<dashboard version="1.1" script="myCustomJS.js" theme="dark">

<label>BSOC\_Investigation\_Dashboard (Test) Clone</label>

<row>

<panel>

<title>Executive Summary</title>

<table>

<title>File Egressed (Note: Assume the Files count as Zero for the classifications missing in this table)</title>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval classification= if(Control="GAS HR SAP Extract (excluding salary information)\_001" OR like(Control,"Human Resources\_BHP Employee SAP Extract - Excluding salary%") OR Policy\_Rule="Titus Confidential Metadata", "Confidential",if(Control="-" OR Control="Copyrighted Content" OR Control="DEFAULT\_CASE\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR like(Control,"GEN\_Copyrighted Content%") OR like(Control,"GEN\_Offensive languages and conversation%") OR Control="MONITOR\_CUSTOMCAT\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR Control="Transfer to Network Share Activity Monitoring" OR Control="USB device | File and Folder Access Attempts" OR Control="USB Removable Media Data Transfer Warning" OR like(Control,"GEN\_Outlook fil%"),"n/c",if(like(Control,"BHP Classification: Confidenti%") OR like(Control,"GEN\_BHP Classified Confidential%") OR like(Control,"Human Resources\_BHP Employee Number%") OR like(Control,"Human Resources\_Passports - Driving Licenses - SS Cards%") OR like(Control,"Human Resources\_PII Employee Information%") OR like(Control,"PII Employee Information\_0%") OR like(Control,"BHP Classification: Confidential%")OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365","Sugg'ed Confidential",if(Control="All DLP Policies" OR like(Control,"BHP Classification: Highly Confidenti%") OR Control="Credentials" OR Control="Credentials\_CE" OR Control="ELT Reports" OR like(Control,"External Affairs\_M and A Project Codes%") OR like(Control,"GEN\_BHP Classified Highly Confidential%") OR like(Control,"GEN\_Credentials%")OR like(Control,"Human Resources\_BHP Employee SAP Extract \_modified - Including salary information%") OR Control="M&amp;A Project Codes" OR Control="M&amp;A Project Codes\_CE" OR Control="All DLP Policies","Sugg'ed Highly Confidential",if(like(Control,"COVID-19 Vaccination Certificates A%") OR like(Control,"EandC\_ECR Case Report\_BHP%") OR like(Control,"GAS HR SAP Extract %") OR Control="ELT Reports\_CE" OR like(Control,"GEN\_ELT-RAC Materials - papers%") OR like(Control,"HSE\_Card Access Data WAIO and BMA\_BHP%") OR Control="HSE Documents" OR like(Control,"MINAUS\_Yandi Mine Integrated Operational Plan%") OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR like(Control,"HSE\_Sensitive Documents%") OR like(Control,"PS and D\_ELT-RAC Materials - papers%") OR like(Control,"PS and D\_Monthly Update Report%") OR like(Control,"PS&amp;D\_Capital Prioritisati%") OR like(Control,"Reporting\_ELT Report%") OR like(Control,"Supply\_NGO Sensitive Documents%") OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook"

OR Control="PS&amp;D\_BHP Asset Summary Model Submission" OR like(Control,"HSEC\_COVID-19 Exposure Tracking Report%") OR like(Control,"Human Resources\_BHP Employee SAP Extract - Including salary information%") OR like(Control,"Human Resources\_Compensation and Tax Documents\_BHP%") OR like(Control,"MINAUS\_High Level Design Documentation\_BHP%") OR like(Control,"MINAUS\_Reporting\_BMA Matrix%") OR like(Control,"PS and D\_5YP Appraisal Report\_%") OR like(Control,"PS and D\_BHP Asset Summary Model Submission%") OR like(Control,"PS and D\_Business Development\_Acquisitions and Divestments%") OR like(Control,"PS and D\_Capital Prioritisation%") ,"Highly Confidential"," ")))))

|search Scope="EGRESS" AND Files!="No\_Attachment" AND Files!="" |stats dc(Files) as Files by classification | addcoltotals Files labelfield=classification label=Total\_Files\_Egressed</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="drilldown">none</option>

<option name="percentagesRow">false</option>

<option name="totalsRow">false</option>

<option name="wrap">false</option>

<format type="number" field="Files">

<option name="precision">0</option>

</format>

<format type="color" field="classification">

<colorPalette type="sharedList"></colorPalette>

<scale type="sharedCategory"></scale>

</format>

</table>

</panel>

</row>

<row>

<panel>

<title>-</title>

<single>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval PII\_der=if(Control="All DLP Policies" OR Control="COVID-19 Vaccination Certificates AUS" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="EandC\_ECR Case Report\_BHP 0365" OR Control="EandC\_ECR Case Report\_BHP 0365" OR

Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP Outlook" OR Control="EandC\_ECR Case Report\_BHP SharePoint" OR Control="GAS HR SAP Extract (excluding salary information)\_001" OR Control="GAS HR SAP Extract (excluding salary information)\_CE" OR Control="GAS HR SAP Extract (including salary information)" OR Control="GAS HR SAP Extract (including salary information)\_\_Int. Emai" OR Control="GAS HR SAP Extract (including salary information)\_001" OR Control="HSE Documents" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP SharePoint" OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_ALL" OR Control="HSE\_Sensitive Documents\_BHP 0365" OR Control="HSE\_Sensitive Documents\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_BHP Outlook" OR Control="HSE\_Sensitive Documents\_BHP SharePoint" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_ALL" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP 0365" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP One Drive" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Outlook" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Sharepoint" OR Control="Human Resources\_BHP Employee Number\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number\_BHP Outlook" OR Control="Human Resources\_BHP Employee Number\_BHP SharePoint" OR Control="Human Resources\_BHP Employee Number\_WebEx" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP SharePoint" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP Outlook" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_ALL" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP SharePoint" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP 0365" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract\_modified - Including salary information\_BHP SharePoint" OR Control="Human Resources\_Compensation and Tax Documents\_BHP WebEx" OR Control="Human Resources\_Compensation and Tax Documents\_BHP OneDrive" OR Control="Human Resources\_Compensation and Tax Documents\_BHP Outlook" OR Control="Human Resources\_Compensation and Tax Documents\_BHP SharePoint" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_ALL" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP 0365" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP OneDrive" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP Outlook" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP SharePoint" OR Control="Human Resources\_PII Employee Information \_ALL" OR Control="Human Resources\_PII Employee Information \_BHP 0365" OR Control="PII Employee Information\_001" OR Control="PII Employee Information\_001\_Int. Email" OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook","May Contain PII","-")

|eval PII=if(PII\_der="-","-",PII\_der+" ( "+ Match\_Count+" hits)")

|search Scope="EGRESS" AND Files!="No\_Attachment" AND PII!="-" |stats dc(Files)</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="colorMode">block</option>

<option name="drilldown">none</option>

<option name="rangeColors">["0x53a051","0xdc4e41"]</option>

<option name="rangeValues">[0]</option>

<option name="refresh.display">progressbar</option>

<option name="underLabel">Files Containing PII Egressed</option>

<option name="useColors">1</option>

</single>

</panel>

<panel>

<title>-</title>

<single>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval PII\_der=if(Control="All DLP Policies" OR Control="COVID-19 Vaccination Certificates AUS" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="EandC\_ECR Case Report\_BHP 0365" OR Control="EandC\_ECR Case Report\_BHP 0365" OR

Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP Outlook" OR Control="EandC\_ECR Case Report\_BHP SharePoint" OR Control="GAS HR SAP Extract (excluding salary information)\_001" OR Control="GAS HR SAP Extract (excluding salary information)\_CE" OR Control="GAS HR SAP Extract (including salary information)" OR Control="GAS HR SAP Extract (including salary information)\_\_Int. Emai" OR Control="GAS HR SAP Extract (including salary information)\_001" OR Control="HSE Documents" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP SharePoint" OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_ALL" OR Control="HSE\_Sensitive Documents\_BHP 0365" OR Control="HSE\_Sensitive Documents\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_BHP Outlook" OR Control="HSE\_Sensitive Documents\_BHP SharePoint" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_ALL" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP 0365" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP One Drive" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Outlook" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Sharepoint" OR Control="Human Resources\_BHP Employee Number\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number\_BHP Outlook" OR Control="Human Resources\_BHP Employee Number\_BHP SharePoint" OR Control="Human Resources\_BHP Employee Number\_WebEx" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP SharePoint" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP Outlook" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_ALL" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP SharePoint" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP 0365" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract\_modified - Including salary information\_BHP SharePoint" OR Control="Human Resources\_Compensation and Tax Documents\_BHP WebEx" OR Control="Human Resources\_Compensation and Tax Documents\_BHP OneDrive" OR Control="Human Resources\_Compensation and Tax Documents\_BHP Outlook" OR Control="Human Resources\_Compensation and Tax Documents\_BHP SharePoint" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_ALL" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP 0365" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP OneDrive" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP Outlook" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP SharePoint" OR Control="Human Resources\_PII Employee Information \_ALL" OR Control="Human Resources\_PII Employee Information \_BHP 0365" OR Control="PII Employee Information\_001" OR Control="PII Employee Information\_001\_Int. Email" OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook","May Contain PII","-")

|eval PII=if(PII\_der="-","-",PII\_der+" ( "+ Match\_Count+" hits)")

|search Scope!="EGRESS" AND Files!="No\_Attachment" AND Files!="" AND PII!="-"|stats dc(Files)</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="colorMode">block</option>

<option name="drilldown">none</option>

<option name="rangeColors">["0x53a051","0xdc4e41"]</option>

<option name="rangeValues">[0]</option>

<option name="refresh.display">progressbar</option>

<option name="underLabel">Files Containing PII Handled</option>

<option name="useColors">1</option>

</single>

</panel>

</row>

<row>

<panel>

<title>User Risky Activity</title>

<chart>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|search Files!=No\_Attachment AND Files!="" AND Risk\_Rating!="Potential" AND Risk\_Rating!="No Risk" AND Risk\_Rating!="Encrypted" AND Action\_Final!="-" |stats count(eval(Risk\_Rating="High")) as high count(eval(Risk\_Rating="Medium")) as Medium count(eval(Risk\_Rating="Low")) as Low count(eval(Risk\_Rating="Blocked")) as Blocked by Action\_Final</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="charting.axisTitleX.visibility">visible</option>

<option name="charting.axisTitleY.visibility">visible</option>

<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.axisY.scale">linear</option>

<option name="charting.axisY2.enabled">1</option>

<option name="charting.axisY2.scale">inherit</option>

<option name="charting.chart">column</option>

<option name="charting.chart.overlayFields">Risk\_Rating</option>

<option name="charting.chart.showDataLabels">all</option>

<option name="charting.chart.stackMode">default</option>

<option name="charting.drilldown">none</option>

<option name="charting.layout.splitSeries">0</option>

<option name="charting.legend.placement">right</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

<panel>

<title>User Internal Activity involving Potential Confidential or Highly Confidential data</title>

<chart>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|eval classification= if(Control="GAS HR SAP Extract (excluding salary information)\_001" OR like(Control,"Human Resources\_BHP Employee SAP Extract - Excluding salary%") OR Policy\_Rule="Titus Confidential Metadata", "Confidential",if(Control="-" OR Control="Copyrighted Content" OR Control="DEFAULT\_CASE\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR like(Control,"GEN\_Copyrighted Content%") OR like(Control,"GEN\_Offensive languages and conversation%") OR Control="MONITOR\_CUSTOMCAT\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR Control="Transfer to Network Share Activity Monitoring" OR Control="USB device | File and Folder Access Attempts" OR Control="USB Removable Media Data Transfer Warning" OR like(Control,"GEN\_Outlook fil%"),"n/c",if(like(Control,"BHP Classification: Confidenti%") OR like(Control,"GEN\_BHP Classified Confidential%") OR like(Control,"Human Resources\_BHP Employee Number%") OR like(Control,"Human Resources\_Passports - Driving Licenses - SS Cards%") OR like(Control,"Human Resources\_PII Employee Information%") OR like(Control,"PII Employee Information\_0%") OR like(Control,"BHP Classification: Confidential%")OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365","Sugg'ed Confidential",if(Control="All DLP Policies" OR like(Control,"BHP Classification: Highly Confidenti%") OR Control="Credentials" OR Control="Credentials\_CE" OR Control="ELT Reports" OR like(Control,"External Affairs\_M and A Project Codes%") OR like(Control,"GEN\_BHP Classified Highly Confidential%") OR like(Control,"GEN\_Credentials%")OR like(Control,"Human Resources\_BHP Employee SAP Extract \_modified - Including salary information%") OR Control="M&amp;A Project Codes" OR Control="M&amp;A Project Codes\_CE" OR Control="All DLP Policies","Sugg'ed Highly Confidential",if(like(Control,"COVID-19 Vaccination Certificates A%") OR like(Control,"EandC\_ECR Case Report\_BHP%") OR like(Control,"GAS HR SAP Extract %") OR Control="ELT Reports\_CE" OR like(Control,"GEN\_ELT-RAC Materials - papers%") OR like(Control,"HSE\_Card Access Data WAIO and BMA\_BHP%") OR Control="HSE Documents" OR like(Control,"MINAUS\_Yandi Mine Integrated Operational Plan%") OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR like(Control,"HSE\_Sensitive Documents%") OR like(Control,"PS and D\_ELT-RAC Materials - papers%") OR like(Control,"PS and D\_Monthly Update Report%") OR like(Control,"PS&amp;D\_Capital Prioritisati%") OR like(Control,"Reporting\_ELT Report%") OR like(Control,"Supply\_NGO Sensitive Documents%") OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook"

OR Control="PS&amp;D\_BHP Asset Summary Model Submission" OR like(Control,"HSEC\_COVID-19 Exposure Tracking Report%") OR like(Control,"Human Resources\_BHP Employee SAP Extract - Including salary information%") OR like(Control,"Human Resources\_Compensation and Tax Documents\_BHP%") OR like(Control,"MINAUS\_High Level Design Documentation\_BHP%") OR like(Control,"MINAUS\_Reporting\_BMA Matrix%") OR like(Control,"PS and D\_5YP Appraisal Report\_%") OR like(Control,"PS and D\_BHP Asset Summary Model Submission%") OR like(Control,"PS and D\_Business Development\_Acquisitions and Divestments%") OR like(Control,"PS and D\_Capital Prioritisation%") ,"Highly Confidential"," ")))))

|eval Exposure=if(Scope="Egress","External",if(Action\_Final="Save to local drive","Private",if(Document\_Exposure="private","Private","Internal"))) |search Files!=No\_Attachment AND Files!="" AND Risk\_Rating="Potential" AND classification!="n/c" |stats count by Action\_Final</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="charting.chart">column</option>

