AuditPolicies

AuditName	Target	Actual
AuditNonSensitivePrivilegeUse	SuccessAndFailure	SuccessAndFailure
AuditUserAccountManagement	Success	SuccessAndFailure
AuditProcessTermination	Success	Success
AuditSAM	SuccessAndFailure	SuccessAndFailure
AuditKerberosAuthenticationService	SuccessAndFailure	SuccessAndFailure
AuditRegistry	SuccessAndFailure	SuccessAndFailure
AuditHandleManipulation	Success	Success
AuditFileSystem	SuccessAndFailure	SuccessAndFailure
AuditLogon	Success	SuccessAndFailure
AuditSpecialLogon	Success	NotConfigured
AuditMPSSVCRule-LevelPolicyChange	Success	Success
AuditLogoff	Success	SuccessAndFailure
AuditDetailedFileShare	SuccessAndFailure	SuccessAndFailure
AuditSensitivePrivilegeUse	SuccessAndFailure	SuccessAndFailure
AuditKernelObject	SuccessAndFailure	SuccessAndFailure
AuditSecurityGroupManagement	SuccessAndFailure	SuccessAndFailure
AuditFileShare	SuccessAndFailure	SuccessAndFailure
AuditKerberosServiceTicketOperations	SuccessAndFailure	SuccessAndFailure
AuditFilteringPlatformConnection	Success	Success
AuditProcessCreation	Success	Success
ForceAuditPolicySubcategory	Enabled	Enabled
Sysmon	InstalledAndRunning	InstalledAndRunning
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