

elastic

Search Elastic

Discover

Options

New

Open

Share

Inspect

Save

file.name=invoice.one

KQL

Apr 28, 2012 @ 01:59:11.755 → now

Refresh

+ Add filter

windows*

Search field names

Filter by type 0

Selected fields1

file.name

Available fields95

_id

_index

_score

_type

@timestamp

agent.ephemeral_id

agent.hostname

agent.id

6 hits

Chart options

Apr 28, 2012 @ 01:59:11.755 - Apr 28, 2025 @ 02:10:30.019

>	Mar 26, 2023 @ 16:06:28.250	-
>	Mar 26, 2023 @ 16:06:11.487	-
>	Mar 26, 2023 @ 16:05:53.601	-
>	Mar 26, 2023 @ 16:05:47.793	invoice.one
>	Mar 26, 2023 @ 16:05:47.791	invoice.one
>	Mar 26, 2023 @ 16:05:47.788	invoice.one

message

File stream created:

RuleName: -

UtcTime: 2023-03-26 20:05:47.793

ProcessGuid: {3f3a32cd-a59b-6420-c601-00000001a00}

ProcessId: 908

Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

TargetFilename: C:\Users\bob\Downloads\invoice.one

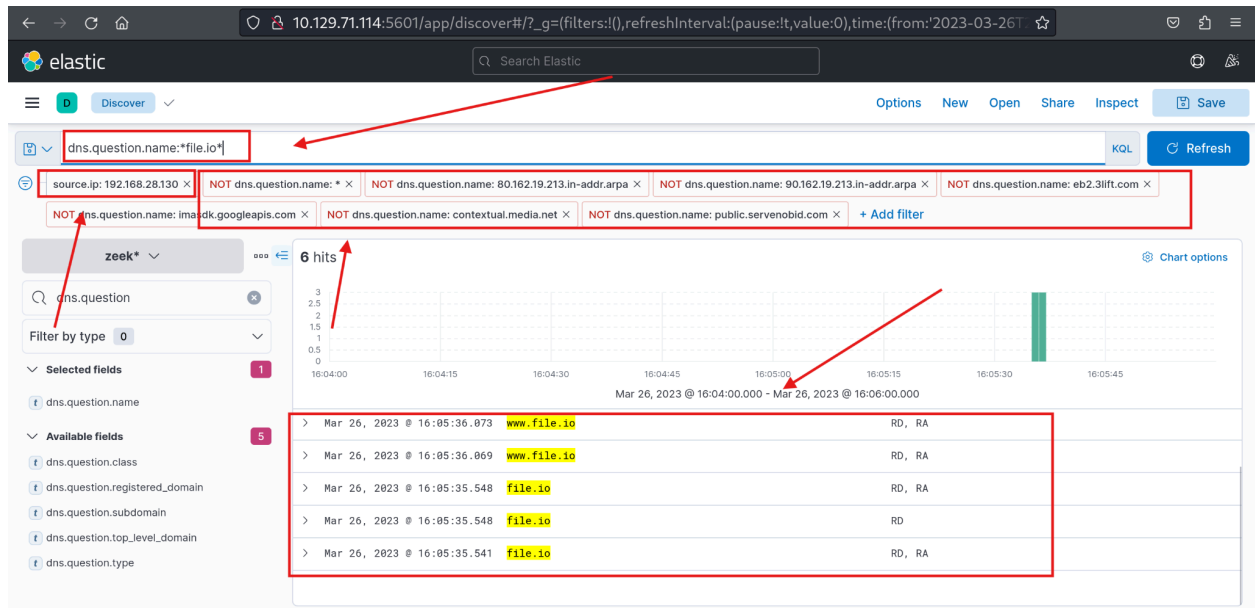
CreationUtcTime: 2023-03-26 20:05:43.609

Hash: MD5=127021207D6415A3B426732B782EFC24, SHA256=AAEE893B24C9474B23E94C725A67D83F2722E4FED8B8BC25CE60B076B30C0954, IMPHASH=00000000000000000000000000000000