<option name="charting.chart.showDataLabels">all</option>

<option name="charting.drilldown">none</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

</row>

<row>

<panel>

<title>User Risky Activity per Destination</title>

<chart>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Destination=split(Destination,",")

|mvexpand Destination

| rex field=Destination "\/\/(?:[^@\/\n]+@)?(?:www\.)?(?&lt;New\_Destination&gt;[^:\/\n]+)"

| rex field=Destination "\@(?&lt;domain&gt;[^ ]\*)"

|eval Domain=domain

|eval dest=if(like(Destination,"qagpublic.qg2.apps.qualys.com%"),"qagpublic.qg2.apps.qualys.com",if(like(Destination,"www.youtube.com%"),"youtube.com",if(like(Destination,"spo.bhpbilliton.com%"),"spo.bhpbilliton.com",if(like(Destination,"%sharepoint.com%"),"sharepoint.com",if(like(Destination,"mysite.bhpbilliton.com%"),"mysite.bhpbilliton.com",if(like(Destination,"mail.google.com%"),"mail.google.com",if(isnull(New\_Destination),Destination,New\_Destination)))))))

|eval Destination\_domain=if(Vector="email" AND isnull(Destination) OR Destination=" ","Unknown\_recipient",if(Vector="email",replace(Destination," ",","),if(Action="View" AND isnull(Destination),"Unknown Source",if(Action="Print","Unidentified Printer",if(Action="Download","Unidentified Destination",if(Action="Edit",Destination,if(app\_activity="FileAccessed" OR app\_activity="FileModified" OR app\_activity="PageViewed" OR app\_activity="FilePreviewed" OR app\_activity="FileDownloaded","User's Endpoint",if(app\_activity="FilesyncDownloadedFull" OR app\_activity="FilesyncUploadedFull" OR app\_activity="FileDeletedFirstStageRecycleBin" OR app\_activity="FolderDeletedFirstStageRecycleBin" OR app\_activity="FolderDeleted" OR app\_activity="FileDeleted" OR app\_activity="FolderCreated" OR app\_activity="FolderRenamed" OR app\_activity="FileRenamed" OR app\_activity="FileUploaded","0365 Sync Client",dest))))))))

|eval Final\_Destination=if(isnull(Domain),Destination\_domain,Domain)

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|search Files!=No\_Attachment AND Files!="" AND Risk\_Rating!="Potential" AND Risk\_Rating!="No Risk" AND Risk\_Rating!="Encrypted" AND Risk\_Rating!="Low" |stats count(eval(Risk\_Rating="High")) as high count(eval(Risk\_Rating="Medium")) as Medium by Final\_Destination |where Final\_Destination!=""</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="charting.chart">bar</option>

<option name="charting.chart.showDataLabels">none</option>

<option name="charting.chart.stackMode">stacked</option>

<option name="charting.drilldown">none</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

</row>

<row>

<panel>

<title>TimeLine of Data Egressed</title>

<chart>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Destination=split(Destination,",")

|mvexpand Destination

| rex field=Destination "\/\/(?:[^@\/\n]+@)?(?:www\.)?(?&lt;New\_Destination&gt;[^:\/\n]+)"

| rex field=Destination "\@(?&lt;domain&gt;[^ ]\*)"

|eval Domain=domain

|eval dest=if(like(Destination,"qagpublic.qg2.apps.qualys.com%"),"qagpublic.qg2.apps.qualys.com",if(like(Destination,"www.youtube.com%"),"youtube.com",if(like(Destination,"spo.bhpbilliton.com%"),"spo.bhpbilliton.com",if(like(Destination,"%sharepoint.com%"),"sharepoint.com",if(like(Destination,"mysite.bhpbilliton.com%"),"mysite.bhpbilliton.com",if(like(Destination,"mail.google.com%"),"mail.google.com",if(isnull(New\_Destination),Destination,New\_Destination)))))))

|eval Destination\_domain=if(Vector="email" AND isnull(Destination),"Unknown\_recipient",if(Vector="email",replace(Destination," ",","),if(Action="View" AND isnull(Destination),"Unknown Source",if(Action="Print","Unidentified Printer",if(Action="Download","Unidentified Destination",if(Action="Edit",Destination,if(app\_activity="FileAccessed" OR app\_activity="FileModified" OR app\_activity="PageViewed" OR app\_activity="FilePreviewed" OR app\_activity="FileDownloaded","User's Endpoint",if(app\_activity="FilesyncDownloadedFull" OR app\_activity="FilesyncUploadedFull" OR app\_activity="FileDeletedFirstStageRecycleBin" OR app\_activity="FolderDeletedFirstStageRecycleBin" OR app\_activity="FolderDeleted" OR app\_activity="FileDeleted" OR app\_activity="FolderCreated" OR app\_activity="FolderRenamed" OR app\_activity="FileRenamed" OR app\_activity="FileUploaded","0365 Sync Client",dest))))))))

|eval Final\_Destination=if(isnull(Domain),Destination\_domain,Domain) |search Scope="EGRESS" AND Files!="No\_Attachment" AND Files!="" |timechart dc(Files) as File\_Egressed</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="charting.chart">column</option>

<option name="charting.chart.showDataLabels">none</option>

<option name="charting.chart.stackMode">default</option>

<option name="charting.drilldown">none</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

</row>

<row>

<panel>

<title>File Egressed by the User</title>

<table>

<title>The list below is ALL the deduplicated files the user egressed during the above mentioned time period. The deduplication is based on the filename (first column)+ the potentiality the file contains Personal Identifiable Information (related to our PII controls) that may pose a Privacy Risk + the classification of the file (also based on our controls supporting business requirements)+ the time at which this event happen</title>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval PII\_der=if(Control="All DLP Policies" OR Control="COVID-19 Vaccination Certificates AUS" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="EandC\_ECR Case Report\_BHP 0365" OR Control="EandC\_ECR Case Report\_BHP 0365" OR

Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP Outlook" OR Control="EandC\_ECR Case Report\_BHP SharePoint" OR Control="GAS HR SAP Extract (excluding salary information)\_001" OR Control="GAS HR SAP Extract (excluding salary information)\_CE" OR Control="GAS HR SAP Extract (including salary information)" OR Control="GAS HR SAP Extract (including salary information)\_\_Int. Emai" OR Control="GAS HR SAP Extract (including salary information)\_001" OR Control="HSE Documents" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP SharePoint" OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_ALL" OR Control="HSE\_Sensitive Documents\_BHP 0365" OR Control="HSE\_Sensitive Documents\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_BHP Outlook" OR Control="HSE\_Sensitive Documents\_BHP SharePoint" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_ALL" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP 0365" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP One Drive" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Outlook" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Sharepoint" OR Control="Human Resources\_BHP Employee Number\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number\_BHP Outlook" OR Control="Human Resources\_BHP Employee Number\_BHP SharePoint" OR Control="Human Resources\_BHP Employee Number\_WebEx" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP SharePoint" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP Outlook" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_ALL" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP SharePoint" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP 0365" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract\_modified - Including salary information\_BHP SharePoint" OR Control="Human Resources\_Compensation and Tax Documents\_BHP WebEx" OR Control="Human Resources\_Compensation and Tax Documents\_BHP OneDrive" OR Control="Human Resources\_Compensation and Tax Documents\_BHP Outlook" OR Control="Human Resources\_Compensation and Tax Documents\_BHP SharePoint" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_ALL" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP 0365" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP OneDrive" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP Outlook" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP SharePoint" OR Control="Human Resources\_PII Employee Information \_ALL" OR Control="Human Resources\_PII Employee Information \_BHP 0365" OR Control="PII Employee Information\_001" OR Control="PII Employee Information\_001\_Int. Email" OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook","May Contain PII","-")

|eval PII=if(PII\_der="-","-",PII\_der+" ( "+ Match\_Count+" hits)")

|eval classification= if(Control="GAS HR SAP Extract (excluding salary information)\_001" OR like(Control,"Human Resources\_BHP Employee SAP Extract - Excluding salary%") OR Policy\_Rule="Titus Confidential Metadata", "Confidential",if(Control="-" OR Control="Copyrighted Content" OR Control="DEFAULT\_CASE\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR like(Control,"GEN\_Copyrighted Content%") OR like(Control,"GEN\_Offensive languages and conversation%") OR Control="MONITOR\_CUSTOMCAT\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR Control="Transfer to Network Share Activity Monitoring" OR Control="USB device | File and Folder Access Attempts" OR Control="USB Removable Media Data Transfer Warning" OR like(Control,"GEN\_Outlook fil%"),"n/c",if(like(Control,"BHP Classification: Confidenti%") OR like(Control,"GEN\_BHP Classified Confidential%") OR like(Control,"Human Resources\_BHP Employee Number%") OR like(Control,"Human Resources\_Passports - Driving Licenses - SS Cards%") OR like(Control,"Human Resources\_PII Employee Information%") OR like(Control,"PII Employee Information\_0%") OR like(Control,"BHP Classification: Confidential%")OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365","Sugg'ed Confidential",if(Control="All DLP Policies" OR like(Control,"BHP Classification: Highly Confidenti%") OR Control="Credentials" OR Control="Credentials\_CE" OR Control="ELT Reports" OR like(Control,"External Affairs\_M and A Project Codes%") OR like(Control,"GEN\_BHP Classified Highly Confidential%") OR like(Control,"GEN\_Credentials%")OR like(Control,"Human Resources\_BHP Employee SAP Extract \_modified - Including salary information%") OR Control="M&amp;A Project Codes" OR Control="M&amp;A Project Codes\_CE" OR Control="All DLP Policies","Sugg'ed Highly Confidential",if(like(Control,"COVID-19 Vaccination Certificates A%") OR like(Control,"EandC\_ECR Case Report\_BHP%") OR like(Control,"GAS HR SAP Extract %") OR Control="ELT Reports\_CE" OR like(Control,"GEN\_ELT-RAC Materials - papers%") OR like(Control,"HSE\_Card Access Data WAIO and BMA\_BHP%") OR Control="HSE Documents" OR like(Control,"MINAUS\_Yandi Mine Integrated Operational Plan%") OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR like(Control,"HSE\_Sensitive Documents%") OR like(Control,"PS and D\_ELT-RAC Materials - papers%") OR like(Control,"PS and D\_Monthly Update Report%") OR like(Control,"PS&amp;D\_Capital Prioritisati%") OR like(Control,"Reporting\_ELT Report%") OR like(Control,"Supply\_NGO Sensitive Documents%") OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook"

OR Control="PS&amp;D\_BHP Asset Summary Model Submission" OR like(Control,"HSEC\_COVID-19 Exposure Tracking Report%") OR like(Control,"Human Resources\_BHP Employee SAP Extract - Including salary information%") OR like(Control,"Human Resources\_Compensation and Tax Documents\_BHP%") OR like(Control,"MINAUS\_High Level Design Documentation\_BHP%") OR like(Control,"MINAUS\_Reporting\_BMA Matrix%") OR like(Control,"PS and D\_5YP Appraisal Report\_%") OR like(Control,"PS and D\_BHP Asset Summary Model Submission%") OR like(Control,"PS and D\_Business Development\_Acquisitions and Divestments%") OR like(Control,"PS and D\_Capital Prioritisation%") ,"Highly Confidential"," ")))))

|search Scope="EGRESS" AND Files!="No\_Attachment" AND Files!="" |stats values(PII) as PII values(classification) as Classification values(Timestamp) count by Files |fields - count</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="drilldown">none</option>

<option name="refresh.display">progressbar</option>

</table>

</panel>

</row>

<row>

<panel>

<title>Other Files Handled by the User</title>

<table>

<title>The list below is ALL the deduplicated files the user handled during the time period (access, copy, move, delete, rename, etc..) on our Information System. The deduplication is based on the filename + the potentiality the file contains Personal Identifiable Information (related to our PII controls) that may pose a Privacy Risk + the classification of the file (also based on our controls supporting business requirements)</title>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|eval PII\_der=if(Control="All DLP Policies" OR Control="COVID-19 Vaccination Certificates AUS" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="COVID-19 Vaccination Certificates AUS\_CE" OR Control="EandC\_ECR Case Report\_BHP 0365" OR Control="EandC\_ECR Case Report\_BHP 0365" OR

Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP OneDrive" OR Control="EandC\_ECR Case Report\_BHP Outlook" OR Control="EandC\_ECR Case Report\_BHP SharePoint" OR Control="GAS HR SAP Extract (excluding salary information)\_001" OR Control="GAS HR SAP Extract (excluding salary information)\_CE" OR Control="GAS HR SAP Extract (including salary information)" OR Control="GAS HR SAP Extract (including salary information)\_\_Int. Emai" OR Control="GAS HR SAP Extract (including salary information)\_001" OR Control="HSE Documents" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP 0365" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP OneDrive" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP Outlook" OR Control="HSE\_Card Access Data WAIO and BMA\_BHP SharePoint" OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_ALL" OR Control="HSE\_Sensitive Documents\_BHP 0365" OR Control="HSE\_Sensitive Documents\_BHP OneDrive" OR Control="HSE\_Sensitive Documents\_BHP Outlook" OR Control="HSE\_Sensitive Documents\_BHP SharePoint" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_ALL" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP 0365" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP One Drive" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Outlook" OR Control="HSEC\_COVID-19 Exposure Tracking Report\_BHP Sharepoint" OR Control="Human Resources\_BHP Employee Number\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number\_BHP Outlook" OR Control="Human Resources\_BHP Employee Number\_BHP SharePoint" OR Control="Human Resources\_BHP Employee Number\_WebEx" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP SharePoint" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract - Excluding salary information\_BHP Outlook" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_ALL" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP SharePoint" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP 0365" OR

Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_ALL" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP 0365" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP One Drive" OR Control="Human Resources\_BHP Employee SAP Extract \_modified - Including salary information\_BHP Outlook" OR Control="Human Resources\_BHP Employee SAP Extract\_modified - Including salary information\_BHP SharePoint" OR Control="Human Resources\_Compensation and Tax Documents\_BHP WebEx" OR Control="Human Resources\_Compensation and Tax Documents\_BHP OneDrive" OR Control="Human Resources\_Compensation and Tax Documents\_BHP Outlook" OR Control="Human Resources\_Compensation and Tax Documents\_BHP SharePoint" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_ALL" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP 0365" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP OneDrive" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP Outlook" OR Control="Human Resources\_Passports - Driving Licenses - SS Cards\_BHP SharePoint" OR Control="Human Resources\_PII Employee Information \_ALL" OR Control="Human Resources\_PII Employee Information \_BHP 0365" OR Control="PII Employee Information\_001" OR Control="PII Employee Information\_001\_Int. Email" OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook","May Contain PII","-")

|eval PII=if(PII\_der="-","-",PII\_der+" ( "+ Match\_Count+" hits)")

|eval classification= if(Control="GAS HR SAP Extract (excluding salary information)\_001" OR like(Control,"Human Resources\_BHP Employee SAP Extract - Excluding salary%") OR Policy\_Rule="Titus Confidential Metadata", "Confidential",if(Control="-" OR Control="Copyrighted Content" OR Control="DEFAULT\_CASE\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR like(Control,"GEN\_Copyrighted Content%") OR like(Control,"GEN\_Offensive languages and conversation%") OR Control="MONITOR\_CUSTOMCAT\_12-GlobalCorporate.AP-AuthGeneral.ID-NONE-NONE-NONE-DefaultGroup-NONE" OR Control="Transfer to Network Share Activity Monitoring" OR Control="USB device | File and Folder Access Attempts" OR Control="USB Removable Media Data Transfer Warning" OR like(Control,"GEN\_Outlook fil%"),"n/c",if(like(Control,"BHP Classification: Confidenti%") OR like(Control,"GEN\_BHP Classified Confidential%") OR like(Control,"Human Resources\_BHP Employee Number%") OR like(Control,"Human Resources\_Passports - Driving Licenses - SS Cards%") OR like(Control,"Human Resources\_PII Employee Information%") OR like(Control,"PII Employee Information\_0%") OR like(Control,"BHP Classification: Confidential%")OR Control="GEN\_BHP Classified Confidential\_BHP OneDrive" OR Control="Human Resources\_BHP Employee Number \_BHP 0365","Sugg'ed Confidential",if(Control="All DLP Policies" OR like(Control,"BHP Classification: Highly Confidenti%") OR Control="Credentials" OR Control="Credentials\_CE" OR Control="ELT Reports" OR like(Control,"External Affairs\_M and A Project Codes%") OR like(Control,"GEN\_BHP Classified Highly Confidential%") OR like(Control,"GEN\_Credentials%")OR like(Control,"Human Resources\_BHP Employee SAP Extract \_modified - Including salary information%") OR Control="M&amp;A Project Codes" OR Control="M&amp;A Project Codes\_CE" OR Control="All DLP Policies","Sugg'ed Highly Confidential",if(like(Control,"COVID-19 Vaccination Certificates A%") OR like(Control,"EandC\_ECR Case Report\_BHP%") OR like(Control,"GAS HR SAP Extract %") OR Control="ELT Reports\_CE" OR like(Control,"GEN\_ELT-RAC Materials - papers%") OR like(Control,"HSE\_Card Access Data WAIO and BMA\_BHP%") OR Control="HSE Documents" OR like(Control,"MINAUS\_Yandi Mine Integrated Operational Plan%") OR Control="HSE\_COVID-19 Certificates\_BHP OneDrive" OR Control="HSE\_COVID-19 Digital Certificate\_BHP OneDrive" OR like(Control,"HSE\_Sensitive Documents%") OR like(Control,"PS and D\_ELT-RAC Materials - papers%") OR like(Control,"PS and D\_Monthly Update Report%") OR like(Control,"PS&amp;D\_Capital Prioritisati%") OR like(Control,"Reporting\_ELT Report%") OR like(Control,"Supply\_NGO Sensitive Documents%") OR Control="MINAUS\_High Level Design Documentation" OR Control="BMA Matrix Result" OR Control="HSE\_COVID-19 Digital Certificate\_BHP Outlook"

OR Control="PS&amp;D\_BHP Asset Summary Model Submission" OR like(Control,"HSEC\_COVID-19 Exposure Tracking Report%") OR like(Control,"Human Resources\_BHP Employee SAP Extract - Including salary information%") OR like(Control,"Human Resources\_Compensation and Tax Documents\_BHP%") OR like(Control,"MINAUS\_High Level Design Documentation\_BHP%") OR like(Control,"MINAUS\_Reporting\_BMA Matrix%") OR like(Control,"PS and D\_5YP Appraisal Report\_%") OR like(Control,"PS and D\_BHP Asset Summary Model Submission%") OR like(Control,"PS and D\_Business Development\_Acquisitions and Divestments%") OR like(Control,"PS and D\_Capital Prioritisation%") ,"Highly Confidential"," ")))))

|eval Exposure=if(Scope="Egress","External",if(Action\_Final="Save to local drive","Private",if(Document\_Exposure="private","Private","Internal")))|search Scope!="EGRESS" AND Files!="No\_Attachment" AND Files!="" |stats values(PII) as PII Values(Exposure) as Exposure values(classification) as classification count by Files |fields - count</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="drilldown">none</option>

<option name="refresh.display">progressbar</option>

</table>

</panel>

</row>

<row>

<panel>

<title>(Potential)Risky Activity</title>

<table>

<title>The list below is ALL actions performed by the user on internal resources (Sharepoint, OneDrive, Local drive, fileservers, etc...) When a control is specified , it means the file triggered one of the controls we deployed to protect BHP data - it is an indication that the file potentially contains sensitive patterns. Despite the fact that these files stayed on our Information System, "Action\_Final" describes what the user did with the data - it gives the indication the user may have 1/ accessed sensitive data he/she is not supposed to access, 2/ modified/deleted data (introducing a potential risk of integrity), 3/ copied or moved data to wrong/unauthorized internal locations."</title>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Destination=split(Destination,",")

|mvexpand Destination

| rex field=Destination "\/\/(?:[^@\/\n]+@)?(?:www\.)?(?&lt;New\_Destination&gt;[^:\/\n]+)"

| rex field=Destination "\@(?&lt;domain&gt;[^ ]\*)"

|eval Domain=domain

|eval dest=if(like(Destination,"qagpublic.qg2.apps.qualys.com%"),"qagpublic.qg2.apps.qualys.com",if(like(Destination,"www.youtube.com%"),"youtube.com",if(like(Destination,"spo.bhpbilliton.com%"),"spo.bhpbilliton.com",if(like(Destination,"%sharepoint.com%"),"sharepoint.com",if(like(Destination,"mysite.bhpbilliton.com%"),"mysite.bhpbilliton.com",if(like(Destination,"mail.google.com%"),"mail.google.com",if(isnull(New\_Destination),Destination,New\_Destination)))))))

|eval Destination\_domain=if(Vector="email" AND isnull(Destination),"Unknown\_recipient",if(Vector="email",replace(Destination," ",","),if(Action="View" AND isnull(Destination),"Unknown Source",if(Action="Print","Unidentified Printer",if(Action="Download","Unidentified Destination",if(Action="Edit",Destination,if(app\_activity="FileAccessed" OR app\_activity="FileModified" OR app\_activity="PageViewed" OR app\_activity="FilePreviewed" OR app\_activity="FileDownloaded","User's Endpoint",if(app\_activity="FilesyncDownloadedFull" OR app\_activity="FilesyncUploadedFull" OR app\_activity="FileDeletedFirstStageRecycleBin" OR app\_activity="FolderDeletedFirstStageRecycleBin" OR app\_activity="FolderDeleted" OR app\_activity="FileDeleted" OR app\_activity="FolderCreated" OR app\_activity="FolderRenamed" OR app\_activity="FileRenamed" OR app\_activity="FileUploaded","0365 Sync Client",dest))))))))

|eval Final\_Destination=if(isnull(Domain),Destination\_domain,Domain)

