Instantly share code, notes, and snippets.

gentilkiwi / dcsync-dcshadow.splunk Secret

Last active last year

Star 38 Fork 4

Code Revisions 3 Stars 38 Forks 4 Embed <script src="https:// Download ZIP

dcsync-dcshadow.splunk Raw

```
sourcetype=XmlWinEventLog:Security AND EventCode=4662 AND NOT (SubjectUserSid="AUTORITE NT\\*" OR SubjectDomainName="Window Manager
(
  (ObjectType="%{19195a5b-6da0-11d0-afd3-00c04fd930c9}" OR ObjectType="domainDNS")
  AND
  (Properties="*Replicating Directory Changes All*" OR Properties="*{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}*" OR Properties = "*{992
)
| rename _time AS DSTime, SubjectUserSid AS DSUserSid, SubjectDomainName AS DSDomainName, SubjectUserName AS DSUserName, SubjectLog
| join type=left Computer, DSLogonId
[
    search sourcetype=XmlWinEventLog:Security AND EventCode=4624 NOT (TargetUserSid="AUTORITE NT\\*" OR TargetDomainName="Window Ma
    | rename _time AS LogonTime, TargetLogonId AS DSLogonId
]
| convert timeformat="%d/%m/%Y %H:%M:%S" ctime(DSTime), ctime(LogonTime)
| table DSTime, Computer, DSUserSid, DSDomainName, DSUserName, DSObjectType, DSObjectName, DSProperties, DSStatus, DSLogonId, Logon

sourcetype="XmlWinEventLog:Security" AND EventCode=4742 AND NOT (SubjectUserSid="AUTORITE NT\\*" OR SubjectDomainName="Window Manag
AND (ServicePrincipalNames="*GC/*" OR ServicePrincipalNames="*E3514235-4B06-11D1-AB04-00C04FC2DCD2/*")
AND NOT (SubjectUserSid = "AUTORITE NT\\*")
| rename _time AS CAMTime, SubjectUserSid AS CAMSubjectUserSid, SubjectDomainName AS CAMSubjectDomainName, SubjectUserName AS CAMSu
| join type=left Computer, CAMSubjectLogonId
[
    search sourcetype=XmlWinEventLog:Security AND EventCode=4624 NOT (TargetUserSid="AUTORITE NT\\*" OR TargetDomainName="Window Ma
    | rename _time AS LogonTime, TargetLogonId AS CAMSubjectLogonId
]
| convert timeformat="%d/%m/%Y %H:%M:%S" ctime(CAMTime), ctime(LogonTime)
| table CAMTime, CAMSubjectUserSid, CAMSubjectDomainName, CAMSubjectUserName, CAMTargetSid, CAMTargetDomainName, CAMTargetUserName,
```

gentilkiwi commented on Jun 11, 2018 Author ···

Be aware that you might have to change AUTORITE NT and filter out DC$ accounts and others particularities
"join" is limited by the product and does not work as expected in SQL 😞

johnmccash commented on Apr 26, 2019 ···

The use of 4662 events has two prerequisites:

1. The logging hosts (All DCs, in this case) must have the following set in its auditing config: DS Access -> Audit Directory Service Access: Success and Failure
2. The AD objects to be monitored (Which, I'm sorry, but I'm unclear exactly which objects must have this ACL applied) must have an Audit ACL applied. Further Question: Do these ACLs need to log all read or write access by anyone at all, or do we just care about write access, or possibly just from a restricted set of users?

Please (Pretty Please? :-))add a description of the exact configuration required to enable the necessary logging.
Thanks

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment