Passive Investigation of Networks and Classification of the discovered Assets according to the IT Basic Protection of the BSI

3rd KuVS Fachgespräch "Machine Learning & Networking"

Stephan Schwinger, Alexandra Meyer, Arnold Krille
genua GmbH

07.10.2022

genua.

Passive Investigation of Networks and Classification of the discovered Assets according to the IT-Basic Protection of the BSI

3rd KuVS Fachgespräch "Machine Learning & Networking"

Neural Networks not included

Stephan Schwinger, Alexandra Meyer, Arnold Krille
genua GmbH

07.10.2022

Wintermute 101

genua.

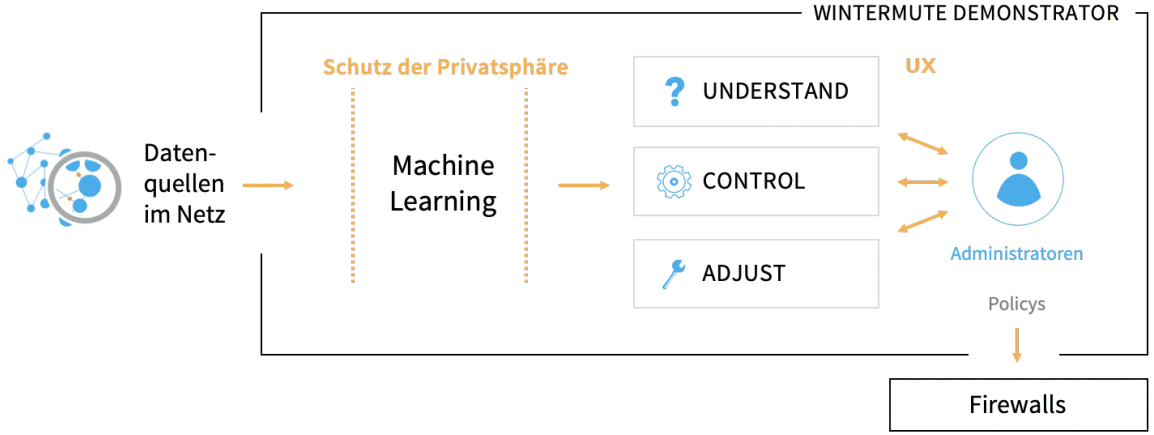
genua.

Wintermute 101

„Within the research project Wintermute, an interactively usable system will be developed, that will enable administrators to control the data traffic even in complex and dynamic networks by close-meshed policies.“

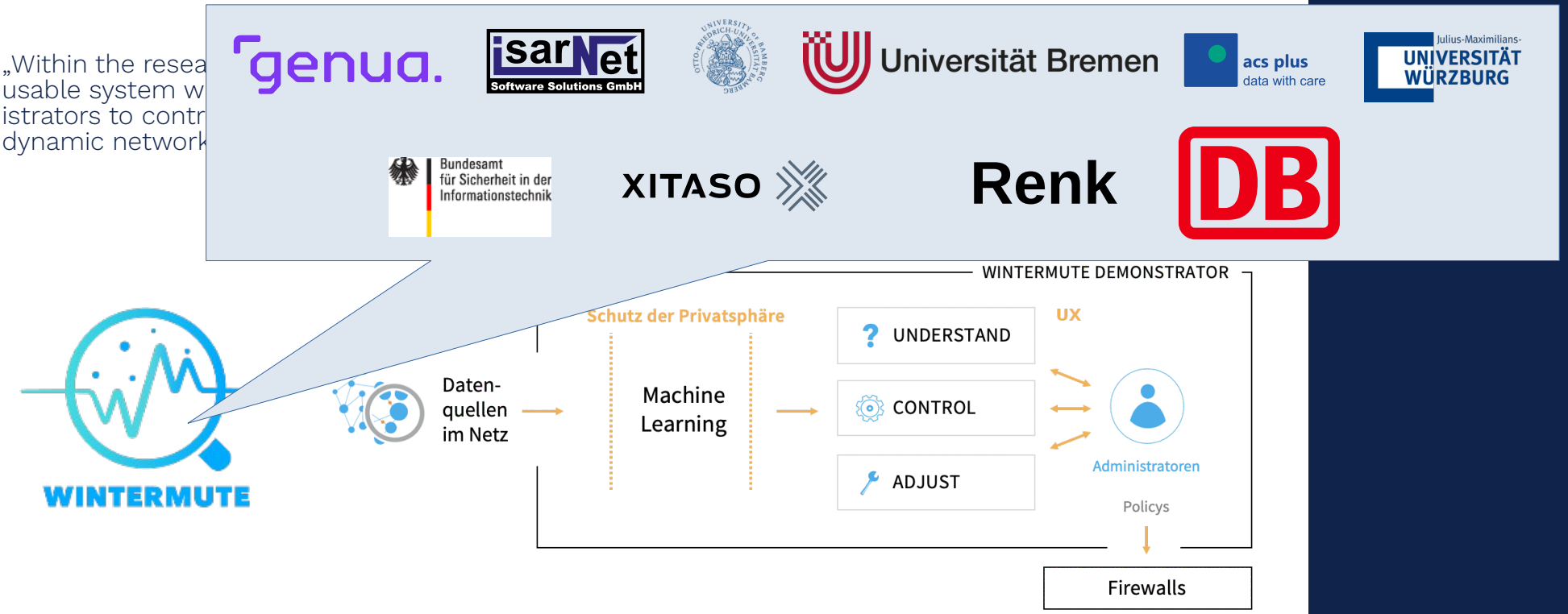
Bundesministerium für Bildung und Forschung

