Preserving Confidentiality When Hunting With Friends

PhD. Paolo Di Prodi (Priam Cyber AI ltd, United Kingdom)

Gabriel Bassett (Liberty Mutual, United States)

Hugo Ideler (Roseman Labs, Netherlands)

Mini agenda today

- A real example the: Trigona Campaign
- Security Operations and Data
- Incident Response frameworks and standards for sharing
- Example of cooperative intra company reporting
- Sharing more with PET frameworks
- The 3 main approaches
- Why MPC+DP are the winners?
- Real deployment in the Netherlands
- Conclusion
- Q&A

Who is Paolo aka "The DOC"

- PhD in multi agent ML
- Founder of Priam AI in UK
- Senior Data Scientist for Fortinet
- Data Scientist for Microsoft
- Contributes to several open source initiatives such as STIX 2.1 and EPSS

OASIS

CYBER THREAT ALLIANCE

OPEN CYBERSECURITY ALLIANCE

MITRE ENGENUITY™

A Foundation for Public Good

EPSS

Exploit Prediction Scoring System

Who is Gabriel Bassett

- Director of Cyber Risk Advisory Services, Liberty Mutual
- Founder, Information Security Analytics LLC
- Former Lead Data Scientist, Verizon DBIR
- BoD & Game Architect, CTF Factory, INC
- Director, BSides Las Vegas Ground Truth Track

Who is Hugo Ideler

- Head of Engineering at **Roseman Labs**, a start-up specializing in Multi-Party Computation
- Lead Engineer in NCSC-NL's SecureNed Platform
- Former Senior Manager at Deloitte's Incident Response practice
- 10 years of experience in DFIR

RosemanLabs
PRIVACY BY DESIGN

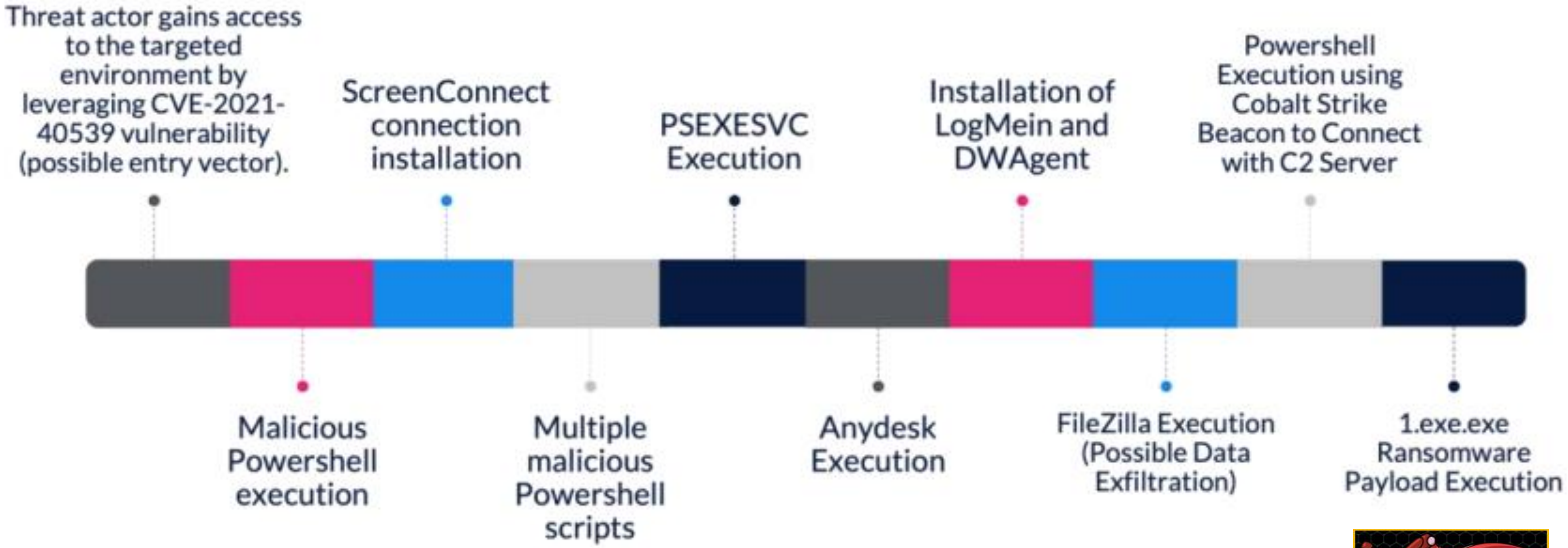
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

The Trigona campaign

CVE-2021-40539
Published: 09/07/2021
CVE Base Score: 9.8 CRITICAL

Not a Zero Day!

The malicious operator would take its time to explore: average 4 months…



Threat actor gains access to the targeted environment by leveraging CVE-2021-40539 vulnerability (possible entry vector).

Malicious Powershell execution

ScreenConnect connection installation

Multiple malicious Powershell scripts

PSEXESVC Execution

Anydesk Execution

Installation of LogMein and DWAgent

FileZilla Execution (Possible Data Exfiltration)

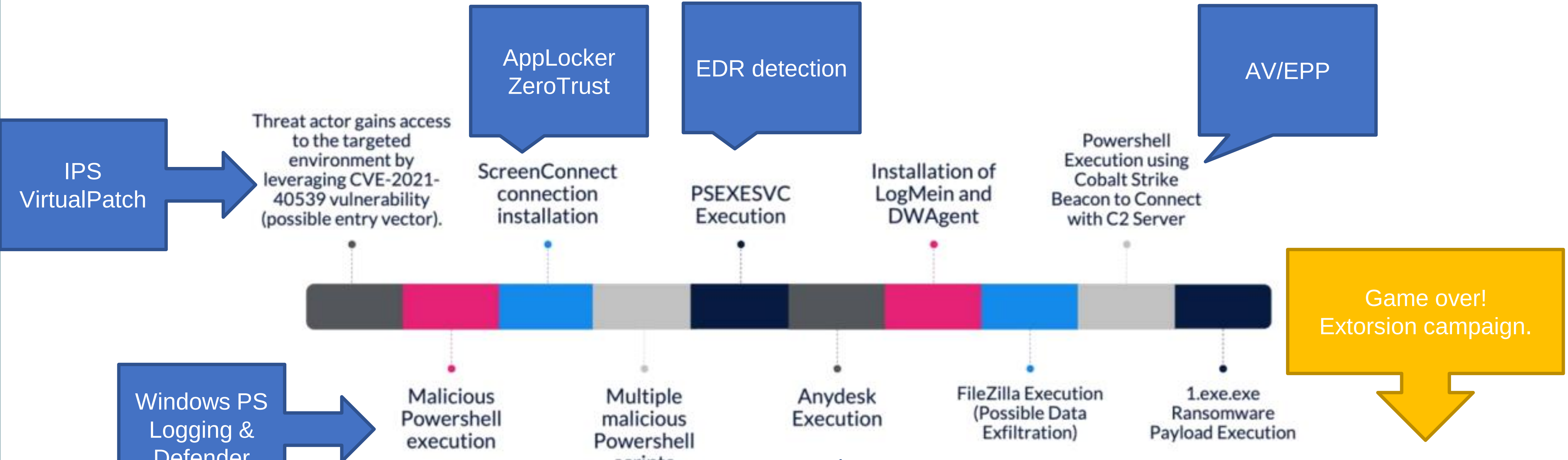
Powershell Execution using Cobalt Strike Beacon to Connect with C2 Server

1.exe.exe Ransomware Payload Execution

Our ground truth: PAN UNIT 42 and ARETE report.
Campaigns: Dec 2022, Jan 2023 and Feb 2023
Total Victims: 15

Trigona discovered in October 2022

The Trigona campaign: detections & mitigations?



IPS VirtualPatch

Threat actor gains access to the targeted environment by leveraging CVE-2021-40539 vulnerability (possible entry vector).