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|search Files!=No\_Attachment AND Files!="" | dedup Timestamp, Vector\_Final, Scope, Action\_Final, Risk\_Rating, Files, Control, Final\_Destination, Subject| table Timestamp Vector\_Final Scope Action\_Final Risk\_Rating Files Control Final\_Destination Subject |where Risk\_Rating="Potential"</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="drilldown">none</option>

<option name="refresh.display">progressbar</option>

<option name="wrap">false</option>

</table>

</panel>

</row>

<row>

<panel>

<title>Risky Activity</title>

<table>

<title>The list below is ALL actions performed by the user through the different egress channels (USB, upload to internet, emails, CD/DVD, etc…). When a control is specified, it means the file triggered one of the controls we deployed to protect BHP data - it is an indication that the file potentially contains sensitive patterns</title>

<search>

<query>index IN(bhp\_sec\_gl\_cloud,bhp\_res\_gl\_netskope, bhp\_sec\_gl\_malware, bhp\_res\_gl\_symantecdlp)

(index=bhp\_res\_gl\_symantecdlp sourcetype="symantec:dlp:syslog" protocol\_device IN ("Endpoint Email/SMTP" "SMTP" "Endpoint Removable Storage Device" "Endpoint HTTP" "Endpoint HTTPS" "Endpoint FTP" "Endpoint Printer/Fax" "Endpoint Local Drive" "Endpoint Copy to Network Share" "Endpoint CD/DVD" "Endpoint Cloud Storage")) OR (sourcetype=pps\_messagelog NOT envelope.rcpts{} IN ("\*@bhp.com\*","\*@bhpbilliton.com\*") NOT final\_action=discard) OR (sourcetype="symantec:ep:behavior:file" \*write\*)

| fillnull value="N/A" url

| fillnull value="No\_instance\_id" instance\_id

| eval url1=if(url="N/A",instance\_id,url)

| fillnull value="No\_object" object

| fillnull value="No\_destinationhost" dsthost

| eval object=case(object="null",No\_object,object="Null",No\_object,object="NULL",No\_object,1=1,object)

| strcat "Application is \*" app "\* its category is \*" appcategory "\* and destination is - " dsthost ". The file type is \*" object\_type "\* and file is - " object explanationofactivity

| fillnull value="N/A" alert\_name

| fillnull value="N/A" policy

| fillnull value="N/A" policy\_name

| fillnull value="No\_app\_activity" app\_activity

| rex field=\_raw "(?ms)^(?:[^ \\n]\* ){6}(?P&lt;Begin\_Time&gt;[^,]+)"

| eval user=if(isnotnull(user\_name), user\_name,user)

| rename msgParts{}.labeledName as file\_name1,msgParts{}.detectedSizeBytes as filesize,envelope.from as sender1, envelope.rcpts{} as recipients1,msg.header.subject{} as subject , connection.ip as src\_ip\_pps,connection.country as src\_country

| rex field=\_raw "(\"labeledName\"\:\s\"(?&lt;file\_name2&gt;[^\",]+)\"\,\s)"

| eval file\_name=coalesce(file\_name1,file\_name2)

| fillnull value="No\_src\_country" src\_country

| fillnull value="No\_src\_location" src\_location

| fillnull value="No\_srcip" srcip

| fillnull value="N/A" dlp\_incident\_id

| fillnull value="No\_dstip" dstip

| rex field=\_raw "occurred\_on=(?&lt;occurred\_date&gt;.\*), policy\_name="

| eval newdate=strptime(occurred\_date,"%B %d, %Y %I:%M:%S %p")

| eval DlpTime1=newdate+46800

| eval DlpTime=strftime(DlpTime1,"%d/%m/%Y %H:%M:%S")

| rex field=\_raw "attachment\_file\_name=(?&lt;attachment\_file\_namex&gt;.\*?), blocked="

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "\sfile\_name=(?&lt;file\_namex&gt;.\*?),\s"

| rex field=\_raw "Module\sName\,\D\:\/(?&lt;ModuleName&gt;[^\,]+)"

| rex field=\_raw "Module\sName\,(?&lt;Source1&gt;[^\,]+)\,User\sName\:\s(?&lt;User1&gt;[^\,]+)"

| rex field=\_raw "Caller MD5=(?&lt;Caller\_ID&gt;[^\,]+)\,File\s(?&lt;action2&gt;[^\,]+)\,Begin:\s(?&lt;Begin\_Time&gt;[^\,]+)\,End\sTime:\s(?&lt;End\_Time&gt;[^\,]+)\,Rule:\s(?&lt;Rule&gt;[^\,]+)"

| rex field=\_raw "File\ssize\s\(bytes\)\:\s(?&lt;file\_size2&gt;[^\,]+)\,Device ID:\s(?&lt;DeviceID&gt;(.\*))"

| rex field=\_raw "blocked=(?&lt;action1&gt;.\*), data\_owner="

| rex field=\_raw "recipients=(?&lt;recipients1&gt;.\*), reported\_on="

| eval starttime1=strptime(Begin\_Time,"%Y-%m-%d %H:%M:%S") | eval starttime2=starttime1+46800 | eval Start\_Time=strftime(starttime2,"%d/%m/%Y %H:%M:%S")

| eval endpoint\_username=if(endpoint\_username="N/A",sender,endpoint\_username)

| eval Filename = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint Copy to Network Share", file\_namex, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP" OR protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint CD/DVD" OR protocol\_device="Endpoint Cloud Storage" OR protocol\_device="SMTP", attachment\_file\_namex, access\_method="Client", url, access\_method="API Connector", file\_path)

| eval Filename = if(host="bhp.goskope.com", object, Filename)

| eval Filename = if(sourcetype="pps\_messagelog", file\_name, Filename)

| eval Filename = if(sourcetype="symantec:ep:behavior:file",ModuleName, Filename)

| rex mode=sed field=Filename "s/^[+|-]/'/g"

| rex field=\_raw "(?ms)^[^=\\n]\*=(?P&lt;Caller\_ID&gt;[^,]+),File (?P&lt;action2&gt;\\w+)(?:[^ \\n]\* ){6}(?P&lt;Rule&gt;[^,]+)"

| eval User = case(host="bhp.goskope.com", user, sourcetype="symantec:dlp:syslog",endpoint\_username, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",User1)

| eval User=lower(User)

