Switch

Threat Hunting Workshop

DeiC Conference, 27 October 2026

Threat Hunting Workshop

Threat Hunting
(08:30 – 09:15)

Kusto Query (KQL)
(09:15 – 09:45)

Threat Hunting Scenarios
(09:45 – 10:30)



(10:30- 11:00)

Q/A

(11:00- 11:XX)

Threat Hunting Challenge



(1 Hour)

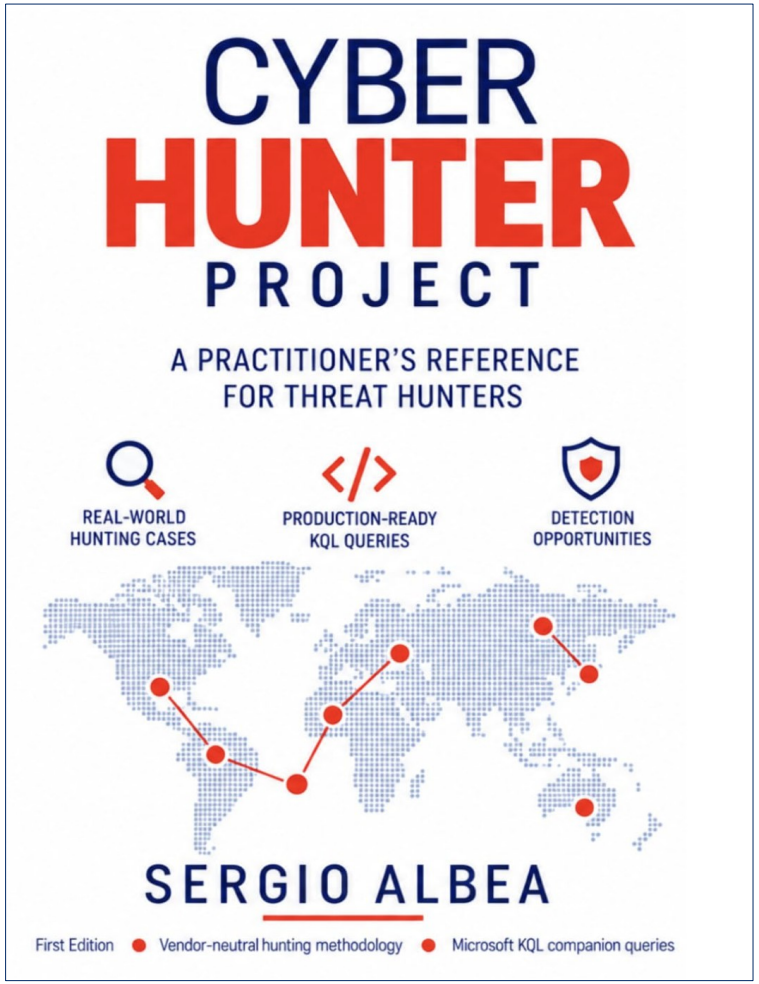
Switch_

Threat Hunting Workshop

(1 hour)

Threat Hunting Challenge





https://book.sergioalbea.com/

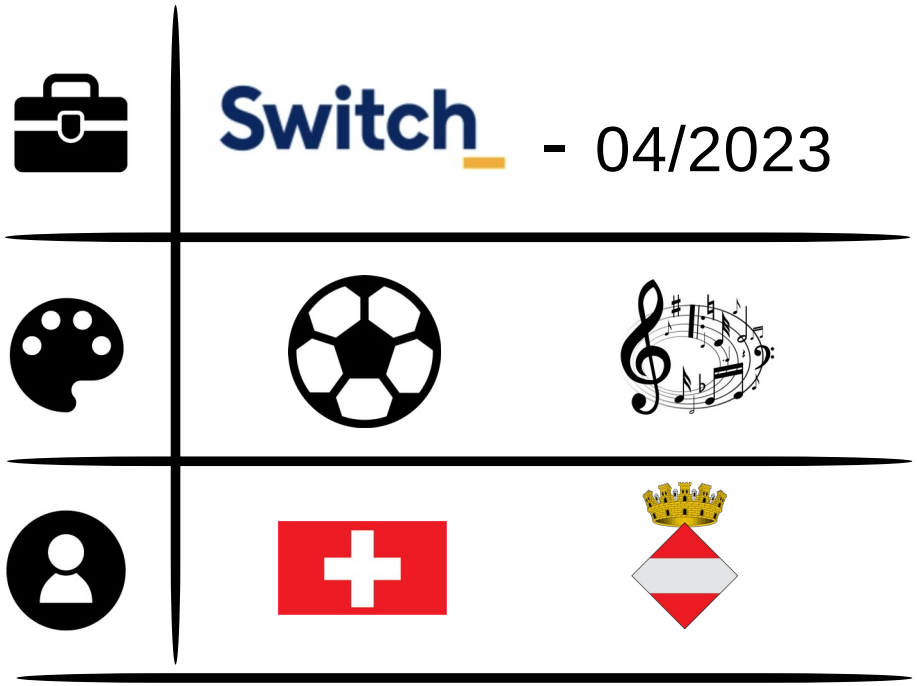
Switch

Sergio Albea

Threat Hunting Expert

Microsoft® MVP Most Valuable Professional

Switch - 04/2023



linkedin.com/in/sergioalbea/

medium.com/@sergio.albea

github.com/Sergio-Albea-Git/Threat-Hunting-KQL-Queries



Which is your experience with Threat Hunting?



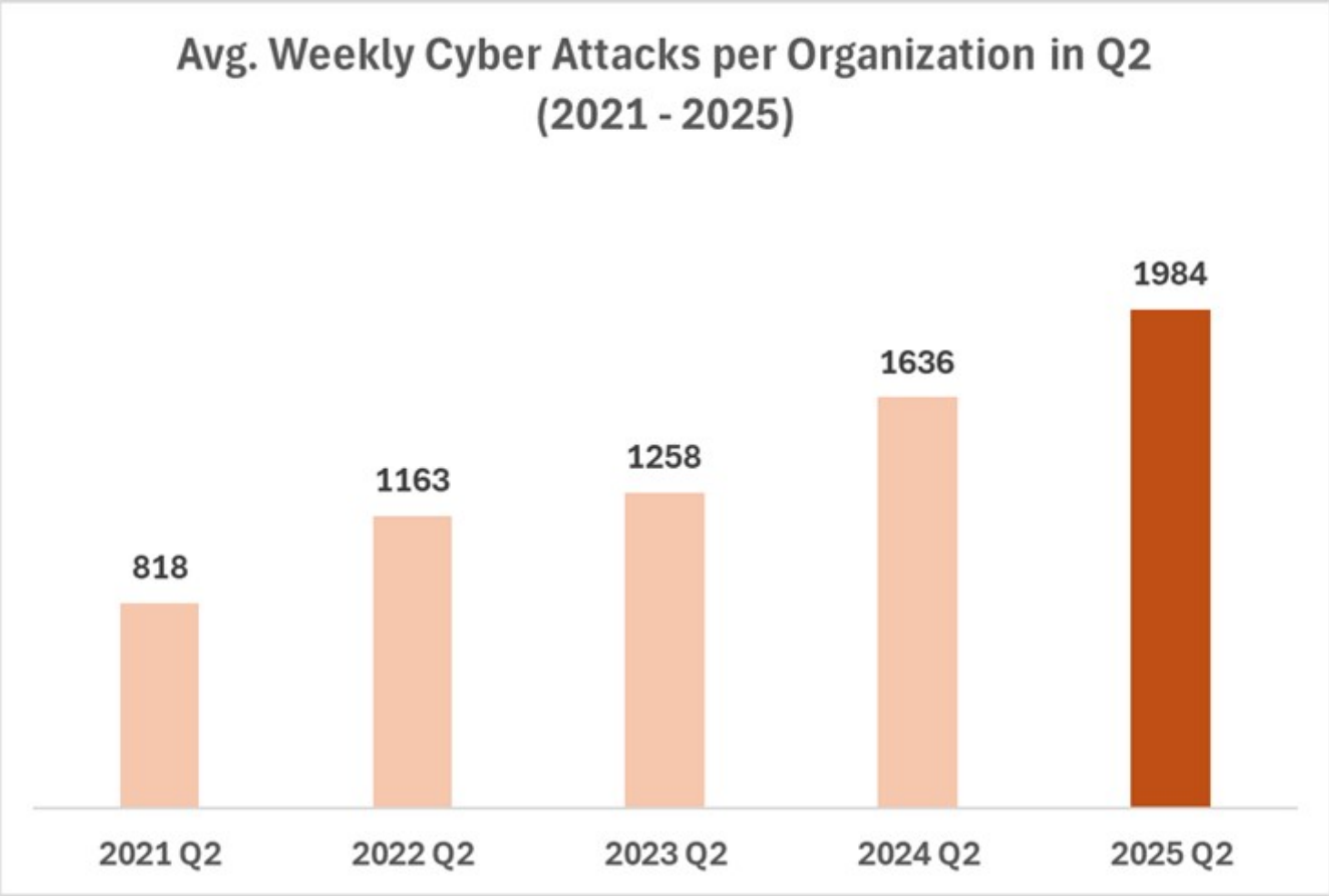


DefenderXDR

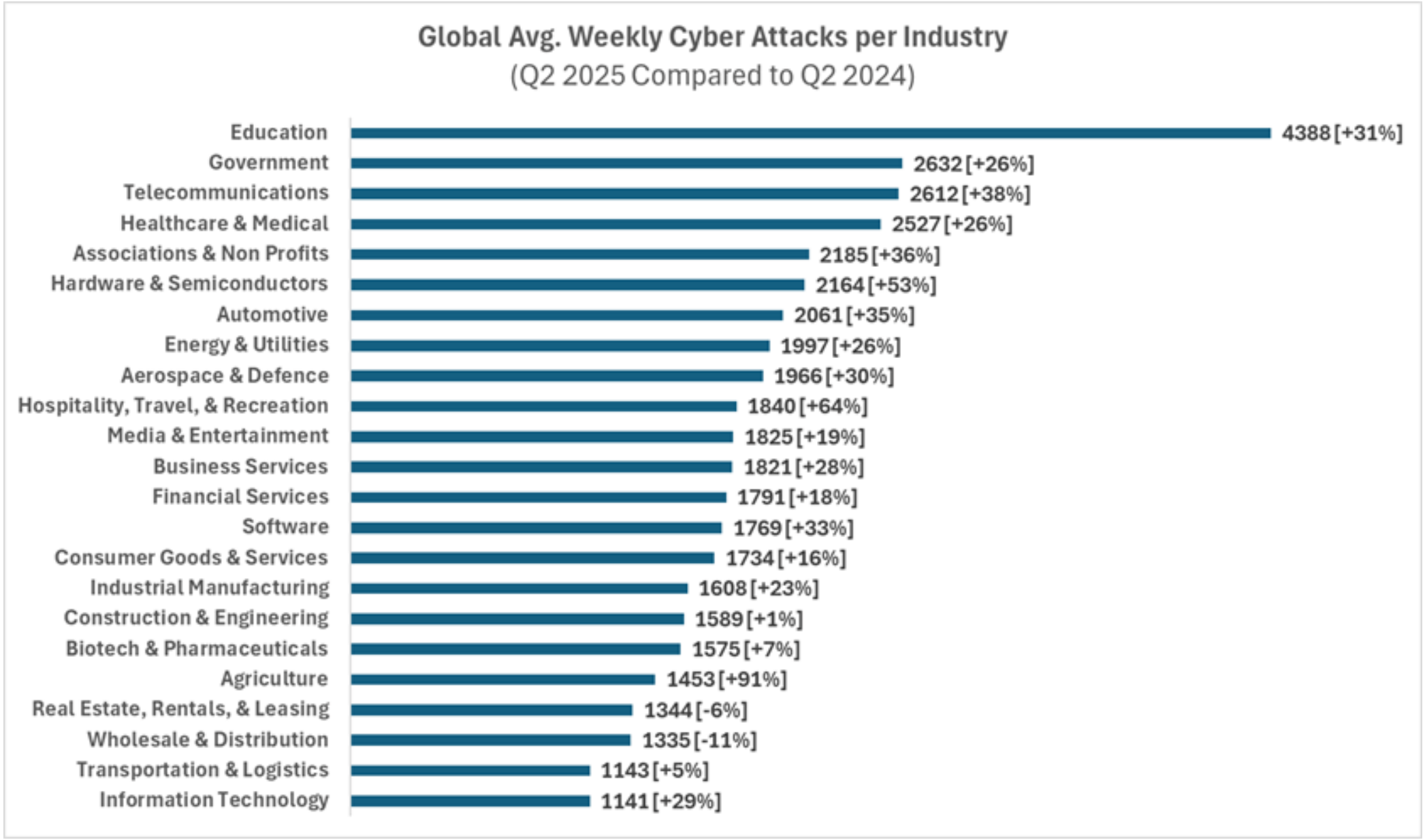




Why is important?



https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/


Global Avg. Weekly Cyber Attacks per Industry
(Q2 2025 Compared to Q2 2024)
Education 4388 [+31%]
Government 2632 [+26%]
Telecommunications 2612 [+38%]
Healthcare & Medical 2527 [+26%]
Associations & Non Profits 2185 [+36%]
Hardware & Semiconductors 2164 [+53%]
Automotive 2061 [+35%]
Energy & Utilities 1997 [+26%]
Aerospace & Defence 1966 [+30%]
Hospitality, Travel, & Recreation 1840 [+64%]
Media & Entertainment 1825 [+19%]
Business Services 1821 [+28%]
Financial Services 1791 [+18%]
Software 1769 [+33%]
Consumer Goods & Services 1734 [+16%]
Industrial Manufacturing 1608 [+23%]
Construction & Engineering 1589 [+1%]
Biotech & Pharmaceuticals 1575 [+7%]
Agriculture 1453 [+91%]
Real Estate, Rentals, & Leasing 1344 [-6%]
Wholesale & Distribution 1335 [-11%]
Transportation & Logistics 1143 [+5%]
Information Technology 1141 [+29%]

Why is important? October 2026



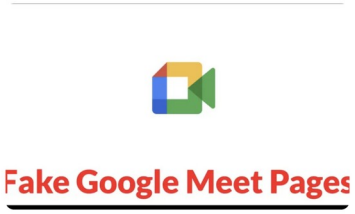
Hackers used Compromised ConnectWise Backup Credentials to Hack 173 Microsoft 365 Accounts

Guru Baran - October 17, 2026

Hackers used a stolen ConnectWise Cloud Backup credential to sign in to 173 Microsoft 365 partner and customer tenants, giving them access through a...

Indicators of Compromise

IOC Type	Indicator	Description
Application name	`ConnectWise Cloud Backup`	Trusted backup application abused to access Microsoft 365 customer tenants
Application ID	`506e08f9-6e9a-4da4-942b-a099a03644ae`	Legitimate ConnectWise Cloud Backup OAuth application, formerly SkyKick Backup



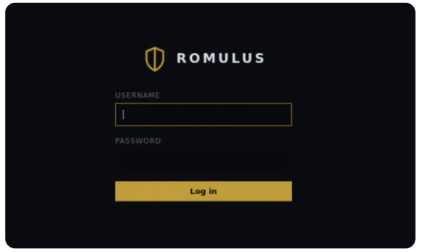
Hackers Using Fake Google Meet Pages to Steal Google Credentials

Tushar Subhra Dutta - October 20, 2026

Two websites are hosting fake Google Meet pages designed to steal Google account credentials and carry out phishing involving two-factor authentication (2FA), according to...

Indicators of compromise (IoCs):-

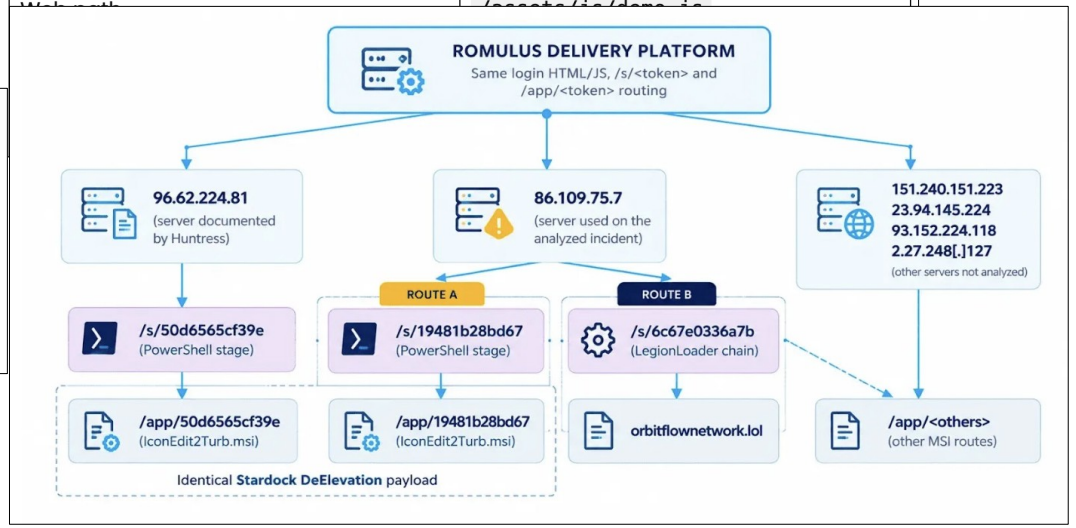
Type	Indicator
Domain	`meet-google[.]cyou`
Domain	`qooglo[.]com`
Web path	`/meet`
Web path	`/install`



Hackers Use New ROMULUS ClickFix Platform to Deliver Malware and Evade Security Detection

Tushar Subhra Dutta - October 16, 2026

Hackers are using a newly identified platform called ROMULUS to deliver malware through ClickFix traps, combining hidden PowerShell scripts, altered software installers, and encrypted...



Switch

Source: https://cybersecuritynews.com/

Differentiate between Theat Hunting and Threat Detection

What bad things could be happening unnoticed? Did something bad happen?

Threat Hunting	Threat Detection
Proactive	Reactive
Human-driven, hypothesis-based	Automated, rule-based
Searches for unknown / hidden threats	Focuses on known threats
Initiated by analysts	Triggered by alerts
Uses behavior & ATT&CK	Uses IOCs & signatures
Output: New detections & insights	Output: Incidents



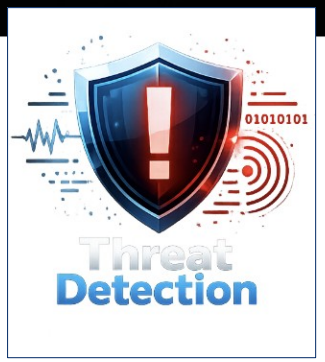


Differentiate between Theat Hunting and Threat Detection















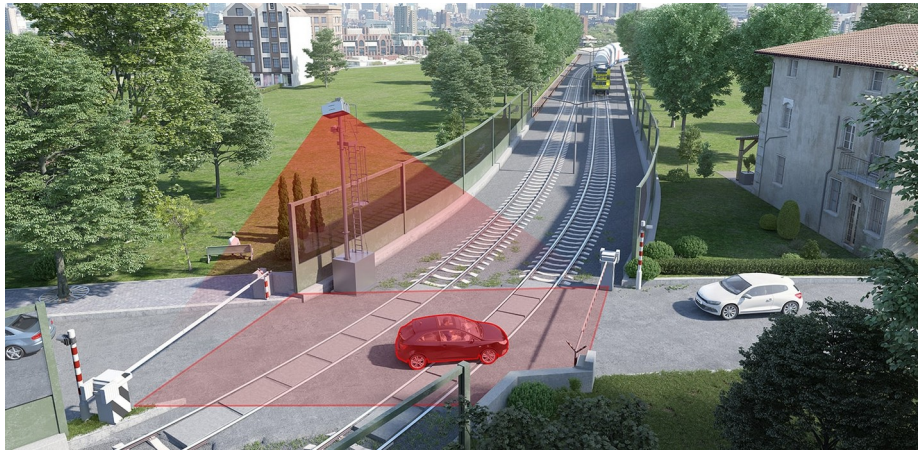


Image Source (https://www.mermecgroup.com/northamerica/protect/level-crossing/1033/level-crossing-obstacle-detection.php)

Switch

Why is important? October 2026



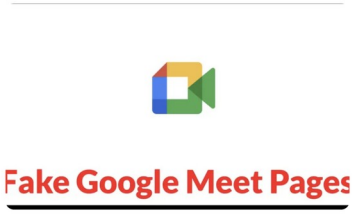
Hackers used Compromised ConnectWise Backup Credentials to Hack 173 Microsoft 365 Accounts

Guru Baran - October 17, 2026

Hackers used a stolen ConnectWise Cloud Backup credential to sign in to 173 Microsoft 365 partner and customer tenants, giving them access through a...

Indicators of Compromise

IOC Type	Indicator	Description
Application name	`ConnectWise Cloud Backup`	Trusted backup application abused to access Microsoft 365 customer tenants
Application ID	`506e08f9-6e9a-4da4-942b-a099a03644ae`	Legitimate ConnectWise Cloud Backup OAuth application, formerly SkyKick Backup



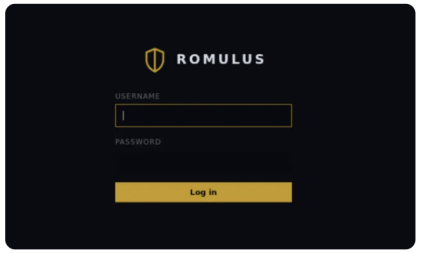
Hackers Using Fake Google Meet Pages to Steal Google Credentials

Tushar Subhra Dutta - October 20, 2026

Two websites are hosting fake Google Meet pages designed to steal Google account credentials and carry out phishing involving two-factor authentication (2FA), according to...

Indicators of compromise (IoCs):-

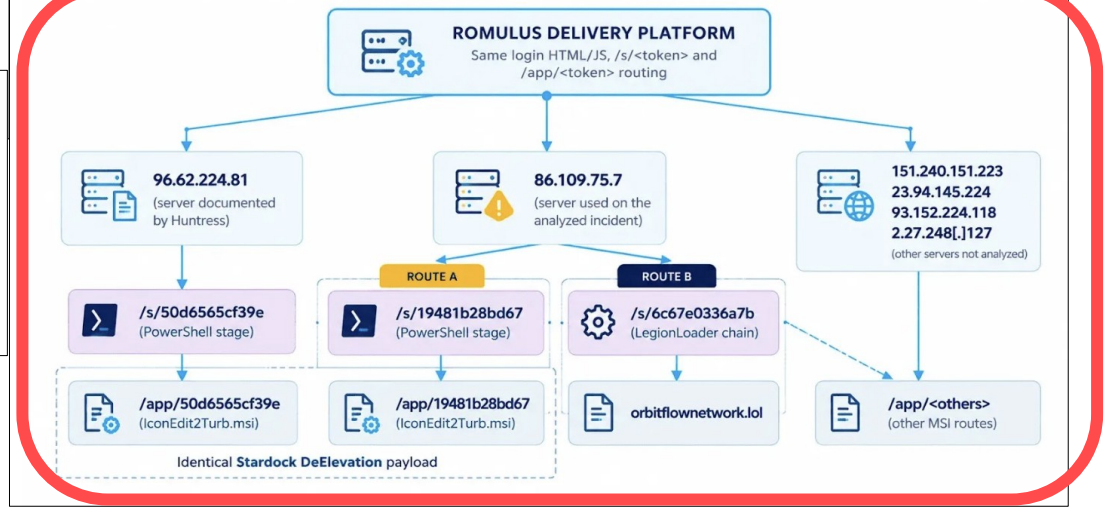
Type	Indicator
Domain	`meet-google[.]cyou`
Domain	`qooglo[.]com`
Web path	`/meet`
Web path	`/install`



Hackers Use New ROMULUS ClickFix Platform to Deliver Malware and Evade Security Detection

Tushar Subhra Dutta - October 16, 2026

Hackers are using a newly identified platform called ROMULUS to deliver malware through ClickFix traps, combining hidden PowerShell scripts, altered software installers, and encrypted...



Source: https://cybersecuritynews.com/

All Hunting in one Image



Switch_

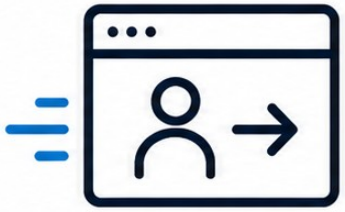
Think Like a Hunter

Think like a Hunter



Curiosity over comfort

If nothing alerted, ask why.



Behaviour over artefacts

Hunt what the attacker has to do, not only today's hash or IP.



Assume breach, then disprove it

Start from the idea that an attacker is already here.



Okay with finding nothing

No attacker can still be a win — a new detection or a blind spot found.

Think like a Hunter

Curiosity over comfort

If nothing alerted, ask why.



Think like a Hunter

Behaviour over artefacts

Hunt what the attacker has to do, not only today's hash or IP.



Think like a Hunter

Assume breach, then disprove it

Start from the idea that an attacker is already here.



Think like a Hunter

Okay with finding nothing

No attacker can still be a win — a new detection or a blind spot found.



Switch_

Threat Hypothesis

A threat hypothesis is a clear **assumption about something bad that might be happening in your environment**.

On cybersecurity, can be translated as a question you try to answer with logs.