AppLocker ZeroTrust

ScreenConnect connection installation

EDR detection

PSEXESVC Execution

Installation of LogMein and DWAgent

AV/EPP

Powershell Execution using Cobalt Strike Beacon to Connect with C2 Server

Game over! Extorsion campaign.

Windows PS Logging & Defender

Malicious Powershell execution

Multiple malicious Powershell scripts

Anydesk Execution

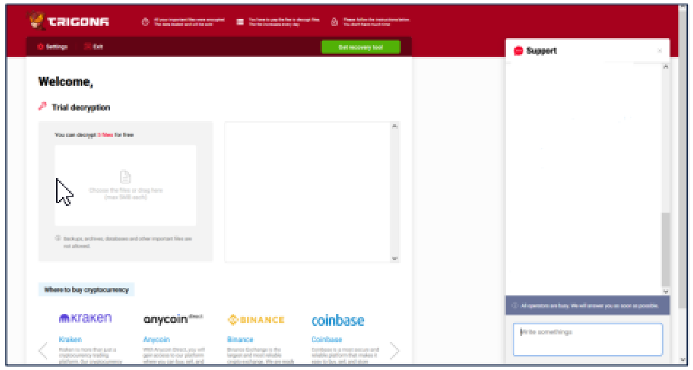
FileZilla Execution (Possible Data Exfiltration)

1.exe.exe Ransomware Payload Execution

PS Policies EDR: bypass PS

SDWan Segmentation

DLP



Welcome,

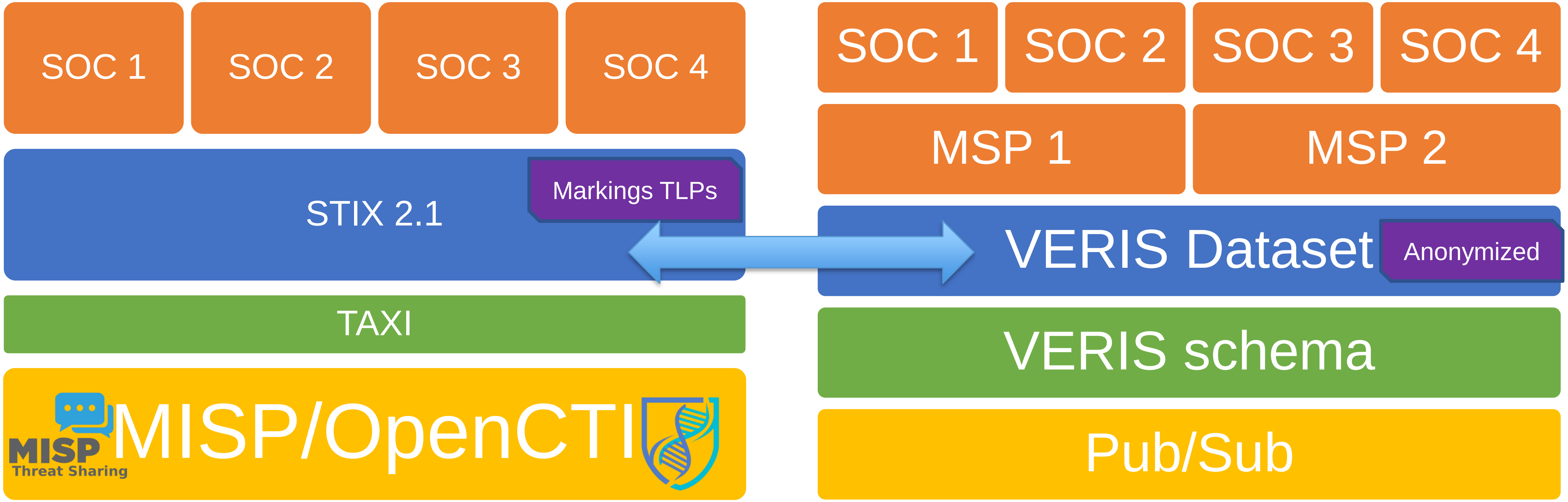
Trial decryption

You can decrypt 3 files for free

For eye candy, add your favourite ATT&CK TTP ….

Classical Sharing Scenarios

- Push/Pull Hub/Spoke 🐇
- Mostly Push/Unidirectional 🐢



SOC 1 | SOC 2 | SOC 3 | SOC 4

STIX 2.1 — Markings TLPs

TAXI

MISP/OpenCTI

MISP Threat Sharing

SOC 1 | SOC 2 | SOC 3 | SOC 4

MSP 1 | MSP 2

VERIS Dataset — Anonymized

VERIS schema

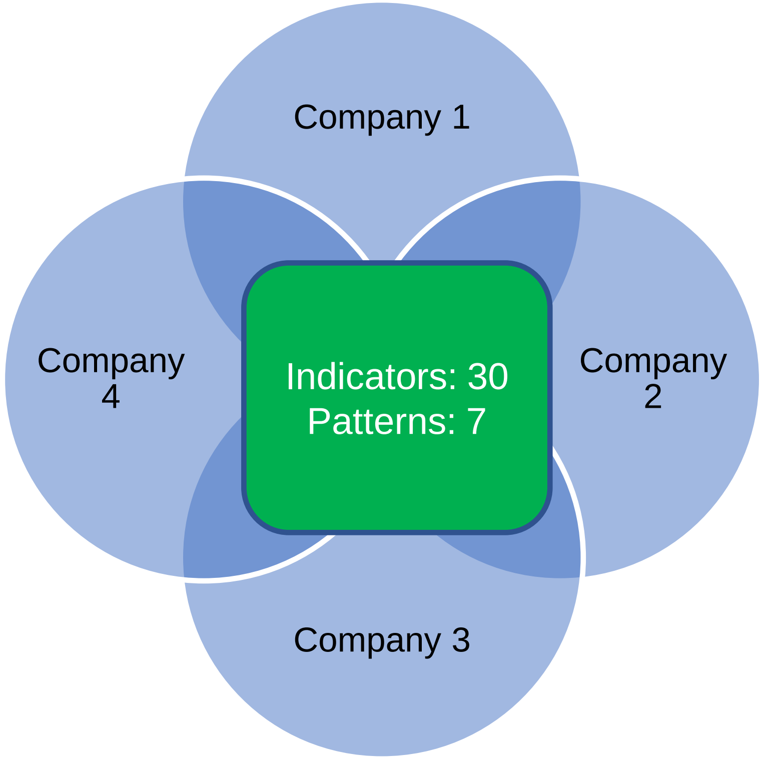
Pub/Sub

Ground Truth and Simulation

- A Stix 2.1 package with …

Entity	Counts
Report	2
Intrusion Set	1
Attack Pattern	32
Campaign	1
Identity	1
Indicator	45
Relationships	99

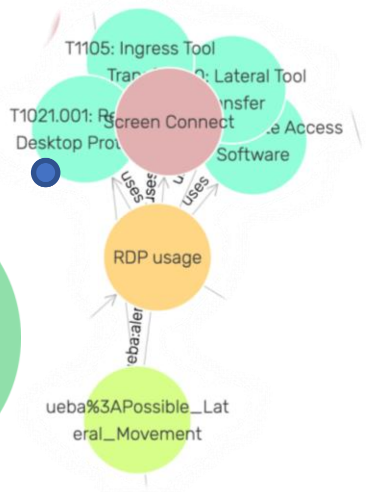
- A pool of 10 companies: 4 impacted



Company Identity	Bundle Size	Notes
Company A	49	Got the attack vector
Company B	49	
Company C	47	Got the attack vector
Company D	47	

Company 1: investigation point

One of the companies finds a suspicious behaviour from one of their security products….