Contents: -

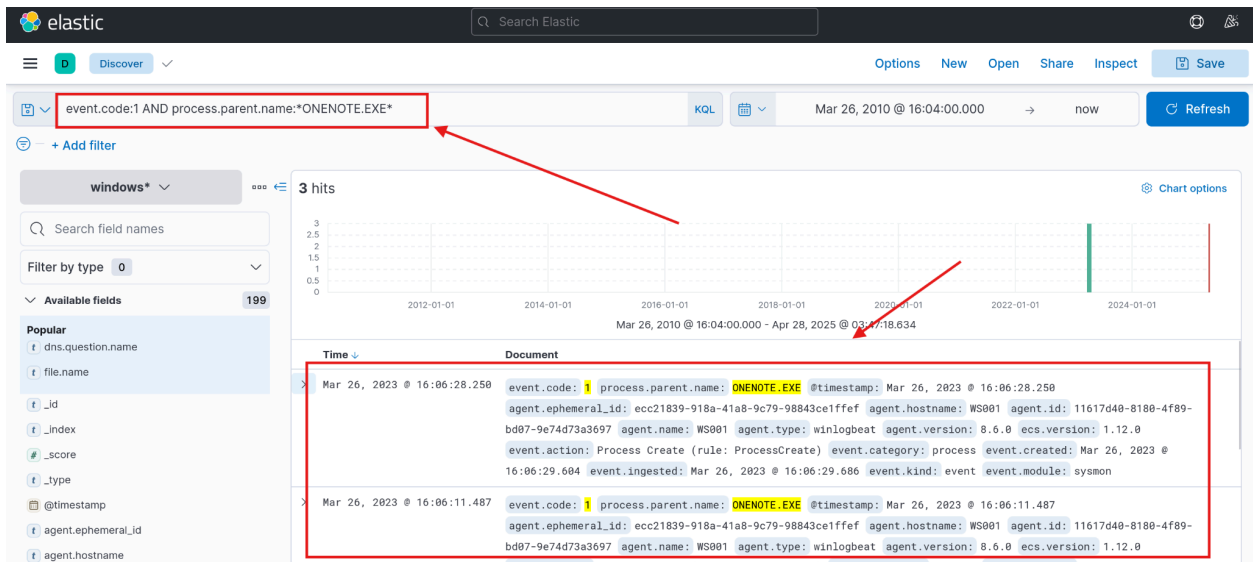
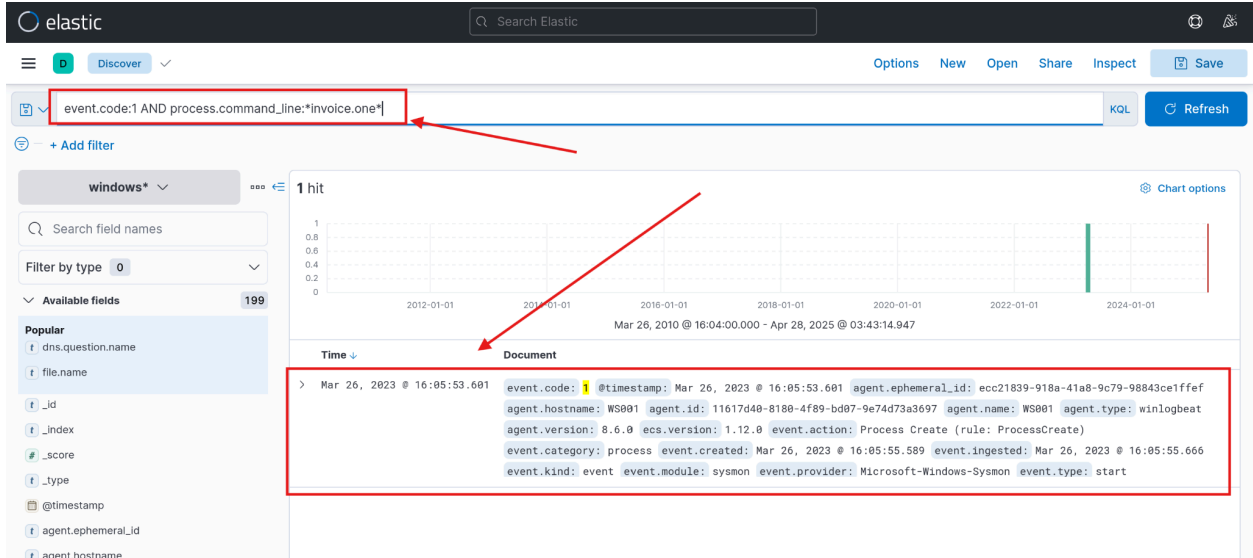
User: EAGLE\bob

winlog.channel	Microsoft-Windows-Sysmon/Operational
winlog.computer_name	WS001.eagle.local
winlog.event_data.Contents	[ZoneTransfer] ZoneId=3 ReferrerUrl=https://www.file.io/ HostUrl=https://file.io/Apog4XXpd1hB
winlog.event_data.CreationUtcTime	2023-03-26 20:05:43.609
winlog.event_id	15
winlog.opcode	Info
winlog.process.pid	3,608




