# **List of Use Cases Demonstrating Broad Capabilities**

**Contents**

[**Daily Status Reports** 1](#_Toc474265292)

[**New Activities Found** 1](#_Toc474265293)

[**Systems Reporting** 3](#_Toc474265294)

[**Critical Auth Logs** 4](#_Toc474265295)

[**Windows Process Logs** 5](#_Toc474265296)

The following list is a compilation of Use cases together with their output.

# **Daily Status Reports**

The following users are currently in an inactive state for the past 30 Days or more:

**RAW DATA RESULTS:**  
{jboyd=1, crosenberger=1, jkautz=1, sboyd=1, esmothers=1, dwhitten=1, jnelson=1, spersaud=1, russells=1, yamargui=1, Reedye=1, robinsona=1, tobenshain=1, lterada=1, rolayinka=1, wranglersystem=1, byrda=1, ablizzard=1, houstona=1, BLModest\_SA=1, rcalvert=1, dgoldman=1, wgibson=1, jstorms=1, rparra=1, ddawson=1, dabotchie=1, skhanal=1, mschultz=1, nhoffman=1, blarson=1, gillemk=1, amartin=1, msandretto=1, mreich=1, mgutknecht=1, swilson=1, jjao=1, jnoseworthy=1, rrizvi=1, drivenbark=1, sewers=1, aosgood=1, gadams=1, ceddy=1, hmartin=1, aoniha=1, pontiac2system=1, rwilson=1}

**EXAMPLES:**

Inactive Users, Suspicious Activities/programs/applications, trends, volume activities

# **New Activities Found**

Pipeline HBSS Logs  
  
   This program captures everything that was created on the network to include new accounts, groups, software deployments, installations, tasks, etc...  
Additionally, this program is designed to track all these new activities into a seperate index. This data store is user agnostic!   
  
 USE CASE: Daily Reporting, User Activity Monitoring, New processes and accounts monitoring, and/or Data Validation   
fshaw :   
          Create Client Task   
          Create deployment   
rorellano :   
          Create Client Task   
          Create deployment   
          Request URL   
snickles :   
          Install Rogue Sensor   
          Remove Rogue Sensor   
          Request URL   
          [DLP] Policy Created   
akronebusch :   
          Request URL   
          Create Client Task   
          Create agent deployment URL data object   
          Create deployment   
system :   
          User viewed the Agent Package Download page   
bmiller :   
          Create Client Task   
          Create deployment   
wdaley :   
          Exception created from events   
          Create Client Task   
ngruden :   
          Request URL   
slambert :   
          Create Client Task   
          Create deployment   
aparris :   
          [DLP] policy Rule Created   
          [DLP] Classification Created   
bmodest :   
          Exception created from events   
          New Group   
jcrew :   
          Request URL   
          [DLP] Policy Created   
jpetitjean :   
          Exception created from events   
nsmigiel :   
          Create Client Task   
          Create deployment   
rthompson :   
          New Tag Group   
srussell :   
          New User   
tborger :   
          Create Client Task   
          Exception created from events   
tglover :   
          Create Client Task   
tstrawser :   
          Create Client Task   
wyi :   
          Exception created from events   
          Trusted Application created from events   
aromanak :   
          Create Client Task   
          Create policy object   
dcohen :   
          Create Client Task   
dmariotti :   
          Request URL   
eyanchuk :   
          New Group   
gtom :   
          Exception created from events   
          Trusted Application created from events   
hkash :   
          Exception created from events   
kwendt :   
          Exception created from events   
thester :   
          Exception created from events   
vbedford :   
          Request URL   
abyrd :   
          New User   
ahouston :   
          New User   
arobinson :   
          New Group   
aweldon :   
          Create Client Task   
dvanhoose :   
          New User   
ereedy :   
          Create Client Task   
lstewart :   
          Exception created from events   
mdalton :   
          Create Client Task   
mjones :   
          Create agent deployment URL data object   
pfulton :   
          Create Client Task   
wvanhoose :   
          New User

# **Systems Reporting**

Pipeline Auth Logs  
  
   The following systems have not reported logs in the last 24h hours using  a 3d window.  
USE CASE: Verify Systems Reporting, Systems connectivity, and/or Data Validation   
Do per each index type.  
  