| eval Vector = case(host="bhp.goskope.com", "Cloud Storage", sourcetype="symantec:dlp:syslog",protocol\_device, sourcetype="pps\_messagelog","Email",sourcetype="symantec:ep:behavior:file","Endpoint Removable Storage Device") | eval Source = case(host="bhp.goskope.com", srcip, sourcetype="symantec:dlp:syslog", endpoint\_machine, sourcetype="pps\_messagelog", sender1,sourcetype="symantec:ep:behavior:file",Source1) | eval DestinationIP = if(host="bhp.goskope.com", dstip, "N/A")|fillnull value="N/A" DestinationIP|fillnull value="N/A" access\_method | eval Action = case(host="bhp.goskope.com", activity, sourcetype="symantec:dlp:syslog", action1 ,sourcetype="pps\_messagelog", final\_action,sourcetype="symantec:ep:behavior:file",action2) | eval Policy = case(host="bhp.goskope.com", policy, sourcetype="symantec:dlp:syslog", policy\_name ,sourcetype="pps\_messagelog", "N/A",sourcetype="symantec:ep:behavior:file",Rule) | eval Incident\_ID = if(host="bhp.goskope.com", dlp\_incident\_id, incident\_ID)| eval Incident\_ID= if(sourcetype="symantec:ep:behavior:file",Caller\_ID, "N/A")| rex field=\_raw "subject=(?&lt;subject&gt;.\*), target=" | eval Subject = if(isnull(subject), "N/A", subject) | eval File\_Size1 = round((file\_size / 1024 ), 3)|eval File\_Size2=round((filesize/1024), 3)|eval File\_Size3=round((file\_size2/1024), 3)|eval pwd\_protected=coalesce(file\_password\_protected,file\_passwd\_protected) | eval Encryption=if(pwd\_protected="yes","YES","NO") | eval Timestamp = strftime(\_time,"%d/%m/%Y %H:%M:%S") | eval Timestamp = if(sourcetype="symantec:dlp:syslog", DlpTime, Timestamp)|eval Timestamp = if(sourcetype="symantec:ep:behavior:file", Start\_Time, Timestamp)| eval Destination = case(protocol\_device="Endpoint Printer/Fax" OR protocol\_device="Endpoint Removable Storage Device" OR protocol\_device="Endpoint CD/DVD", device\_instance\_ip, protocol\_device="Endpoint Email/SMTP" OR protocol\_device="SMTP" OR protocol\_device="Endpoint HTTP" OR protocol\_device="Endpoint HTTPS" OR protocol\_device="Endpoint FTP", recipients1, protocol\_device="Endpoint Copy to Network Share", file\_full\_path, protocol\_device="Endpoint Local Drive" OR protocol\_device="Endpoint Cloud Storage", file\_parent\_directory\_path, access\_method="Client" OR access\_method="API Connector", if(url = "N/A", shared\_with, url), sourcetype="pps\_messagelog", recipients1,sourcetype="symantec:ep:behavior:file",DeviceID)

| search User IN("\*galvgr\*","\*greg.galvin@bhp.com\*")

| eval Activity\_Type= case(sourcetype="symantec:ep:behavior:file","Data\_Sent\_Externally",match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com") OR match(Action,"View") OR match(Action,"Edit") OR match(Action,"Delete") OR match(Action,"Restore") OR match(Action,"Rename"),"Data\_is\_Internal",match(Destination,"C:"),"Data\_is\_Internal",match(policy\_name,"USB Removable Media Data Transfer Warning") OR match(policy\_name,"Printing Activity Monitoring") OR match(policy\_name,"Endpoint CD/DVD"),"Data\_Sent\_Externally",match(Action,"Download") AND match(access\_method,"custom-splunkigw"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"Client"),"Data\_is\_Internal",match(Source,"145.34.128.") OR match(Source,"145.34.129.") OR match(Source,"145.34.130.") OR match(Source,"145.34.131.") OR match(Source,"145.34.132.") OR match(Source,"145.34.133.") OR match(Source,"145.34.134.") OR match(Source,"145.34.135.") OR match(Source,"145.34.136.") OR match(Source,"145.34.137.") OR match(Source,"145.34.138.") OR match(Source,"145.34.139.") OR match(Source,"145.34.140.") OR match(Source,"145.34.141.") OR match(Source,"145.34.142.") OR match(Source,"145.34.143.") OR match(Source,"145.34.0.") OR match(Source,"145.34.1.") OR match(Source,"145.34.4.") OR match(Source,"145.34.5.") OR match(Source,"145.34.112.") OR match(Source,"145.34.113.") OR match(Source,"103.108.252.") OR match(Source,"103.108.253.") OR match(Source,"4.14.205.") OR match(Source,"64.125.43.") OR match(Source,"180.167.229.") OR match(Source,"45.250.160.") AND match(access\_method,"API Connector"),"Data\_is\_Internal", match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileSyncDownloaded"),"Data\_is\_Internal",match(Action,"Download") AND match(access\_method,"API Connector") AND match(app\_activity,"FileDownloaded"),"Review\_the\_Data",match(Destination,"spo.bhpbilliton.com") AND match(policy\_name,"Upload Activity Monitoring"),"Data\_is\_Internal",match(explanationofactivity,"atlassian.net"),"Data\_is\_Internal",match(explanationofactivity,"concursolutions.com"),"Data\_is\_Internal",match(url1,"blob.core.windows.net") OR match(url1,"mysite.bhpbilliton.com") OR match(url1,"spo.bhpbilliton.com") OR match(url1,"bhp.service-now.com") OR match(url1,"api.powerapps.com") OR match(Destination,"case.bhpbilliton.com") OR match(Destination,"wbx2.com") OR match(Destination,"ciscospark.com") OR match(Destination,"ciscospark.com") OR match(Destination,"concursolutions.com") OR match(Destination,"bhp.service-now.com") OR match(Destination,"spo.bhpbilliton.com") OR match(Destination,"mysite.bhpbilliton.com") OR match(Destination,"bhpbilliton.net"),"Data\_is\_Internal", NOT (match(Destination,"@bhp.com") OR match(Destination,"@bhpbilliton.com")),"Data\_Sent\_Externally")

| rex field=\_raw "user\_justification=(?P&lt;User\_Justification&gt;.[^,]+)"

| eval User\_Justification=case(sourcetype="symantec:dlp:syslog", User\_Justification,1=1,"NA")

| eval Source\_File=case(sourcetype="symantec:dlp:syslog", file\_full\_path,1=1,"N/A")

| eval Document\_Exposure=case(sourcetype="netskope:application", exposure, sourcetype="netskope:connection", exposure, sourcetype="netskope:alert", exposure, sourcetype="netskope:clients", exposure, sourcetype="netskope:audit", exposure)|fillnull Document\_Exposure value="N/A"

| eval DLP\_Profile=case(sourcetype="netskope:application", dlp\_profile, sourcetype="netskope:connection", dlp\_profile, sourcetype="netskope:alert", dlp\_profile, sourcetype="netskope:clients", dlp\_profile, sourcetype="netskope:audit", dlp\_profile)|fillnull DLP\_Profile value="N/A"

| eval Policy\_Rule=case(sourcetype="symantec:dlp:syslog",policy\_rule,match(sourcetype,"netskope:\*"),dlp\_rule)|fillnull Policy\_Rule value="N/A"

| eval Match\_Count=case(sourcetype="symantec:dlp:syslog",match\_count,match(sourcetype,"netskope:\*"),dlp\_rule\_count)|fillnull Match\_Count value="N/A"

| eval File\_Size =coalesce(File\_Size1,File\_Size2,File\_Size3 )