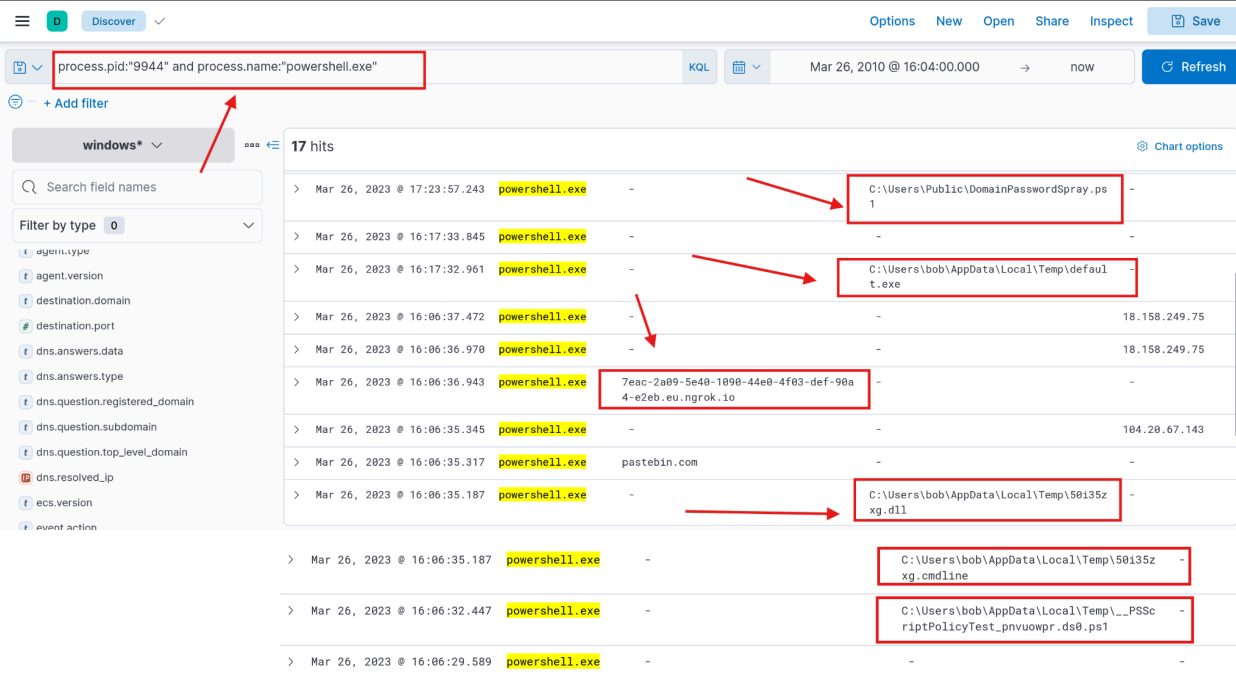
dns.question.class	IN
dns.question.name	file.io
dns.question.registered_domain	file.io
dns.question.top_level_domain	io
dns.question.type	A
dns.resolved_ip	34.197.10.85, 3.213.216.16