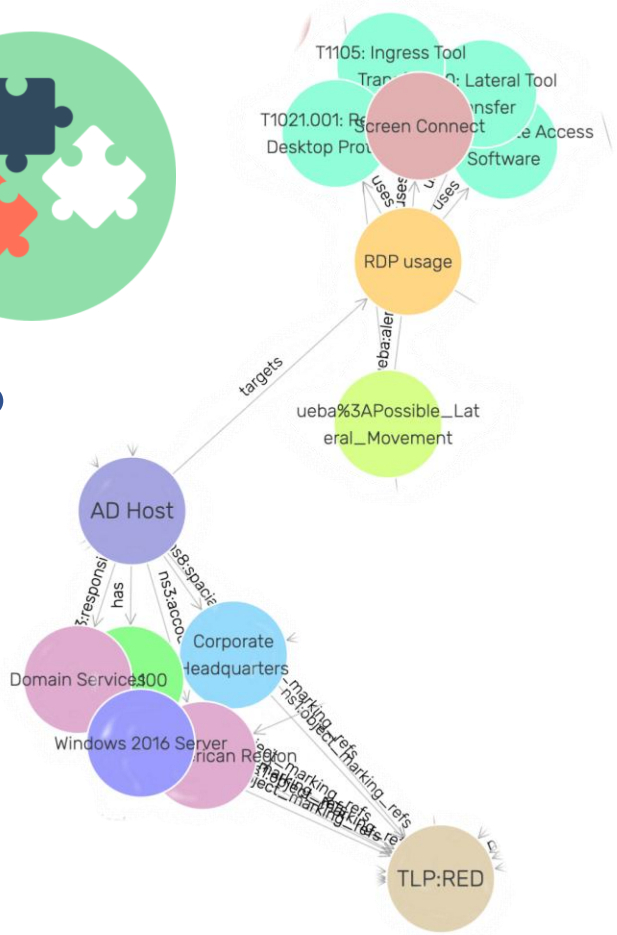
Fast query: how common is this technique given the context?

Query MITRE ATT&CK Sightings and ATT&CK Top Techniques?

UEBA: anomaly?
EDR: lateral movement?

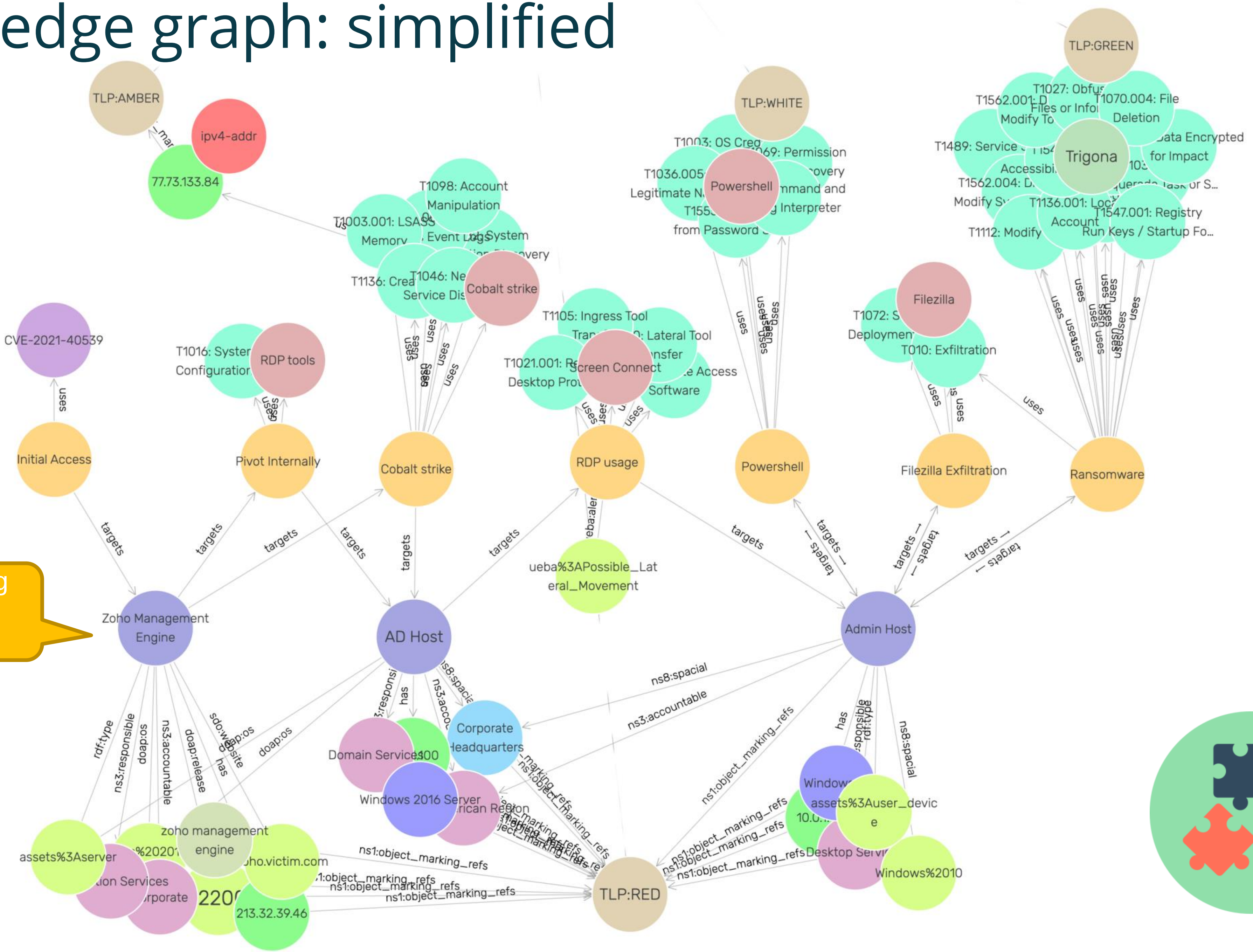
Company 2: contextual info

The activity originates from an active directory host with a windows server from their main headquarters.



