AuditPolicies

With this policies it is possible to detect 3 out of 14 attack categories

The following attack categories cannot be detected with certainty:

- CommandExecution (AuditLogoff, AuditLogon, AuditRegistry)
- PasswordHashAcquisation (AuditRegistry)
- MaliciousCommunicationRelay (AuditRegistry)
- RemoteLogin (AuditLogon, AuditRegistry)
- PassTheHashAndTicket (AuditLogoff, AuditLogon, AuditRegistry)
- PrivilegeEscalation (AuditRegistry)
- CapturingDomainAdministratorAndAccountCredentials (AuditLogoff, AuditLogon, AuditRegistry)
- FileSharing (AuditLogon)
- DeletingEvidence (AuditRegistry)
- DeletingEventLog (AuditLogon)
- AcquisitionOfAccountInformation (AuditLogoff, AuditLogon, AuditRegistry)

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