Mar 26, 2023 @ 16:05:04.168	-	-
Mar 26, 2023 @ 16:05:02.733	-	-
Mar 26, 2023 @ 16:05:02.717	-	-
Mar 26, 2023 @ 16:05:02.703	mail.google.com	RD
Mar 26, 2023 @ 16:05:02.703	-	-
Mar 26, 2023 @ 16:05:02.702	mail.google.com	RD, RA



process.args	C:\WINDOWS\system32\cmd.exe, /c, C:\Users\bob\AppData\Local\Temp\OneNote\16.0\Export ed\{EC284AA9-1F31-4DC4-B3C5-3EEE8137EBC3}\NT\0\invoice.bat
process.args_count	3
process.command_line	C:\WINDOWS\system32\cmd.exe /c "C:\Users\bob\AppData\Local\Temp\OneNote\16.0\Export ed\{EC284AA9-1F31-4DC4-B3C5-3EEE8137EBC3}\NT\0\invoice.bat" "
process.entity_id	{3f3a32cd-a5c4-6420-e101-000000001a00}
process.executable	C:\Windows\System32\cmd.exe

elastic 



elastic Search Elastic

Discover

Options New Open Share Inspect Save

18.158.249.75 KQL Mar 26, 2010 @ 16:04:00.000 now Refresh

+ Add filter

zeek* 24 hits Chart options

destination Filter by type 0

Selected fields 2

- destination.ip
- destination.port

Available fields 3

Popular

- destination.address
- destination.bytes
- destination.packets

Time	destination.ip	source.ip	destination.port
> Mar 27, 2023 @ 17:25:58.197	18.158.249.75	192.168.28.130	443
> Mar 27, 2023 @ 17:25:58.171	18.158.249.75	192.168.28.130	443
> Mar 27, 2023 @ 17:25:58.135	192.168.28.2	192.168.28.200	53
> Mar 27, 2023 @ 17:25:58.134	192.168.28.200	192.168.28.130	53
> Mar 27, 2023 @ 12:44:14.062	18.158.249.75	192.168.28.130	443
> Mar 27, 2023 @ 04:09:06.082	18.158.249.75	192.168.28.130	443
> Mar 26, 2023 @ 18:10:18.937	18.158.249.75	192.168.28.130	443
> Mar 26, 2023 @ 18:10:17.607	18.158.249.75	192.168.28.130	443
> Mar 26, 2023 @ 18:10:17.573	18.158.249.75	192.168.28.130	443
> Mar 26, 2023 @ 18:10:17.197	18.158.249.75	192.168.28.130	443

elastic Search Elastic

Discover

Options New Open Share Inspect Save

"ngrok.io" KQL Last 15 years Show dates Refresh

+ Add filter

zeek* 49 hits Chart options

dns Filter by type 0

Selected fields 1

- dns.answers.data

Available fields 28

Popular

- dns.header.flags
- dns.question.name
- dns.answers.ttl
- dns.id
- dns.question.class
- dns.question.registered_domain

Time	destination.ip	source.ip	destination.port	dns.answers.data
> Mar 29, 2023 @ 16:49:01.421	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 16:49:01.421	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 16:49:01.421	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 16:49:01.421	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 16:49:01.421	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 12:39:27.458	192.168.28.200	192.168.28.132	53	-
> Mar 29, 2023 @ 12:39:27.437	192.168.28.2	192.168.28.200	53	3.125.102.39
> Mar 29, 2023 @ 12:39:27.436	192.168.28.200	192.168.28.132	53	3.125.102.39
> Mar 27, 2023 @ 18:41:23.113	192.168.28.2	192.168.28.200	53	18.192.31.165
> Mar 27, 2023 @ 18:41:23.111	192.168.28.200	192.168.28.132	53	18.192.31.165

elastic Search Elastic

Discover

Options New Open Share Inspect Save

3.125.102.39 KQL Refresh

+ Add filter

zeek* 29 hits Chart options

dns Filter by type 0

Selected fields 1

- dns.answers.data

Available fields 28

Popular

- dns.header.flags
- dns.question.name
- dns.answers.ttl
- dns.id
- dns.question.class
- dns.question.registered_domain

Time	destination.ip	source.ip	destination.port	dns.answers.data
> Mar 29, 2023 @ 12:39:27.507	3.125.102.39	192.168.28.132	443	-
> Mar 29, 2023 @ 12:39:27.488	3.125.102.39	192.168.28.132	443	-
> Mar 29, 2023 @ 12:39:27.437	192.168.28.2	192.168.28.200	53	3.125.102.39
> Mar 29, 2023 @ 12:39:27.436	192.168.28.200	192.168.28.132	53	3.125.102.39
> Mar 27, 2023 @ 18:57:23.900	3.125.102.39	192.168.28.130	443	-
> Mar 27, 2023 @ 18:34:35.855	3.125.102.39	192.168.28.132	443	-
> Mar 27, 2023 @ 18:34:11.000	3.125.102.39	192.168.28.132	443	-
> Mar 27, 2023 @ 18:18:14.700	3.125.102.39	192.168.28.132	443	-
> Mar 27, 2023 @ 18:18:13.374	3.125.102.39	192.168.28.132	443	-
> Mar 27, 2023 @ 18:18:13.353	3.125.102.39	192.168.28.132	443	-

elastic Search Elastic

Discover

process.name:"default.exe"