128.63.93.64    
128.63.18.63    
2001:480:90:142:baca:3aff:fea3:9d5d    
130.203.244.155    
158.12.64.13    
67.63.198.131    
128.63.66.89    
134.164.56.34    
2001:480:30:602:baac:6fff:fe3c:fc7    
140.31.68.20    
158.12.37.69    
158.12.44.94    
205.68.95.65    
134.194.200.185    
131.92.254.10    
2001:480:91:5401::7f5    
2001:480:31:4420:225:90ff:fe5d:9fe4    
158.12.62.33

# **Critical Auth Logs**

175 Critical Errors have occured in Auth Pipeline within past 24 hours  
  
MESSAGE: fatal: Cannot bind any address.  
TIME: 2017-02-03T22:16:26.000Z  
HOST: 128.63.27.61  
SOURCE: foehn-wind.arl.army.mil  
  
MESSAGE: pam\_krb5: authenticate error: Client not found in Kerberos database (-1765328378)  
TIME: 2017-02-03T21:58:02.000Z  
HOST: 128.63.27.61  
SOURCE: ls17011-l  
  
MESSAGE: pam\_krb5: authenticate error: Decrypt integrity check failed (-1765328353)  
TIME: 2017-02-03T21:58:01.000Z  
HOST: 128.63.27.61  
SOURCE: ls17011-l  
  
MESSAGE: fatal: Cannot bind any address.  
TIME: 2017-02-03T21:45:30.000Z  
HOST: 128.63.27.61  
SOURCE: magic.arl.army.mil  
  
MESSAGE: pam\_krb5: authenticate error: Client not found in Kerberos database (-1765328378)  
TIME: 2017-02-03T21:19:13.000Z  
HOST: 128.63.27.61  
SOURCE: excelsior  
  
MESSAGE: pam\_krb5: authenticate error: Preauthentication failed (-1765328360)  
TIME: 2017-02-03T21:19:11.000Z  
HOST: 128.63.27.61  
SOURCE: excelsior  
  
MESSAGE: pam\_krb5: authenticate error: Client not found in Kerberos database (-1765328378)  
TIME: 2017-02-03T20:33:41.000Z  
HOST: 128.63.27.61  
SOURCE: pilsner  
  
MESSAGE: pam\_krb5: authenticate error: Client name mismatch (-1765328309)  
TIME: 2017-02-03T20:33:39.000Z  
HOST: 128.63.27.61  
SOURCE: pilsner  
  
MESSAGE: fatal: Cannot bind any address.  
TIME: 2017-02-03T19:41:29.000Z  
HOST: 128.63.27.61  
SOURCE: motion.arl.army.mil  
  
MESSAGE: fatal: Cannot bind any address.  
TIME: 2017-02-03T19:40:55.000Z  
HOST: 128.63.27.61  
SOURCE: sophia.arl.army.mil

# **Windows Process Logs**

Pipeline Windows Logs  
  
This Alert collects executables ran across the windows domains for a 30-day period, aggregates them according to process, and further aggregates them according to username (also, source ip possible)  
  
 USE CASE: Daily Reporting, User Activity Monitoring, Process Management, Security Monitoring  
   
  
C:\Windows\SysWOW64\cmd.exe     
          NAE\IITEL13$ Results: 2464625  
          NAE\ADLCWKLS2715K$ Results: 4935  
          NAE\lynn.edmiston.ao Results: 435  
          NAE\lynn.edmiston Results: 373  
          NT AUTHORITY\LOCAL SERVICE Results: 22  
          NAE\edward.c.albert2.ao Results: 2  
          NAE\thuan.nguyen2 Results: 1  
C:\Windows\System32\conhost.exe     
          NAE\IITEL13$ Results: 2428339  
          NAE\ADLCWKLS2715K$ Results: 24636  
C:\Windows\SysWOW64\netsh.exe     
          NAE\IITEL13$ Results: 89331  
          NAE\lynn.edmiston.ao Results: 25  
          NAE\lynn.edmiston Results: 20  
          NAE\ADLCWKLS2715K$ Results: 1  
C:\Windows\SysWOW64\sc.exe     
          NAE\IITEL13$ Results: 81146  
          NAE\ADLCWKLS2715K$ Results: 12  
          NAE\lynn.edmiston.ao Results: 4  
C:\Program Files (x86)\McAfee\Policy Auditor Agent\fimcli.exe     
          NAE\ADLCWKLS2715K$ Results: 12380  
          NAE\IITEL13$ Results: 8627  
C:\Windows\SysWOW64\tasklist.exe     
          NAE\IITEL13$ Results: 16566  
          NAE\ADLCWKLS2715K$ Results: 2939  
C:\Windows\System32\SearchFilterHost.exe     
          NAE\ADLCWKLS2715K$ Results: 14085  
          NAE\IITEL13$ Results: 864  
C:\Windows\System32\SearchProtocolHost.exe     
          NAE\ADLCWKLS2715K$ Results: 13742  
          NAE\IITEL13$ Results: 909  
C:\Program Files (x86)\McAfee\Common Framework\MfeServiceMgr.exe     
          NAE\ADLCWKLS2715K$ Results: 7074  
          NAE\IITEL13$ Results: 6315  
C:\Windows\SysWOW64\wbem\WmiPrvSE.exe     
          NAE\ADLCWKLS2715K$ Results: 7588  
          NAE\IITEL13$ Results: 5410