|eval DLP\_Hit= if(Policy IN("N/A","Upload Activity Monitoring","Printing Activity Monitoring")," ","DLP")

|eval destination=replace(Destination, "@", "")|eval Email\_Recipients=if(isnull(Destination),"0",len(Destination)- len(destination))

|eval E=replace(Destination, "@bhp", "")|eval External\_Recipients= (len(Destination)- len(destination))- (len(Destination)-len(E))/4

|eval File= replace(replace(replace(replace(replace(replace(Filename,"text.txt",""),"text.html",""),"text-calendar",""),"image001.png",""),"No\_object",""),"image002.png","") |eval Files=if((isnull(Action) OR Action="Continue"),"No\_Attachment",if(File="","No\_Attachment",if(File=" ","No\_Attachment",File)))

|eval Control= if(DLP\_Hit="DLP",Policy,"-")

|eval Scope= if(like(Destination,"%qualys%"),"EXCEPTION",if(like(Destination,"spo.bhpbilliton%") OR like(Destination,"mysite.bhpbilliton%") OR like(Destination,"%bhp.com%") OR like(Destination,"%teams.microsoft.com%") OR like(Destination,"%pageup.people.com%"),"INTERNAL",if((Activity\_Type="Data\_is\_internal"AND access\_method="Client"AND Action="Upload")OR(Activity\_Type="Data\_Sent\_Externally") OR (External\_recipients&gt;0),"EGRESS","INTERNAL")))

|eval Attachment=if(Files="No\_Attachment","No","Yes")

|eval conca= Scope+DLP\_Hit+Attachment |eval risk=if(conca="INTERNAL Yes" OR conca="INTERNAL No" OR conca="EXCEPTION Yes" OR conca="EXCEPTION No" OR conca="EXCEPTIONDLPYes" OR conca="EXCEPTIONDLPNo","No Risk",if(conca="EGRESSDLPYes" OR conca="EGRESSDLPNO","High",if(conca="INTERNALDLPYes" OR conca="INTERNALDLPNo","Potential",if(conca="EGRESS Yes","Medium","Low"))))

|eval Risk\_Rating=if(Encryption="YES","Encrypted",if(Action="View","Potential",if(Encryption="YES","Encrypted",if(Vector="Network Share" OR Action="Delete","Potential",if(Action="reject" OR Action="User Notified User:Cancelled" OR Action="User Notified,Timeout:Cancelled" OR Action="Action Blocked","Blocked",risk)))))

|eval Vector\_Final=if(Vector="Endpoint Email/SMTP" OR Vector="Email" OR Vector="SMTP","Email",if(Vector="Endpoint HTTPS" OR Vector="Endpoint Cloud Storage" OR Vector="Endpoint HTTP","Web/Cloud",if(Vector="Endpoint Removable Storage Device","Removable Storage Device",if(Vector="Endpoint Local Drive","Local Drive",if(Vector="Endpoint Printer/Fax","Printer/Fax",if(Vector="Endpoint Copy to Network Share","Network Share",Vector))))))

|eval Action\_Key= Action+Email\_Recipients+Vector\_Final

|eval Destination=split(Destination,",")

|mvexpand Destination

| rex field=Destination "\/\/(?:[^@\/\n]+@)?(?:www\.)?(?&lt;New\_Destination&gt;[^:\/\n]+)"

| rex field=Destination "\@(?&lt;domain&gt;[^ ]\*)"

|eval Domain=domain

|eval dest=if(like(Destination,"qagpublic.qg2.apps.qualys.com%"),"qagpublic.qg2.apps.qualys.com",if(like(Destination,"www.youtube.com%"),"youtube.com",if(like(Destination,"spo.bhpbilliton.com%"),"spo.bhpbilliton.com",if(like(Destination,"%sharepoint.com%"),"sharepoint.com",if(like(Destination,"mysite.bhpbilliton.com%"),"mysite.bhpbilliton.com",if(like(Destination,"mail.google.com%"),"mail.google.com",if(isnull(New\_Destination),Destination,New\_Destination)))))))

|eval Destination\_domain=if(Vector="email" AND isnull(Destination),"Unknown\_recipient",if(Vector="email",replace(Destination," ",","),if(Action="View" AND isnull(Destination),"Unknown Source",if(Action="Print","Unidentified Printer",if(Action="Download","Unidentified Destination",if(Action="Edit",Destination,if(app\_activity="FileAccessed" OR app\_activity="FileModified" OR app\_activity="PageViewed" OR app\_activity="FilePreviewed" OR app\_activity="FileDownloaded","User's Endpoint",if(app\_activity="FilesyncDownloadedFull" OR app\_activity="FilesyncUploadedFull" OR app\_activity="FileDeletedFirstStageRecycleBin" OR app\_activity="FolderDeletedFirstStageRecycleBin" OR app\_activity="FolderDeleted" OR app\_activity="FileDeleted" OR app\_activity="FolderCreated" OR app\_activity="FolderRenamed" OR app\_activity="FileRenamed" OR app\_activity="FileUploaded","0365 Sync Client",dest))))))))

|eval Final\_Destination=if(isnull(Domain),Destination\_domain,Domain)

|eval Action\_Final=if(Action\_Key="Introspection Scan0Cloud Storage" OR like(Action\_Key,"Read%Removable Storage Device") OR like(Action\_Key,"View%Cloud Storage"),"View",if(like(Action\_Key,"%Removable Storage Device"),"Copy to Removable Media",if(like(Action\_Key,"Create%Cloud Storage"),"Create",if(like(Action\_Key,"Delete%"),"Delete",if(like(Action\_Key,"Download%Cloud Storage"),"Download",if(like(Action\_Key,"Edit%Cloud Storage"), "Edit",if(like(Action\_Key,"None%Network Share"),"Network share",if(like(Action\_Key,"None%Printer/Fax"),"Print",if(like(Action\_Key,"reject%Email"),"reject",if(like(Action\_Key,"Rename%Cloud Storage"),"Rename",if(like(Action\_Key,"Restore%Cloud Storage"),"restore",if(like(Action\_Key,"None%Local Drive"),"Save to Local drive",if(like(Action\_Key,"%Web/Cloud") OR like(Action\_Key,"Upload%Cloud Storage"), "Upload",if(like(Action\_Key,"Share%Cloud Storage"),"Share",if(like(Action\_Key,"%Email") OR like(Action\_Key,"Introspection Scan%Cloud Storage"),"Send Email",if(like(Vector\_Final,"%Endpoint FTP"),"Transfer via S/FTP","-"))))))))))))))))

|search Files!=No\_Attachment AND Files!="" | dedup Timestamp, Vector\_Final, Scope, Action\_Final, Risk\_Rating, Files, Control, Final\_Destination, Subject

| table Timestamp Vector\_Final Scope Action\_Final Risk\_Rating Files Control Final\_Destination Subject |where Risk\_Rating!="Potential" AND Risk\_Rating!="No Risk" AND Risk\_Rating!="Low"|fillnull value=0 Final\_Destination |sort Risk\_Rating</query>

<earliest>-7d@d</earliest>

<latest>-6d@d</latest>

</search>

<option name="drilldown">none</option>

<option name="refresh.display">progressbar</option>

<option name="wrap">false</option>

</table>

</panel>

</row>

</dashboard>