KQL Last 15 years Show dates Refresh

+ Add filter

windows*

68 hits

Chart options

Search field names

Filter by type 0

Selected fields 6

- process.name
- process.args
- event.code
- file.path
- destination.ip
- dns.question.name

Available fields 139

Popular destination.port

dns.question.name

Time	process.name	process.args	event.code	file.path	destination.ip	dns.question.name
Mar 26, 2023 @ 18:12:44.594	default.exe	-	13	-	-	-
Mar 26, 2023 @ 18:12:43.663	default.exe	-	11	-	-	-
Mar 26, 2023 @ 18:10:19.033	default.exe	-	3	-	18.158.249.75	-
Mar 26, 2023 @ 18:10:18.596	default.exe	-	3	-	18.158.249.75	-
Mar 26, 2023 @ 18:10:18.566	default.exe	-	22	-	-	7eac-2a09-5e40-1090-44e0-4f03-def-90a4-e2eb.eu.ngrok.io
Mar 26, 2023 @ 18:10:18.246	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	1	-	-	-

elastic Search Elastic

Discover

process.name:"SharpHound.exe"

KQL Refresh

+ Add filter

windows*

4 hits

Chart options

Search field names

Filter by type 0

Selected fields 6

- process.name
- process.args
- event.code
- file.path
- destination.ip
- dns.question.name

Available fields 139

Popular destination.port

Time	process.name	process.args	event.code	file.path	destination.ip	dns.question.name
Mar 26, 2023 @ 18:19:30.147	SharpHound.exe	-	5	-	-	-
Mar 26, 2023 @ 18:19:30.119	SharpHound.exe	SharpHound.exe, -c, all	1	-	-	-
Mar 26, 2023 @ 18:17:58.409	SharpHound.exe	-	5	-	-	-
Mar 26, 2023 @ 18:17:58.000	SharpHound.exe	sharpHound.exe, -c collectionmethod, all	1	-	-	-

elastic Search Elastic

Discover

process.hash.sha256:018d37cbd3878258c29db3bc3f2988b6ae688843801b9abc28e6151141ab66d4 KQL Last 15 years Show dates Refresh

+ Add filter

windows* 12 hits

Search field names

Filter by type 0

- host.id
- host.ip
- host.mac
- host.os.build
- host.os.family
- host.os.kernel
- host.os.name
- host.os.platform
- host.os.type
- host.os.version
- log.level

Time	process.name	process.args	host.name
Mar 27, 2023 @ 18:38:03.169	default.exe	default.exe	PKI.eagle.local
Mar 27, 2023 @ 18:23:52.239	svchost.exe	C:\Users\svc-sql1\AppData\Local\Temp\svchost.exe	PKI.eagle.local
Mar 27, 2023 @ 18:18:12.402	default.exe	default.exe	PKI.eagle.local
Mar 27, 2023 @ 17:25:58.652	svchost.exe	C:\Users\bob\AppData\Local\Temp\svchost.exe	WS001.eagle.local
Mar 27, 2023 @ 17:23:30.020	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	WS001.eagle.local
Mar 26, 2023 @ 18:12:44.276	svchost.exe	C:\Users\bob\AppData\Local\Temp\svchost.exe	WS001.eagle.local
Mar 26, 2023 @ 18:10:18.246	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	WS001.eagle.local
Mar 26, 2023 @ 17:51:16.584	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	WS001.eagle.local
Mar 26, 2023 @ 17:49:29.436	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	WS001.eagle.local
Mar 26, 2023 @ 17:47:37.424	default.exe	C:\Users\bob\AppData\Local\Temp\default.exe	WS001.eagle.local

elastic Search Elastic

Discover

process.hash.sha256:018d37cbd3878258c29db3bc3f2988b6ae688843801b9abc28e6151141ab66d4 KQL Last 15 years Show dates Refresh

