SYSMON EVENTS

ID	Event	ID	Event
1	Process Creation	17	Pipe Created
2	File Creation Time Changed	18	Pipe Connected
3	Network Connection Detected	19	WMI Filter
4	Sysmon Service State Change	20	WMI Consumer
5	Process Terminated	21	WMI Consumer Filter
6	Driver Loaded	22	DNS Query
7	Image Loaded	23	FileDelete
8	CreateRemoteThread	24	New Content in the Clipboard
9	RawAccessRead	25	Process Tampering
10	ProcessAccess	26	File Delete Logged
11	FileCreate	27	File Block Executable
12	Registry Object Created or Deleted	28	File Block Shredding
13	Registry Value Set	29	File Executable Detected
14	Registry Object Renamed		
15	FileCreateStreamHash		
16	Sysmon Config State Change		

WINLOG EVENTS

ID	Event Summary	ID	Event Summary
1102	The audit log was cleared	4720	A user account was created
4616	The system time was changed	4722	A user account was enabled
4624	An account was logged on	4723	An attempt was made to change an account's password
4625	An account failed to log on	4724	An attempt was made to reset an account's password
4634	An account was logged off	4735	A security-enabled local group was changed
4648	A logon was attempted using explicit credentials	4737	A security-enabled global group was changed
4657	A registry value was modified	4738	A user account was changed
4672	Special privileges assigned to new logon	4740	A user account was locked out
4673	A privileged service was called	4755	A security-enabled universal group was changed
4688	A new process has been created	4768	A Kerberos authentication ticket (TGT) was requested
4689	A process has exited	4769	A Kerberos service ticket was requested
4697	A service was installed on the system	4771	Kerberos pre-authentication failed
4698	A scheduled task was created	4772	A Kerberos authentication ticket request failed
4699	A scheduled task was deleted	4777	The Domain Controller failed to validate the credentials for an account
4700	A scheduled task was enabled	4946	A rule was added in the Windows Firewall exception list
4701	A scheduled task was disabled	4947	A rule was modified in the Windows Firewall exception list
4702	A scheduled task was updated	4948	A rule was deleted in the Windows Firewall exception list
4719	System audit policy was changed	5051	A file was virtualized