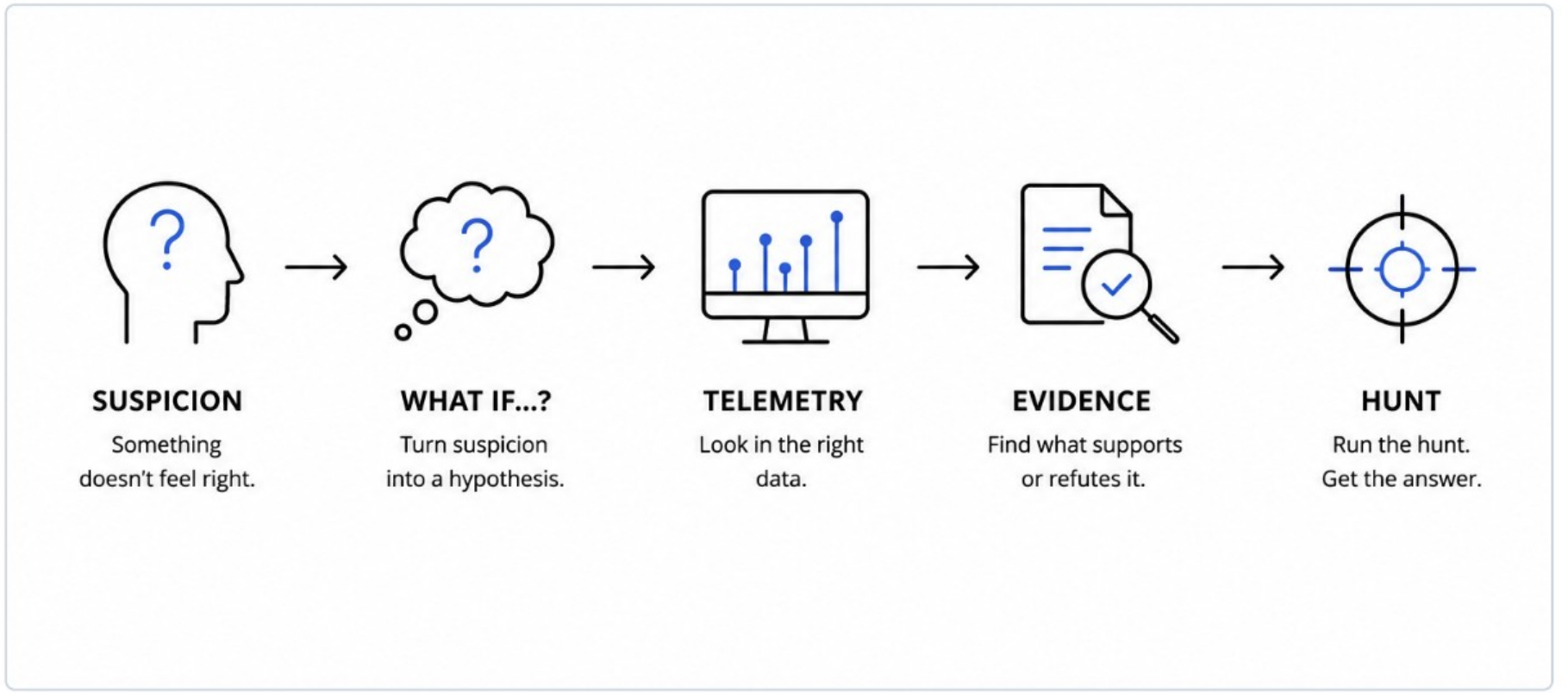


- **What if someone is logging in with stolen credentials from another country?**

- **What if a compromised device is talking to the internet when it**

Threat hypothesis

Threat hunting is not about finding alerts — it’s about testing assumptions.

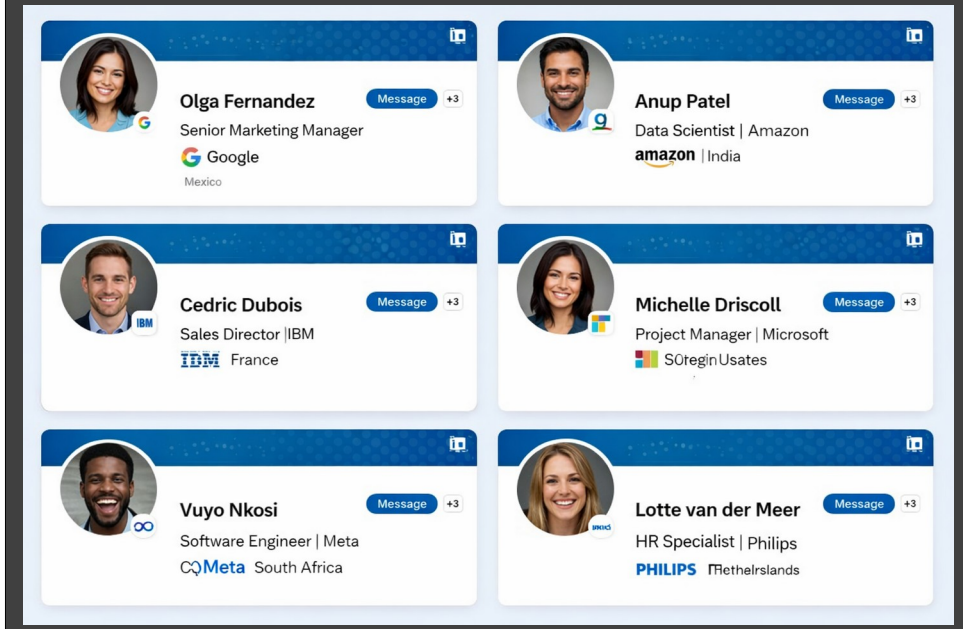


Threat hypothesis Example – Sign-Attempt Location

Conditional Access
Non Allowed Countries:
Block Countries



Social Engineering:
Social Network



Threat hypothesis Example – Sign-Attempt Location

Conditional Access:
Block VPN Network Ranges/ASN

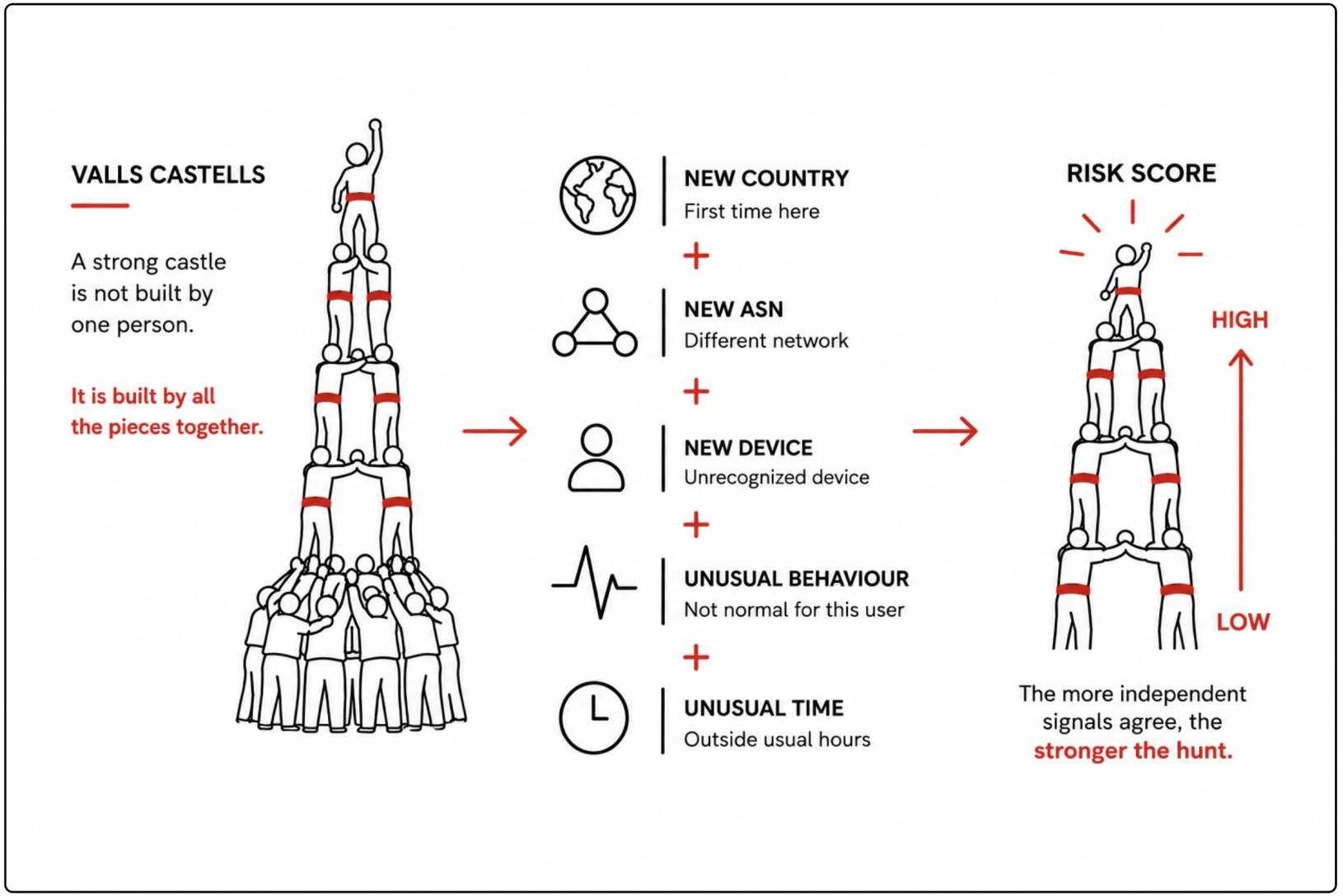
Detection Rule:
When the latitude and longitude based on sign-in attempt are too far.



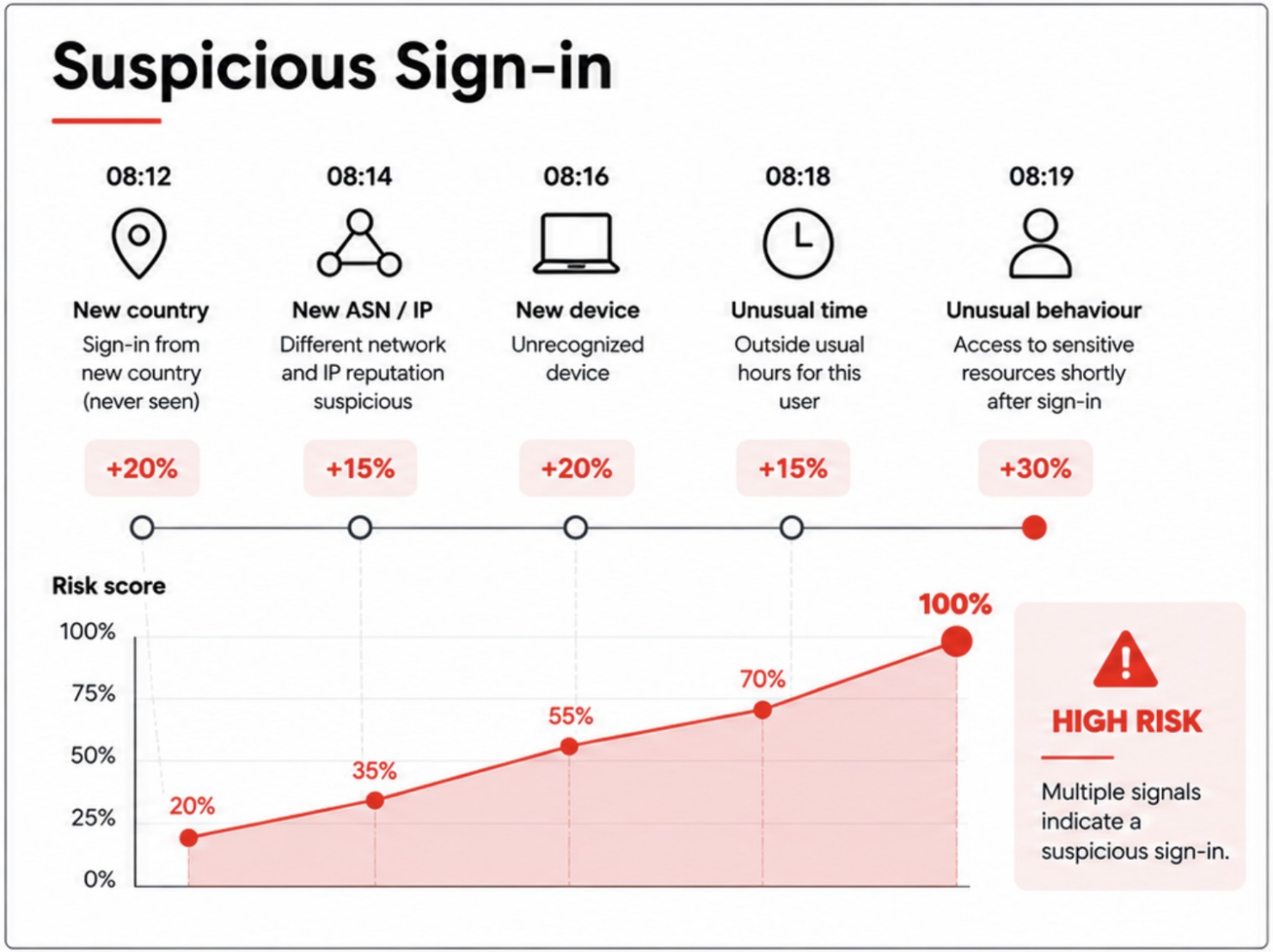
Switch

Incident Risk Score

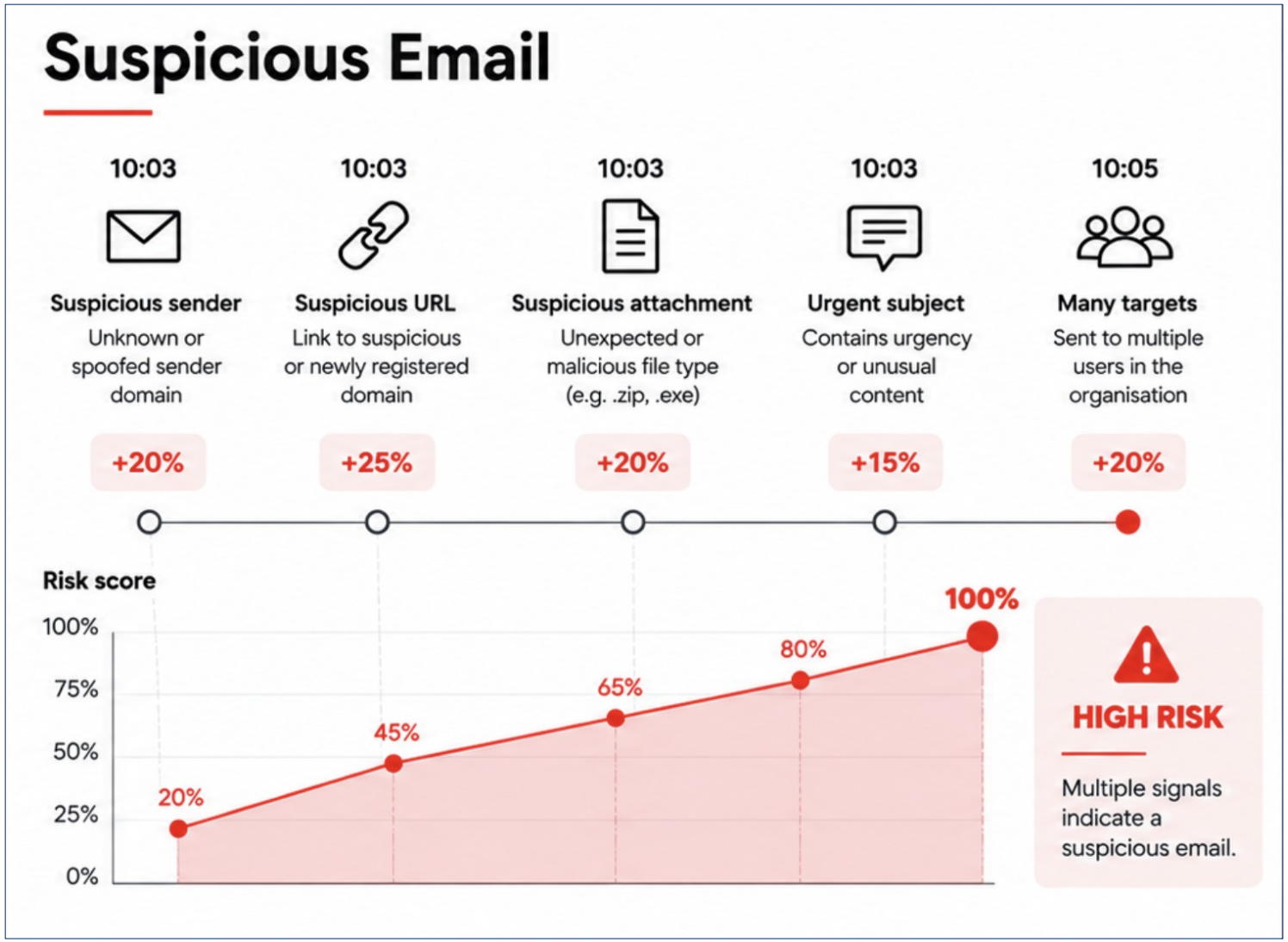
Incident Risk Score



Incident Risk Score - Case 01



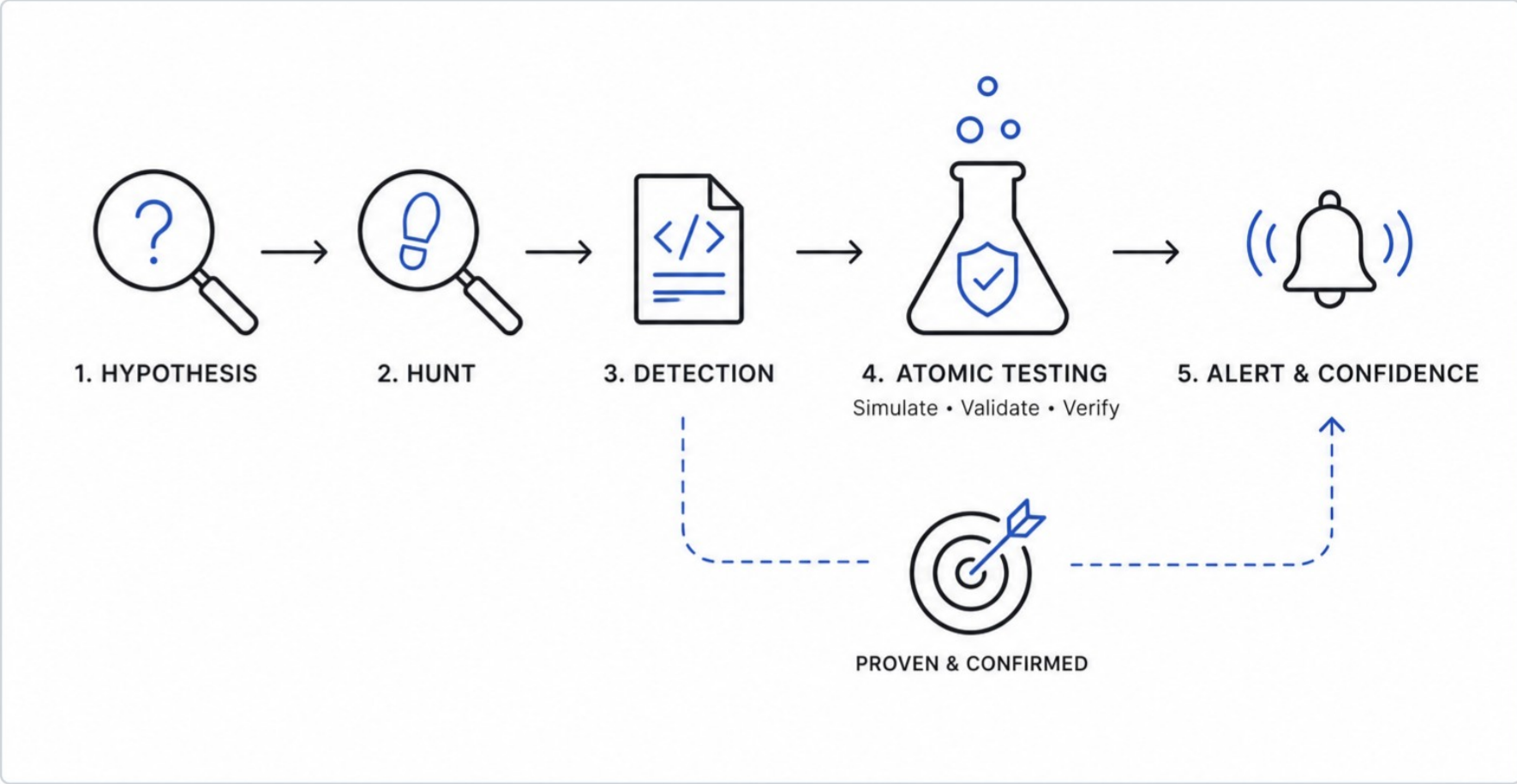
Incident Risk Score – Case 02



Switch_

Atomic Testing

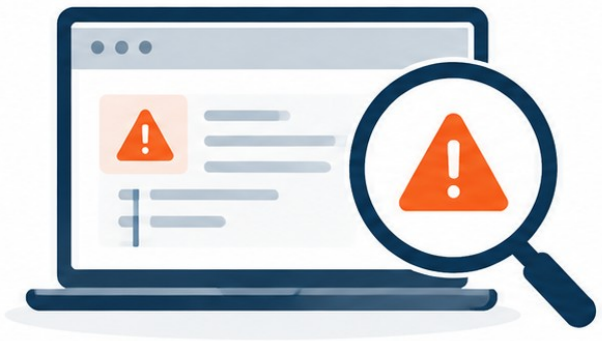
Atomic Testing



Atomic Testing

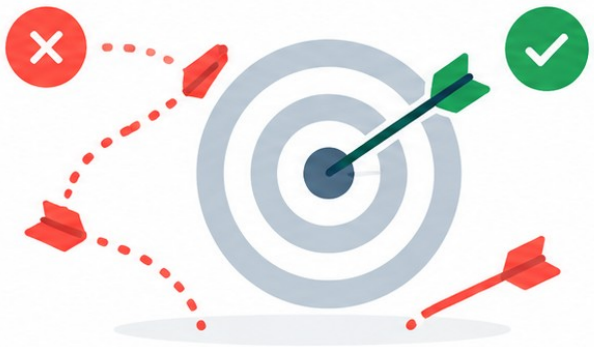
1 Validate before real attacks

Find out your rule is broken on a quiet Tuesday of your choosing — not mid-incident.



2 Show blind spots & false positives

A test fails quietly (a gap to close) or fires on something harmless (noise to tune out). Both give you something to fix.



3 Build real confidence

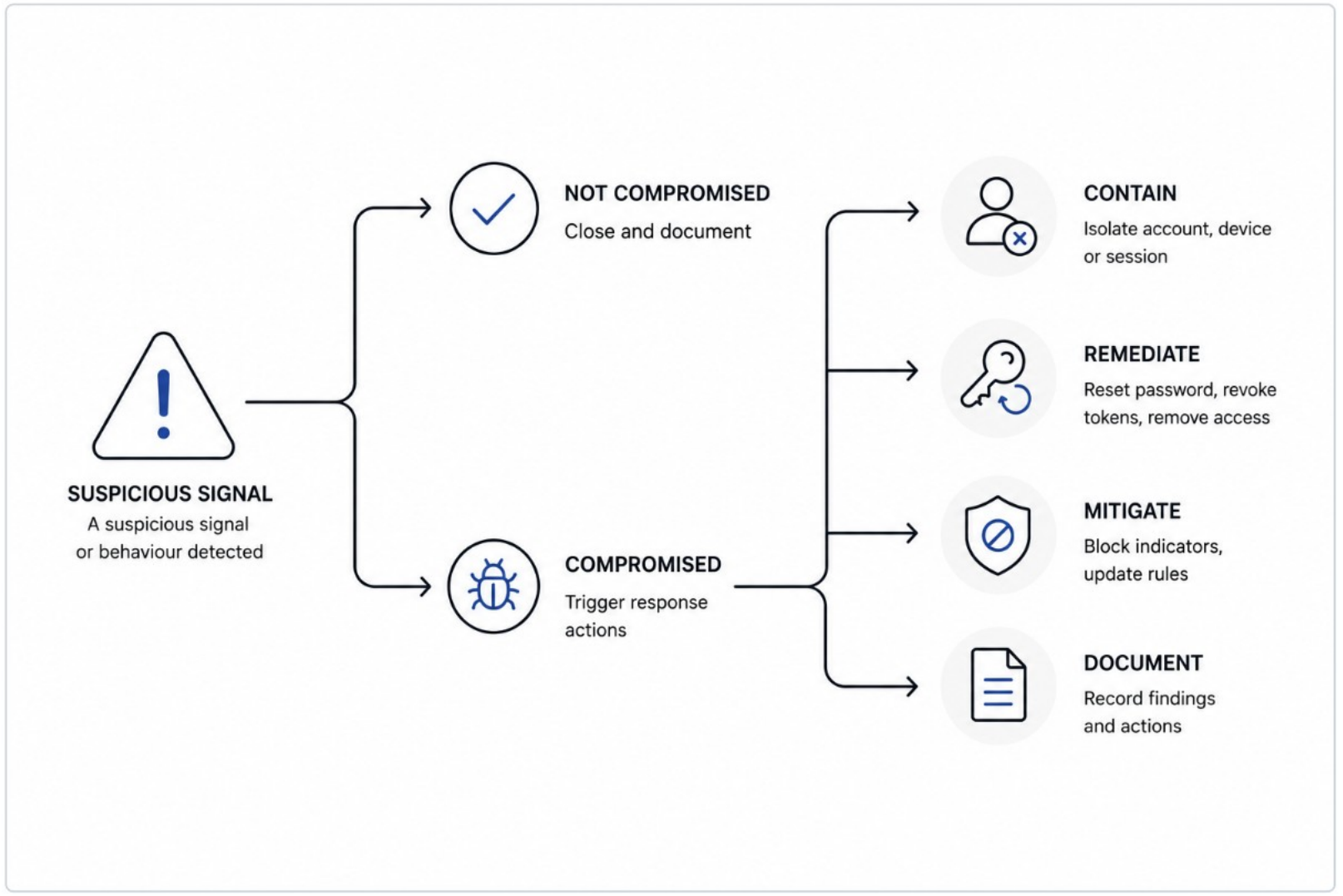
Know which ATT&CK techniques or behaviours you have actually tested, instead of assuming your detection works.



