Cheatography

Microsoft Sentinel Tools Cheat Sheet

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

Online Tools

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

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 AccountName contains "SVC_AC-COUNT"
| where ActionType contains "ADFS"
| extend AdditionalFields
| 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	App

By **pengsecurity**

cheatography.com/pengsecurity/

Not published yet.
Last updated 9th January, 2025.