+ Add filter

windows* 12 hits

Search field names

Filter by type 0

- host.id
- host.ip
- host.mac
- host.os.build
- host.os.family
- host.os.kernel
- host.os.name
- host.os.platform
- host.os.type
- host.os.version
- log.level

RuleName: -

UtcTime: 2023-03-27 22:18:12.402

ProcessGuid: {0b5600e8-1624-6422-d102-000000001f00}

ProcessId: 832

Image: C:\Windows\default.exe

process.args	default.exe
process.args_count	1
process.command_line	"default.exe"
process.entity_id	{0b5600e8-1624-6422-d102-000000001f00}
process.executable	C:\Windows\default.exe
process.hash.md5	83fb8ca62353872b3db0a7838ff9199c
process.hash.sha256	018d37cbd3878258c29db3bc3f2988b6ae688843801b9abc28e6151141ab66d4
process.name	default.exe
process.parent.args	C:\Windows\PSEXESVC.exe

elastic

Search Elastic

Discover

Options New Open Share Inspect Save

(event.code:4624 OR event.code:4625) AND winlog.event_data.LogonType:3 AND source.ip:192.168.28.130 KQL Last 15 years Show dates Refresh

+ Add filter

windows* 1,904 hits

user.

Filter by type 0

Available fields

- user.domain
- user.effective.name
- user.id
- user.name
- winlog.user.domain
- winlog.user.identifier
- winlog.user.name
- winlog.user.type

Top 5 values

WS001\$	70.6%
bob	28.6%
svc-sql1	0.8%

Exists in 500 / 500 records

Multi fields

- user.name.text

Visualize

Document

event.code: 4624 winlog.event_data.LogonType: 3 @timestamp: Mar 29, 2023 @ 16:47:48.942 agent.ephemeral_id: 69607514-2da9-497e-9b85-a2941c890f3b agent.hostname: DC1 agent.id: c10ef88e-4394-4edb-a5b2-1ae38d9f53d4 agent.name: DC1 agent.type: winlogbeat agent.version: 8.6.0 ecs.version: 1.12.0 event.action: logged-in event.category: authentication event.created: Mar 29, 2023 @ 16:47:50.580 event.ingested: Mar 29, 2023 @ 16:47:50.140 event.kind: event event.module: security event.outcome: success

event.code: 4624 winlog.event_data.LogonType: 3 @timestamp: Mar 29, 2023 @ 16:47:44.421 agent.ephemeral_id: 69607514-2da9-497e-9b85-a2941c890f3b agent.hostname: DC1 agent.id: c10ef88e-4394-4edb-a5b2-1ae38d9f53d4 agent.name: DC1 agent.type: winlogbeat agent.version: 8.6.0 ecs.version: 1.12.0 event.action: logged-in event.category: authentication event.created: Mar 29, 2023 @ 16:47:45.538 event.ingested: Mar 29, 2023 @ 16:47:45.501 event.kind: event event.module: security event.outcome: success

event.code: 4624 winlog.event_data.LogonType: 3 @timestamp: Mar 29, 2023 @ 16:47:44.360 agent.ephemeral_id: 69607514-2da9-497e-9b85-a2941c890f3b agent.hostname: DC1 agent.id: c10ef88e-4394-4edb-a5b2-1ae38d9f53d4 agent.name: DC1 agent.type: winlogbeat agent.version: 8.6.0 ecs.version: 1.12.0 event.action: logged-in event.category: authentication event.created: Mar 29, 2023 @ 16:47:45.538

(event.code:4624 OR event.code:4625) AND winlog.event_data.LogonType:3 AND source.ip:192.168.28.130

NOT user.name: bob NOT user.name: WS001\$ + Add filter

6 hits

Time	event.code	agent.hostname	user.name
Mar 28, 2023 @ 00:37:41.697	4624	PKI	svc-sql1
Mar 28, 2023 @ 00:17:50.401	4624	PKI	svc-sql1
Mar 28, 2023 @ 00:06:20.432	4624	PAW	svc-sql1
Mar 28, 2023 @ 00:00:18.309	4624	PAW	svc-sql1
Mar 26, 2023 @ 23:53:26.928	4625	DC1	administrator
Mar 26, 2023 @ 23:34:57.232	4625	DC1	administrator

Successful logon

Failed logon