AuditPolicies

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	-

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