**KVP Master List**

* **Active Directory Admin**

timestamp

source\_user

target\_user

source\_user\_domain

target\_user\_domain

action

source\_account

target\_account

source\_data

* **Asset Authentication**

timestamp

source\_asset

destination\_asset

source\_asset\_address

destination\_asset\_address

source\_local\_account

destination\_local\_account

logon\_type

result

new\_authentication

service

source\_data

* **Cloud Service Activity**

timestamp

source\_user

target\_user

service

action

source\_account

source\_data

* **Cloud Service Admin Activity**

timestamp

source\_user

target\_user

service

action

source\_account

target\_account

user\_agent

source\_data

* **DNS Query**

timestamp

asset

user

source\_address

query

public\_suffix

top\_private\_domain

source\_data

* **Endpoint Query**
* **Exploit Mitigation Alert**
* **External Detection Alert**
* **File Access Activity**
* **File Modification Activity**

timestamp

user

account

asset

asset\_address

asset\_os\_family

file\_event

file\_path

file\_name

file\_extension

process

process\_id

source\_json

sourceName

insertionStrings

eventCode

computerName

sid

isDomainController

* **Firewall Activity**

timestamp

asset

user

source\_address

source\_port

destination\_address

destination\_port

direction

incoming\_bytes

outgoing\_bytes

geoip\_organization

geoip\_country\_code

geoip\_country\_name

geoip\_city

geoip\_region

source\_data

* **Host to IP Observation**

timestamp

asset

action

host

ip

observation\_status

source\_data

* **IDS Alert**
* **Ingress Auth**

timestamp

user

account

result

source\_ip

service

geoip\_organization

geoip\_country\_code

geoip\_country\_name

geoip\_city

geoip\_region

source\_data

* **Raw Log**
* **SSO Authentication**

timestamp

user

account

source\_ip

service

sso\_provider

geoip\_organization

geoip\_country\_code

geoip\_country\_name

geoip\_city

geoip\_region

source\_data

* **Unparsed Data**
* **Virus Alert**

timestamp

asset

user

source\_address

account

risk

action

source\_data

* **Web Servers**
* groupby(geoip\_country\_name)
* where(status) groupby(status) calculate(count) sort(desc) limit(350)
* <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4768>
* where(destination\_account="exagent")groupby(source\_asset)
* where(result!="SUCCESS")groupby(result)
* service="vpn" AND result="SUCCESS" AND geoip\_country\_name!="United States"
* groupby(geoip\_country\_name)
* where(geoip\_country\_name=/GB|NL/)groupby(service)
* where(geoip\_country\_name=/GB|NL/)groupby(geoip\_organization\_name)
* where(Christopher Chung) or case insensitive with where(/christopher chung/i)
* where(result AND result!="SUCCESS)groupby(result)
* where(result AND result=/failed.\*/i)groupby(result)
* where(geoip\_country\_code!="US") groupby(geoip\_country\_name) sort(desc)
* where(stuff AND stuff)
* where(stuff OR stuff)
* where((stuff AND stuff) OR stuff)

DNS

* where(result AND result!="SUCCESS)groupby(result)
* where(result AND result=/fail\*/i)groupby(result)
* where(result AND result!="SUCCESS)groupby(result)
* where(result AND result=/failed.\*/i)groupby(result)
* where((public\_suffix != com AND public\_suffix != net AND public\_suffix != org) AND (user!=InsightIDR AND user!=unknown) groupby(user)
* where((public\_suffix != com AND public\_suffix != net AND public\_suffix != org) AND (user!=InsightIDR AND user!=unknown)) groupby(user)
* where(/facebook/ AND user!=unknown)groupby(user)sort(desc)
* where(/sophosxl/)calculate(count)
* where(result!=SUCCESS)
* where(/src\_country\_code/)
* where(/src\_country\_code/ AND NOT /USA/)
* where(/src\_country\_code/ AND NOT /USA/ AND NOT /\=R1/)
* where(/src\_country\_code/ AND NOT /USA/ AND NOT /\=R1/ AND NOT /src\_country\_code\=\s/)
* where(/src\_country\_code/ AND NOT /USA/ AND NOT /\=R1/ AND NOT /\\_code\=\s/)

Blanks

* where(/src\_country\_code/ AND /code\=\s/)
* where(/src\_country\_code/ AND /code\=\s/)
* where(/src\_country\_code/ AND NOT /code\=\s/ AND /\=R1/ AND /USA/)
* where(/src\_country\_code/ AND NOT /code\=\s/ OR NOT /\=R1/ OR NOT /USA/)
* where(/src\_country\_code/ AND NOT /code\=\s/ OR (NOT /\=R1/ AND NOT /USA/))
* where(/src\_country\_code/ AND NOT /code\=\s/ OR (NOT /R1/ AND NOT /USA/))
* where(/src\_country\_code/ AND NOT /code\=\s/ (NOT /\=R1/ OR NOT /USA/))

• Partial word match is formatted as where(/bleed/)

• If you want case insensitive - where(/bleed/i)

• Fields are designated with quotes

• Using fields - where(severity=high/i)

• To see all severities - groupby(severity)

• To count values - where(China) calculate(count)

• Sum firewall activity - where(direction=INBOUND)groupby(source\_address)calculate(sum:incoming\_bytes)sort(desc)

• Active Directory admin activity - Want to see who created all the accounts in the past 30 days

     Where(action=/account/i) groupby(source\_user)