Switch_

PlayBooks

Hunting Playbooks



Hunting Playbooks

1 Suspicious user account



- Reset password
- Revoke sessions tokens
- Check account activity
- Hunt and scope across environment

2 Suspicious email



- Move to quarantine or remove
- Check if user clicked the link
- Check if attachment was opened
- See if same email reached other users

3 Suspicious device or login



- Block device or IP
- Revoke sessions enforce reauth
- Investigate device, IP and session details
- Monitor for similar activity

4 Malicious domain or network activity

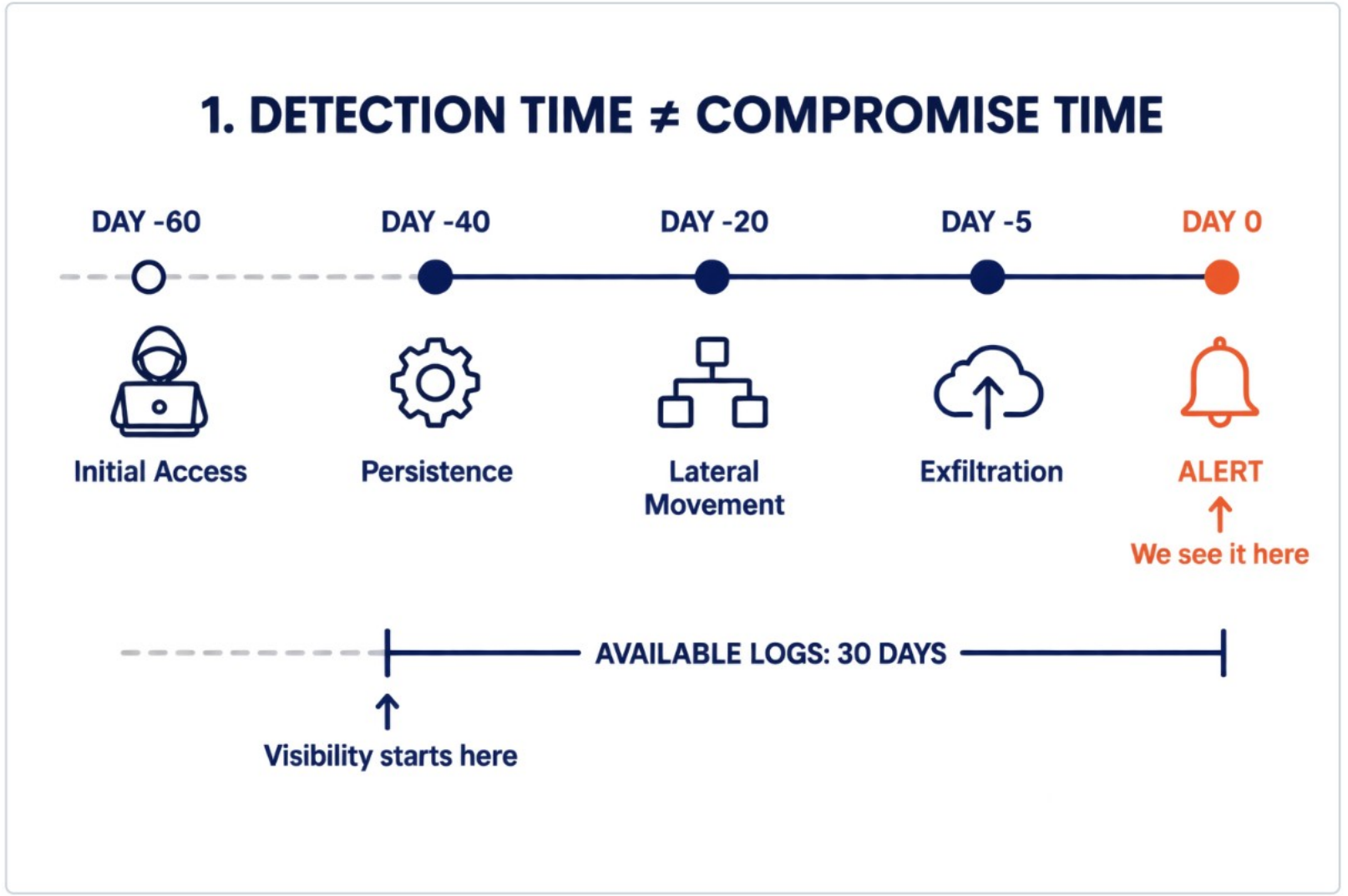


- Block domain or IP
- Check connections and affected devices
- Hunt for same IOC across environment
- Document findings and monitor

Switch

Log Retention

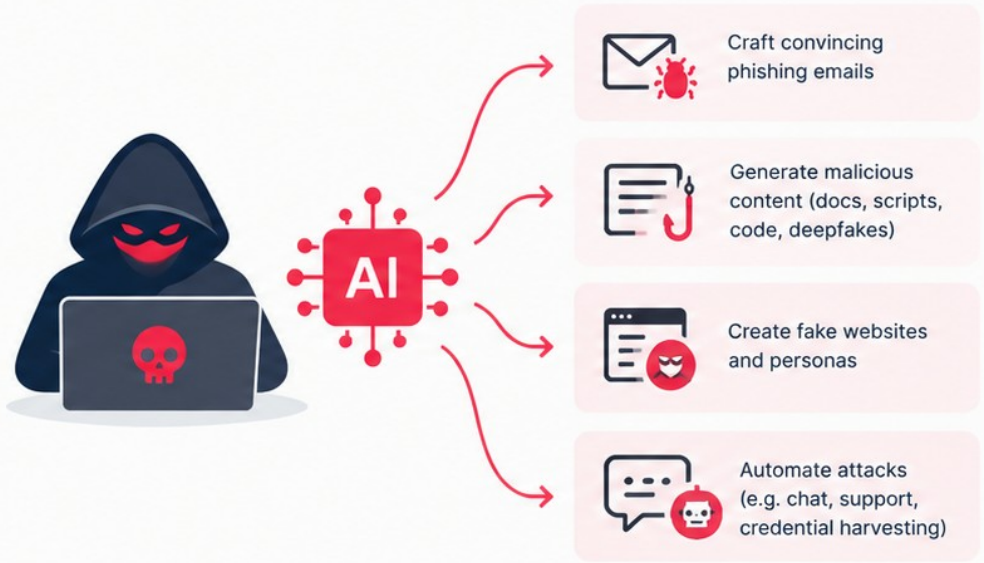
Log Retention



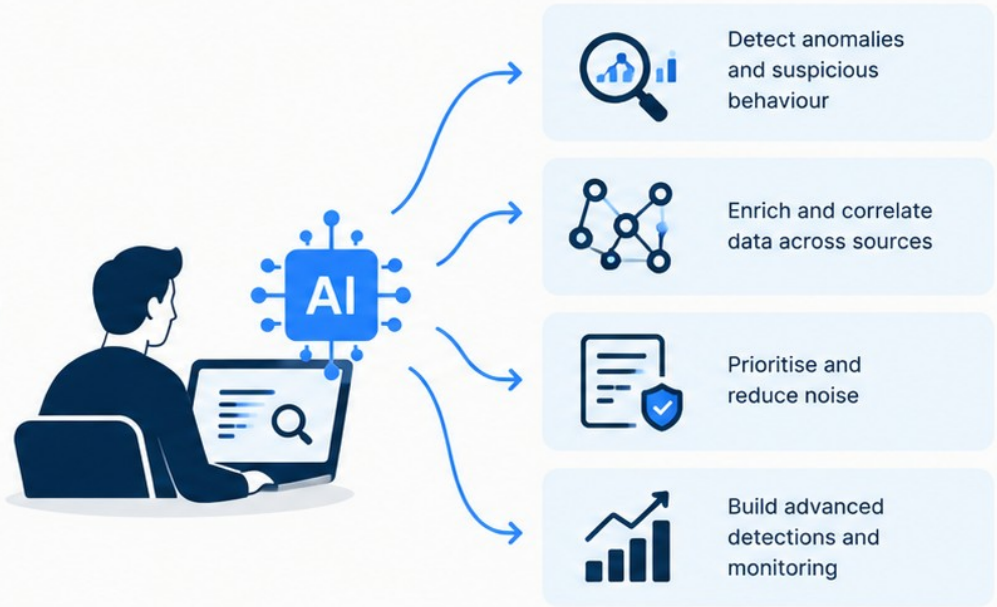
Switch

Threat Hunting and AI

Threat Hunting on the AI era



VS



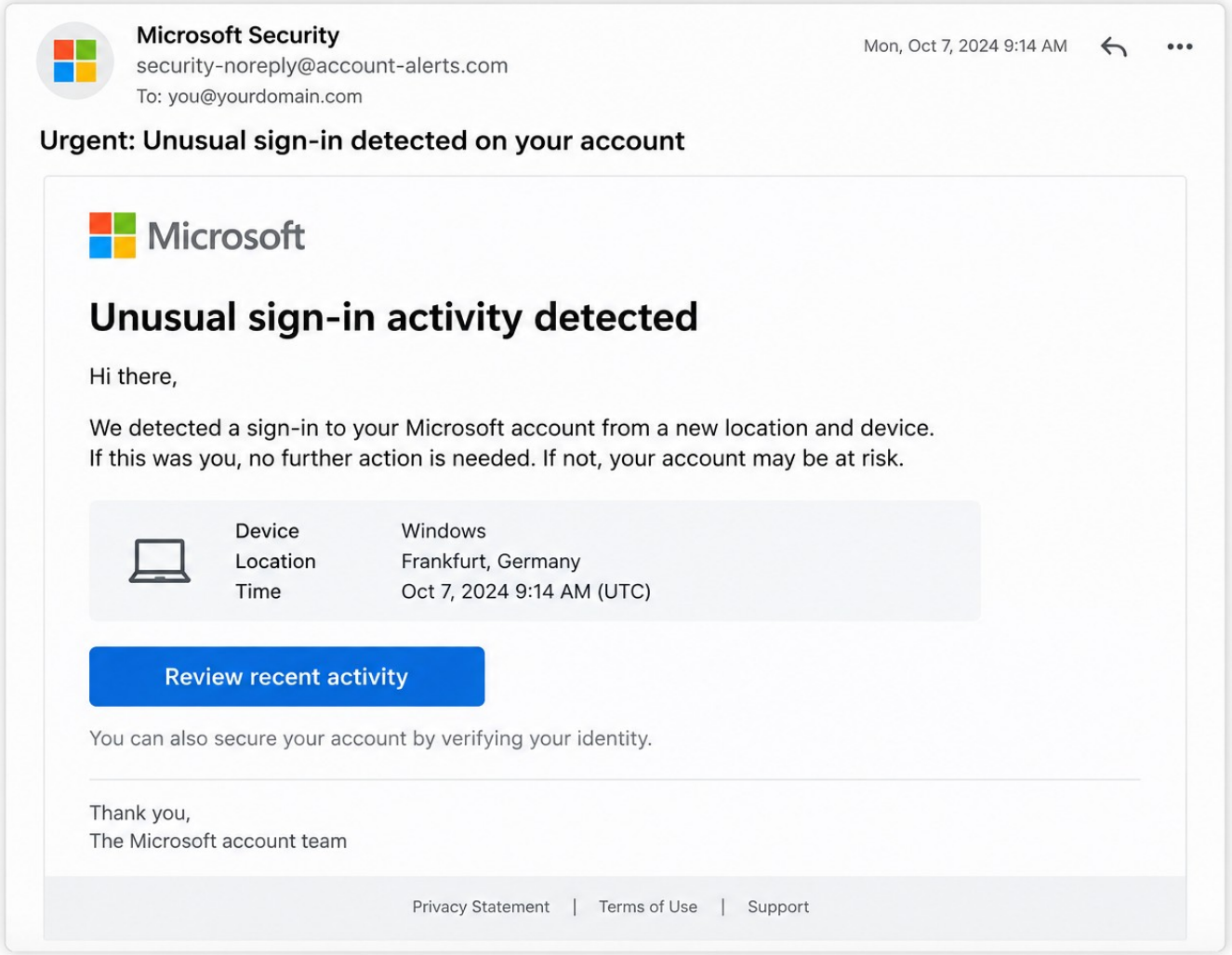
Adversaries use AI to:

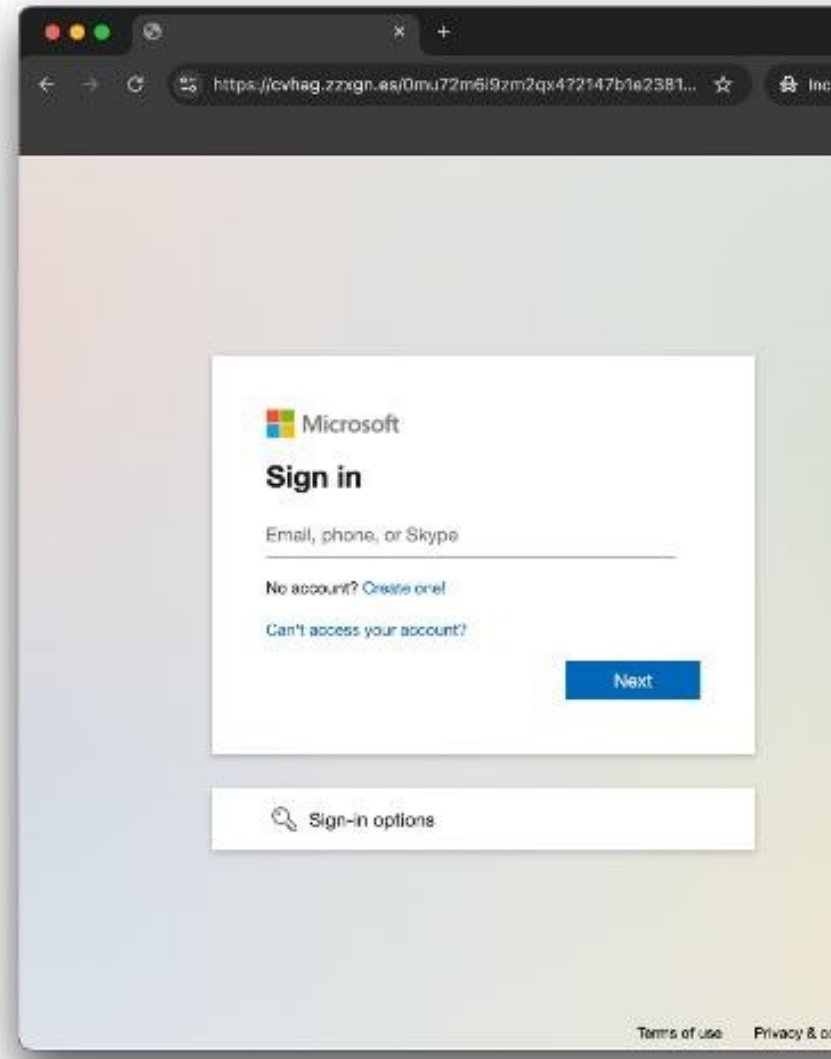
Scale their attacks, create realistic content, and automate social engineering — faster, cheaper and with higher success rates.

Threat hunters use AI to:

Find what others might miss, correlate signals, understand the bigger picture and detect threats earlier and with more precision.

AI Reality over Threat Hunting





Source: https://www.isaca.org/resources/isaca-journal/issues/2025/volume-1/artificial-intelligences-dual-role-in-phishing-attacks

Switch

Threat Hunting Community

Threat Hunting Community

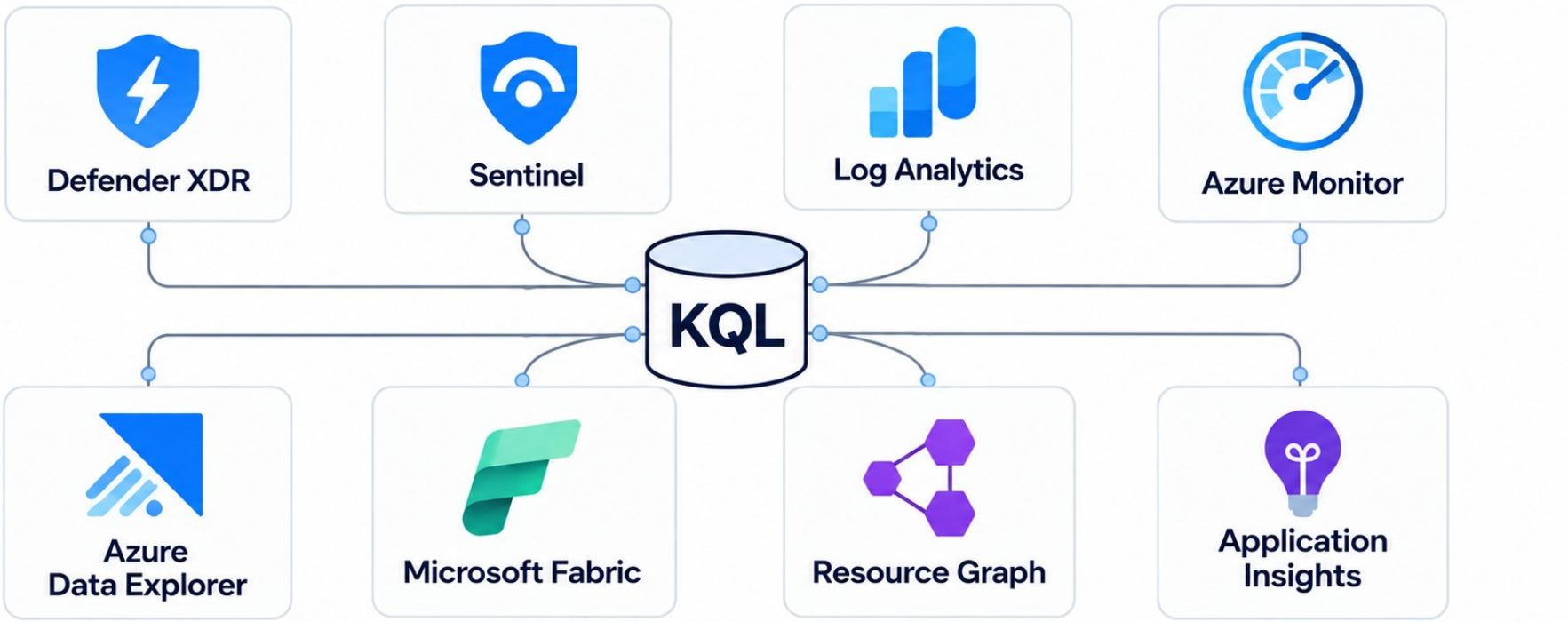


Switch

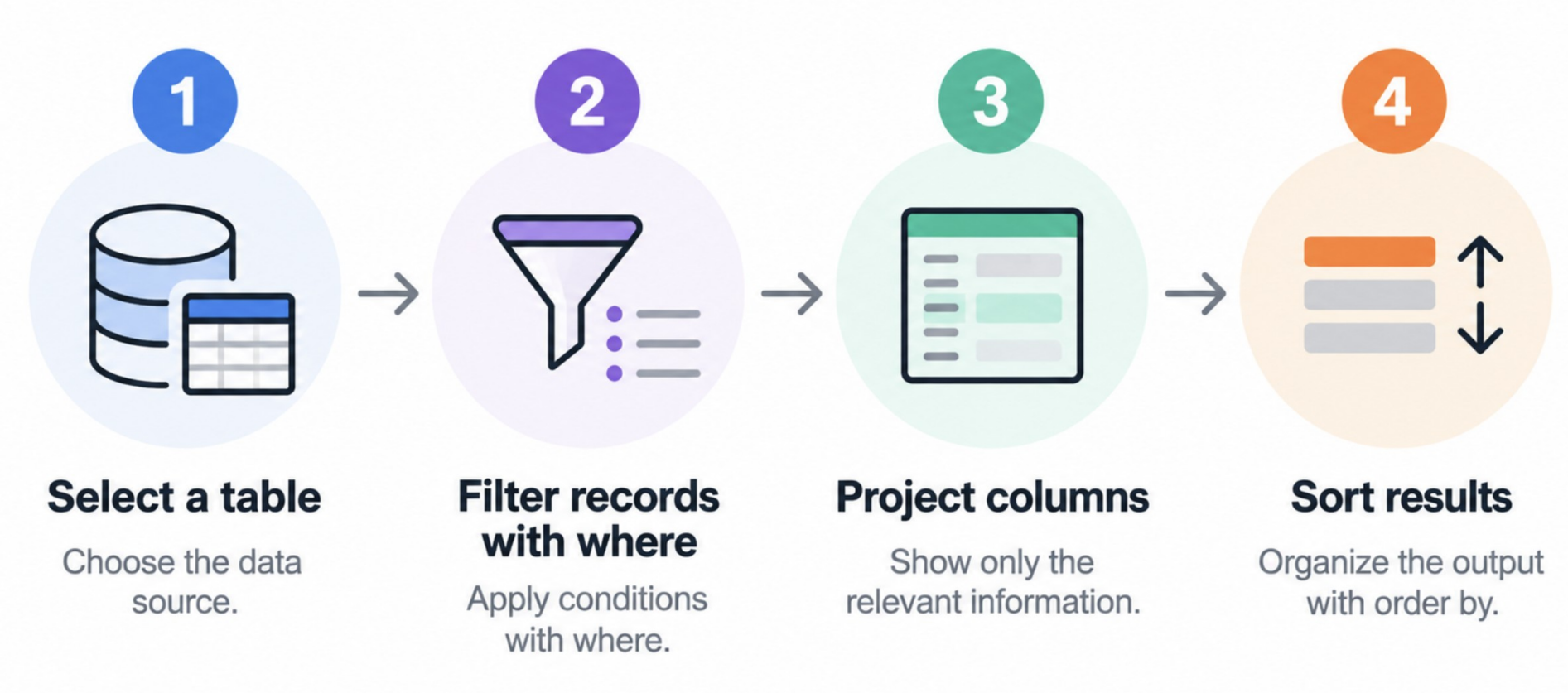
Kusto Query Language (KQL)

Kusto Query Language (KQL)

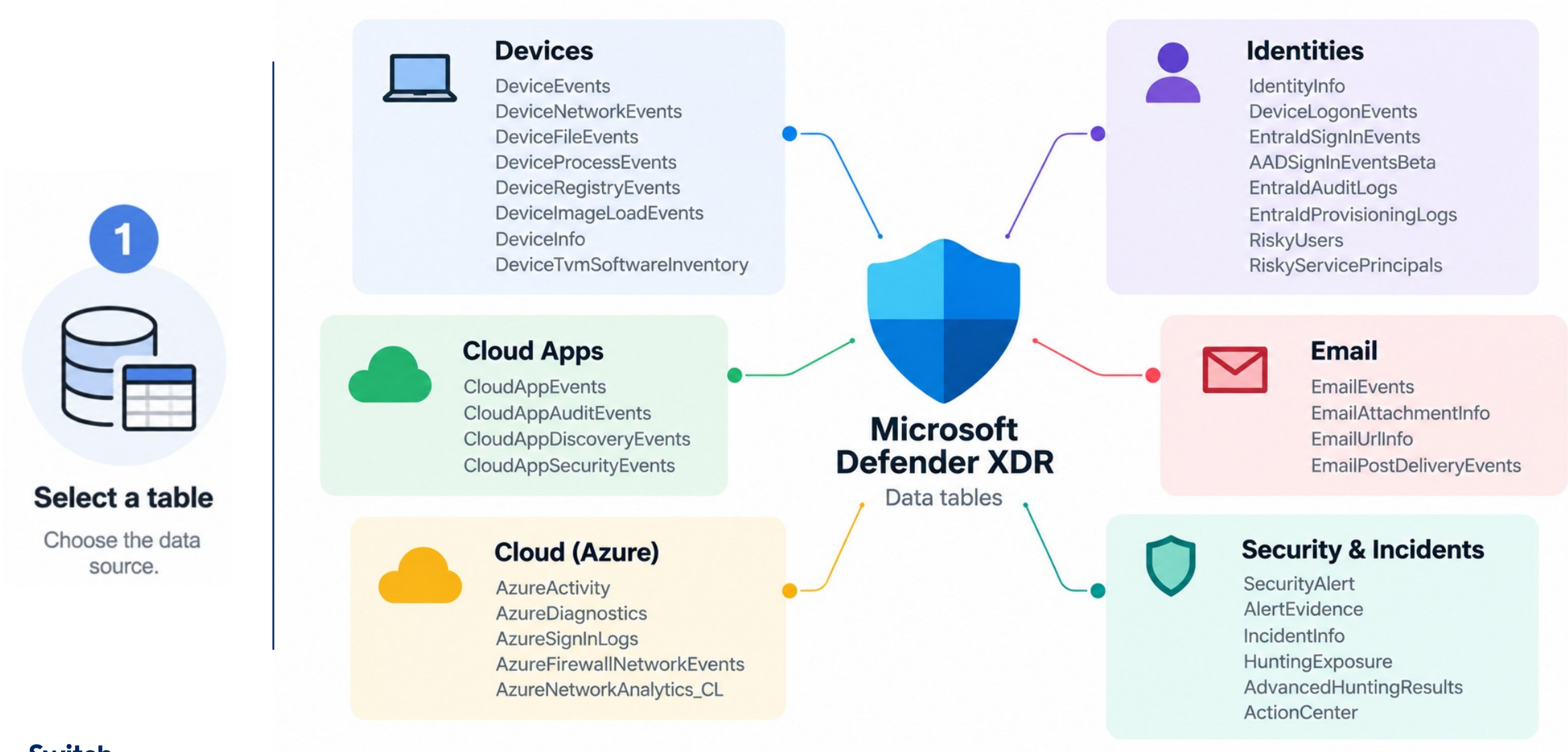
KQL is a language developed by Microsoft, designed to explore, filter, analyze, and correlate large volumes of data efficiently.
KQL shares similarities with SQL, as both support filtering, sorting, aggregations, and joins.
KQL is particularly well-suited for log analysis, threat hunting, and detection engineering, making it easier to identify patterns, investigate suspicious activities, and transform raw data into actionable insights.



Kusto Query Language (KQL)



Kusto Query Language (KQL)



Kusto Query Language (KQL)

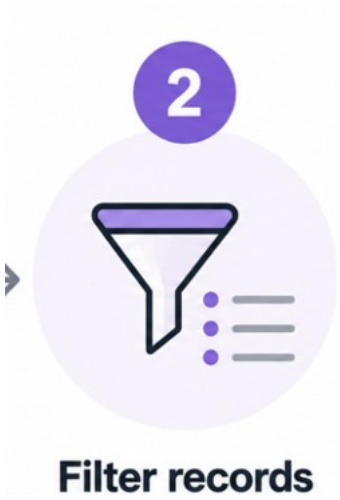
KQL reads from left to right: each pipe transforms the previous result.

- **Source table**
- **Chained operators**
- **Result ready to explore**

```
EmailEvents
| where TimeGenerated > ago(1d)
| distinct Subject, SenderDomain
```

```
EmailEvents
| where TimeGenerated > ago(1d)
| summarize count() by
NetworkMessageId
```

Kusto Query Language (KQL)



where

Filter rows that match a condition.

```
EmailEvents
| where ThreatTypes == "Phish"
```



Operators

Compare values in where.

