AuditPolicies

With this policies it is possible to detect 11 out of 14 attack categories

The following attack categories cannot be detected with certainty:

- CommandExecution
- CapturingDomainAdministratorAndAccountCredentials
- DeletingEventLog

AuditName	Target	Actual	Prio
AuditNonSensitivePrivilegeUse	SuccessAndFailure	SuccessAndFailure	Low
AuditUserAccountManagement	Success	SuccessAndFailure	Low
AuditProcessTermination	Success	Success	High
AuditSAM	SuccessAndFailure	SuccessAndFailure	Low
AuditKerberosAuthenticationService	SuccessAndFailure	SuccessAndFailure	Low
AuditRegistry	SuccessAndFailure	SuccessAndFailure	High
AuditHandleManipulation	Success	Success	Low
AuditFileSystem	SuccessAndFailure	SuccessAndFailure	High
AuditLogon	Success	SuccessAndFailure	Medium
AuditSpecialLogon	Success	NotConfigured	Low
AuditMPSSVCRule-LevelPolicyChange	Success	Success	Low
AuditLogoff	Success	SuccessAndFailure	Medium
AuditDetailedFileShare	SuccessAndFailure	SuccessAndFailure	Low
AuditSensitivePrivilegeUse	SuccessAndFailure	SuccessAndFailure	Low
AuditKernelObject	SuccessAndFailure	SuccessAndFailure	High
AuditSecurityGroupManagement	SuccessAndFailure	SuccessAndFailure	Low
AuditFileShare	SuccessAndFailure	SuccessAndFailure	Low
AuditKerberosServiceTicketOperations	SuccessAndFailure	SuccessAndFailure	Low
AuditFilteringPlatformConnection	Success	Success	Low
AuditProcessCreation	Success	Success	High
ForceAuditPolicySubcategory	Enabled	Enabled	-
Sysmon	InstalledAndRunning	InstalledAndRunning	High
CAPI2LogSize	4194304	4422736	-
CAPI2	EnabledGoodLogSize	EnabledGoodLogSize	-

WindowsLogs

EventID6	present
EventID21	missing
EventID24	missing
EventID102	missing
EventID104	missing
EventID106	missing
EventID129	missing
EventID169	missing
EventID200	missing
EventID201	missing
EventID4624	present
EventID4634	present
EventID4648	present
EventID4656	present
EventID4658	present
EventID4660	missing
EventID4661	missing
EventID4663	present
EventID4672	present
EventID4673	present
EventID4688	present
EventID4689	present
EventID4690	present
EventID4720	missing
EventID4726	missing
EventID4728	missing
EventID4729	missing
EventID4768	missing
EventID4769	missing
EventID4946	present
EventID5140	missing
EventID5142	present
EventID5144	missing
EventID5145	missing
EventID5154	present
EventID5156	present
EventID7036	missing
EventID7045	present
EventID8222	missing
EventID20001	present

AppAndServLogs

EventID106	present
EventID200	present
EventID129	present
EventID201	present
EventID102	present
EventID6	missing
EventID169	missing
EventID21	present
EventID24	present