	Microsoft-Windows-Sysmon	1	6	73	99	1	180	13
Category	ps_script	Microsoft-Windows-PowerShell - PowerShellCore	0	22	87	51	3	163	4104
Category	file_event	Microsoft-Windows-Sysmon	0	8	54	80	7	149	11
Service	security	Security	2	16	43	72	7	140	4697, 4674, 4661, 4663, 4611, 4904, 4660, 4658, 4742, 4794, 1102, 4698, 4729, 4825, 5140, 634, 4898, 4648, 4625, 4673, 4766, 4800, 675, 4706, 5038, 6281, 517, 4741, 6423, 4719, 4656, 6416, 4672, 4905, 4899, 4701, 4720, 5145, 4776, 4702, 4647, 4781, 4771, 4616, 4765, 633, 4657, 4634, 5156, 5379, 4743, 4738, 4649, 632, 4964, 4704, 5136, 4699, 4732, 4768, 4624, 4730, 4728, 4662, 4692, 4769
Category	image_load	Microsoft-Windows-Sysmon	1	5	41	44	1	92	7
Service	system	System	1	2	22	32	5	63	1034, 5829, 217, 98, 16991, 41, 16990, 7045, 10001, 42, 26, 16, 213, 55, 24, 7036, 7023, 50, 56, 20, 1033, 1031, 104, 5723, 1032, 39, 6038, 5805, 6039, 7034
Category	network_connection	Microsoft-Windows-Sysmon	0	2	22	22	0	46	3
Category	registry_event	Microsoft-Windows-Sysmon	0	0	8	17	11	36	12, 13, 14
Category	ps_module	Microsoft-Windows-PowerShell - PowerShellCore	1	4	10	16	1	32	4103
Category	process_access	Microsoft-Windows-Sysmon	0	0	4	19	0	23	10
Service	application	Application	0	5	6	10	1	23	216, 524, 200, 1034, 325, 882, 18456, 865, 327, 868, 1042, 866, 15457, 1033, 867, 1040, 201, 1, 1001, 1000, 33205, 326, 11724, 1511
Category	pipe_created	Microsoft-Windows-Sysmon	1	0	5	5	6	17	17, 18
Category	dns_query	Microsoft-Windows-Sysmon	0	2	9	3	1	15	22
Category	driver_load	Microsoft-Windows-Sysmon	0	1	2	8	1	12	6
Service	windefend	Microsoft-Windows-Windows Defender	0	1	2	9	0	12	5001, 1117, 1121, 1015, 5010, 5013, 1013, 5012, 3002, 1006, 1116, 1009, 3007, 5007, 5101
Category	file_delete	Microsoft-Windows-Sysmon	0	1	7	4	0	12	23, 26
Category	create_remote_thread	Microsoft-Windows-Sysmon	0	0	1	10	0	11	8
Category	ps_classic_start	Windows PowerShell	0	2	6	3	0	11	400
Service	codeintegrity-operational	Microsoft-Windows-CodeIntegrity	0	0	1	9	0	10	3077, 3037, 3104, 3032, 3023, 3083, 3022, 3034, 3001, 3021, 3036, 3033, 3082, 3035
Category	create_stream_hash	Microsoft-Windows-Sysmon	0	0	3	6	0	9	15
Category	registry_add	Microsoft-Windows-Sysmon	0	1	4	4	0	9	12
Service	firewall-as	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	0	4	2	2	0	8	2082, 2033, 2008, 2009, 2004, 2071, 2052, 2060, 2002, 2006, 2083, 2003, 2032, 2073, 2059, 2005
Service	appxdeployment-server	Microsoft-Windows-AppXDeploymentServer	0	0	5	2	0	7	400, 454, 453, 401, 441, 442, 854, 412
Service	bits-client	Microsoft-Windows-Bits-Client	0	2	2	3	0	7	3, 16403
Service	msexchange-management	MSExchange Management	0	0	1	3	3	7	6
Category	registry_delete	Microsoft-Windows-Sysmon	0	0	3	3	0	6	12
Service	dns-client	Microsoft-Windows-DNS Client Events	0	1	1	2	1	5	3008
Category	file_access	Microsoft-Windows-Kernel-File	0	2	3	0	0	5	
Service	sysmon	Microsoft-Windows-Sysmon	0	0	2	2	0	4	27, 28, 29, 16
Category	wmi_event	Microsoft-Windows-Sysmon	0	0	1	2	0	3	21, 20, 19
Service	ntlm	Microsoft-Windows-NTLM	0	1	2	0	0	3	8004, 8002, 8001
Service	taskscheduler	Microsoft-Windows-TaskScheduler	0	0	2	1	0	3	141, 129
Service	powershell-classic	Windows PowerShell	0	0	2	1	0	3	
Service	dns-server	DNS Server	0	0	1	1	0	2	6004, 150, 771, 770
Service	security-mitigations	Microsoft-Windows-Security-Mitigations/Kernel Mode - Microsoft-Windows-Security-Mitigations/User Mode	0	0	0	2	0	2	12, 11
Category	file_change	Microsoft-Windows-Sysmon	0	0	0	2	0	2	2
N/A	N/A	N/A	0	0	0	1	0	1	15
Category	process_tampering	Microsoft-Windows-Sysmon	0	0	1	0	0	1	25
Category	raw_access_thread	Microsoft-Windows-Sysmon	0	1	0	0	0	1	9
Category	sysmon_error	Microsoft-Windows-Sysmon	0	0	0	1	0	1	255
Category	sysmon_status	Microsoft-Windows-Sysmon	0	0	0	1	0	1	16, 4
Service	applocker	Microsoft-Windows-AppLocker/MSI and Script - Microsoft-Windows-AppLocker/EXE and DLL - Microsoft-Windows-AppLocker/Packaged	0	0	1	0	0	1	8004, 8007, 8022, 8025
Service	appmodel-runtime	Microsoft-Windows-AppModel-Runtime/Admin	0	1	0	0	0	1	201
Service	appxpackaging-om	Microsoft-Windows-AppxPackaging	0	0	1	0	0	1	157
Service	capi2	Microsoft-Windows-CAPI2	0	0	1	0	0	1	70
Service	certificateservicesclient-lifecycle-system	Microsoft-Windows-CertificateServicesClient-Lifecycle-System	0	0	1	0	0	1	1007
Service	driver-framework	Microsoft-Windows-DriverFrameworks-UserMode	0	1	0	0	0	1	2100, 2102, 2003
Service	ldap	Microsoft-Windows-LDAP-Client/Debug	0	0	1	0	0	1	30
Service	lsa-server	Microsoft-Windows-LSA	0	0	1	0	0	1	300
Service	openssh	OpenSSH	0	0	1	0	0	1	4
Service	microsoft-servicebus-client	Microsoft-ServiceBus-Client	0	0	0	1	0	1	40300, 40302, 40301
Service	shell-core	Microsoft-Windows-Shell-Core	0	0	1	0	0	1	28115
Service	terminalservices-localsessionmanager	Microsoft-Windows-TerminalServices-LocalSessionManager	0	0	0	1	0	1	21
Service	wmi	Microsoft-Windows-WMI-Activity	0	0	1	0	0	1	5861, 5859
Service	diagnosis-scripted	Microsoft-Windows-Diagnosis-Scripted	0	0	0	1	0	1	101
Service	smbclient-security	Microsoft-Windows-SmbClient/Security	0	0	1	0	0	1	31017
Category	file_rename	Microsoft-Windows-Kernel-File	0	0	1	0	0	1	
Category	ps_classic_provider_start	Windows PowerShell	0	0	0	1	0	1	600