AuditPolicies

With this policies it is possible to detect 10 out of 14 attack categories

The following attack categories cannot be detected with certainty:

- CommandExecution(AuditLogoff,)
- PassTheHashAndTicket(AuditLogoff,)
- CapturingDomainAdministratorAndAccountCredentials(AuditLogoff,)
- AcquisitionOfAccountInformation(AuditLogoff,)

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

WindowsLogs

EventID6	present
EventID21	missing
EventID24	present
EventID102	missing
EventID104	missing
EventID106	missing
EventID129	present
EventID169	missing
EventID200	missing
EventID201	missing
EventID1102	missing
EventID4624	present
EventID4634	missing
EventID4648	missing
EventID4656	present
EventID4658	present
EventID4660	present
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	missing
EventID5140	missing
EventID5142	missing
EventID5144	missing
EventID5145	missing
EventID5154	missing
EventID5156	present
EventID7036	present
EventID7045	present
EventID8222	missing
EventID20001	present

AppAndServLogs

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