More context during the investigation…

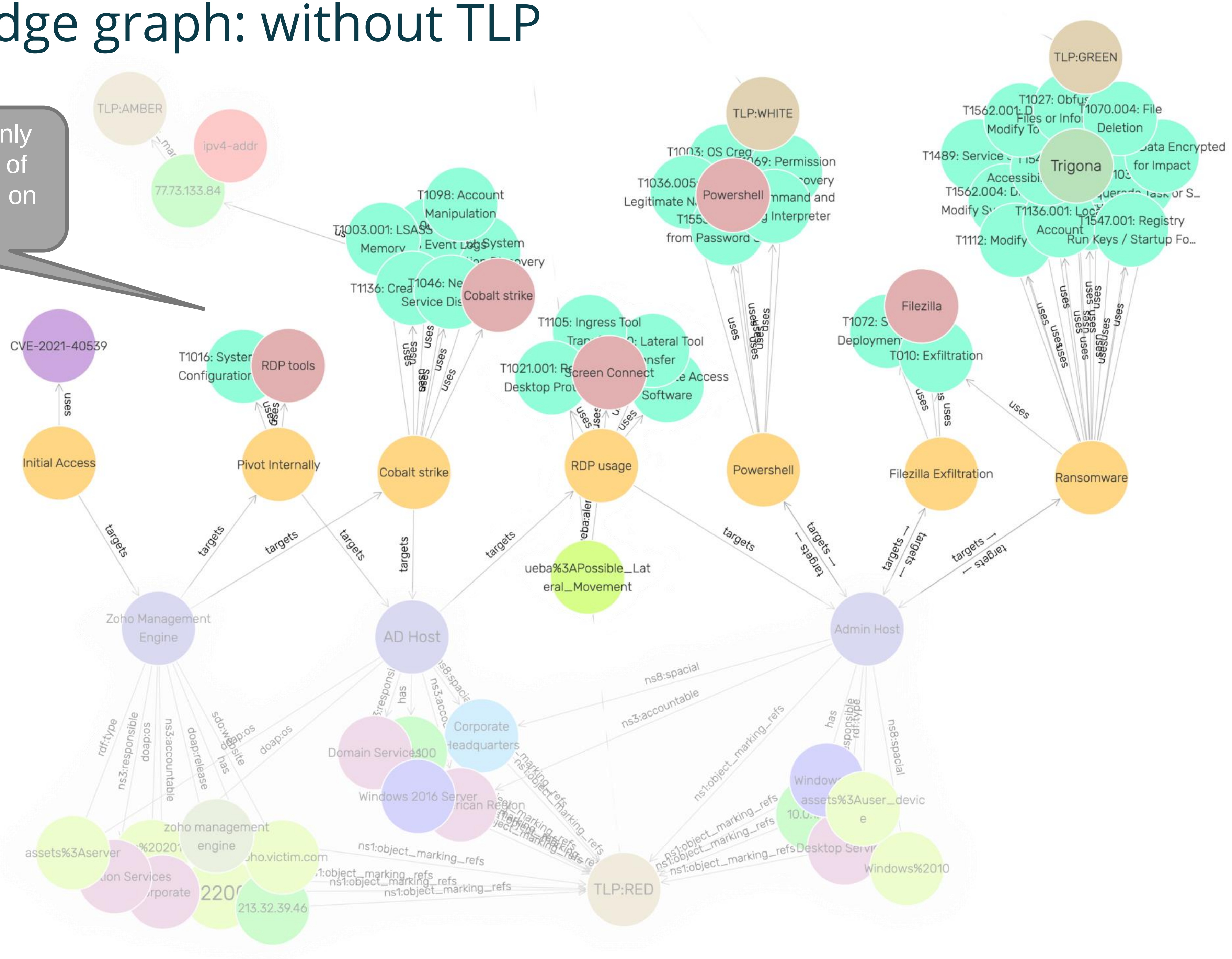
Full knowledge graph: simplified



Public facing unpatched CVE

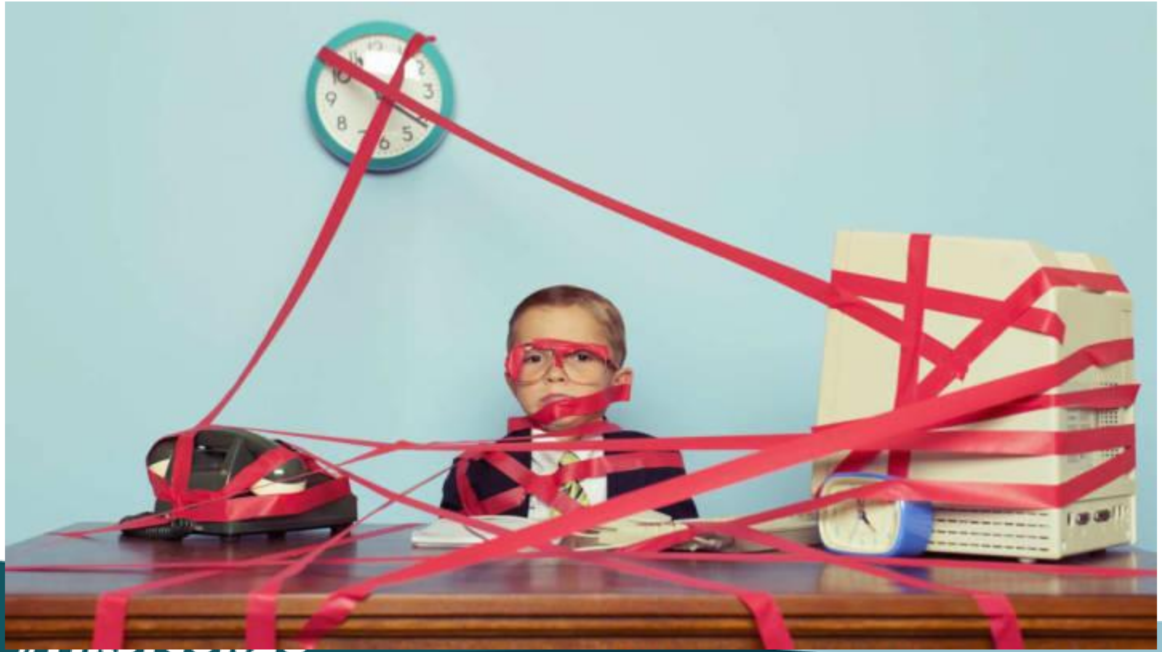
Full knowledge graph: without TLP

The companies will only be able to share part of the information based on TLP levels.

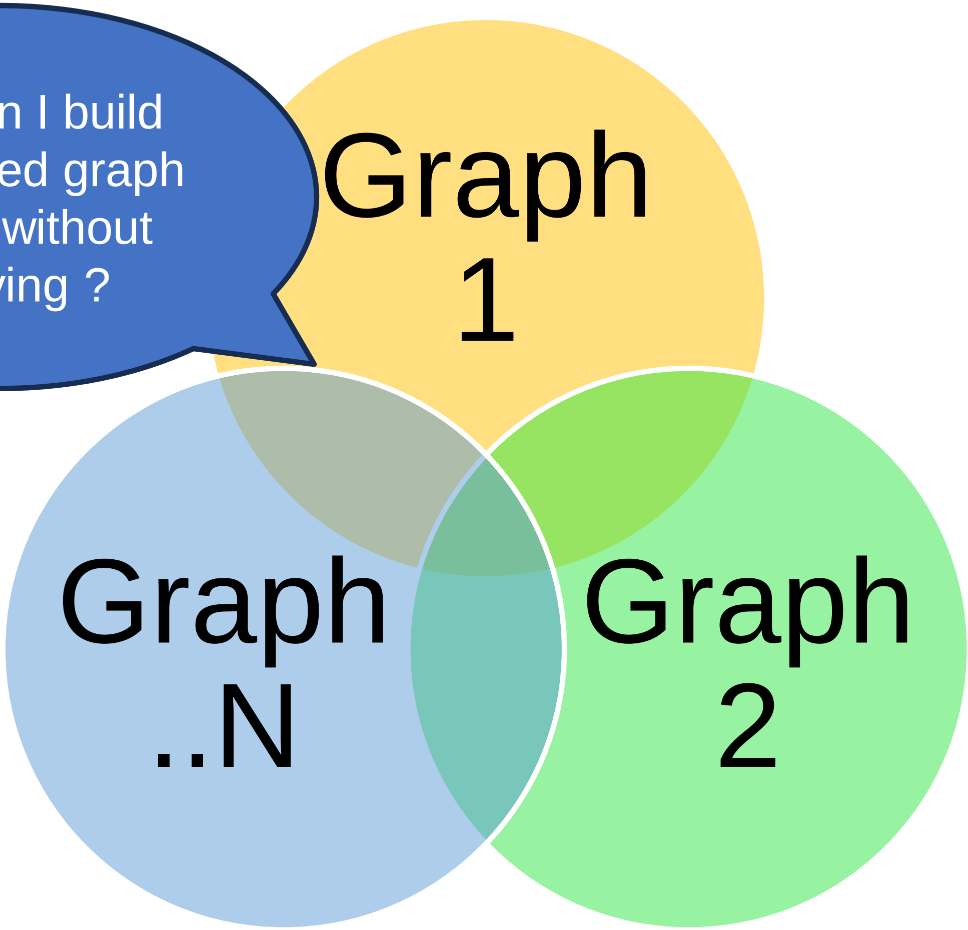


How do we make red more transparent?

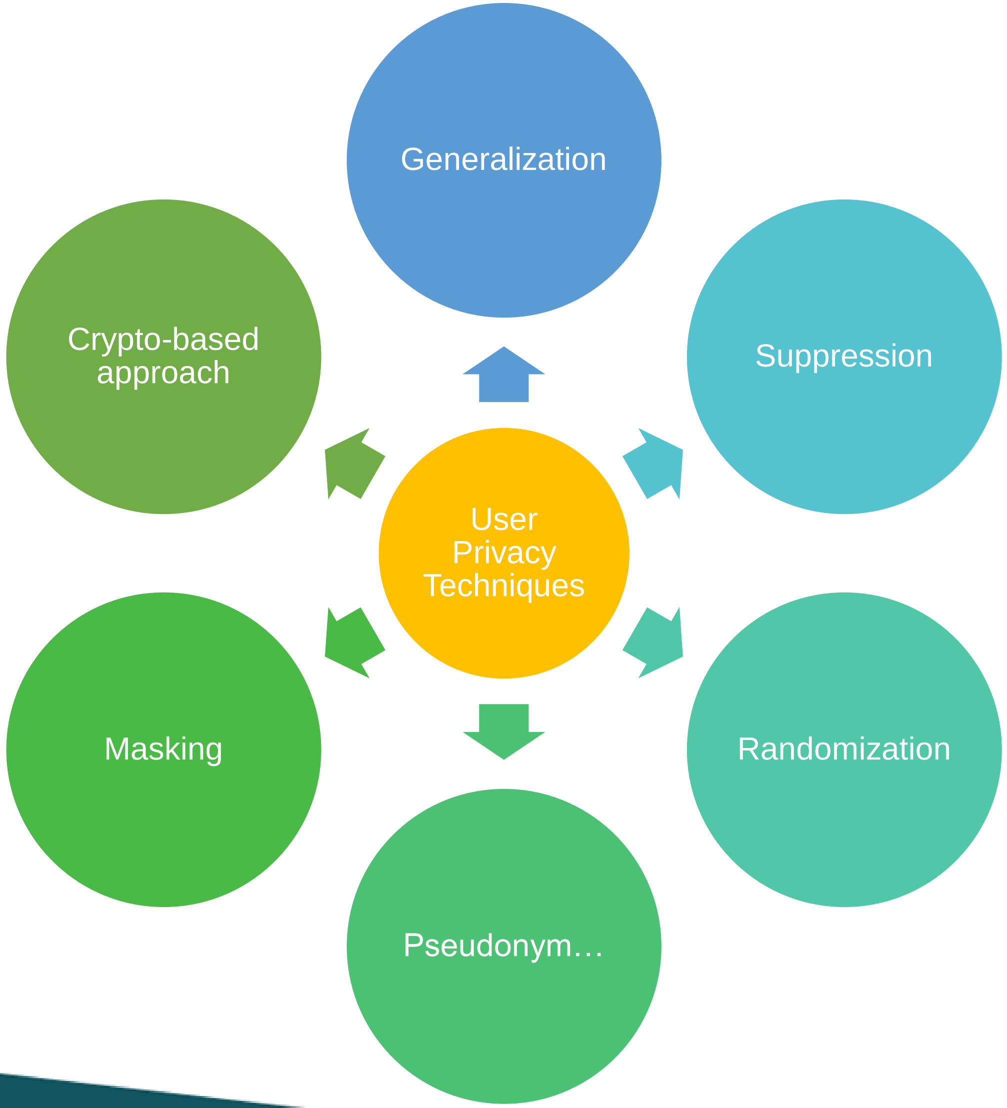
Assuming you have a perfect incident sharing platform with real time sharing and querying, standardized & extended formats like STIX 2.1, VERIS, ATTACK FLOW, ATT&CK, CACAO, OpenC2….
Tools like OpenCTI, MISP for exchanging.



How can I build this shared graph rapidly without worrying ?



Privacy-enhancing Technologies (PETs) for cyber sharing



User Privacy Techniques

Generalization

Suppression

Randomization

Pseudonym…

Masking

Crypto-based approach

Most traditional techniques offer weak mathematical guarantees of privacy.

We need something more powerful and with stronger mathematical guarantees, known as Privacy-enhancing Technologies (PETs).

Privacy-enhancing Techniques (PETs)

Fully-homorphic encryption (FHE)

- High computation cost
- Low communication cost

Multi-party Computation (MPC)

- Low computational cost
- High communication cost

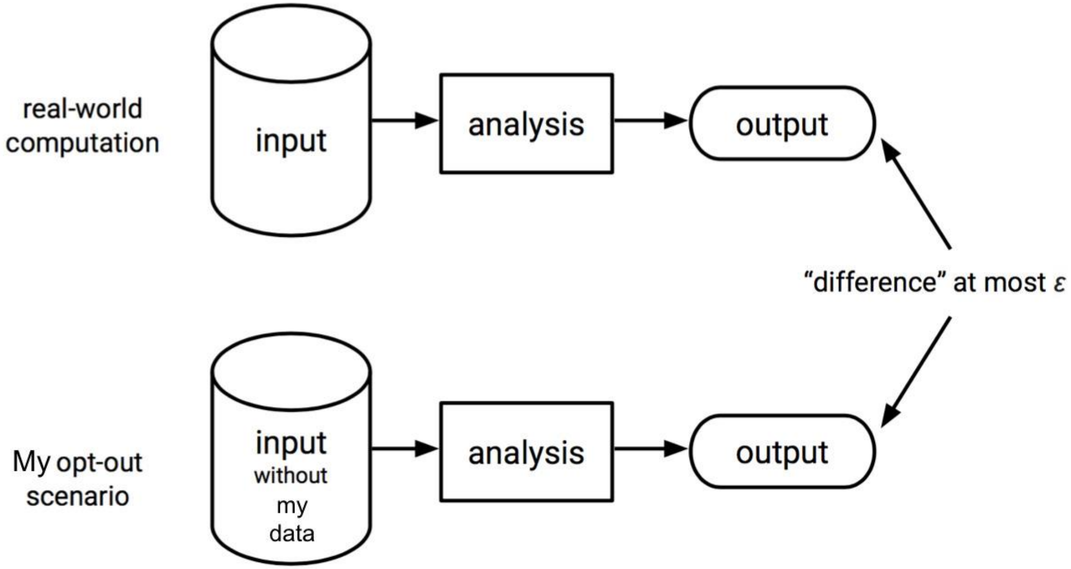
Differential Privacy (DP)

- Very fast to compute
- Support most queries

Differential Privacy Example

Challenge
You want to create a survey for your team to measure how many bagels they eat every day.

Some people in your team are afraid to participate because they are on a "diet" and they don't want to risk to be identified if future information is released.



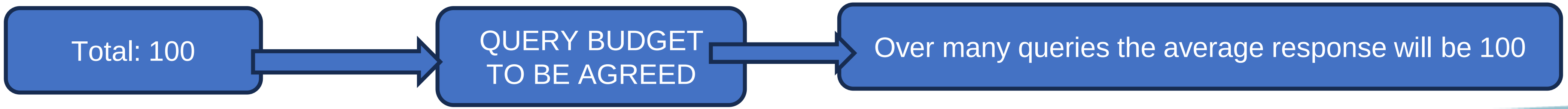
Differential privacy randomization

- Each participant spin a dial and add noise to their true answer.

ID	True Answer	Randomized	Coin Toss
Paolo	2	2	Head
Gabe	3	4	Tail
…			
Hugo	5	3	Tail

- Your HR team then starts to query the database for bagel consumption

HR	Response
Jon	120
Tim	90
Ryu	150


Total: 100

QUERY BUDGET TO BE AGREED

Over many queries the average response will be 100

Multi-party computation (MPC) example

Gabe	6
Paolo	10

Challenge
Gabe and Paolo each have a number of Montreal bagels.

They want to know how many bagels they have together, without revealing their own stacks.

How can they do this?

Multi-party computation (MPC) example

Gabe and Paolo each split their stacks and give their bagels to three helpers (MPC nodes).

			N_0		N_1		N_2
Gabe	6	=	3	+	1	+	2
Paolo	10	=	2	+	5	+	3

Note: Simplified example; in reality, the numbers should be randomly selected from a large finite field.

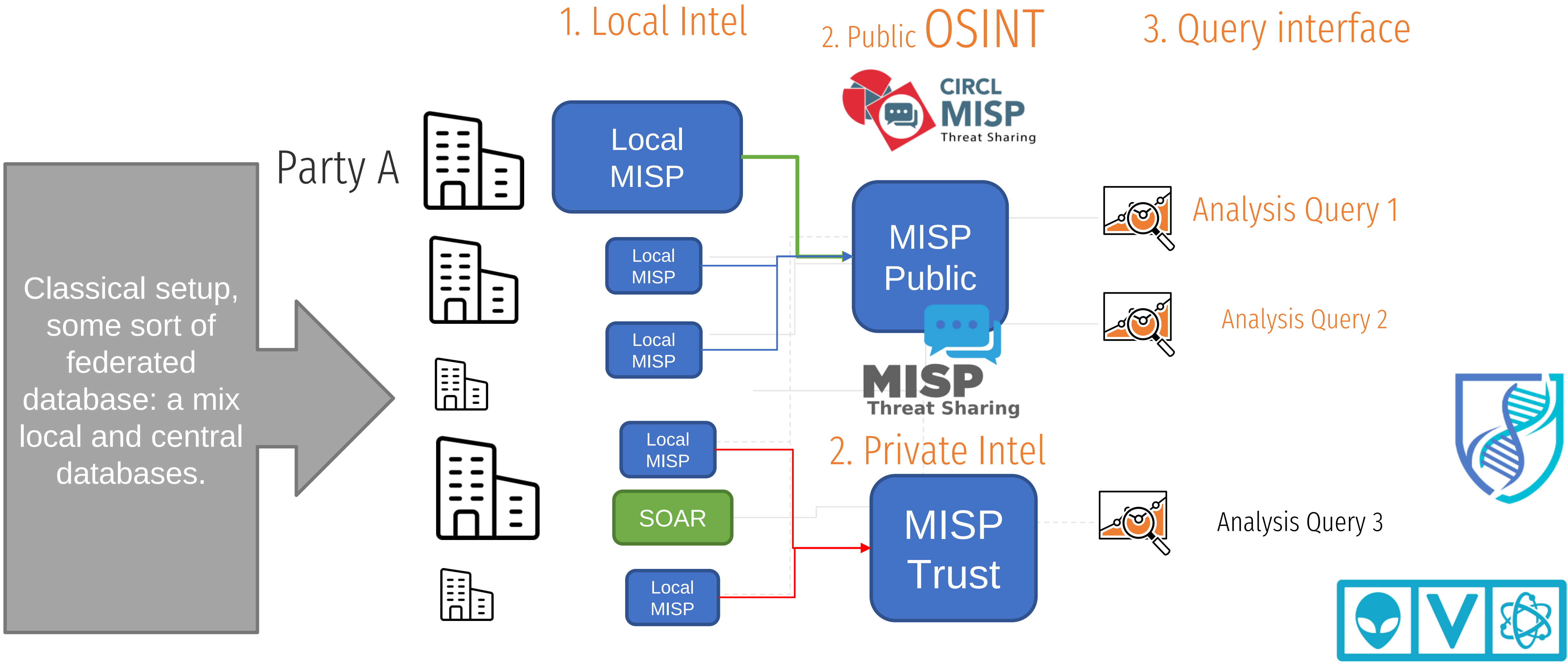
Multi-party computation (MPC) example

Each helper adds his bagels together. Finally, the helpers add their numbers together.

			N_0		N_1		N_2
Gabe	6	=	3	+	1	+	2
	+		+		+		+
Paolo	10	=	2	+	5	+	3
	=		=		=		=
Answer	16	=	5	+	6	+	5

None of the helpers learn anything about the original amount of bagels from either Gabe or Paolo.

Cooperative threat hunting: traditional



Examples with Trigona campaign

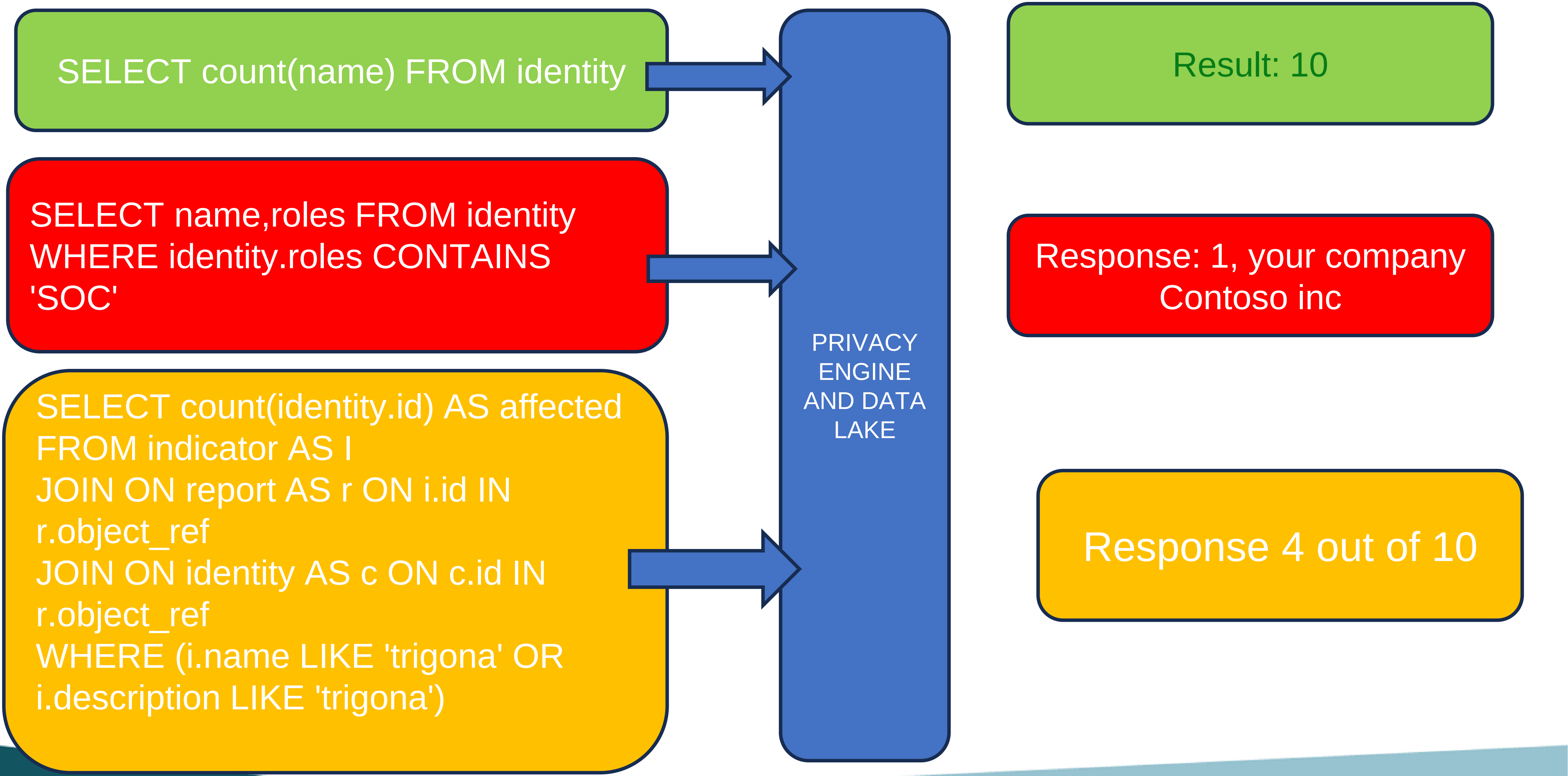
Union

- All malware hashes
- Include compiled Delphi
- Include command-line flags
- Include ransomware TTP
- Count incidents in the last month
- Count total companies
- Count total records/users
- Total payments demand

Join

- All malware hashes
- All exfiltration URL,IP, Domain
- All tools used on Window
- Count vulnerabilities involved
- List vulnerabilities
- List OS versions affected

Example queries



```
SELECT count(name) FROM identity
```

```
SELECT name,roles FROM identity
WHERE identity.roles CONTAINS
'SOC'
```

```
SELECT count(identity.id) AS affected
FROM indicator AS I
JOIN ON report AS r ON i.id IN
r.object_ref
JOIN ON identity AS c ON c.id IN
r.object_ref
WHERE (i.name LIKE 'trigona' OR
i.description LIKE 'trigona')
```

PRIVACY ENGINE AND DATA LAKE

Result: 10

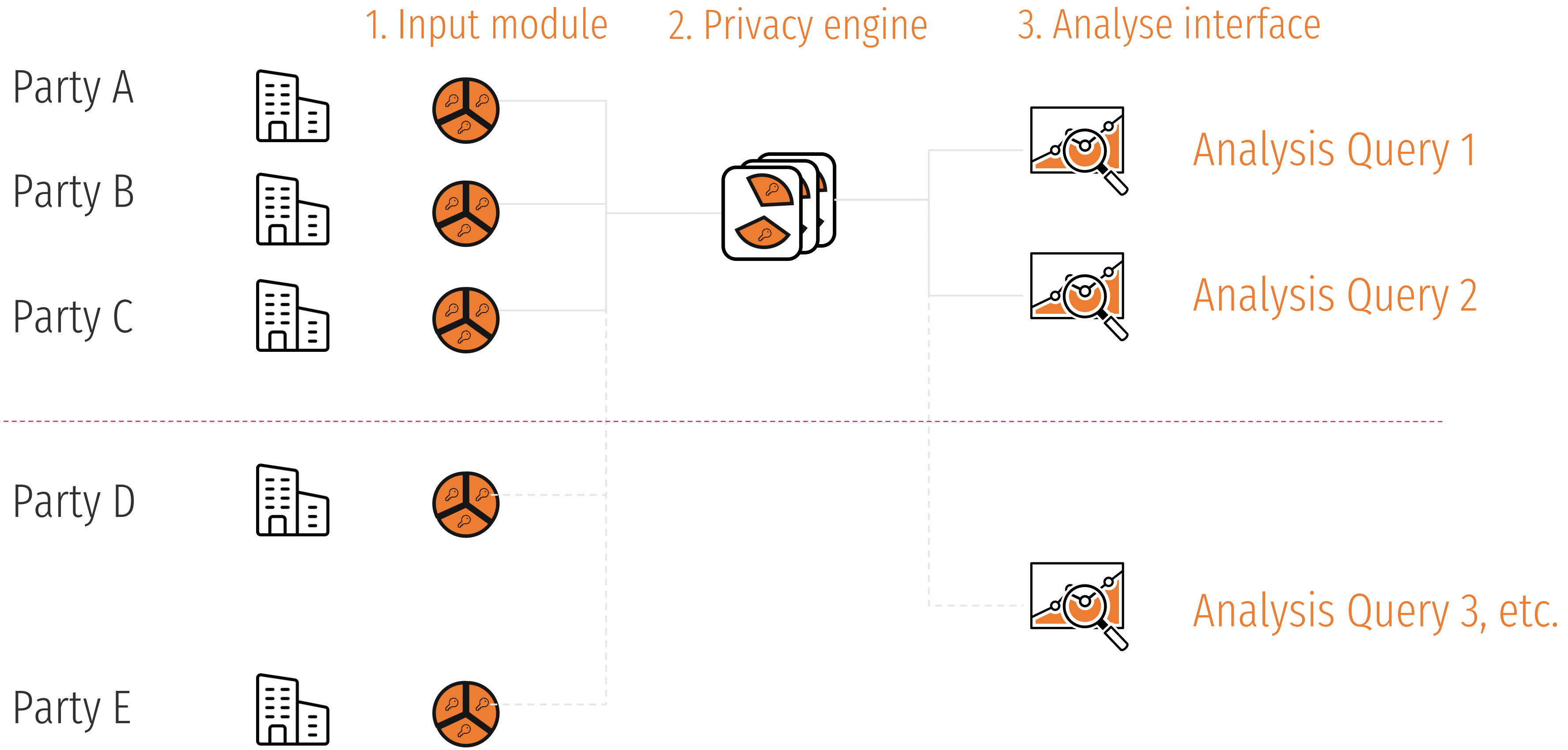
Response: 1, your company Contoso inc

Response 4 out of 10

Cooperative threat-hunting: MPC

Initial cooperation between three security operation teams...

...easy to expand with additional participants



Stack components

IDE

- JupyterLab
- PyCharm

Visualization

- Streamlit
- Dash

Data Operations

- Pandas
- Spark
- Others

Application

- Flask/Django
- Vue.JS
- Others

Schema/Protocols

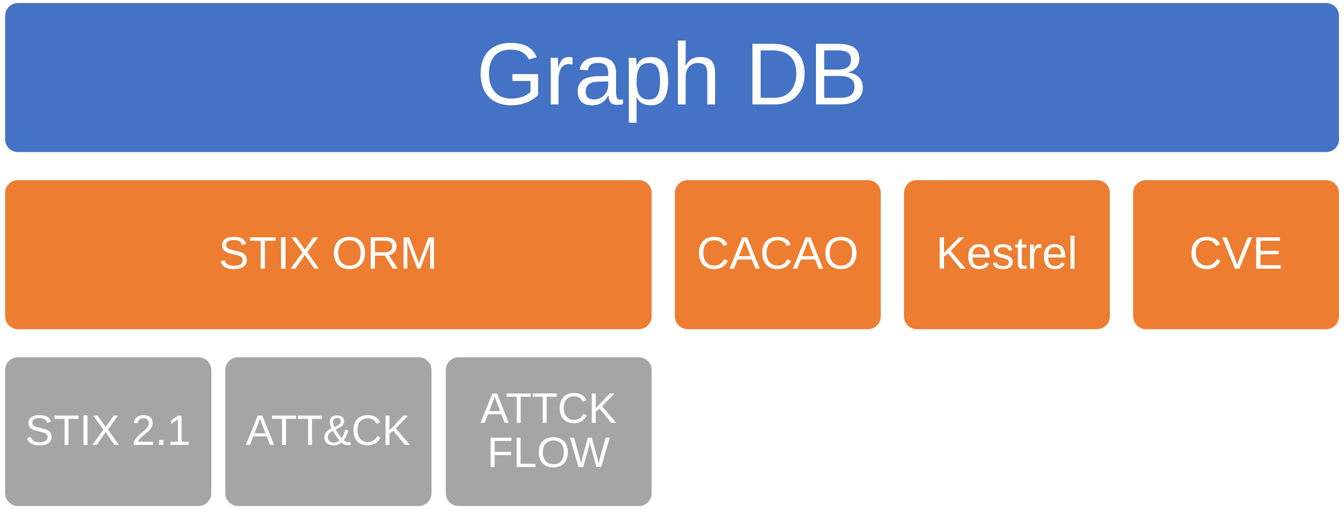
- VERIS
- STIX2.1
- ATT&CK
- CACAO

MPC Engine

- MPyC
- Others

DP Engine

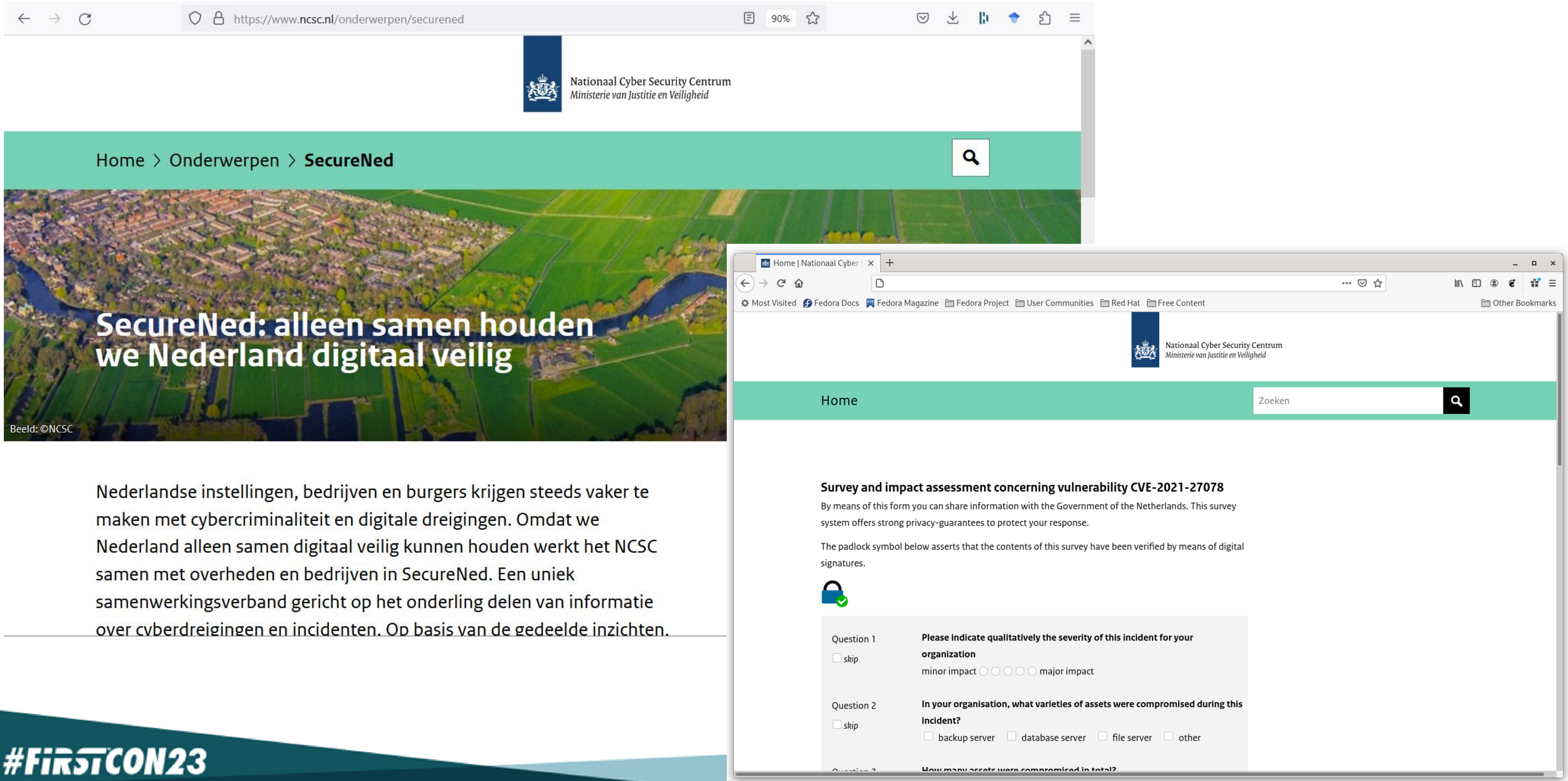
- OpenMined
- DiffPrivLib
- Others



A lot of moving parts to orchestrate and maintain, plus performance optimizations required.

An example of a growing network: SecureNed

Anonymous collection of sensitive cyber threat intelligence



https://www.ncsc.nl/onderwerpen/securened

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Home > Onderwerpen > **SecureNed**

SecureNed: alleen samen houden we Nederland digitaal veilig

Beeld: ©NCSC

Nederlandse instellingen, bedrijven en burgers krijgen steeds vaker te maken met cybercriminaliteit en digitale dreigingen. Omdat we Nederland alleen samen digitaal veilig kunnen houden werkt het NCSC samen met overheden en bedrijven in SecureNed. Een uniek samenwerkingsverband gericht op het onderling delen van informatie over cyberdreigingen en incidenten. Op basis van de gedeelde inzichten,

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Home

Zoeken

Survey and impact assessment concerning vulnerability CVE-2021-27078

By means of this form you can share information with the Government of the Netherlands. This survey system offers strong privacy-guarantees to protect your response.

The padlock symbol below asserts that the contents of this survey have been verified by means of digital signatures.

Question 1
□ *skip*

Please indicate qualitatively the severity of this incident for your organization

minor impact ○ ○ ○ ○ ○ major impact

Question 2
□ *skip*

In your organisation, what varieties of assets were compromised during this incident?

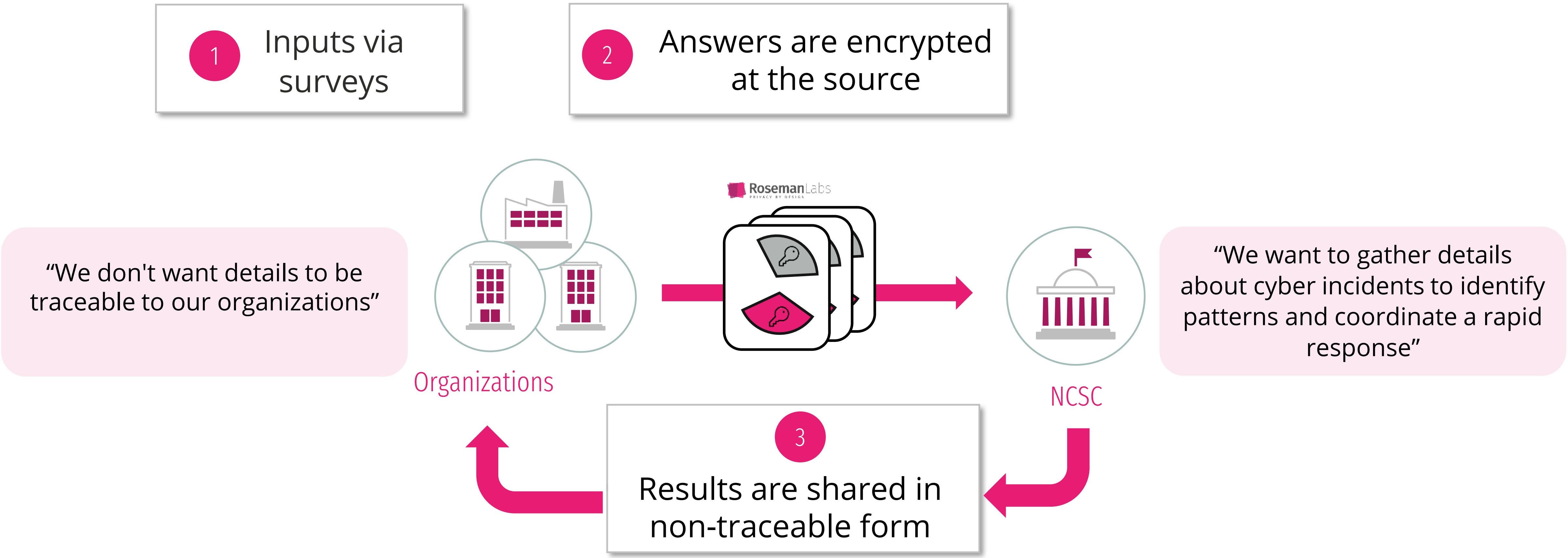
□ backup server □ database server □ file server □ other

Question 3

How many assets were compromised in total?

An example of a growing network: SecureNed

Anonymous collection of sensitive cyber threat intelligence



1 Inputs via surveys

2 Answers are encrypted at the source

3 Results are shared in non-traceable form

“We don't want details to be traceable to our organizations”

“We want to gather details about cyber incidents to identify patterns and coordinate a rapid response”

Conclusions

Strong data model

Secure computation is a reality

Share sensitive data securely

Join our community

Slack – https://bit.ly/43D4uRs

Reach out to us

paolo@priam.ai

gabriel.bassett@libertymutual.com

hugo.ideler@rosemanlabs.com