==	Equal to
!=	Not equal to
>	Greater than
>=	Greater or equal
<	Less than
<=	Less or equal

Logical operators

Combine multiple conditions.

```
DeviceEvents
| where ActionType == "ProcessCreated"
        and FileName endswith ".exe"
```



Filter data

Keep only the relevant records

String and set operators

Work with text values.

```
EmailEvents
| where Subject has "invoice"
  or SenderFromDomain in ("microsoft.com",
     "office.com")
```

Functions

Use functions inside where.

```
SigninEvents
| where tolower(UserPrincipalName)
        endswith "@contoso.com"
```



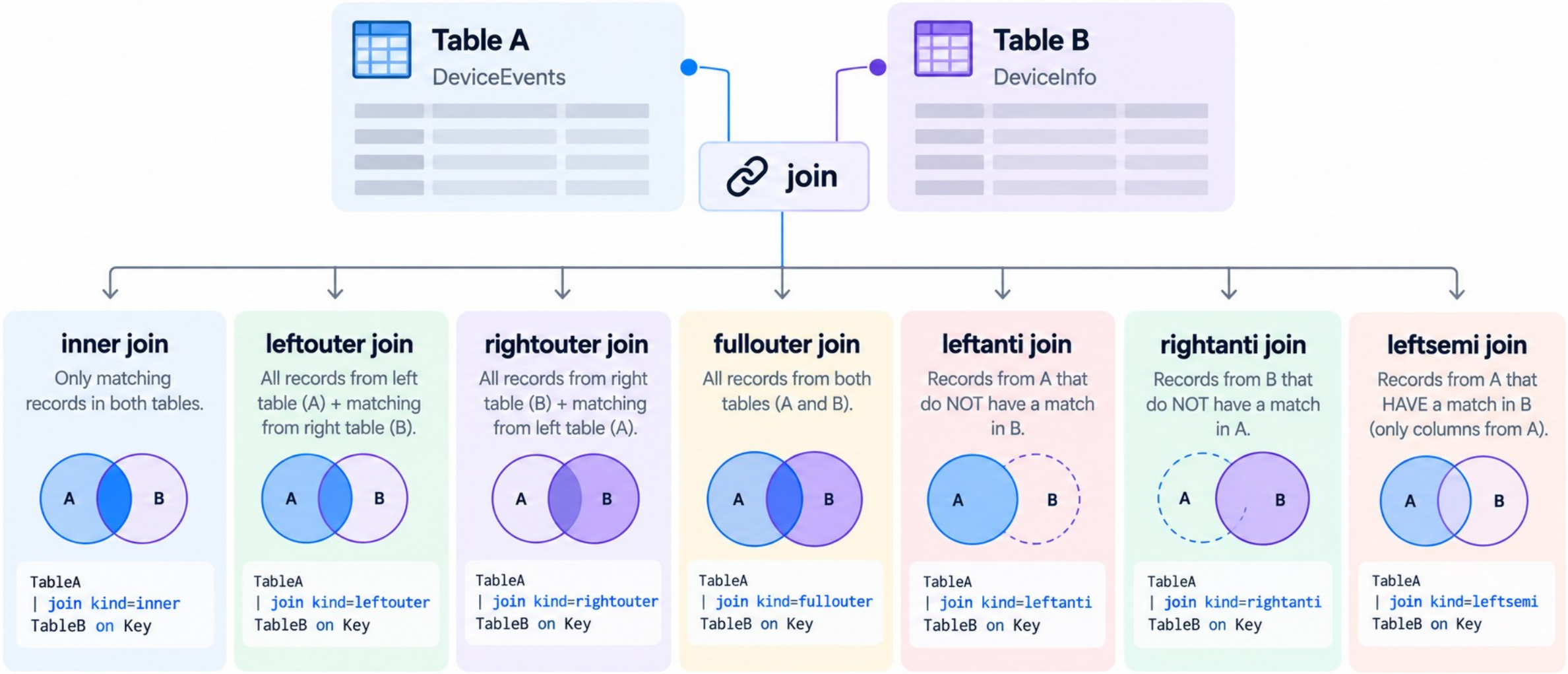
Conditional filtering with if()

Create dynamic conditions.

```
EmailEvents
| extend Risk = iff(ThreatTypes has "Phish",
                    "High", "Low")
| where Risk == "High"
```

Switch_

Kusto Query Language (KQL)



Essential Aggregations in KQL

Summarize, calculate and analyze your data

count()

Count the number of records.




```
DeviceEvents
| summarize count()
```

dcount()

Count distinct values (unique).




```
DeviceEvents
| summarize dcount(
  AccountName)
```

sum()

Calculate the sum of numeric values.

10
20
30

→ 60

```
DecurityAlert
| summarize sum(Count)
```

avg()

Calculate the average of numeric values.

10
20
30

→ 20

```
DeviceNetworkEvents
| summarize avg(BytesSent)
```

min() / max()

Get the minimum or maximum value.

2026-10-01
2026-10-05
2026-10-08

→ min 2026-10-01

→ max 2026-10-08

```
DeviceEvents
| summarize min(Timestamp),
            max(Timestamp)
```

make_set()

Create a set of distinct values (unique list).

contoso.com
microsoft.com
contoso.com
google.com

→ contoso.com, microsoft.com, google.com

```
DeviceNetworkEvents
| summarize make_set(
  RemoteUrl)
```

make_list()

Create a list of values (including duplicates).

80
443
80
8080

→ [80, 443, 80, 8080]

```
DeviceNetworkEvents
| summarize make_list(
  RemotePort)
```

arg_max() / arg_min()

Get the full record with the max/min value.

User	Time
user1	10:00
user2	12:30
user3	09:15

```
DeviceLogonEvents
| summarize arg_max(
  Timestamp, *)
```

countif()

Count records that meet a condition.

Type	Count
Success	120
Failure	35

```
DeviceLogonEvents
| summarize countif(
 ActionType == "LogonSuccess")
```

percentiles()

Calculate percentiles (e.g. 50, 90, 95).

Percentile	Value
P50	120
P90	850
P95	1,200

```
DeviceNetworkEvents
| summarize percentiles(
  BytesSent, 50, 90, 95)
```

Switch_

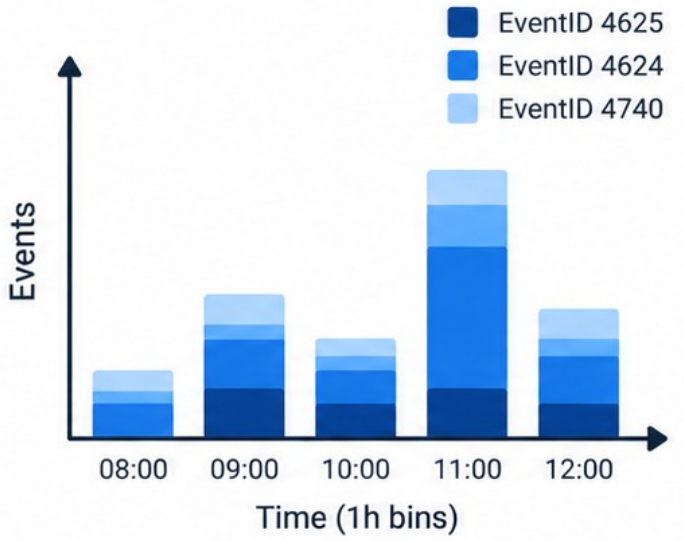
Group and Count in KQL

SecurityEvent

TimeGenerated	EventID	Account
2026-10-20 10:12:34		
2026-10-20 10:25:11		
2026-10-20 10:48:07		
2026-10-20 11:03:21		
2026-10-20 11:15:42		
2026-10-20 11:37:56		

bin()
1 hour

```
SecurityEvent
| summarize Events=count()
  by bin(TimeGenerated, 1h),
  EventID
```



Raw events
Many individual events with timestamps.

Group and count
Aggregates events by time interval and EventID.

Results
Event counts per hour and EventID, revealing patterns.

Detection Rules + Actions

New query* | New query*

Run query | Last 7 days | Save | Share link | Create detection rule

Query

```
1  DeviceEvents
2  | where FolderPath contains "Users\\Public" and FileName !endswith ".lnk"
3  | distinct Timestamp,DeviceName, DeviceId, ActionType, FileName, FolderPath, ReportId
```

Azure Sentinel

DefenderXDR

Switch_

Notification Alert

Action

Devices

- Isolate device
- Collect investigation package
- Run antivirus scan
- Initiate investigation
- Restrict app execution

Files

- Allow/Block
- Quarantine file

Users

- Mark user as compromised
- Disable user
- Force password reset

Emails

- Move to mailbox folder
- Delete email

KQL First Contact → sergioalbea.com/465-2/

Case1: Which is the senderdomain sending emails with the IP: **5.79.109.115** ?

Run Ctrl ↵ | Clear | Ctrl+

```
EmailEvents
| where SenderIPv4 has '5.79.109.115'
| summarize by SenderFromDomain
```

1 result 3.00 ms

SenderFromDomain
foreste-art.shop

Case2: How many different **Threat Names** are identified into the received Emails?

```
EmailEvents
| distinct ThreatNames
```

9 results 1.00 ms

ThreatNames
Phish.MailBait.A
Trojan:Script/Phonzy.B!ml
Spam.Bulk
Trojan:Win32/Qakbot
Backdoor:Win32/Qbot
Trojan:Script/Wacatac.B!ml
Phish.Credential.B
TrojanDownloader:O97M/Emotet

Case3: Which recipients have received Email with **Malware** and have been delivered into **Inbox** Folder?

```
EmailEvents
| where ThreatTypes has 'Malware' and DeliveryLocation has 'Inbox'
| summarize by RecipientEmailAddress
```

4 results 2.00 ms | Copy as CSV

RecipientEmailAddress
lena.kaufmann@contoso.ch
legal@contoso.ch
sofia.moser@contoso.ch
nina.frei@contoso.ch

Case4: How many **distinct** emails have been **delivered** into **Inbox** Location?

```
EmailEvents
| where DeliveryLocation has 'Inbox'
| summarize dcount(NetworkMessageId) by DeliveryLocation
```

1 result 1.00 ms | Copy as CSV

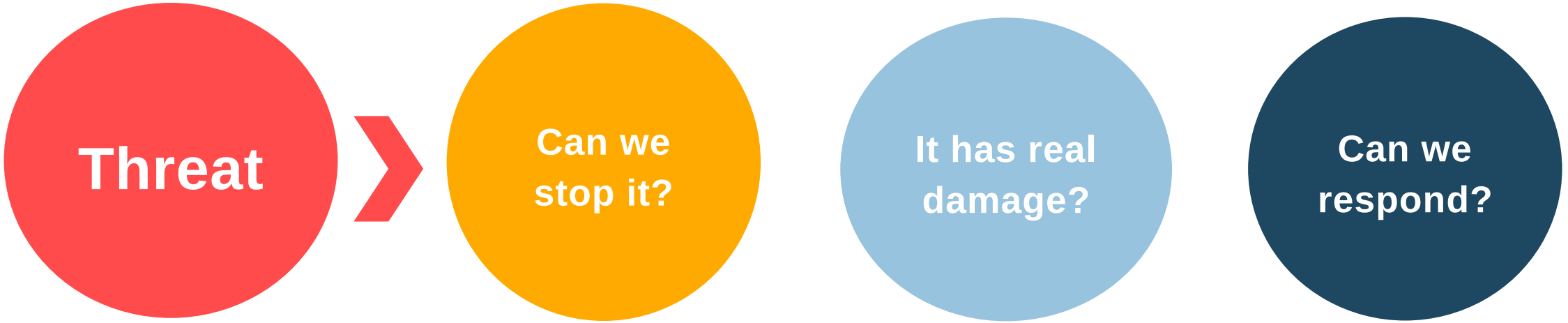
DeliveryLocation	dcount(NetworkMessageId)
Inbox	235

Switch

Switch

Threat Hunting scenarios

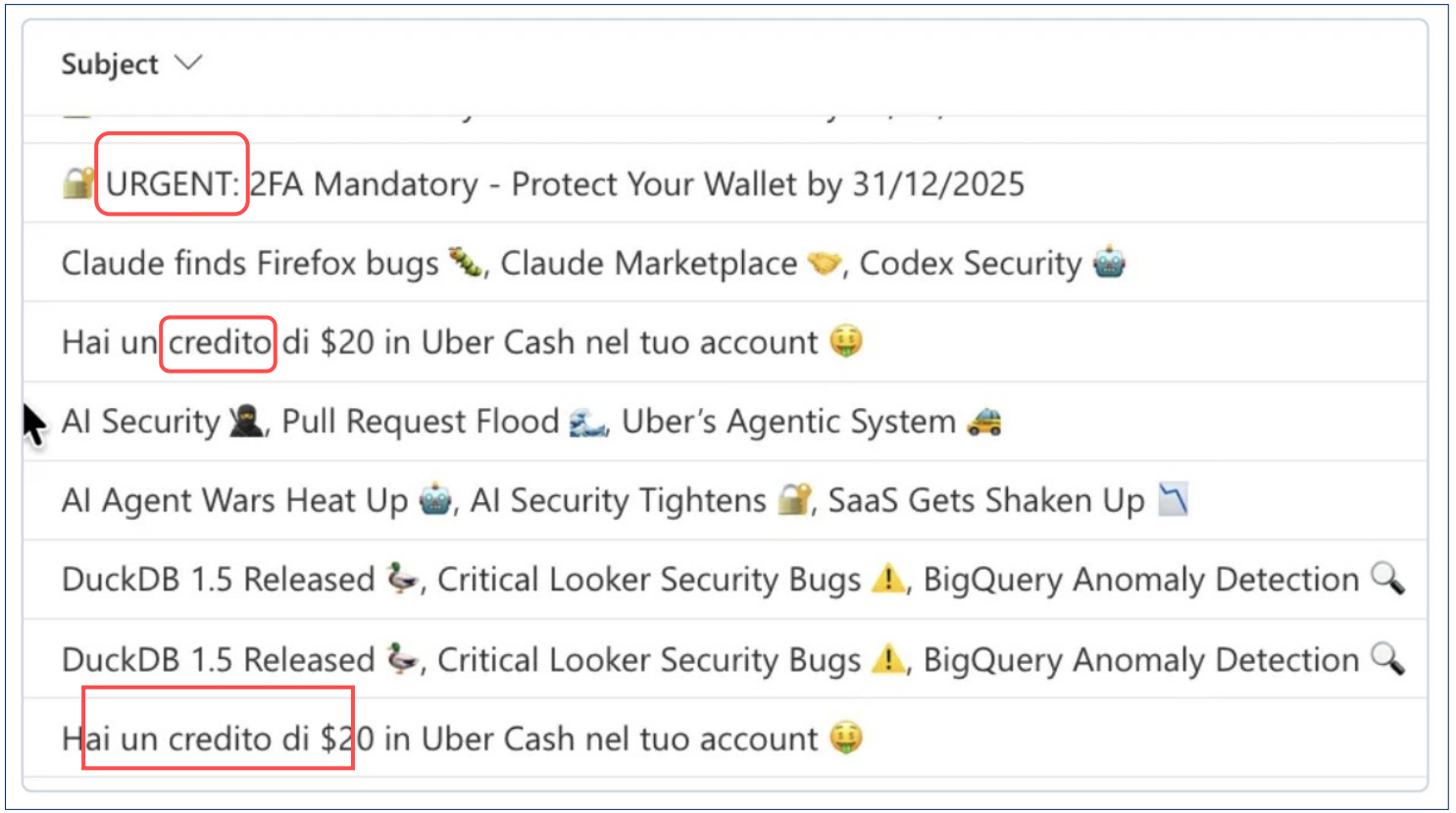
Threat Hunting Result Analysis



Switch

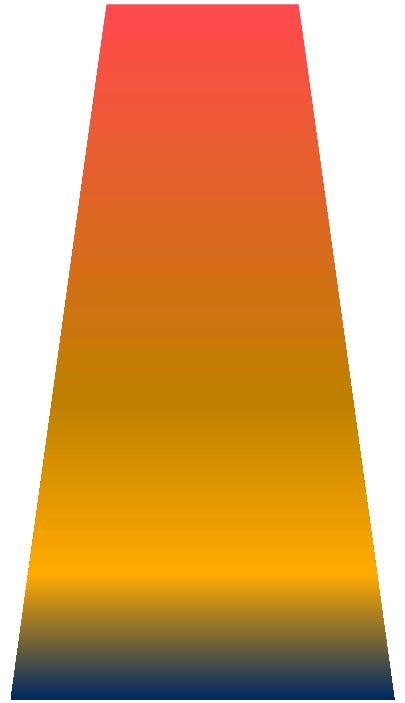
Threat Hunting applied on Emails

Email with Emojis in the Subjects



Threat Hunting

Risk Score

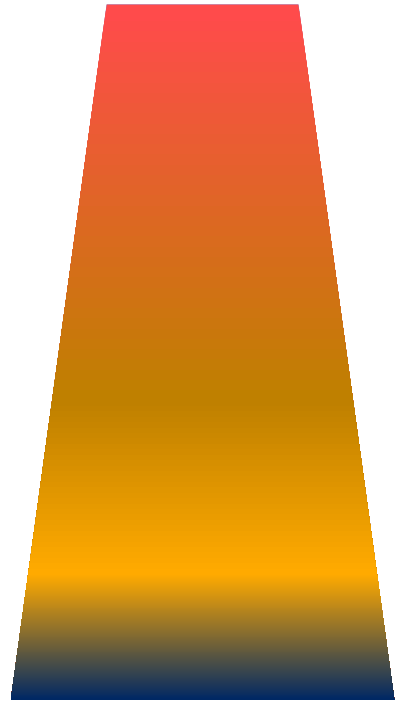


Email with Emojis in the Subjects

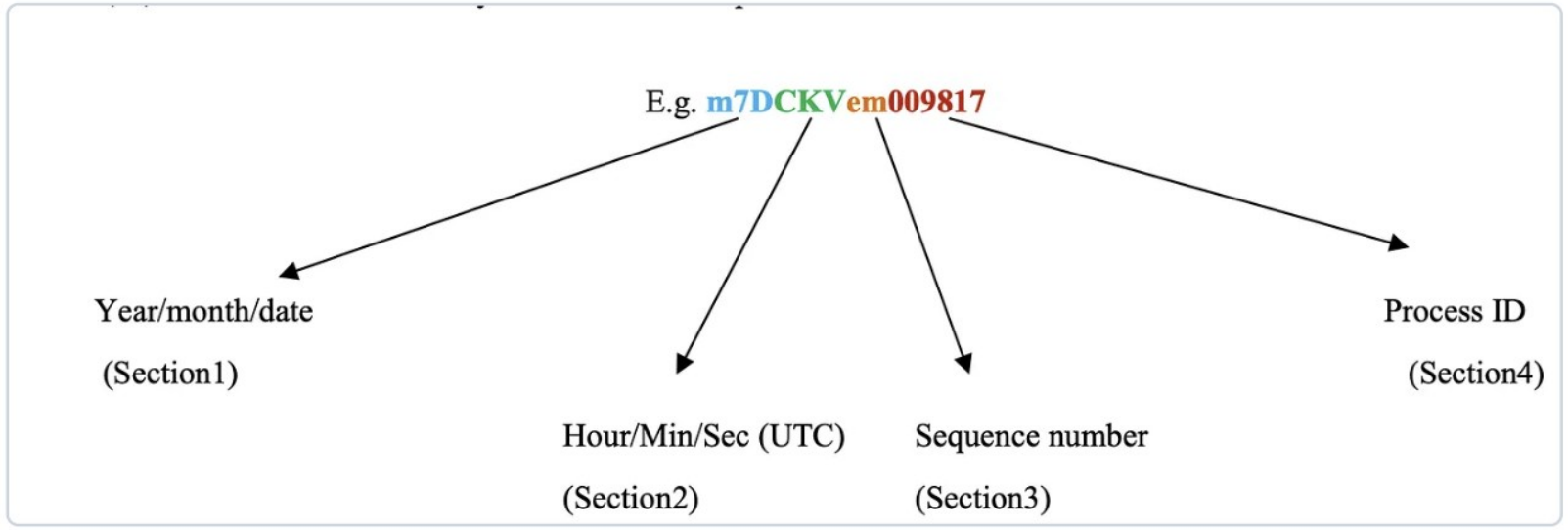
Country	DetectedLanguage	EmailLanguage	EmailCount	ThreatTypes
Argentina	de	de	5	["Phish"]
Serbia	de	de	4	["Phish, Spam"]
France	en	en	1	["Phish, Spam"]
Seychelles	de	de	1	["Phish, Spam"]
Seychelles	de	de	4	["Spam","Phish, Spam"]
Russia	de	de	1	["Phish"]
Ireland	de	de	8	["","Phish, Spam"]
Ireland	de	de	4	["","Phish","Phish, Spam"]
Japan	en	en	7	["Spam","Phish, Spam"]
France	en	en	1	["Phish, Spam"]

Threat Hunting

Risk Score



Email Hunting over InternetMessageId



SecurityEvent

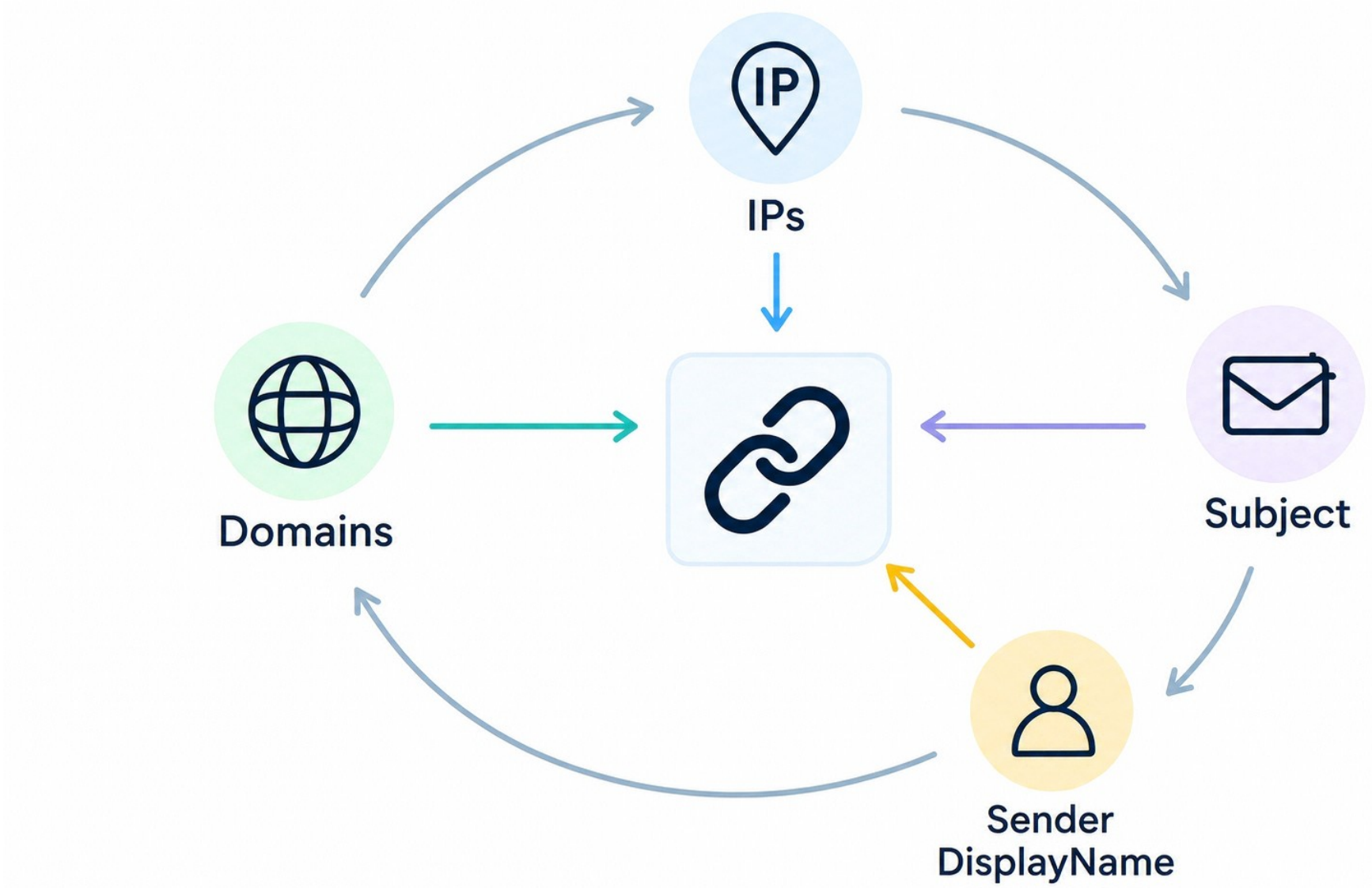
TimeGenerated	EventID	Account
2026-10-20 10:12:34		
2026-10-20 10:25:11		
2026-10-20 10:48:07		
2026-10-20 11:03:21		
2026-10-20 11:15:42		
2026-10-20 11:37:56		

For sending systems where the identifier contains **the message creation time**, those two timestamps are expected to be close. But what happens when they are not?

A large gap can surface messages generated long before delivery and give us another signal to investigate.

The true-positive ratio was surprisingly high, and several suspicious emails surfaced that had not been flagged by any other detection.

Phishing Campaigns Classification

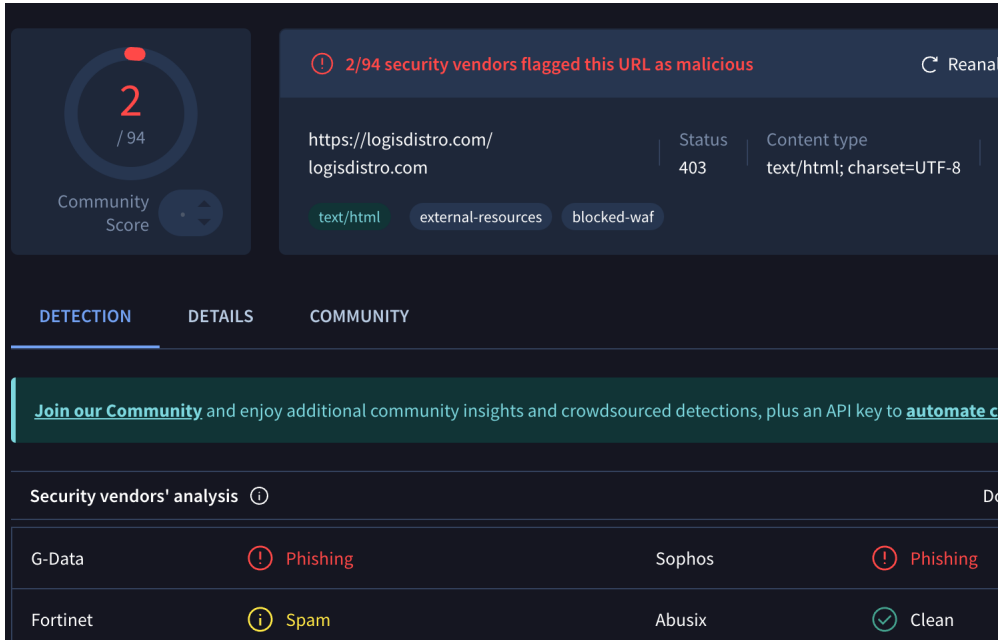


Switch

Phishing Campaigns statistics (*dcount*)

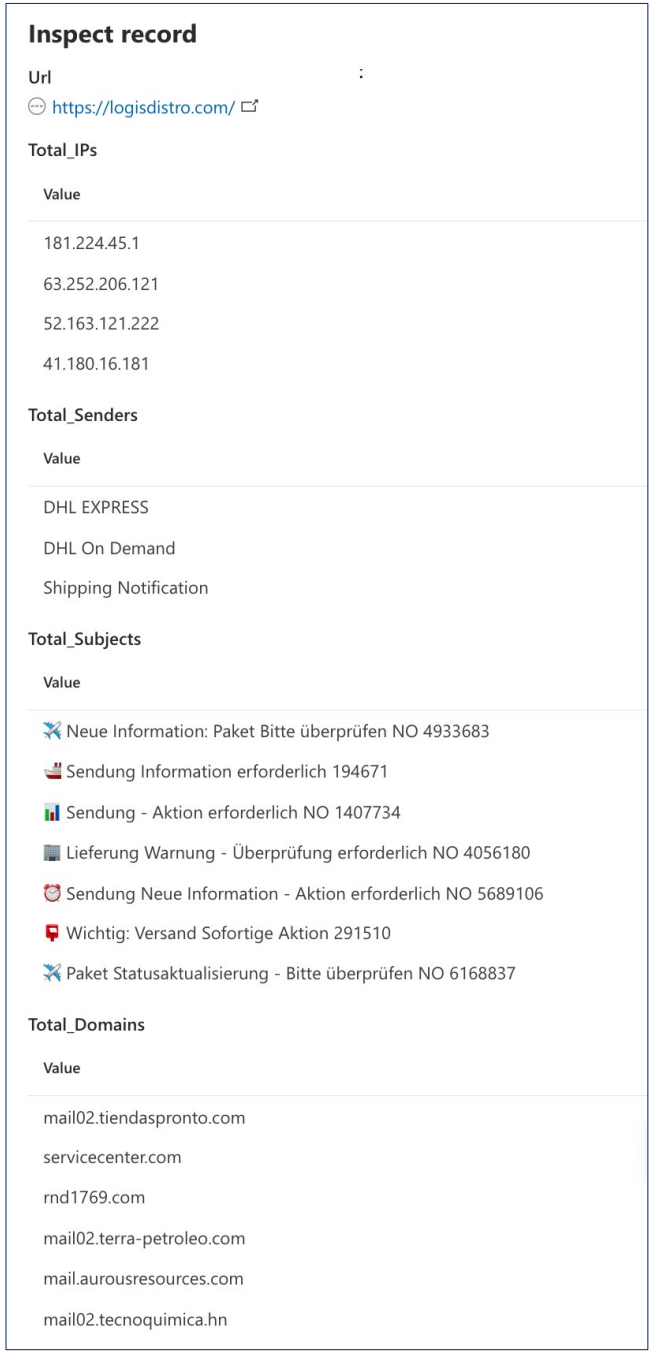
ThreatTypes	Url	Total_IPs	Total_Senders	Total_Subjects	Total_Domains
Phish	https://logisdistro.com/	5	3	10	7

```
EmailEvents
| where ThreatTypes has 'Phish'
| join kind=inner (EmailUrlInfo) on NetworkMessageId
| extend SenderIP =
iff(isnotempty( SenderIPv4),SenderIPv4,SenderIPv6)
| summarize Total_IPs=
dcount(SenderIP),Total_Senders=dcount(SenderDisplayName)
,Total_Subjects=dcount(Subject),
Total_Domains= dcount(SenderFromDomain) by Url
```



Phishing Campaigns summary (*make_set*)

```
EmailEvents
| where ThreatTypes has 'Phish'
| join kind=inner (EmailUrlInfo) on NetworkMessageId
| extend SenderIP =
iff(isnotempty( SenderIPv4),SenderIPv4,SenderIPv6)
| summarize Total_IPs=
make_set(SenderIP),Total_Senders=make_set(SenderDisplayName),Total
_Subjects=make_set(Subject),Total_Domains=
make_set(SenderFromDomain) by Url
```



Phishing Campaigns summary (*Distinct Days + DeliveryLocation*)

ThreatTypes	Url	Total_IPs	Total_Senders	Total_Subjects	Total_Domains	dcount_Time_	set_Time_	Delivered_on
Phish	https://ssl.gstatic.cor	["2607:f8b0:4864:20::847","'	["Céline Etter (über Google	["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-20	["Inbox/folder","Quarantine"]
Phish	https://www.gstatic.c	["2607:f8b0:4864:20::847","'	["Céline Etter (über Google	["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-20	["Inbox/folder","Quarantine"]
Phish	https://www.google.	["2607:f8b0:4864:20::847","'	["Céline Etter (über Google	["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-20	["Inbox/folder","Quarantine"]
Phish	http://zoho.com/inv	["2a01:111:f403:c214::1","1	["Galaxus AG","NESPRESSC	["🧯 NUR HEUTE: 99% spai	["sender.zohoinvoice.com	7	["02-02-2026","29-01-202	["Quarantine","Junk folder","Inbox/folder"]
Phish	https://zoho.com/in	["2a01:111:f403:c214::1","1	["Galaxus AG","NESPRESSC	["🧯 NUR HEUTE: 99% spai	["sender.zohoinvoice.com	7	["02-02-2026","29-01-202	["Quarantine","Junk folder","Inbox/folder"]
Phish	https://zoho.com/in	["2a01:111:f403:c214::1","1	["Galaxus AG","NESPRESSC	["🧯 NUR HEUTE: 99% spai	["sender.zohoinvoice.com	7	["02-02-2026","29-01-202	["Quarantine","Junk folder","Inbox/folder"]
Phish	https://www.zoho.co	["2a01:111:f403:c214::1","1	["Galaxus AG","NESPRESSC	["🧯 NUR HEUTE: 99% spai	["sender.zohoinvoice.com	7	["02-02-2026","29-01-202	["Quarantine","Junk folder","Inbox/folder"]
Phish	https://email.notify.tl	["2607:f8b0:4864:20::e48","'	["Spotify","Spotify Premiur	["Ihre letzte Zahlung für Sp	["sqduiorn.firebaseapp.c	7	["24-01-2026","21-01-202	["Quarantine","Failed","On-premises/external"]
Phish	https://dhliteship.co	["20.211.160.68","211.105.(	["Liefer-Schnellversand","S	["📋 Schritt-für-Schritt: Zoll	["mail.tthgroup.com","rn	7	["10-01-2026","11-01-202	["Quarantine","Dropped","On-premises/external","Failed
Phish	http://www.phbern.c	["2a01:111:f403:da13::","2a	["","International Student (	["Undeliverable: Neuer Lin	["edu.schule-pieterlen.ch	7	["05-01-2026","13-01-202	["Quarantine","Failed","Junk folder"]
Phish	https://message-edit	["2607:f8b0:4864:20::948","'	["Spotify Premium","Spotif	["Ihre letzte Zahlung für Sp	["user-86647.firebaseapp	7	["20-01-2026","21-01-202	["Quarantine"]
Phish	https://email.notify.tl	["2607:f8b0:4864:20::e45","'	["Spotify Premium","Spotif	["Ihre letzte Zahlung für Sp	["user-86647.firebaseapp	7	["20-01-2026","21-01-202	["Quarantine"]
Phish	https://message-edit	["2607:f8b0:4864:20::e45","'	["Spotify Premium","Spotif	["Ihre letzte Zahlung für Sp	["user-86647.firebaseapp	7	["20-01-2026","21-01-202	["Quarantine"]
Phish	https://dhliteship.co	["23.90.103.66","211.105.6!	["Express-Zustellung","Kun	["[SPAM] 🚚 LKW-Sendung	["esa2.hc530-66.smtpi.co	7	["14-01-2026","15-01-202	["Quarantine","Dropped"]
Phish	https://zidf.miphsg.c	["217.26.49.147","217.26.4!	["UpdraftPlus on zidf.miph	["Backed up: Zug in die Fre	["zidf.miphsg.ch"]	7	["31-01-2026","28-01-202	["Quarantine","Junk folder"]
Phish	https://teamupdraft.	["217.26.49.147","217.26.4!	["UpdraftPlus on zidf.miph	["Backed up: Zug in die Fre	["zidf.miphsg.ch"]	7	["31-01-2026","28-01-202	["Quarantine","Junk folder"]
Phish	http://www.serafe.ch	["103.123.158.58","103.216	["Serafe.AG","SERAFE","SEF	["Abgabejahr 2026 – Bitte	["kpu.go.id","collins-ph.c	7	["05-01-2026","07-01-202	["Quarantine","Junk folder"]
Phish	https://static2.sharep	["2a01:111:f403:d200::2","2	["Florina Gjergji Lukic","Ra	["Florina Gjergji Lukic \"En	["outlook.com","goldbac	7	["05-01-2026","31-01-202	["Junk folder","Quarantine","Inbox/folder","Failed"]
Phish	https://static2.sharep	["2a01:111:f403:d200::2","2	["Florina Gjergji Lukic","Ra	["Florina Gjergji Lukic \"En	["outlook.com","sharepo	7	["05-01-2026","28-01-202	["Junk folder","Failed","Quarantine","Inbox/folder"]

Phishing Emails

Can we stop it?

```
EmailEvents
| where ThreatTypes has 'Phish' and ThreatTypes !contains "Spam"
| join kind=inner (EmailUrlInfo) on NetworkMessageId
| extend SenderIP = iff(isnotempty( SenderIPv4),SenderIPv4,SenderIPv6)
| extend Time_ = format_datetime( Timestamp, 'dd-MM-yyyy')
| summarize Total_IPs=make_set(SenderIP),Total_Senders=make_set(SenderDisplayName),
Total_Subjects=make_set(Subject),Total_Domains= make_set(SenderFromDomain),dcount(Time_),
make_set(Time_),Delivered_on=make_set(DeliveryLocation) by Url
```

It has real damage?

Total_Subjects	Total_Domains	dcount_Time_	set_Time_	Delivered_on
["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-202	["Inbox/folder","Quarantin
["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-202	["Inbox/folder","Quarantin
["Ein Dokument wurde für	["gmail.com"]	7	["17-01-2026","21-01-202	["Inbox/folder","Quarantin



Can we respond?









Switch

Threat Hunting applied on Network

Malicious Hotspot Networks shared via Iphone



Malicious Hotspot Networks shared via Iphone

Can we stop it?

```
DeviceNetworkInfo // Table
| where DefaultGateways has "172.20.10.1" //Iphone Gateways
| extend Network_Name = tostring(parse_json(ConnectedNetworks)[0]["Name"])
| where isnotempty(Network_Name)
//| where (Network_Name contains "Free" or Network_Name  contains "Open"  or Network_Name  contains "Airport" or Network_Name  contains "hotel")
| summarize by  Network_Name, DefaultGateways
```

It has real damage?

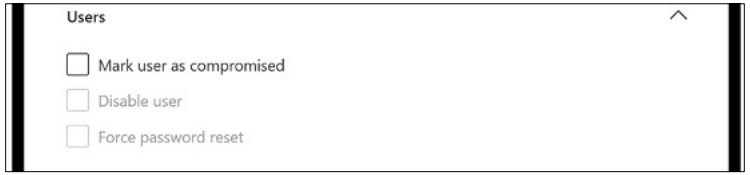
Network_Name	DefaultGateways
iPhone v[redacted]i	["172.20.10.1"]
[redacted]Phone	["172.20.10.1"]
[redacted]ela's iPhone 2	["172.20.10.1"]
Free Wifi	["172.20.10.1"]
AENA Airport	["172.20.10.1"]
[redacted]s iPhone	["172.20.10.1"]



Can we responsd?



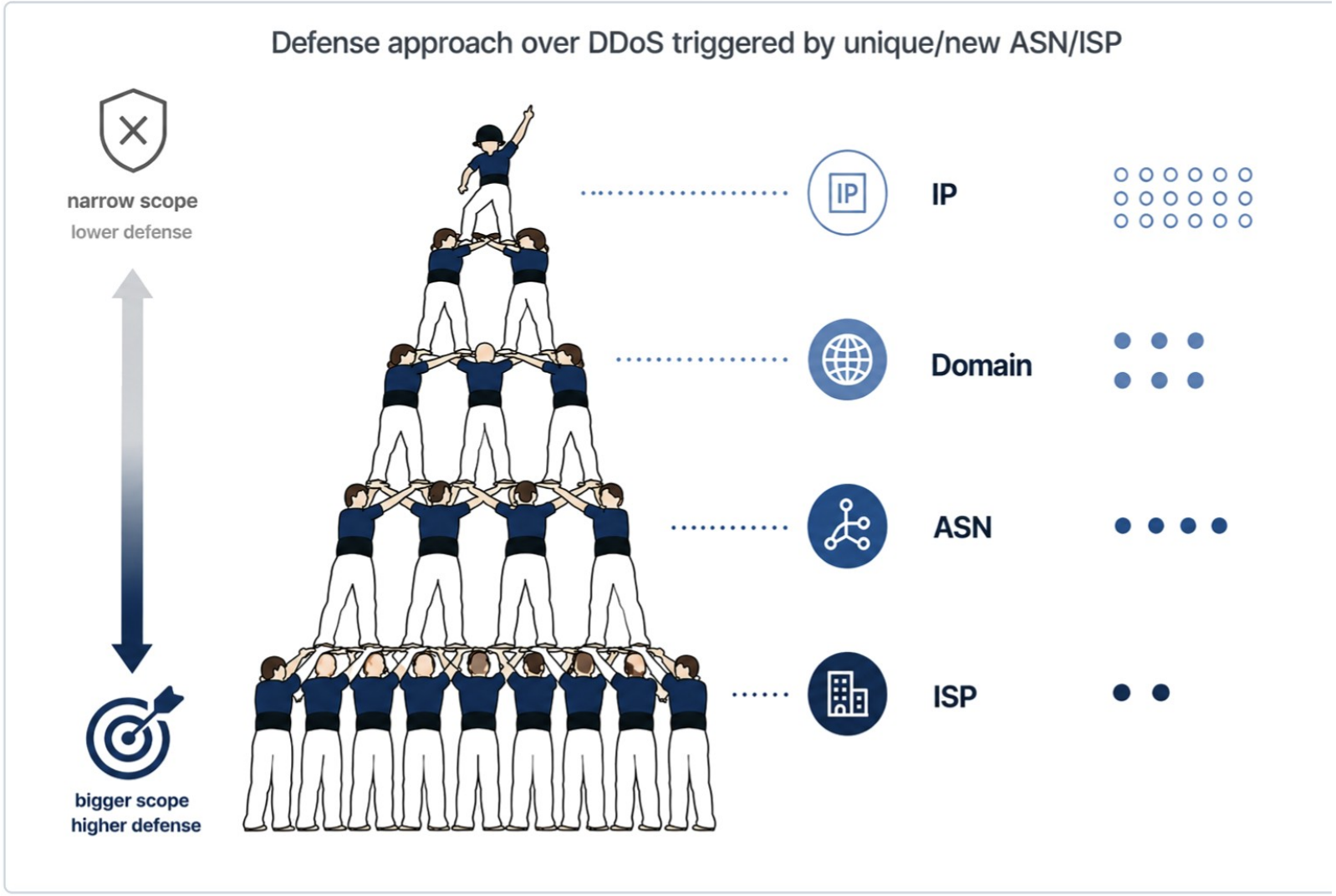




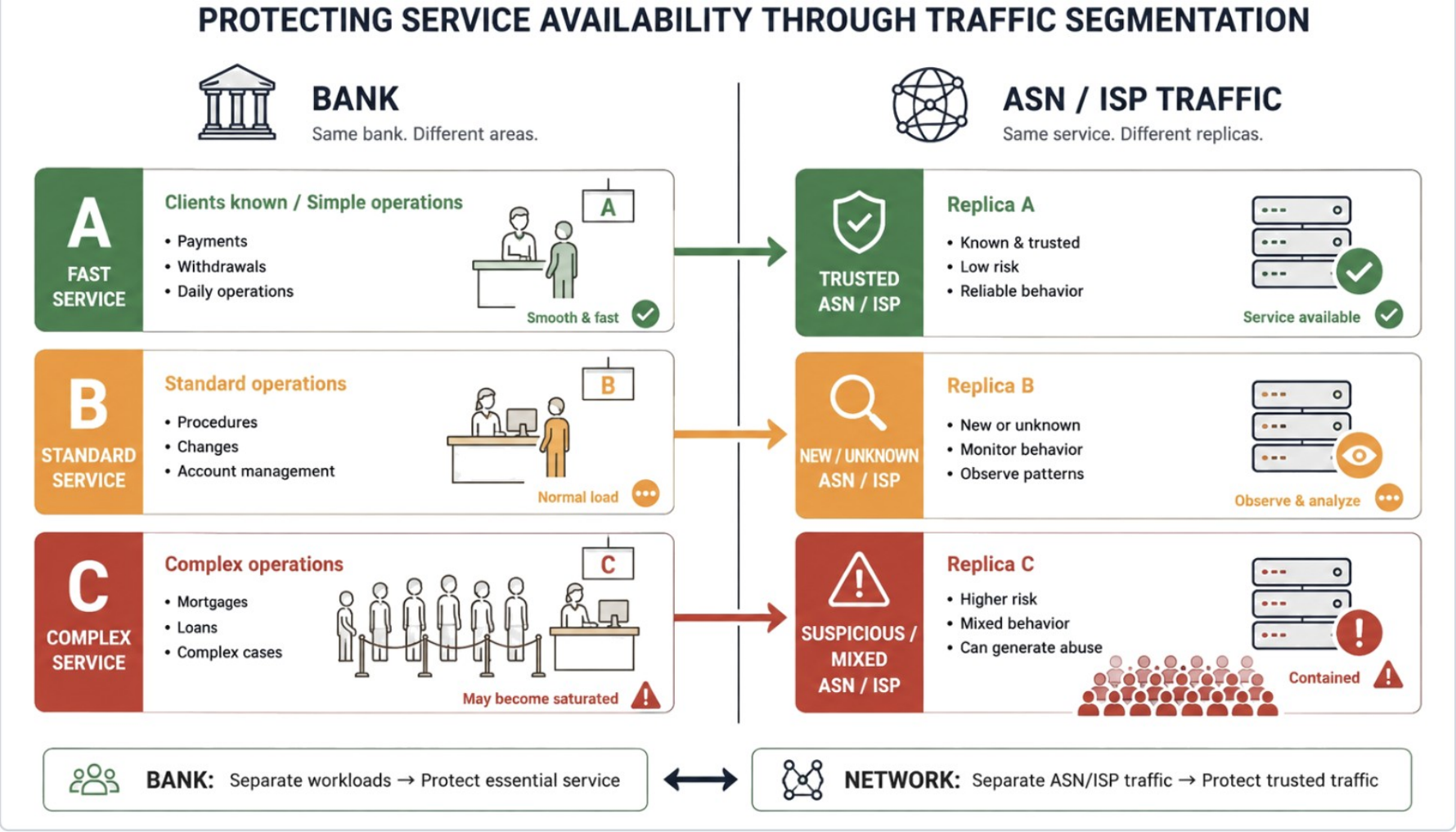


Switch_

Threat Hunting over DDoS Attacks



Threat Hunting over DDoS Attacks



Threat Hunting over DDoS Attacks

`Network-02` · `KQL-02` — High number of connections in a day when the average x day is X times lower

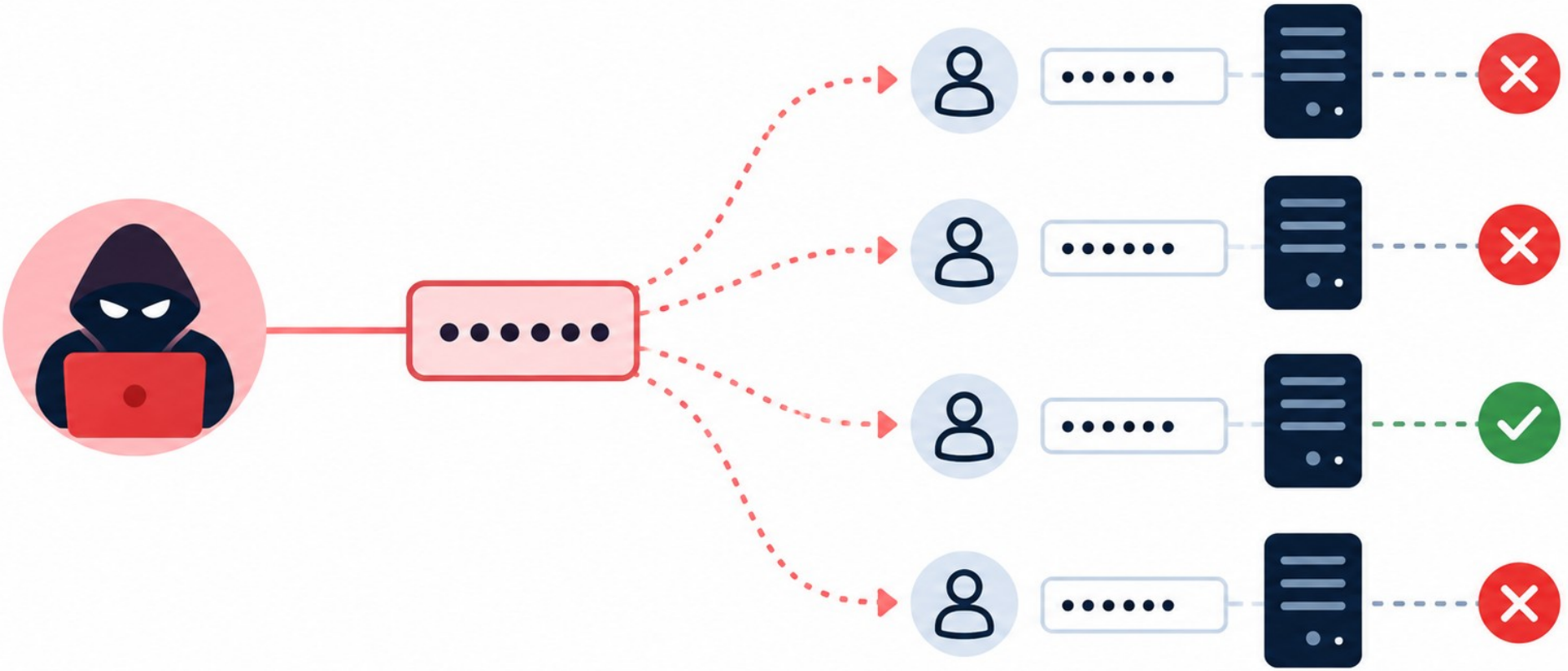
```
let CIDRASN = (externaldata (CIDR:string, CIDRASN:int, CIDRASNName:string)
['https://firewalliplists.gypthecat.com/lists/kusto/kusto-cidr-asn.csv.zip'] with
(ignoreFirstRecord=true));
let daily =
    DeviceNetworkEvents
    | where isnotempty(RemoteIP) and RemoteIPType !has "Private"
    | where Timestamp >= ago(7d)
    | evaluate ipv4_lookup(CIDRASN, RemoteIP, CIDR, return_unmatched=true)
    | where isnotempty (CIDRASN)
    | extend Day = format_datetime(startofday(Timestamp), 'yyyy-MM-dd')
    | summarize    Success_Connections = countif(ActionType == "ConnectionSuccess"),
                   Attempts_Connections = countif(ActionType == "ConnectionAttempt" or
ActionType =="ConnectionFailed"),
                   Inspected_Connections = countif( ActionType endswith "inspected"),
                   Requested_Connections = countif(ActionType == "ConnectionRequest"),
                   make_set(CIDR),make_set(RemoteIP),Connections_x_day = count() by
CIDRASN,CIDRASNName, Day;
let summary =
    daily  | summarize TotalConnections = sum(Connections_x_day),Distinct__Days =
count(),AvgConnectionsPerDay = avg(Connections_x_day)by CIDRASN;
daily
| join kind=inner (summary) on CIDRASN
| extend Multiply_avg = AvgConnectionsPerDay * 4
| where Multiply_avg < Connections_x_day or (Distinct__Days == 1 and Attempts_Connections
> 1000)
| project  CIDRASNName,CIDRASN,set_CIDR,set_RemoteIP, Day,Distinct__Days
,Connections_x_day, AvgConnectionsPerDay, TotalConnections, Success_Connections,
Attempts_Connections, Inspected_Connections,Requested_Connections
| order by Attempts_Connections
```

Switch

Switch

Threat Hunting applied on Identities

Password Spray Attacks



Password Spray Attacks



Can we stop it?

```
AlertEvidence //Table
| where Title has "Password Spray" and isnotempty(RemoteIP) //Condition
|join kind=inner (IdentityLogonEvents) on $left.RemoteIP == $right.IPAddress
| summarize
Sign_in_Result=make_set(ActionType),Logon_Types=make_set(LogonType),count() by
IPAddress,Location, AccountDisplayName, Application1
```

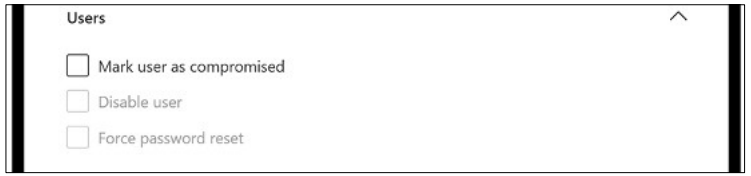
It has real damage?

IPAddress	Location	AccountDisplayName	Application1	Sign_in_Result	Logon_Types
155.2.192.216	US		Microsoft 365	["LogonFailed"]	["Login:logi
38.86.196.141	US		Microsoft 365	["LogonSuccess","LogonFailed"]	["SAS:Proce
201.201.88.199	CR		Microsoft 365	["LogonSuccess","LogonFailed"]	["SAS:Proce
27.72.62.165	VN		Microsoft 365	["LogonSuccess","LogonFailed"]	["SAS:Proce

Can we respond?





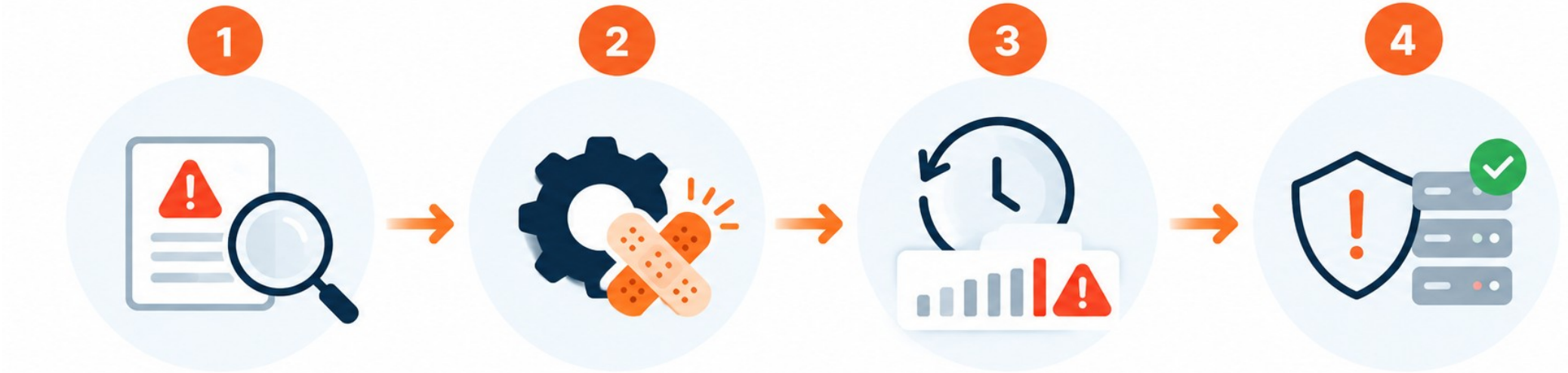




Switch

Threat Hunting applied on Software

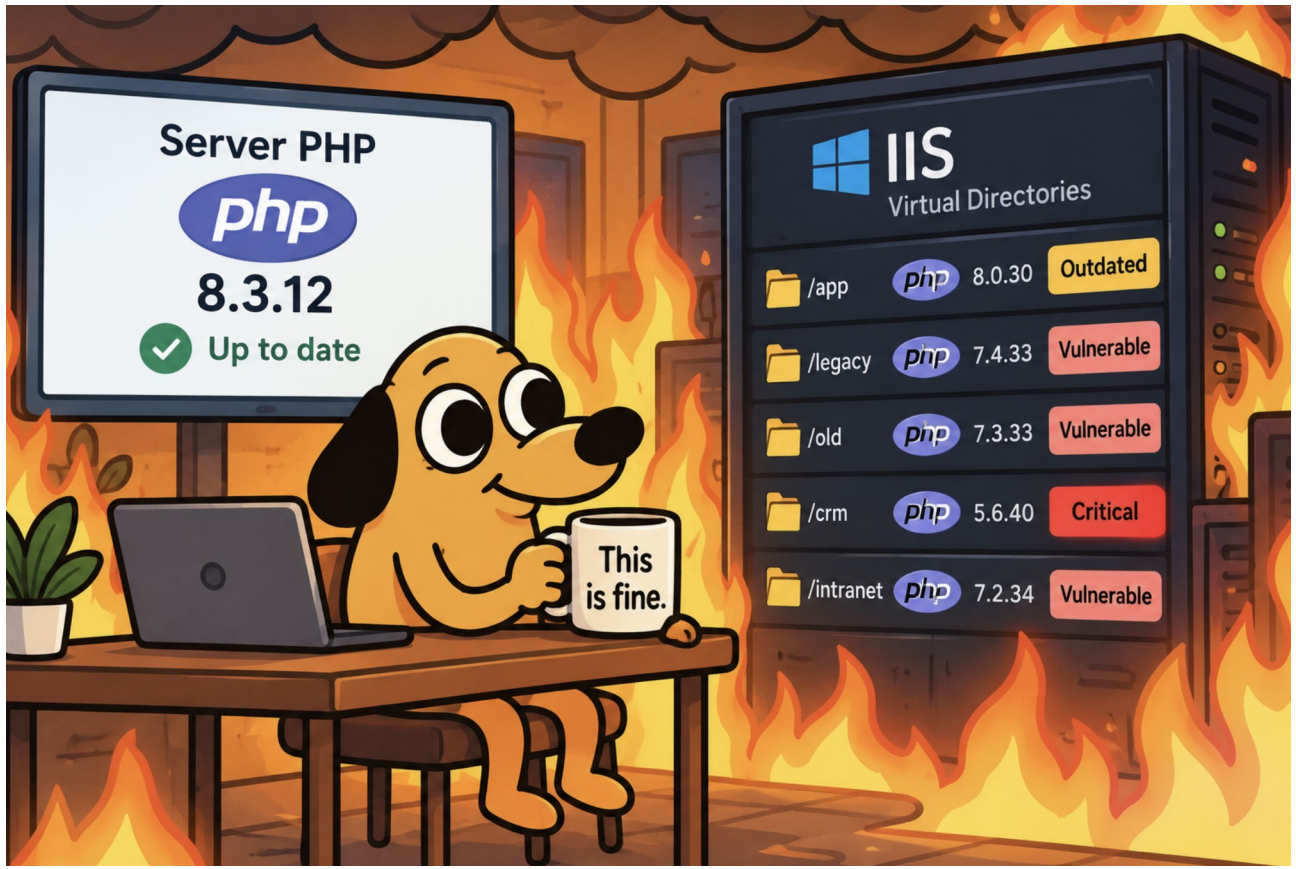
Threat Hunting over Software Vulnerabilities



Switch

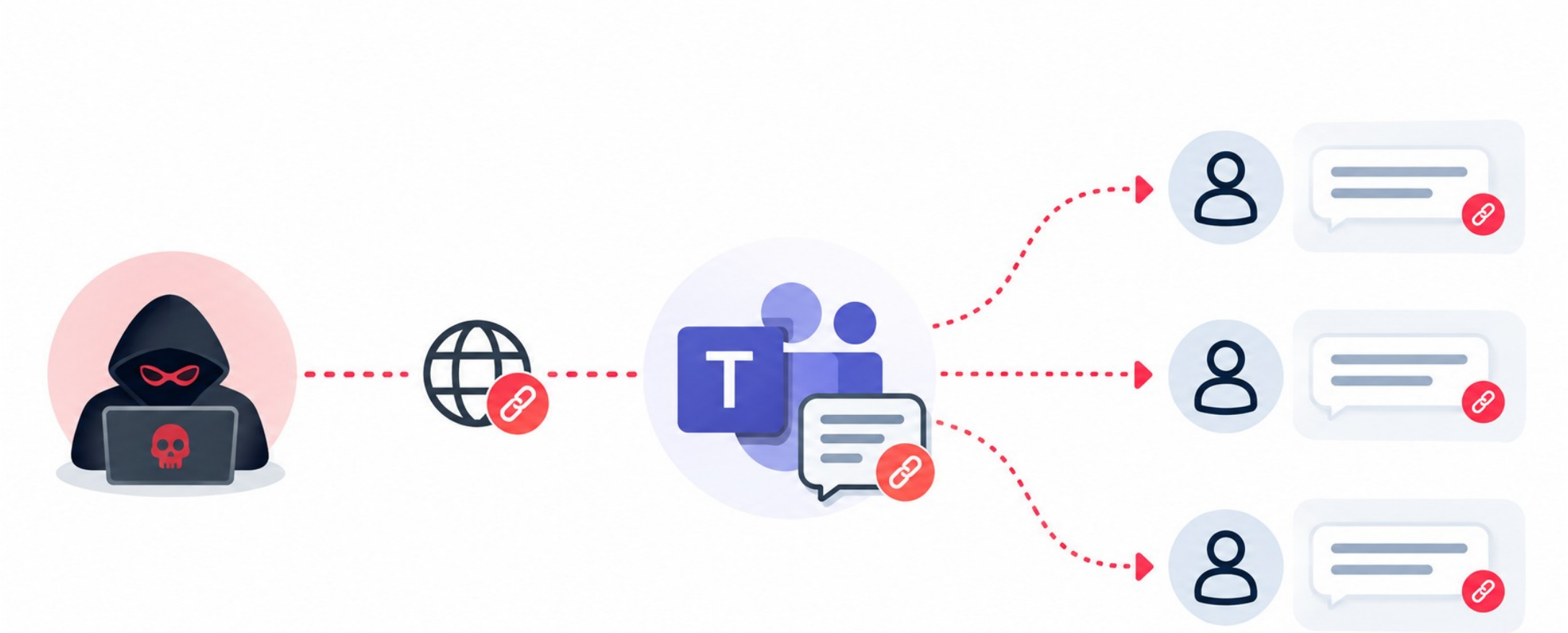
PHP2Shell





Switch

Hunting One to One Teams Chats by External Domains



Switch

1:1 Teams Chats from unexpected countries

```
CloudAppEvents //Table
| where Application has "Microsoft Teams" and isnotempty(IPAddress) //Condition
| extend Geo_IP = tostring(geo_info_from_ip_address(IPAddress).country),ChatName = todynamic(RawEventData).ChatName,
TeamName = todynamic(RawEventData).TeamName, ChannelName = todynamic(RawEventData).ChannelName, Operation =
todynamic(RawEventData).Operation, CommunicationType = todynamic(RawEventData).CommunicationType
| where  Operation has "ChatCreated" and CommunicationType has "OneOnOne"
| mv-expand  ParticipantsInfo = (todynamic(parse_json(RawEventData).ParticipantInfo))
|  mv-expand  ParticipatingDomains =  (ParticipantsInfo).ParticipatingDomains
|  mv-expand  ParticipatingSIPDomains =  (ParticipantsInfo).ParticipatingSIPDomains
|  mv-expand  ParticipatingSIPDomains =  (ParticipatingSIPDomains).DomainName
| where  Operation has "ChatCreated" and CommunicationType has "OneOnOne" //Condition
| project  AccountDisplayName,ChatCreatedFrom= IPAddress,ChannelName,ChatName, TeamName,Geo_IP,
CountryCode,Operation,ParticipatingSIPDomains,ParticipatingDomains, ISP
```

AccountDisplayName	ChatCreatedFrom	ChannelName	Geo_IP	Operation	ParticipatingSIPDomains	ParticipatingDomains	ISP
[redacted]			Taiwan	ChatCreated	[redacted]		taiwan mobile co. ltd.
			Taiwan	ChatCreated			taiwan mobile co. ltd.
			South Africa	ChatCreated			vodacom
			South Africa	ChatCreated			vodacom
			South Africa	ChatCreated			vodacom
			South Africa	ChatCreated			vodacom
			Germany	ChatCreated			icomera ab
			Germany	ChatCreated			icomera ab

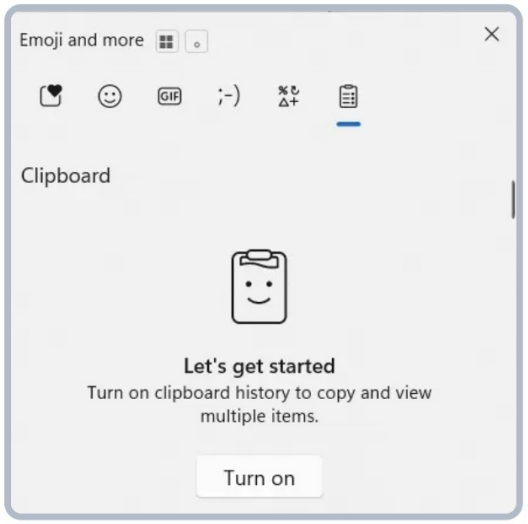
1:1 Teams Chats from unexpected countries

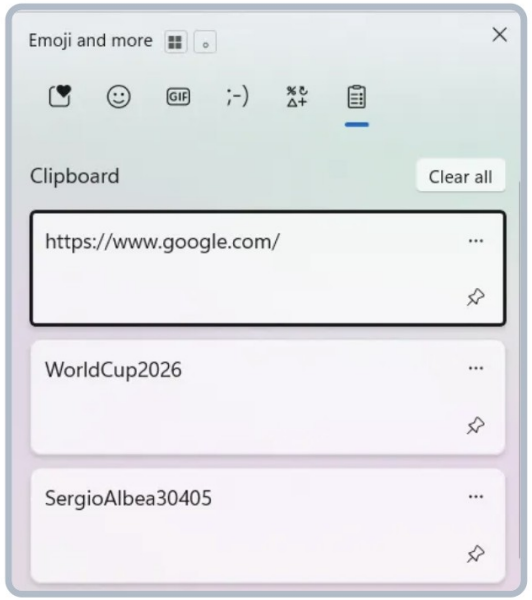
Geo_IP	Operation	ParticipatingSIPDomains	ParticipatingDomains	ISP
Taiwan	ChatCreated	[redacted]		taiwan mobile co. ltd.
Taiwan	ChatCreated			taiwan mobile co. ltd.
South Africa	ChatCreated			vodacom
South Africa	ChatCreated			vodacom
South Africa	ChatCreated			vodacom
South Africa	ChatCreated			vodacom
Germany	ChatCreated			icomera ab
Germany	ChatCreated			icomera ab

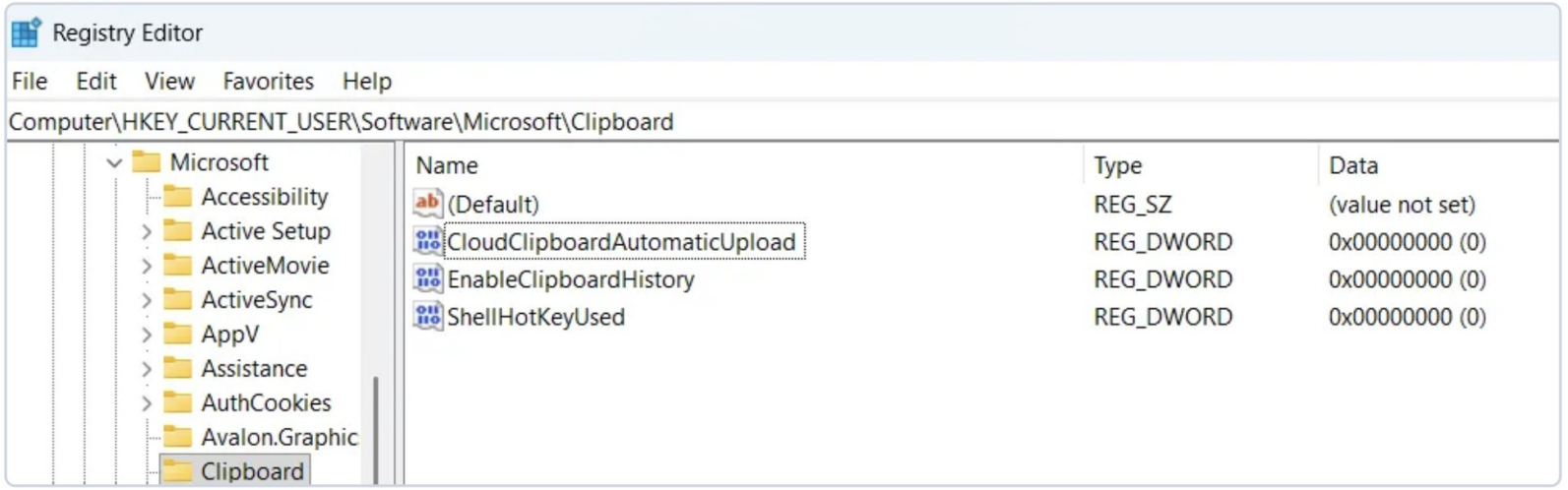
Switch

Threat Hunting applied on Devices

Hunting Clipboard-Based Threats







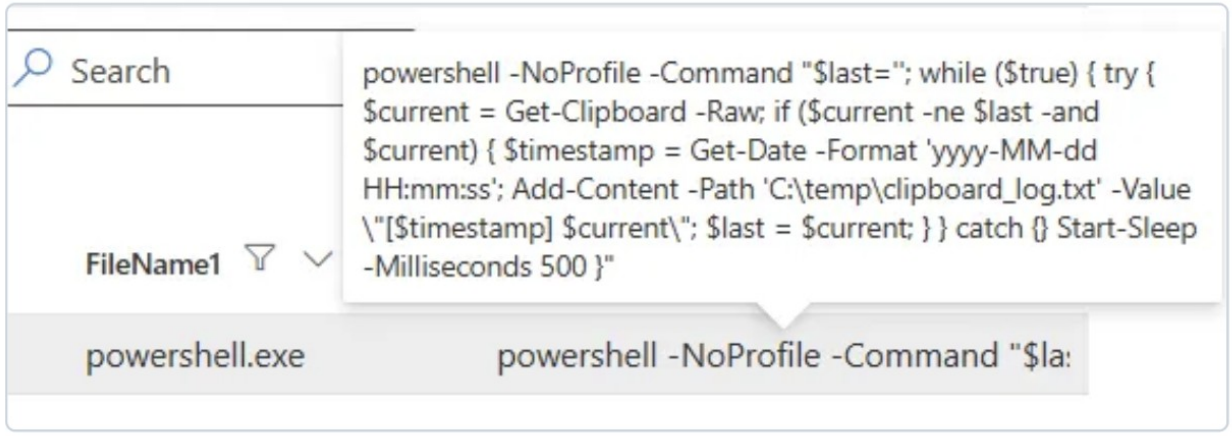
Hunting Clipboard-Based Threats

PowerShell clipboard cmdlets

In the environments where I tested this, direct use of clipboard cmdlets (`Get-Clipboard` , `Set-Clipboard`) was extremely rare. That low baseline is exactly what made them interesting to hunt.

Clipboard-History / sync enablement

Monitor the registry keys (`EnableClipboardHistory` , `CloudClipboardAutomaticUpload` , `ShellHotKeyUsed`) so you are alerted whenever the feature or its cloud sync is turned on where your policy says it should be off.



Switch

Hunting Device Vendors



🏭 **Vendor by inbound connection** → 🌍 **Add country context** → 🚩 **Remote IPs using multiple vendors**

vendor	Different_Countries_using_...	set_geo_ip	Total_devices_by_vendor	Total_different_RemoteIPs
VMware	138	["Switzerland","The Neth...	13	25317
Intel_Corporate	36	["United States","The Ne...	3	5809
Dell_Inc.	37	["Switzerland","Ireland","...	4	2861
Intel_Corporate	40	["The Netherlands","Unit...	4	7302
Quanta_Storage_Inc.	31	["Ireland","The Netherla...	6	2120
VMware	9	["The Netherlands","Ger...	2	173
Intel_Corporate	11	["Switzerland","United St...	3	102
Top_Victory_Electronics_(Taiwan)_Co.	22	["Germany","Switzerland...	4	1249
HP_Inc.	42	["Sweden","Ireland","Uni...	8	7541
Intel_Corporate	37	["United States","India","...	2	3406
Top_Victory_Electronics_(Taiwan)_Co.	19	["France","Switzerland","...	3	1019
HP_Inc.	40	["United Kingdom","Ger...	6	4095

Device Lateral Movement



Can we stop it?

```
SecurityEvents
| where LogonType == 3 // (NetLogon)
|  summarize dcount(Computer) by IpAddress
```

It has real damage?

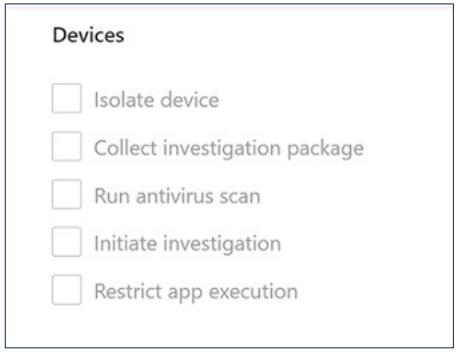
IpAddress	dcount_Computer	LM_Assessment	Why
10.10.5.12	47	**Likely TP**	One source IP authenticating to many hosts = common lateral movement pattern (e.g., admin tool abuse, pass-the-hash, remote service execution prep).
10.10.20.8	31	**Likely TP**	High fan-out from a single workstation subnet IP is suspicious unless it's a known management node.
10.10.1.5	120	**Likely FP**	Typical of infrastructure: DC, file server, SCCM/MECM, monitoring, AV mgmt, backup server, jump host.



Can we respond?









Switch

Device Lateral Movement



Can we stop it?

```
SecurityEvents
| where LogonType == 3 // (NetLogon)
|  summarize dcount(Computer) by IpAddress
```

It has real damage?

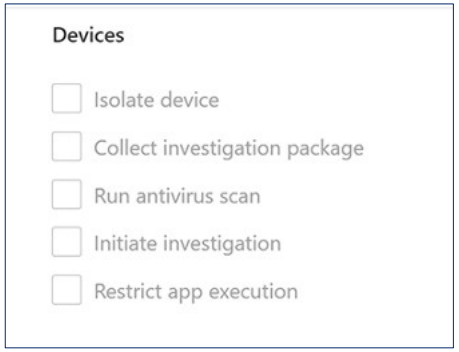
IpAddress	dcount_Computer	LM_Assessment	Why
10.10.5.12	47	**Likely TP**	One source IP authenticating to many hosts = common lateral movement pattern (e.g., admin tool abuse, pass-the-hash, remote service execution prep).
10.10.20.8	31	**Likely TP**	High fan-out from a single workstation subnet IP is suspicious unless it's a known management node.
10.10.1.5	120	**Likely FP**	Typical of infrastructure: DC, file server, SCCM/MECM, monitoring, AV mgmt, backup server, jump host.



Can we respond?









Switch

Switch_

Threat Hunting applied on Threat Intelligence

IOC vs IOA

Indicator of Compromise(IoC)







Domains

Indicator of Attack (IoA)

Post Scanning

Remote Command Execution

DNS Tunnelling

IOAs are active in nature and focus on identifying a cyber attack that is in process. They also explore the identity and motivation of the threat actor, whereas an IOC only helps the organization understand the events that took place.

Indicator of Compromises (IOCs) are responsive measures while Indicator of Attack are proactive measures.

Why is important? April 2026

Cyber Security News | Threats

Hackers Clone CERT-UA Site to Trick Victims Into Installing Go-Based RAT

By Tushar Subhra Dutta - April 2, 2026

The messages told recipients to download a password-protected archive named "CERT_UA_protection_tool.zip" or "protection_tool.zip" from the file-sharing service Files.fm, with the claim that it held a specialized security tool requiring immediate installation

Once persistence is in place, AGEWHEEZE connects to its C2 server at 54[.]36.237.92 over port 8443 using WebSockets for live, two-way communication.

Remcos RAT Infection Chain Hides Behind Obfuscated Scripts and Trusted Windows Binaries

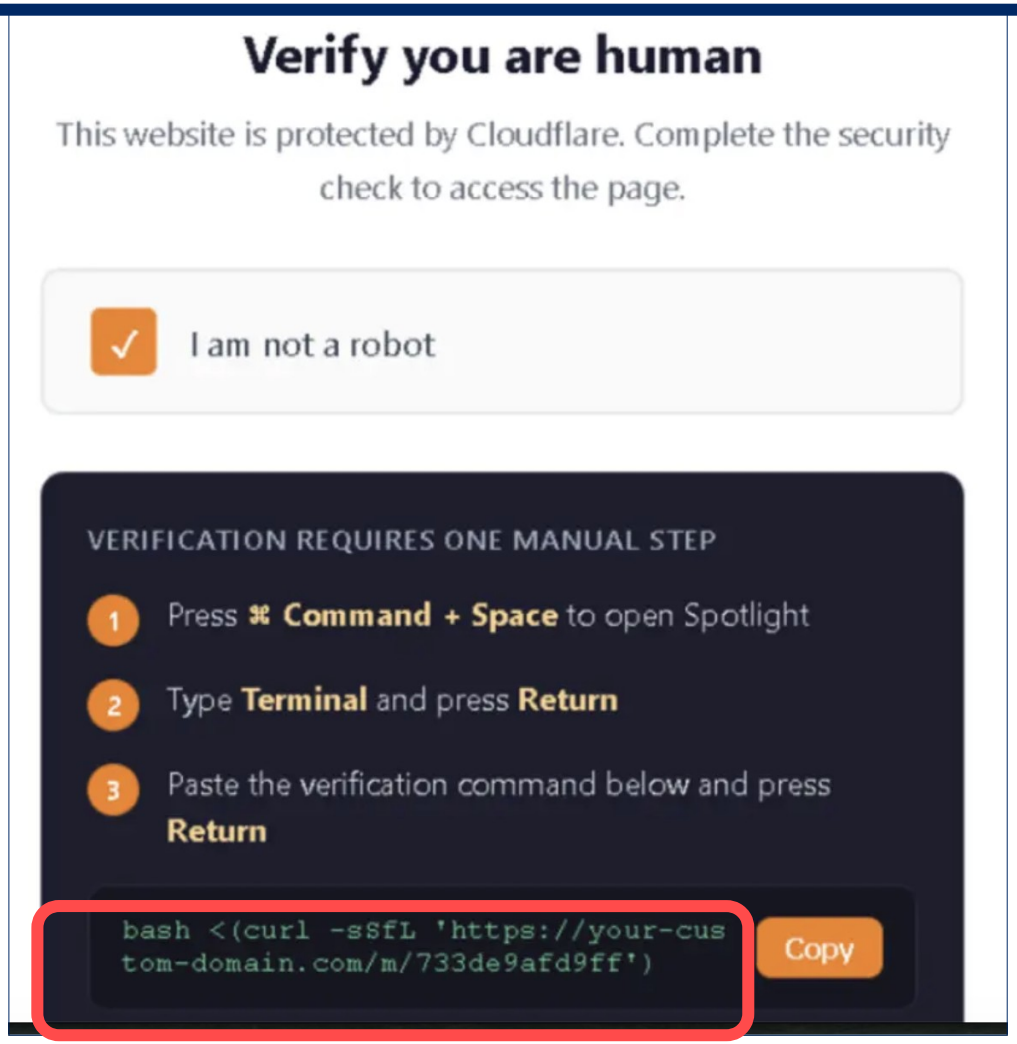
By Tushar Subhra Dutta - April 2, 2026

The campaign's impact is serious. Once fully deployed, Remcos establishes a persistent connection to a remote C2 server at 192[.]3[.]27[.]141:8087 actively sending and receiving data.

Evidence of data collection was confirmed through the creation of a log file at `C:\ProgramData\remcos\logs.dat`, which stores captured keystrokes and other system information. This indicates the malware was actively staging data for exfiltration.

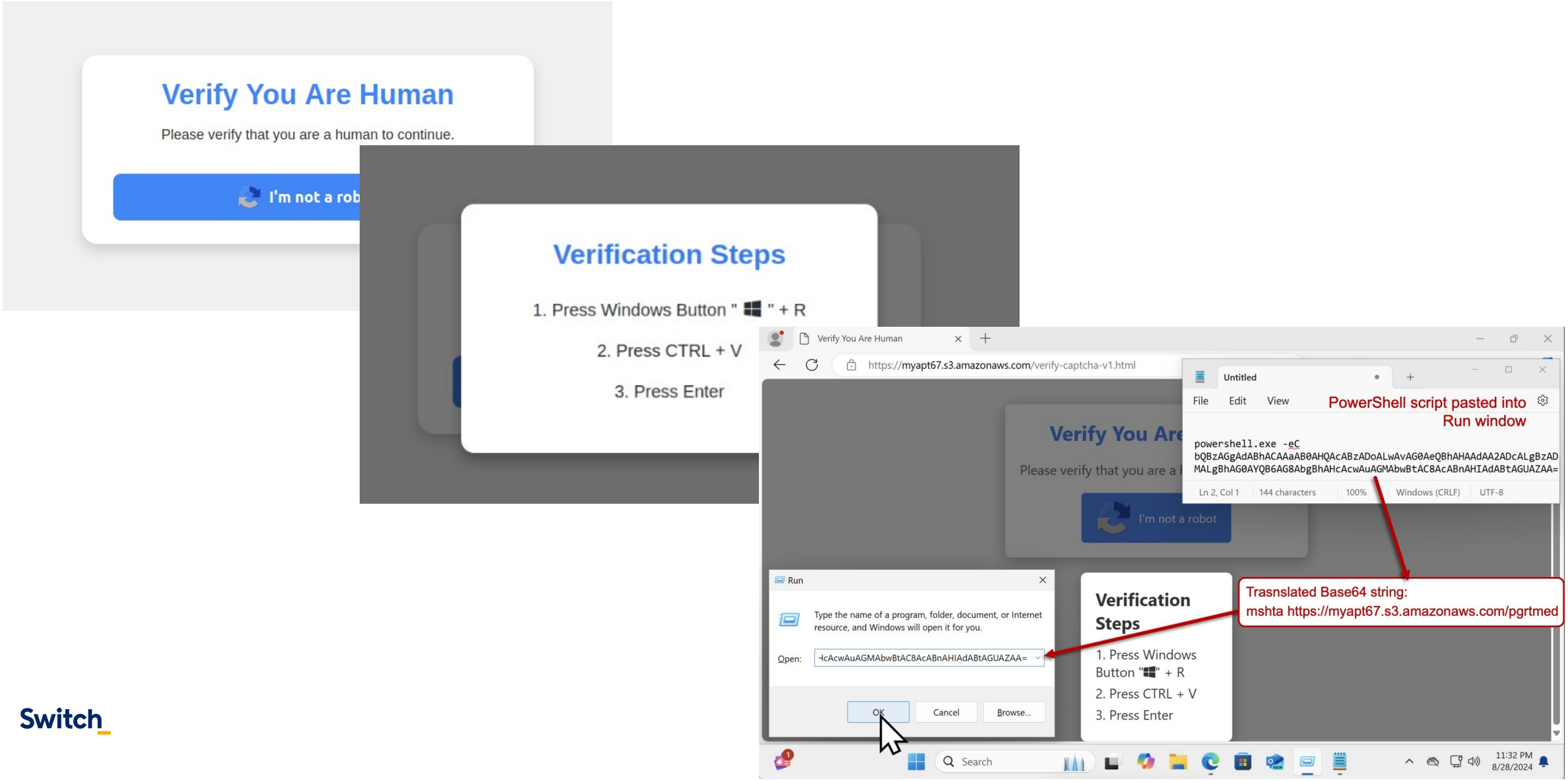
Hackers Use Venom Stealer to Turn ClickFix Lures Into Full Data Exfiltration Pipelines

By Tushar Subhra Dutta - April 3, 2026



Source: https://cybersecuritynews.com/

KQL Examples – Click Fix Case



Switch

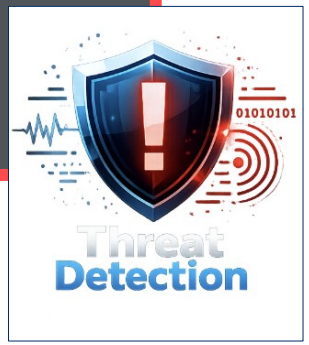
KQL Examples – Click Fix Case

Indicator of Compromise (IoC)

```
let ioc_ip_addr = dynamic(["185.234.72.186", "3.23.103.13", "83.242.96.159", "5.8.9.77"]);
DeviceNetworkEvents
| where RemoteIP has_any (ioc_ip_addr)
```

Indicator of Attack (IoA)

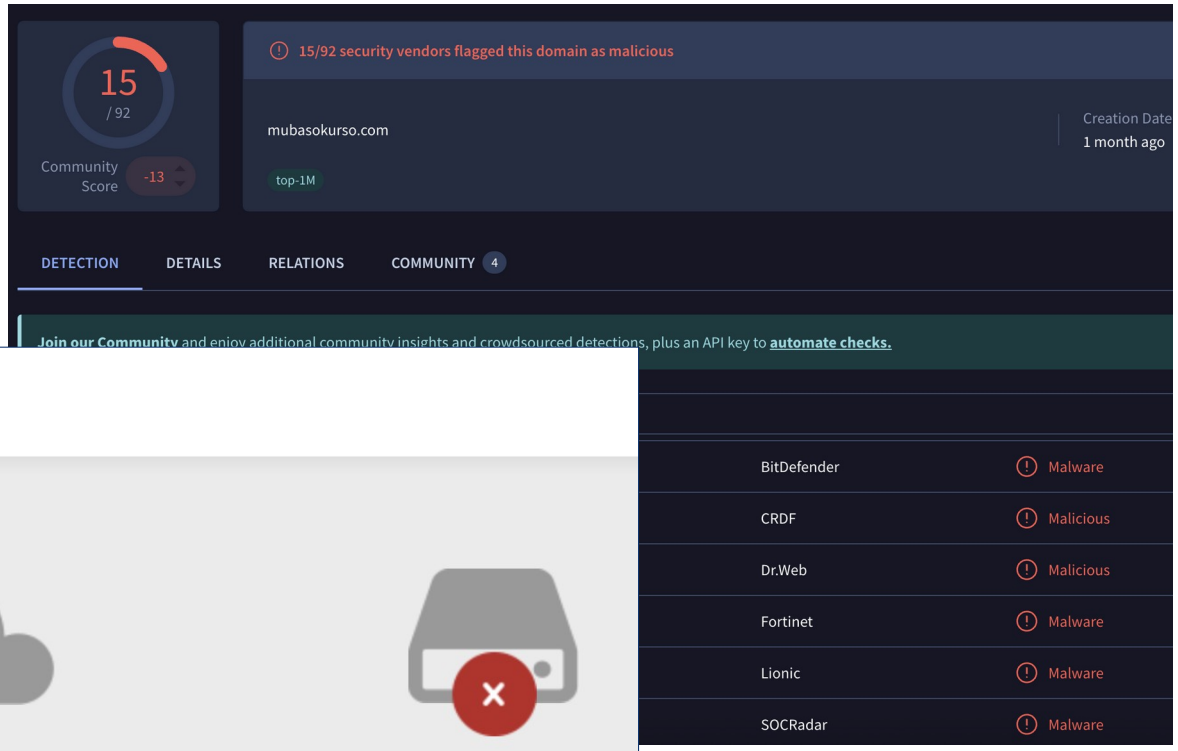
```
DeviceFileEvents
| where InitiatingProcessCommandLine contains "mshta"
| distinct DeviceName,InitiatingProcessCommandLine
```

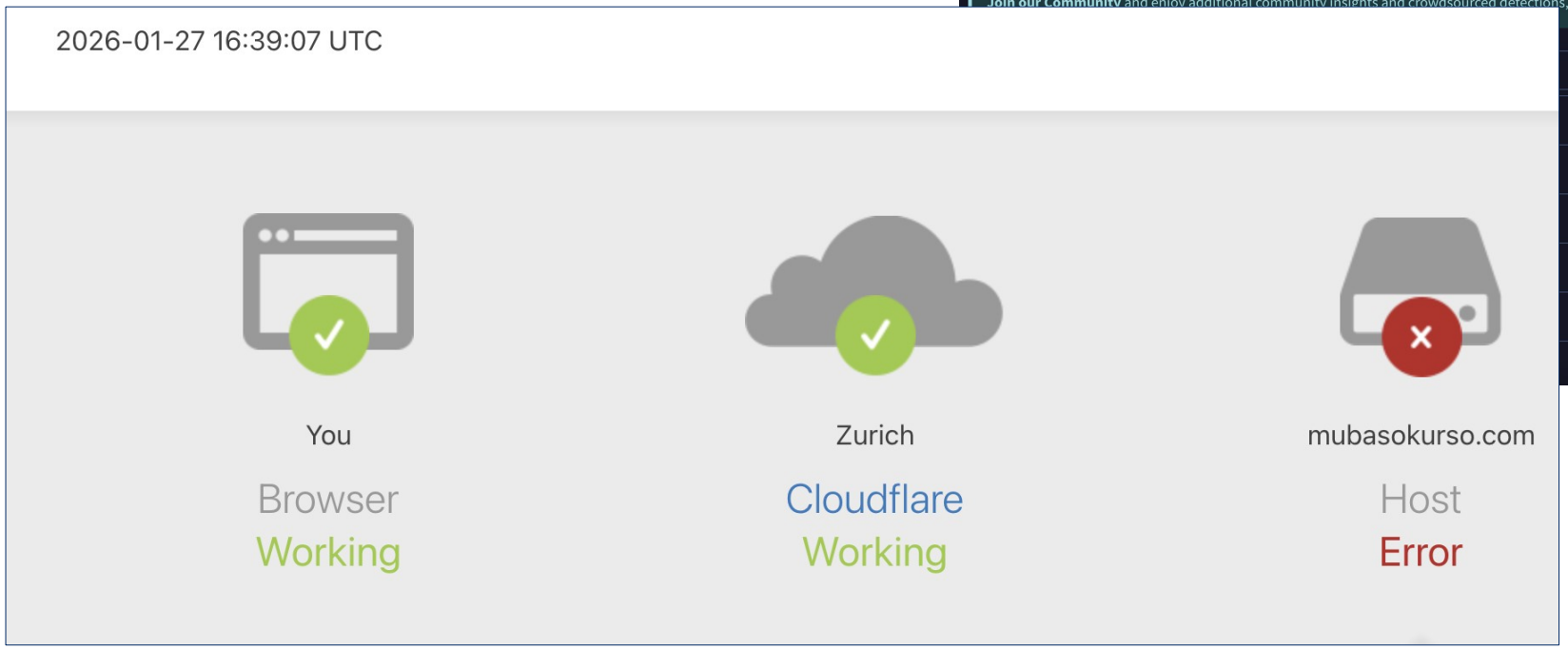


Threat Detection based on IOC

Indicator of Compromise (IoC)

```
EmailUrlInfo
| where Url has 'mubasokurso.com'
```





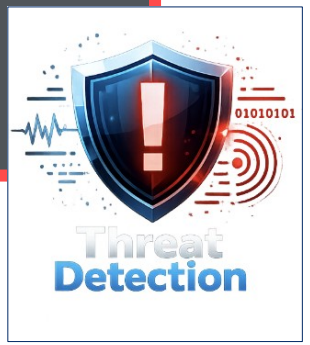
Validate URL/Domain before configuring detection Rules!

Switch

Threat Detection based on IOA

Indicator of Attack (IoA)

```
DeviceFileEvents
| where InitiatingProcessCommandLine contains 'mshta'
| distinct InitiatingProcessCommandLine
```



InitiatingProcessCommandLine
"mshta.exe" C:\Users\EXTULR~1\AppData\Local\Temp\TeamViewer\TeamViewer11_Exit.hta

Validate the queries results before to implement detections to avoid flood of false positive alerts!

Threat Hunting based on IOCs

Can we stop it?

```
UrlClickEvents
| where isnotempty(ThreatTypes)
| distinct Url,ActionType, ThreatTypes, IsClickedThrough
```

It has real damage?

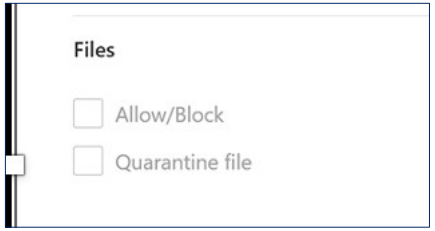
Url	ActionType	ThreatTypes	IsClickedThrough
https://doi.org/10.22	UrlErrorPage		0
https://youtu.be/9g4	ClickAllowed		0
https://youtu.be/9p9	ClickBlocked	Phish	0
https://youtu.be/9Pi	ClickAllowed		0
https://youtu.be/9YN	ClickAllowed	Phish	0



Can we respond?









Threat Intelligence Feeds

A Threat Intelligence (TI) feed is a continuous source of data that provides indicators and information about known or emerging cyber threats.

🌐 Network-based IOCs

Indicators related to internet communication:

- **IP addresses** (e.g. servers used by attackers)
- **Domains** (malicious websites)

📁 File-based IOCs

Indicators related to malicious files:

- **File hashes** (fingerprints of bad files)
- **File names**
- **File paths**

🖥️ Host-based IOCs

Indicators observed on a device:

- **Suspicious processes**
- **Unusual startup programs**
- **Registry or system changes**

📧 Email-based IOCs

Indicators found in emails:

- **Sender addresses**
- **Malicious links or attachments**
- **Phishing subjects or pattern**

TI Feeds Challenges



Duplicated Content



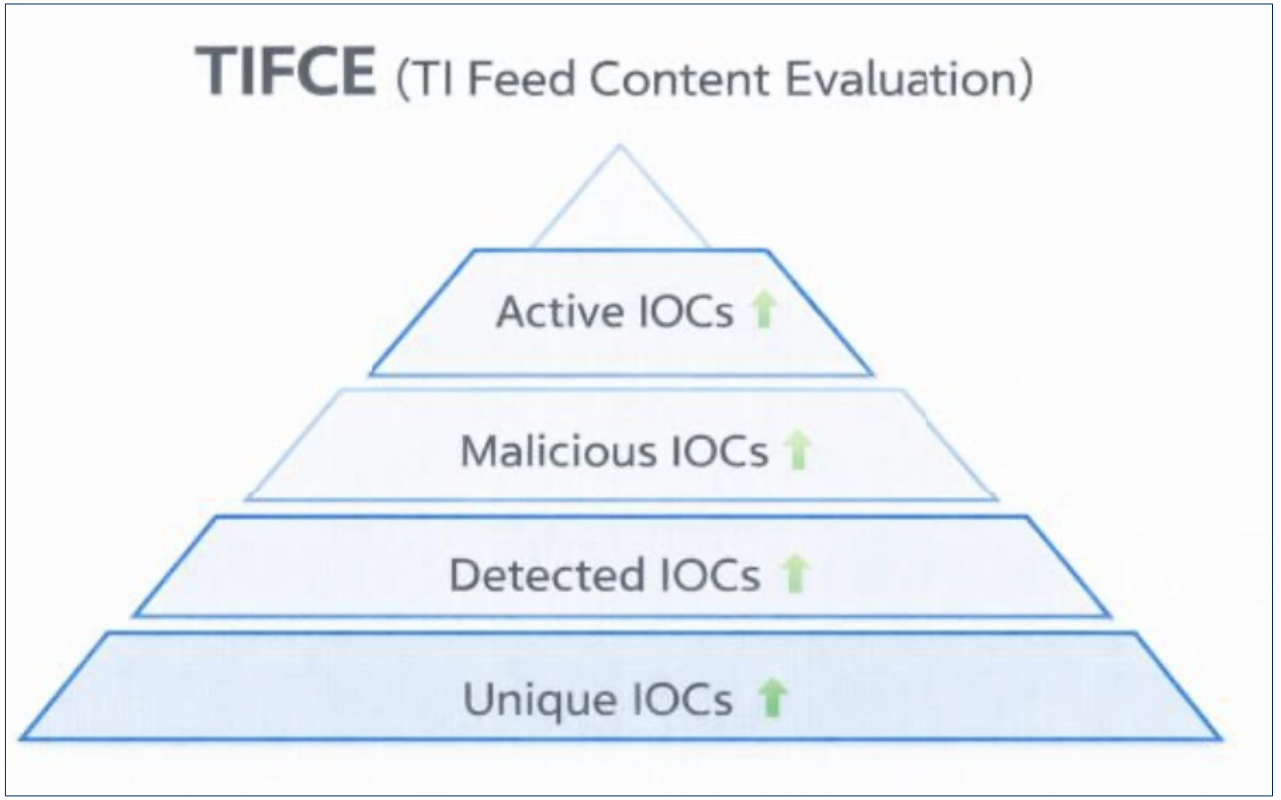
Obsoleted projects



Low-Level contributions

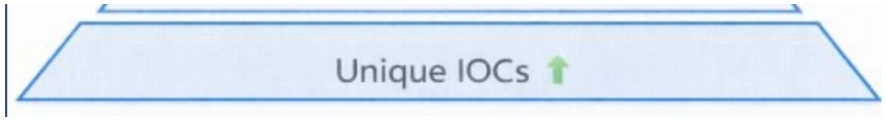
(Wordpress.com/asiei49
Wordpress.com
Yammer.com/40rtphp
Yammer.com)

TIFCE (TI Feed Content Evaluation)



https://doi.org/10.5281/zenodo.18208974

TIFCE (TI Feed Content Evaluation)




```
//Importing TI Feeds
let CertPL =externaldata(Domains:string)[@'https://hole.cert.pl/domains/v2/domains.txt']with (format = 'txt',ignoreFirstRecord = true)
| project TIFeed= 'CertPL',IOC= Domains,Reference = 'https://hole.cert.pl/domains/v2/domains.txt';
let PhishingArmyFeed = externaldata(Domain: string)[@'https://phishing.army/download/phishing_army_blocklist.txt']
 with (format='txt', ignoreFirstRecord=True) | project Domain = tolower(Domain)| where Domain !startswith '#'
| project TIFeed= 'PhishingArmyFeed',IOC= Domain,Reference = 'https://phishing.army/download/phishing_army_blocklist.txt';
let SpydiDomainList =externaldata(Domains:string)[@'https://spydisec.com/maliciousblocklist.txt']with (format='csv')
| where Domains !startswith '#' | project TIFeed= 'SpydiDomainList',IOC= Domains,
 Reference = 'https://spydisec.com/maliciousblocklist.txt';
let Domain_TweetFeedMonth =externaldata(DateUTC: datetime,SourceUser: string,Type: string,Value: string,Tags: string,Tweet: string)
[@'https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/month.csv']with (format='csv') | where Type has 'domain'
| project TIFeed='TweetFeedMonth',IOC= Value,Reference='https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/month.csv';
let Domains_IOCs =union  SpydiDomainList,PhishingArmyFeed,CertPL,Domain_TweetFeedMonth; //create a Table with the TIFeeds
 Domains_IOCs | summarize dcount(TIFeed),make_set(TIFeed) by IOC | order by dcount_TIFeed
```

IOC	dcount_TIFeed	set_TIFeed
xalurxojup.cyou	3	["Domain_TweetFeedMonth","CertPL","SpydiDomainList"]
roblox.com.ml	3	["Domain_TweetFeedMonth","CertPL","SpydiDomainList"]
trumpgift.sx	3	["Domain_TweetFeedMonth","CertPL","SpydiDomainList"]
ai-tradingesn.com	2	["CertPL","SpydiDomainList"]
sendaire.jfiqte.cn	2	["Domain_TweetFeedMonth","SpydiDomainList"]
allegrolokalnie.pl-729610.cfd	2	["CertPL","SpydiDomainList"]
cake-wallet-web.at	2	["Domain_TweetFeedMonth","SpydiDomainList"]

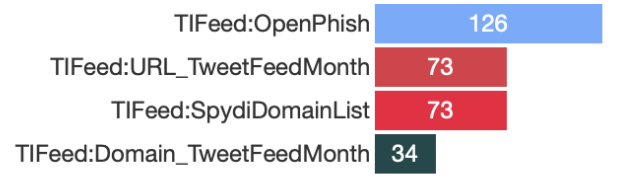
MISP (Malware Information Sharing Platform)

Detected IOCs

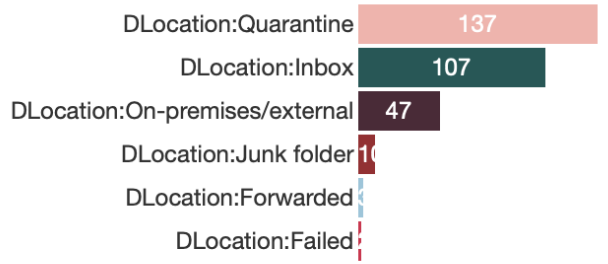
Dashboard | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Logs | API | Bookmarks

SWITCH CERT SWITCH CERT 23696	source:DXDR/TIFeed, tlp:amber, TIFeed:SpydiDomainList, TIDomain:links.invtdu.to, V:8, DLocation:Inbox, T:[Spearphishing Link (T1566.002)], PAP:AMBER	5	2026-02-02	2026-02-02 09:01:13	2026-02-02 09:01:17
SWITCH CERT SWITCH CERT 23690	source:DXDR/TIFeed, tlp:amber, TIFeed:URL_TweetFeedMonth, IP:129.199.96.40, MailFrom:sjaonrl.cn, IOC:https://manety.sctrcjt.cn/Rfuncc1013000extfunc/, DLocation:Quarantine, T:[Spearphishing Link (T1566.002)], TZ:Z7UP, PAP:AMBER	4	2026-01-31	2026-02-01 09:07:20	2026-02-01 09:07:24
SWITCH CERT SWITCH CERT 23687	source:DXDR/TIFeed, tlp:amber, TIFeed:URL_TweetFeedMonth, IP:129.199.96.40, MailFrom:chpbcx.cn, IOC:https://electionture.ykdwqlef.cn/Pe, DLocation:Quarantine, T:[Spearphishing Link (T1566.002)], PAP:AMBER	4	2026-02-01	2026-02-01 09:07:13	2026-02-01 09:07:14
SWITCH CERT SWITCH CERT 23688	source:DXDR/TIFeed, tlp:amber, TIFeed:URL_TweetFeedMonth, IP:1, MailFrom:chpbcx.cn, IOC:https://electionture.ykdwqlef.cn/Pe, DLocation:On-premises/external, T:[Spearphishing Link (T1566.002)], PAP:AMBER				

TIFeed Matches



Delivered Location based on TIFeeds



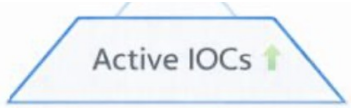
MISP (Malware Information Sharing Platform)

Malicious IOCs

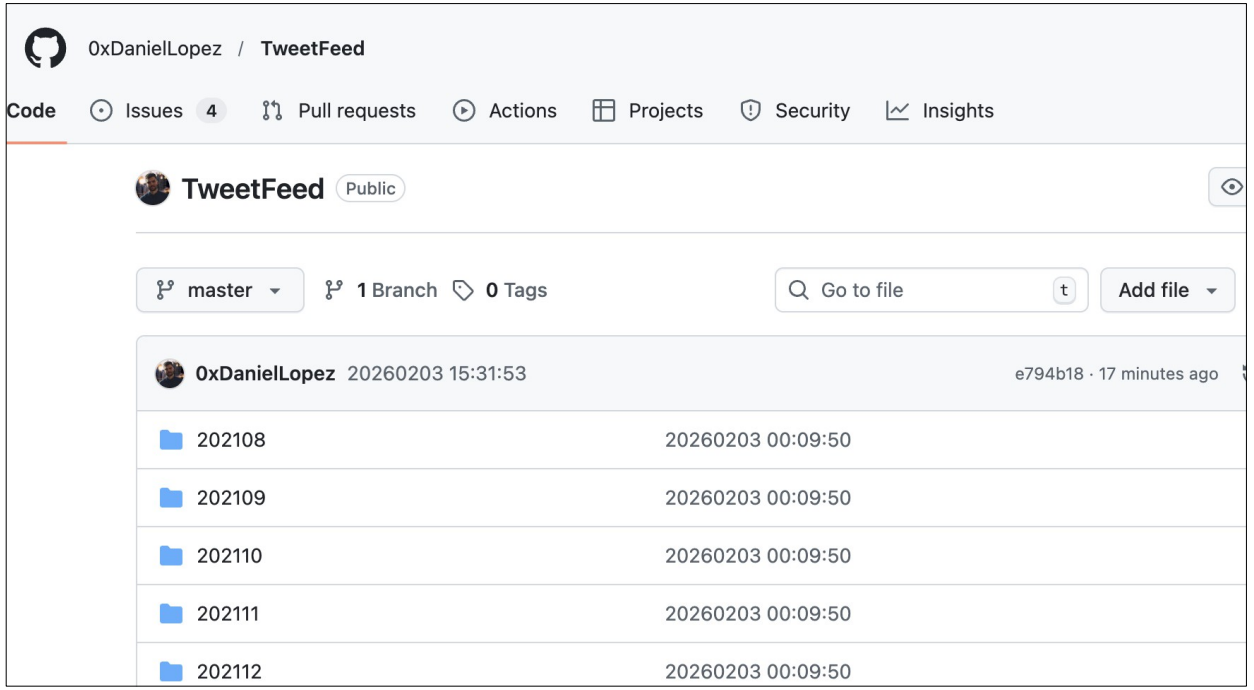
**V:X → Number of vendors tagging the URL as malicious based on VirusTotal request*

✔ SWITCH CERT SWITCH CERT 23597	source:DXDR/TIFeed, tlp:amber, TIFeed:SpydiDomainList, TIDomain:blinq.me, V:5, DLocation:Inbox, TZ:T6F2, T:[Spearphishing Link (T1566.002)], PAP:AMBER	5	2026-01-30	2026-01-30 09:06:30	2026-01-30 09:06:31	URL Match between Email URL and entry on the TIFeed SpydiDomainList
✔ SWITCH CERT SWITCH CERT 23587	source:DXDR/TIFeed, tlp:amber, TIFeed:SpydiDomainList, TIDomain:qrco.de, V:4, DLocation:Inbox, TZ:T6F2, T:[Spearphishing Link (T1566.002)], PAP:AMBER	5	2026-01-29	2026-01-30 09:05:59	2026-01-30 09:06:01	URL Match between Email URL and entry on the TIFeed SpydiDomainList
✔ SWITCH CERT SWITCH CERT 23591	TIFeed:SpydiDomainList, TIDomain:l1nq.com, V:8, DLocation:Inbox, PAP:AMBER	5	2026-01-29	2026-01-30 09:05:59	2026-01-30 09:06:01	URL Match between Email URL and entry on the TIFeed SpydiDomainList
✔ SWITCH CERT SWITCH CERT 23592	source:DXDR/TIFeed, TIFeed:SpydiDomainList, TIDomain:dub.sh, V:6, T:[Spearphishing Link (T1566.002)], PAP:AMBER	5	2026-01-29	2026-01-30 09:05:59	2026-01-30 09:06:01	URL Match between Email URL and entry on the TIFeed SpydiDomainList
✔ SWITCH CERT SWITCH CERT 23584	source:DXDR/TIFeed, tlp:amber, TIFeed:SpydiDomainList, TIDomain:spemail5.online, V:12, DLocation:Inbox, T:[Spearphishing Link (T1566.002)], PAP:AMBER	5	2026-01-29	2026-01-30 09:01:18	2026-01-30 09:01:21	URL Match between Email URL and entry on the TIFeed SpydiDomainList

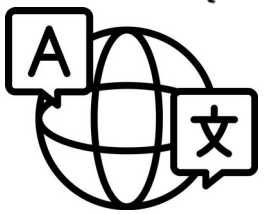
MISP (Malware Information Sharing Platform)




```
let Domain_TweetFeedMonth =externaldata(DateUTC: datetime,SourceUser: string,Type: string,Value: string,Tags: string,Tweet: string)
[@'https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/month.csv']with (format='csv')| where Type has 'domain'
| project TIFeed='TweetFeedMonth',IOC= Value,Reference='https://raw.githubusercontent.com/0xDanielLopez/TweetFeed/master/month.csv';
```



Threat Intelligence Sources Challenges




```
],
"1538391": [
    {
        "ioc_value": "secretariaa.shop",
        "ioc_type": "domain",
        "threat_type": "botnet_cc",
        "malware": "win.formbook",
        "malware_alias": "win.xloader",
        "malware_printable": "Formbook",
        "first_seen_utc": "2025-06-01 10:21:49",
        "last_seen_utc": null,
```





```
],
"1538421": [
    {
        "ioc_value": "medellin2029.duckdns.org",
        "ioc_type": "domain",
        "threat_type": "botnet_cc",
        "malware": "win.xworm",
        "malware_alias": null,
        "malware_printable": "XWorm",
        "first_seen_utc": "2025-06-01 16:26:17",
        "last_seen_utc": null,
```





```
],
"1537835": [
    {
        "ioc_value": "windowsmsn-cn.live",
        "ioc_type": "domain",
        "threat_type": "botnet_cc",
        "malware": "js.fakeupdates",
        "malware_alias": "FakeUpdate,SocGholish",
        "malware_printable": "FAKEUPDATES",
        "first_seen_utc": "2025-05-31 06:15:00",
        "last_seen_utc": null
```





```
],
"1411661": [
    {
        "ioc_value": "http://www.kytraders.university/b101/",
        "ioc_type": "url",
        "threat_type": "botnet_cc",
        "malware": "win.formbook",
```