**Queries Provided**

*Asset Authentication*

* where(action=”MEMBER\_ADDED\_TO\_SECURITY\_GROUP” AND group="domain admins")groupby(target\_user)

*DNS Query*

* where(/facebook/ AND user!="unknown")groupby(user)

# Facebook is just one example here as a site that people could be visiting #

* where(public\_suffix="ru")groupby(query)sort(desc)

# This query will provide any websites from Russia #

*Firewall Activity*

* where(geoip\_country\_name!="United States")groupby(geoip\_country\_name)

# This is showing all traffic going outside the US #

* where(direction="OUTBOUND" AND connection\_status="DENY")calculate(count)

# Any blocked outbound connections made #

* where(direction=OUTBOUND)groupby(destination\_address)calculate(sum:outgoing\_bytes)sort(desc)

# This is for calculating outgoing Bytes #

* where(connection\_status AND connection\_status="ACCEPT" AND direction="OUTBOUND" AND destination\_port!=/443|80|53/)groupby(destination\_port)

# This is for outgoing data across 443, 80, and 53 #

*Ingress Authentication*

* where(geoip\_country\_name="Russia")

# This will show any login hits from Russia #

* where(service!="vpn")groupby(user)

# This will show if someone logged in via Ingress through the service of VPN #

Firewall

where(direction="OUTBOUND" AND destination\_address=“x.x.x.x") groupby(user) sort(desc)

where(connection\_status AND connection\_status="DENY" AND geoip\_country\_code!="US") groupby(geoip\_country\_name) sort(desc)

where(direction="OUTBOUND" AND connection\_status="DENY") calculate(count)

Ingress

where(geoip\_country\_code!="US") groupby(geoip\_country\_name) sort(desc)

where(geoip\_country\_name="Russian Federation")

where(service="box") groupby(user) sort(desc)

DNS

where(public\_suffix AND public\_suffix!="com" AND public\_suffix!="net"AND public\_suffix!="org") groupby(public\_suffix) sort(desc)

where(public\_suffix="ru")

where(public\_suffix="ru") groupby(top\_private\_domain) sort(desc)

Use these queries to determine total OUTBOUND and total INBOUND traffic destinations and sources to determine top hitters for

analysis

where(direction=OUTBOUND)groupby(destination\_address)calculate(sum:outgoing\_bytes)sort(desc)

where(direction=INBOUND)groupby(source\_address)calculate(sum:incoming\_bytes)sort(desc)

Admin Activity/Active Directory

Admin Account Created by Host

where(/:\d{2} (?P<host>\w+)./ AND /4732 EVENT/ OR /\s636 EVENT/) groupby(host)

Accounts Locked out by Host

where(/:\d{2} (?P<host>\w+)./ AND /4740 EVENT/ OR /\s644 EVENT/) groupby(host)

Audit Log cleared by Host

where(/:\d{2} (?P<host>\w+)./ AND /1102 EVENT/ OR /\s517 EVENT/) groupby(host)

Audit Policy Changed

where(/4719 EVENT/ OR /\s612 EVENT/)

Failed Logins by IP (ReGex)

where(/(?P<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/) groupby(ip) calculate(count)

Failed logon - Non Kerberos

where(service!="krbtgt" AND service!="kerberos" AND result="FAILED\_BAD\_PASSWORD” )

Non-Kerberos Logon by Dest Asset

where(service!="krbtgt" AND service!="kerberos" AND result="FAILED\_BAD\_PASSWORD" )groupby("destination\_asset”)

Invalid Logins

where(/4625 EVENT/ OR /\s529 EVENT/)

Invalid Logons by Host

where(/:\d{2} (?P<host>\w+)./ AND /4625 EVENT/ OR /\s529 EVENT/) groupby(host)

Firewall

Demo for Blacklisted Countries

where(geoip\_country\_name = /Czechia|Russia|Hong Kong/ AND connection\_status = "ACCEPT" AND direction="INBOUND")groupby(geoip\_country\_name)

External Firewall Denies by subnet

where(connection\_status = DENY AND source\_address != /10.\*/ AND source\_address != /172.27.\*/ AND source\_address != /169.254.\*/ AND source\_address != /192.168.\*/ AND source\_address != /172.16.\*/)

Visual Search for Firewalls

user!="unknown" AND connection\_status = DENY AND source\_address != /10.\*/ AND source\_address != /172.27.\*/ AND source\_address != /169.254.\*/ AND source\_address != /192.168.\*/ AND source\_address != /172.16.\*/

Foreign Invalid connection attempts

where(connection\_status="DENY" AND geoip\_country\_name!="United States") groupby(geoip\_country\_name) calculate(count)

Inbound Denies by Country

where(connection\_status=DENY AND direction=INBOUND and geoip\_country\_name!="United States") groupby(geoip\_country\_name) calculate(count)

Large Data Transmission - Box

where(direction="OUTBOUND" AND outgoing\_bytes>50000000 AND geoip\_organization="[Box.com](http://box.com/)”)

Example for Docker Traffic (RAW) - Received in Bytes

where([stats.networks.eth0.rx\_bytes!=null](http://stats.networks.eth0.rx_bytes!=null/)) calculate(average:[stats.networks.eth0.rx\_bytes](http://stats.networks.eth0.rx_bytes/))

DNS Traffic

Queries to [safebrowsing.google.com](http://safebrowsing.google.com/) where we know the user, and limits to 20 users only

where(query="[safebrowsing.google.com](http://safebrowsing.google.com/)" AND user!="unknown")groupby(user)limit(20)