

Tools Cheat Sheet

by pengsecurity via cheatography.com/204588/cs/43611/

Online Tools	;
URL/IP	https://www.maxmind.com/-
Lookup:	en/home
	https://ip.teoh.io/vpn-detection
	https://otx.alienvault.com/
	https://www.abuseipdb.com/
URL	https://urlscan.io/
Scanners:	
	https://radar.cloudflare.com
Sandbox:	https://app.any.run/
	https://www.browserling.com/
	https://tria.ge
IP/Hash	https://www.virustotal.com/-
Lookup:	gui/home/upload
	https://opentip.kaspersky.com/

KQL and Hunting Common Tables				
Common Tables:				
CommonSecurityLog(Firewall Logs)				
AuditLog				
SignInLogs				
Security(Incident, Event, Alert)				
Heartbeat(Firewall check)				

Online Tools		KQL and H	unting Commor	Filters	
URL/IP	https://www.maxmind.com/-	where		summarize	
Lookup:	en/home	contains / h	as / ==	distinct	
	https://ip.teoh.io/vpn-detection	project		search	
	https://otx.alienvault.com/	take		count	
	https://www.abuseipdb.com/	! (Used in fi	ont for DOES	ex. !contains ,	
URL	https://urlscan.io/	NOT)		!has	
Scanners:					
	https://radar.cloudflare.com	KQL & Hun	ting Example		
Sandbox:	https://app.any.run/	CommonSe	CommonSecurityLog where Computer contains "172.168.1.1"		
	https://www.browserling.com/	•			
	https://tria.ge	where DestinationIP contains "192.16- 8.2.1"			
IP/Hash	https://www.virustotal.com/-	where SourcePort !contains "22"			
Lookup:	gui/home/upload	IdentityDire	IdentityDirectoryEvents		
	https://opentip.kaspersky.com/	y.com/ where AccountName		contains "SVC_AC-	
		COUNT"			
KQL and Hur	nting Common Tables	•	ionType contair	ns "ADFS"	
Common Tables:		extend AdditionalFields where AdditionalFields contains "4798f4- 01-7de0-4d91-966b-96985695891e"			
CommonSecurityLog(Firewall Logs)					
AuditLog		017400-40			
SignInLogs		Identity Ent	ities		
Security(Incident, Event, Alert)		User's	Browser	Device	
Heartheat(Firewall check)		Location		Info	

KQL and Hunting Common Filters					
where	summarize				
contains / has / ==	distinct				
project	search				
take	count				
! (Used in front for DOES NOT)	ex. !contains , !has				
KQL & Hunting Example					
CommonSecurityLog where Computer contains "172.168.1.1" where DestinationIP contains "192.16-8.2.1" where SourcePort !contains "22" IdentityDirectoryEvents					

where AdditionalFields contains "4798f4- 01-7de0-4d91-966b-96985695891e"						
Identity Entities						
User's Location	Browser	Device Info				
User Agent	Conditional Access	Location				
IP Address	Authentication	Арр				

Not published yet. Last updated 11th June, 2024. Page 1 of 1.

Defender Tools Investigation & Incidents & Response Alerts Hunting **Email and Collaboration** Explorer Review Cloud Apps Files Activity log

By pengsecurity

cheatography.com/pengsecurity/

Sponsored by ApolloPad.com Everyone has a novel in them. Finish https://apollopad.com