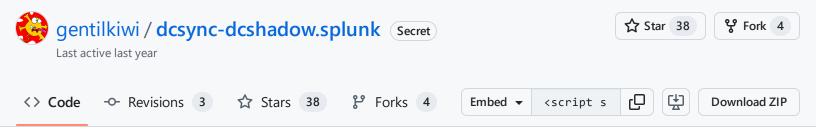
GitHub Gist Search... All gists Back to GitHub Sign in Sign up

Instantly share code, notes, and snippets.



```
  dcsync-dcshadow.splunk

                                                                                                        Raw
     sourcetype=XmlWinEventLog:Security AND EventCode=4662 AND NOT (SubjectUserSid="AUTORITE NT\\*" OR Subje
 2
       (ObjectType="%{19195a5b-6da0-11d0-afd3-00c04fd930c9}" OR ObjectType="domainDNS")
 3
 4
       (Properties="*Replicating Directory Changes All*" OR Properties="*{1131f6ad-9c07-11d1-f79f-00c04fc2dc
 5
 6
     )
     rename _time AS DSTime, SubjectUserSid AS DSUserSid, SubjectDomainName AS DSDomainName, SubjectUserNa
 7
     | join type=left Computer, DSLogonId
 8
 9
         search sourcetype=XmlWinEventLog:Security AND EventCode=4624 NOT (TargetUserSid="AUTORITE NT\\*" OR
10
         rename _time AS LogonTime, TargetLogonId AS DSLogonId
11
12
     convert timeformat="%d/%m/%Y %H:%M:%S" ctime(DSTime), ctime(LogonTime)
13
     | table DSTime, Computer, DSUserSid, DSDomainName, DSUserName, DSObjectType, DSObjectName, DSProperties
14
15
     sourcetype="XmlWinEventLog:Security" AND EventCode=4742 AND NOT (SubjectUserSid="AUTORITE NT\\*" OR Sub
16
     AND (ServicePrincipalNames="*GC/*" OR ServicePrincipalNames="*E3514235-4B06-11D1-AB04-00C04FC2DCD2/*")
17
     AND NOT (SubjectUserSid = "AUTORITE NT\\*")
18
     rename _time AS CAMTime, SubjectUserSid AS CAMSubjectUserSid, SubjectDomainName AS CAMSubjectDomainName
19
     | join type=left Computer, CAMSubjectLogonId
20
21
22
         search sourcetype=XmlWinEventLog:Security AND EventCode=4624 NOT (TargetUserSid="AUTORITE NT\\*" OR
         rename _time AS LogonTime, TargetLogonId AS CAMSubjectLogonId
23
24
     convert timeformat="%d/%m/%Y %H:%M:%S" ctime(CAMTime), ctime(LogonTime)
25
     table CAMTime, CAMSubjectUserSid, CAMSubjectDomainName, CAMSubjectUserName, CAMTargetSid, CAMTargetDo
26
```



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

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information



© 2024 GitHub, Inc.