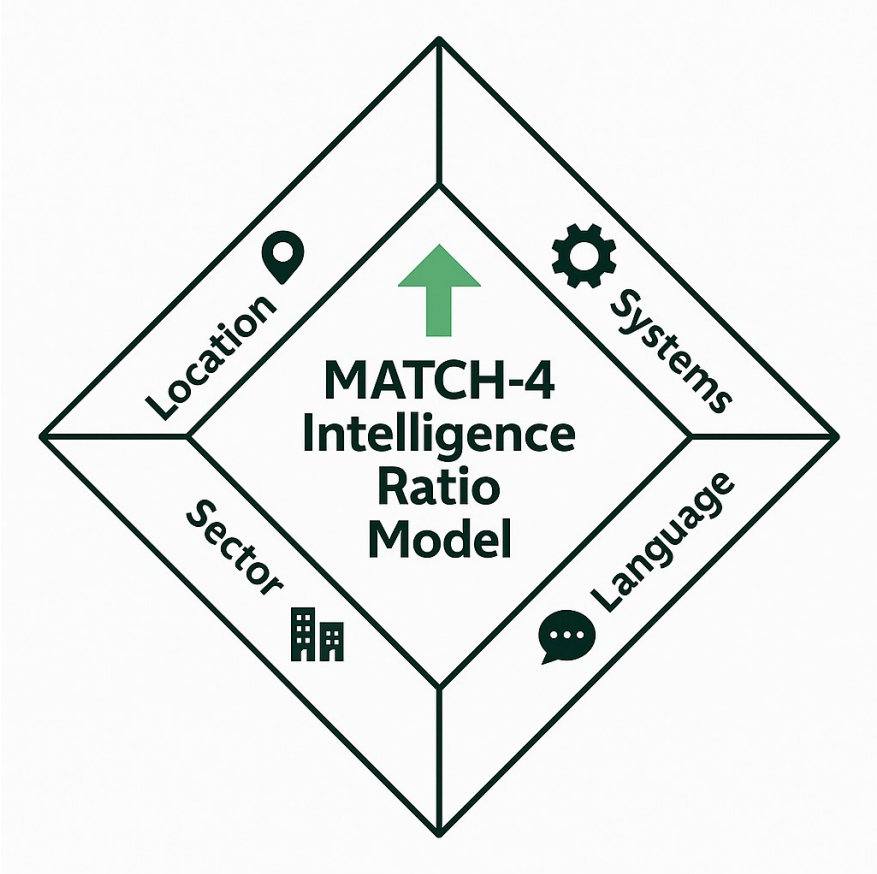


```
],
"1514671": [
    {
        "ioc_value": "https://dogalmedical.org/xap",
        "ioc_type": "url",
        "threat_type": "botnet_cc",
        "malware": "win.lumma",
```

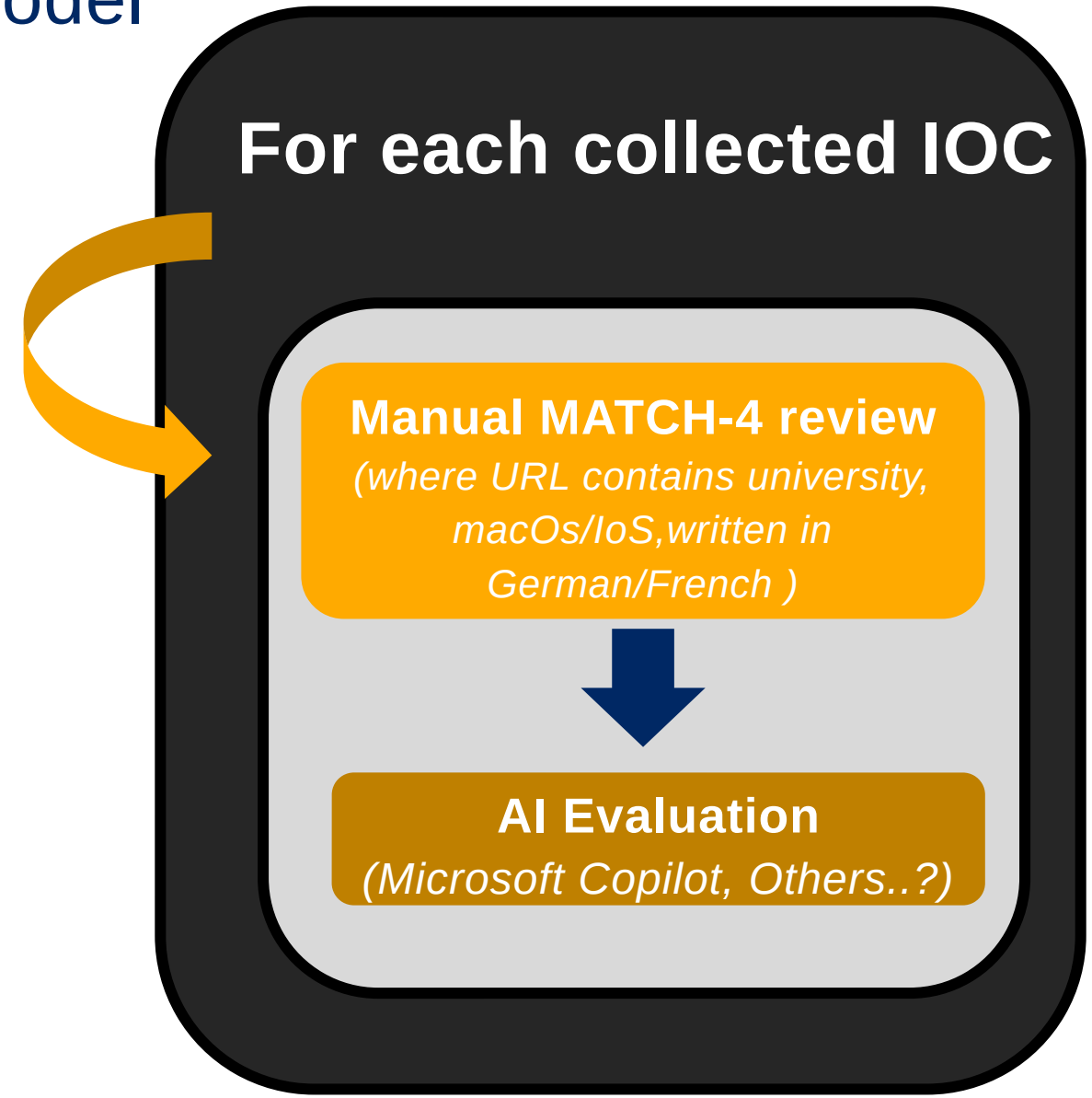
```
],
"1412773": [
    {
        "ioc_value": "http://www.aixabank.video/o10c/",
        "ioc_type": "url",
        "threat_type": "botnet_cc",
        "malware": "win.formbook",
```


Switch

MATCH-4 Intelligence Ratio Model

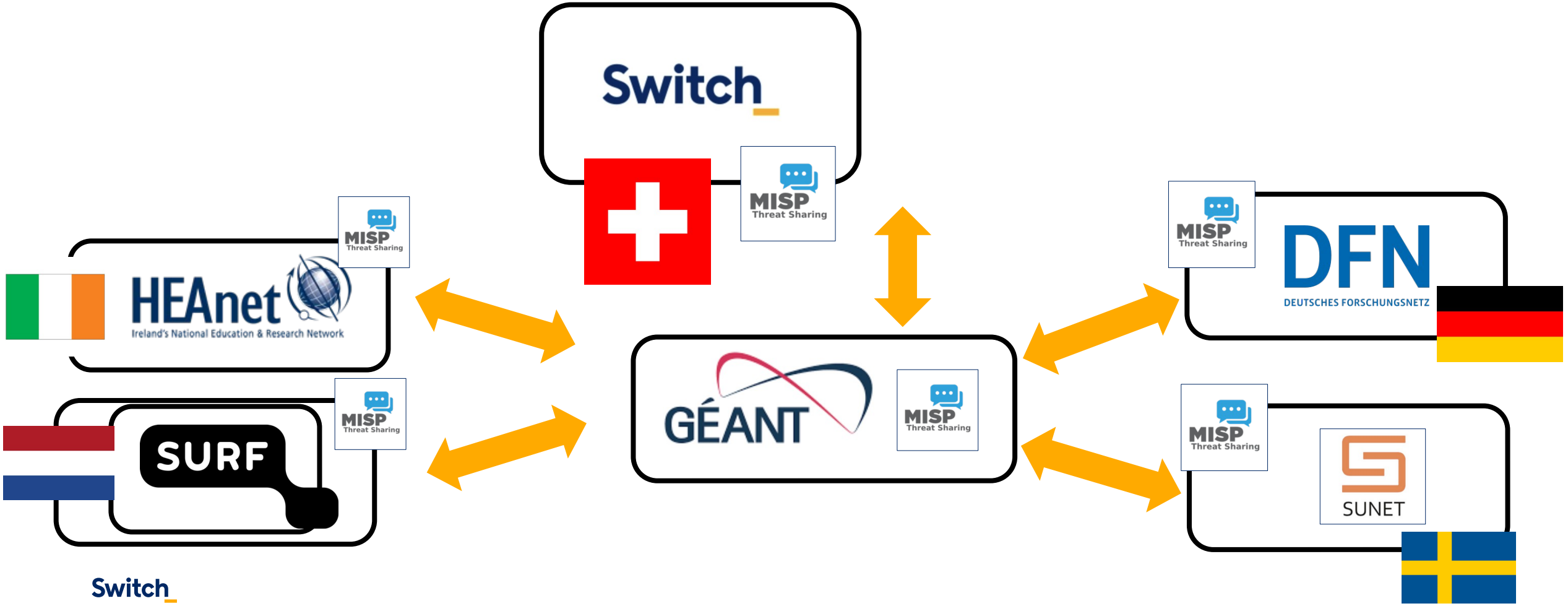


https://doi.org/10.5281/zenodo.17012869



GEANT TI Feeds

2026 Q1/Q2 (Already integraded since 2025 for Malware and phishing cases)



Switch

Turn hunting and IA

Identifying Suspicious Fake Installer Software

Create an agent that maintains a **daily-updated list of legitimate software filenames and** their latest **known file hashes**. Instead of manually checking whether Chrome, AnyDesk WinSCP or another application has released a new version, the agent keeps that baseline updated for me. **I can then consume the list directly from KQL and compare what I see in my environment against what I currently expect to see.**

> ***Known filename + Unknown hash = First signal***

> ***Known filename + Unknown hash + Untrusted download source = Investigate***

> ***Similar trusted filename + Unknown hash + Untrusted download source = Investigate***

Identifying Suspicious Fake Installer Software

Create an agent that maintains a **daily-updated list of legitimate software filenames and** their latest **known file hashes**. Instead of manually checking whether Chrome, AnyDesk WinSCP or another application has released a new version, the agent keeps that baseline updated for me. **I can then consume the list directly from KQL and compare what I see in my environment against what I currently expect to see.**

> ***Known filename + Unknown hash = First signal***

> ***Known filename + Unknown hash + Untrusted download source = Investigate***

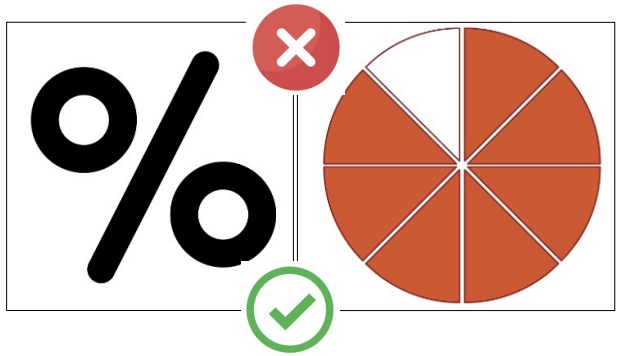
> ***Similar trusted filename + Unknown hash + Untrusted download source = Investigate***

Switch_

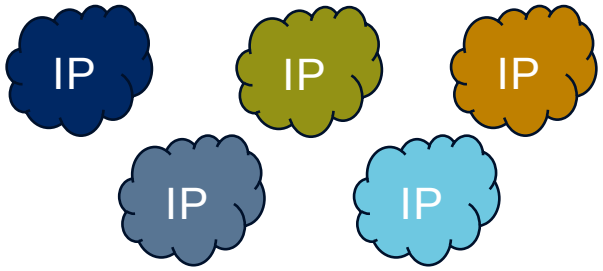
Turn raw data into real detections

Key measures

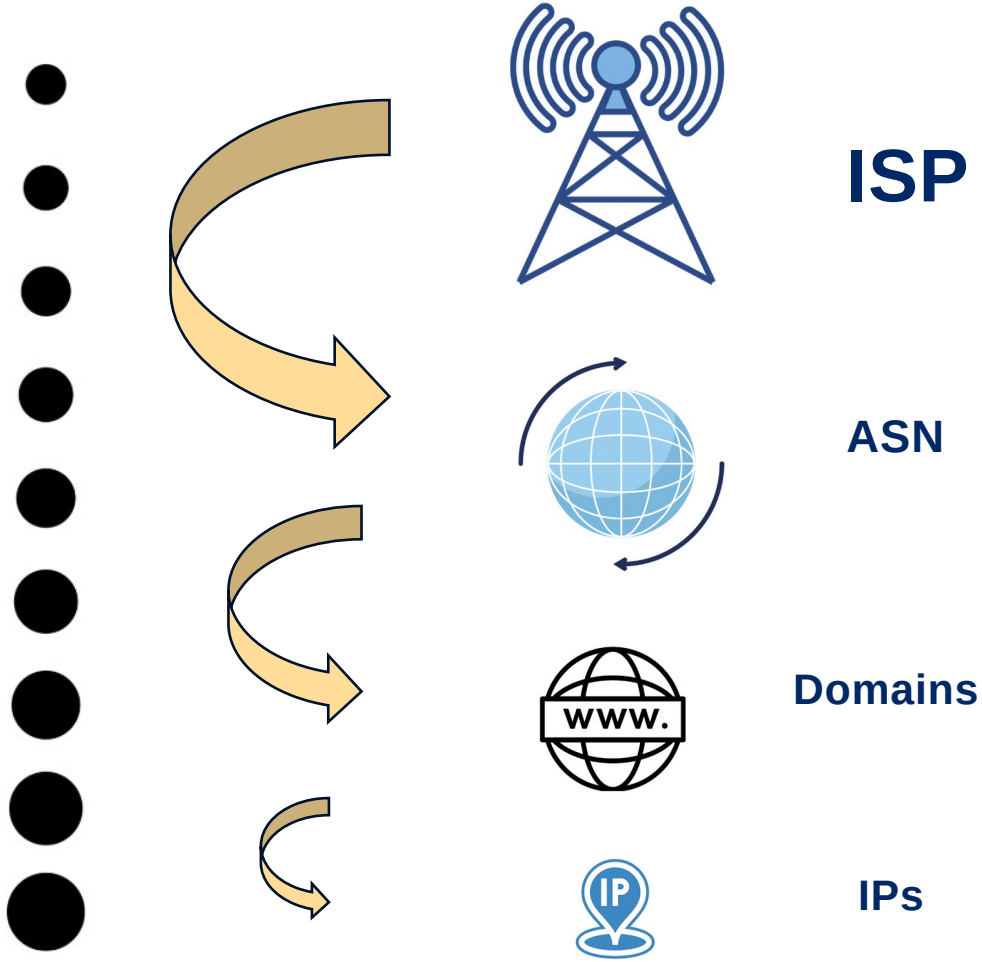
Percentage & Ratios



Distinct IP's



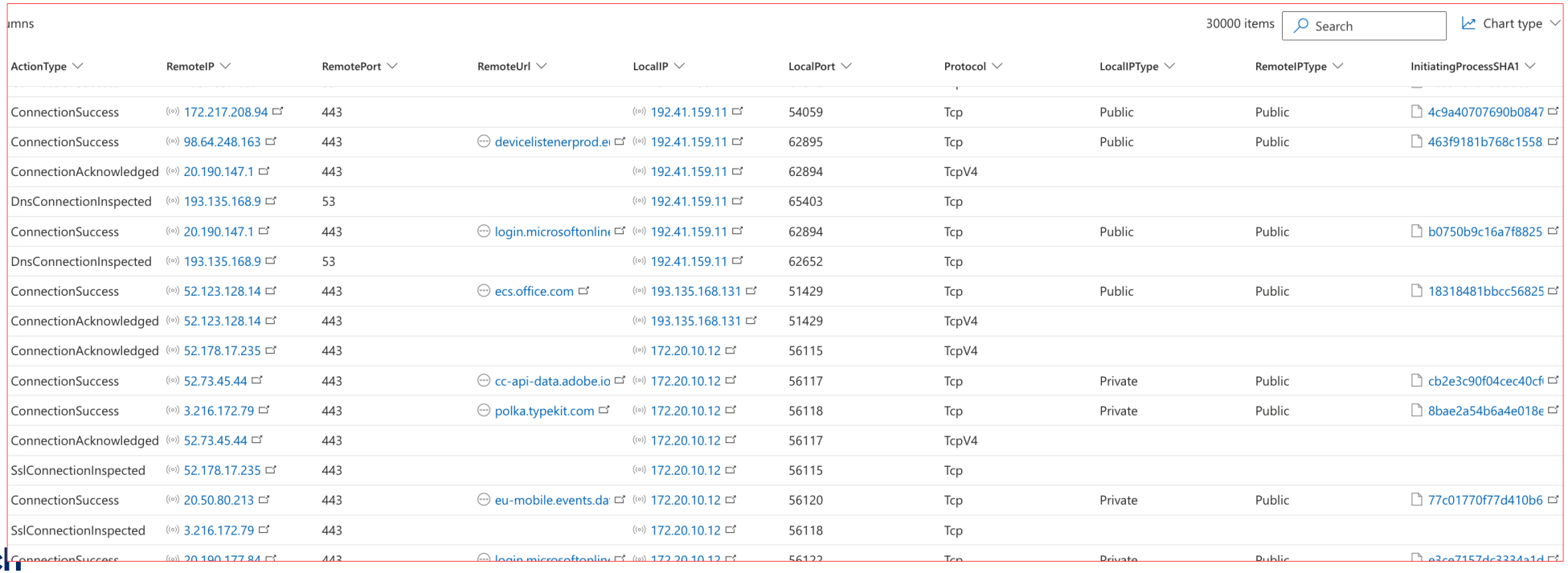
Classification



Turn raw data into real detections

```
let CIDRASN = (externaldata (CIDR:string, CIDRASN:int, CIDRASNName:string)
['https://firewalliplists.gypthecat.com/lists/kusto/kusto-cidr-asn.csv.zip'] with (ignoreFirstRecord=true));
DeviceNetworkEvents
| evaluate ipv4_lookup(CIDRASN, RemoteIP, CIDR, return_unmatched=true)
```

⚠ Up to 50,000 records can be returned in total. Each tenant's results can return up to 50,000 records divided by the number of queried tenants.



umns — 30000 items — Search — Chart type

ActionType	RemoteIP	RemotePort	RemoteUrl	LocalIP	LocalPort	Protocol	LocalIPType	RemoteIPType	InitiatingProcessSHA1
ConnectionSuccess	172.217.208.94	443		192.41.159.11	54059	Tcp	Public	Public	4c9a40707690b0847
ConnectionSuccess	98.64.248.163	443	devicelistenerprod.e	192.41.159.11	62895	Tcp	Public	Public	463f9181b768c1558
ConnectionAcknowledged	20.190.147.1	443		192.41.159.11	62894	TcpV4			
DnsConnectionInspected	193.135.168.9	53		192.41.159.11	65403	Tcp			
ConnectionSuccess	20.190.147.1	443	login.microsoftonlin	192.41.159.11	62894	Tcp	Public	Public	b0750b9c16a7f8825
DnsConnectionInspected	193.135.168.9	53		192.41.159.11	62652	Tcp			
ConnectionSuccess	52.123.128.14	443	ecs.office.com	193.135.168.131	51429	Tcp	Public	Public	18318481bbcc56825
ConnectionAcknowledged	52.123.128.14	443		193.135.168.131	51429	TcpV4			
ConnectionAcknowledged	52.178.17.235	443		172.20.10.12	56115	TcpV4			
ConnectionSuccess	52.73.45.44	443	cc-api-data.adobe.io	172.20.10.12	56117	Tcp	Private	Public	cb2e3c90f04cec40cf
ConnectionSuccess	3.216.172.79	443	polka.typekit.com	172.20.10.12	56118	Tcp	Private	Public	8bae2a54b6a4e018e
ConnectionAcknowledged	52.73.45.44	443		172.20.10.12	56117	TcpV4			
SslConnectionInspected	52.178.17.235	443		172.20.10.12	56115	Tcp			
ConnectionSuccess	20.50.80.213	443	eu-mobile.events.da	172.20.10.12	56120	Tcp	Private	Public	77c01770f77d410b6
SslConnectionInspected	3.216.172.79	443		172.20.10.12	56118	Tcp			

Connections from unexpected ISP

```
let CIDRASN = (externaldata (CIDR:string, CIDRASN:int, CIDRASNName:string)
['https://firewalliplists.gypthecat.com/lists/kusto/kusto-cidr-asn.csv.zip'] with (ignoreFirstRecord=true));
DeviceNetworkEvents //Table
| evaluate ipv4_lookup(CIDRASN, RemoteIP, CIDR, return_unmatched=true) //Matching IPs with ASN
| where isnotempty(RemoteIP) and ActionType has 'ConnectionSuccess' //Condition
| extend PrivateIP=ipv4_is_private(RemoteIP)
| where PrivateIP == 0  //Condition
| extend GeoIPData = tostring(geo_info_from_ip_address(RemoteIP).country)
| summarize
Different_IPs=make_set(RemoteIP),make_set(ActionType),make_set(InitiatingProcessCommandLine),make_set(InitiatingPr
ocessFileName),make_set(CIDR),make_set(GeoIPData),count() by  CIDRASNName, DeviceName
```

CIDRASNName	DeviceName	Different_IPs	set_ActionType	set_InitiatingProcessCo...	set_InitiatingProcessFile...	set_CIDR	set_GeoIPData	count_
Microsoft Corporation	pc2	[redacted]	["ConnectionSuccess"]	["\"ms-teams.exe\" ","\"OL	["ms-teams.exe","outlook.e	["	["Switzerland","France","Br	1138
Akamai International B.V.	pc2		["ConnectionSuccess"]	["\"OUTLOOK.EXE\" ","\"m:	["outlook.exe","msedge.ex	["	["Switzerland"]	32
Amazon.com, Inc.	pc2		["ConnectionSuccess"]	["\"Creative Cloud Helper.e	["creative cloud helper.exe'	["	["United States","Ireland","	189
Sunrise GmbH	pc2		["ConnectionSuccess"]	["updateInstalled /backgro	["onedrive.exe","svchost.ex	["	["Switzerland"]	192
Fastweb	pc2		["ConnectionSuccess"]	["svchost.exe -k netsvcs -p	["svchost.exe"]	["	["Italy"]	43
Google LLC	pc2		["ConnectionSuccess"]	["\"msedge.exe\" --type=u	["msedge.exe","svchost.exe	["	["United States"]	82
Neue Medien Muennich	pc2		["ConnectionSuccess"]	["\"msedge.exe\" --type=u	["msedge.exe"]	["	["Germany"]	4
Cloudflare, Inc.	pc2		["ConnectionSuccess"]	["\"msedge.exe\" --type=u	["msedge.exe","svchost.exe	["	[""]	40
SWITCH	pc2		["ConnectionSuccess"]	["\"msedge.exe\" --type=u	["msedge.exe"]	["	["Switzerland"]	3

KQL Collectors by ASN/ISP (Email Threats)



```
let CIDRASN = (externaldata (CIDR:string, CIDRASN:int, CIDRASNName:string)
['https://firewalliplists.gypthecat.com/lists/kusto/kusto-cidr-asn.csv.zip']with (ignoreFirstRecord=true));
EmailEvents
| evaluate ipv4_lookup(CIDRASN, SenderIPv4, CIDR, return_unmatched=true)
| extend GeoIPData = tostring(geo_info_from_ip_address(SenderIPv4).country)
| summarize Different_IPs=make_set(SenderIPv4), Countries= make_set(GeoIPData), make_set(CIDR), make_set(SenderFromDomain),
Distinct_IPs=dcount(SenderIPv4) ,Total_emails = count(),make_set(ThreatTypes),Delivered_on_Inbox= countif(DeliveryLocation has "Inbox/folder"),  Email_Threat= count(isnotempty(ThreatTypes)),
Email_Valid = count( isempty(ThreatTypes)) by GeoIPData, CIDR, CIDRASNName,CIDRASN
| extend SuspiciousRatio = Email_Threat * 1.0 / Total_emails, ValidRatio = Email_Valid * 1.0 / Total_emails
| extend SuspiciousPercentage = SuspiciousRatio * 100, ValidPercentage = ValidRatio * 100
| where SuspiciousPercentage == 100
| project CIDRASNName,set_SenderFromDomain, set_CIDR,CIDRASN, Different_IPs, Countries,Distinct_IPs, set_ThreatTypes,Total_emails, Delivered_on_Inbox, Email_Threat, Email_Valid, SuspiciousPercentage, ValidPercentage
```

Getting started | **Results**

Export | Show empty columns | 1980 items | Search | Chart type | Full screen

Filters: Add filter

CIDRASNName	set_CIDR	Countries	Distinct_IPs	Total_emails ↓	Delivered_on_Inbox	Email_Threat	Email_Valid	SuspiciousPercentage	ValidPercentage
LeaseWeb Netherl...	["212.32.224.0/19"]	["The Netherlands"]	1	2556	0	2556	0	100	0
Eletric Telecomuni...	["143.0.180.0/22"]	["Brazil"]	1	1233	0	1233	0	100	0
ALGAR TELECOM SA	["200.146.192.0/18"]	["Brazil"]	1	624	0	624	0	100	0
China Telecom Gr...	["116.224.0.0/12"]	["China"]	1	542	0	542	0	100	0
PONYNET	["198.98.48.0/20"]	["United States"]	14	308	0	308	0	100	0
Hostgnome Ltd	["185.91.69.0/24"]	["United Kingdom"]	20	237	0	237	0	100	0
WKVE Asses. em S...	["189.76.224.0/20"]	["Brazil"]	1	170	0	170	0	100	0
China Telecom Gr...	["116.224.0.0/12"]	["China"]	1	169	0	169	0	100	0
Webglobe, s.r.o.	["213.109.164.0/22"]	["Czechia"]	45	98	0	98	0	100	0
OVH SAS	["54.36.0.0/14"]	["Canada"]	40	42	0	42	0	100	0

Switch

Thank you