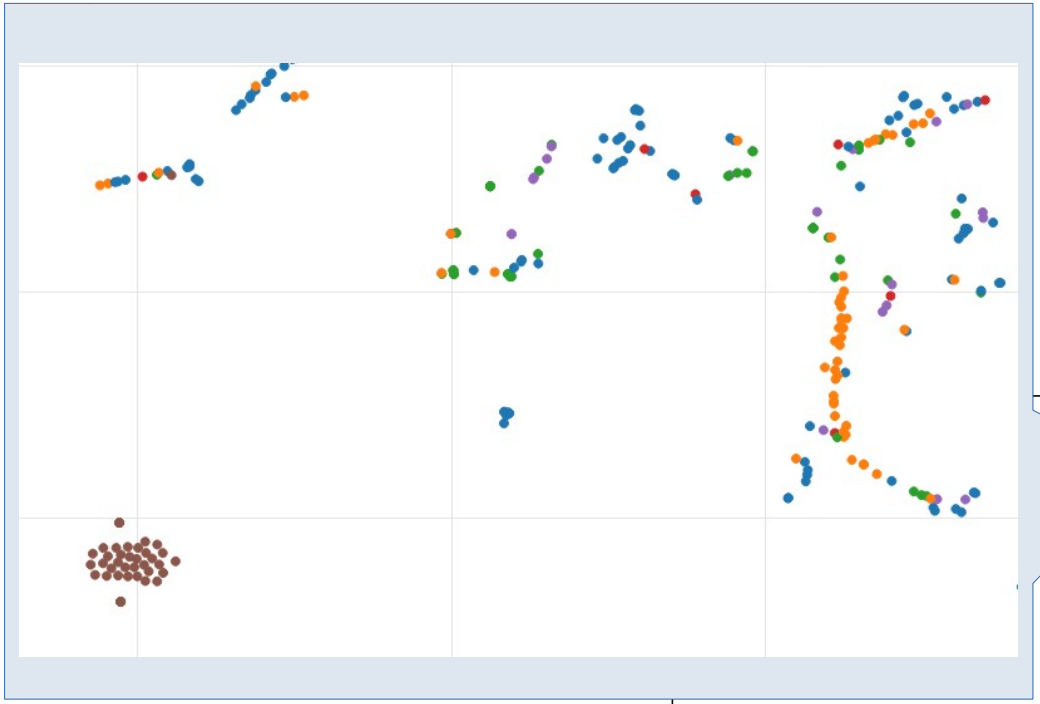
WINTERMUTE



Wintermute 101

„Within the resea
usable system w
istrators to contr
dynamic network





Bundesministerium
für Bildung
und Forschung

WINTERMUTE DEMONSTRATOR

UX

NDERSTAND

CONTROL

ADJUST

Administratoren

Policys

Firewalls

Bundesministerium für Bildung und Forschung

WINTERMUTE DEMONSTRATOR

UX

NDERSTAND

CONTROL

ADJUST

Administratoren

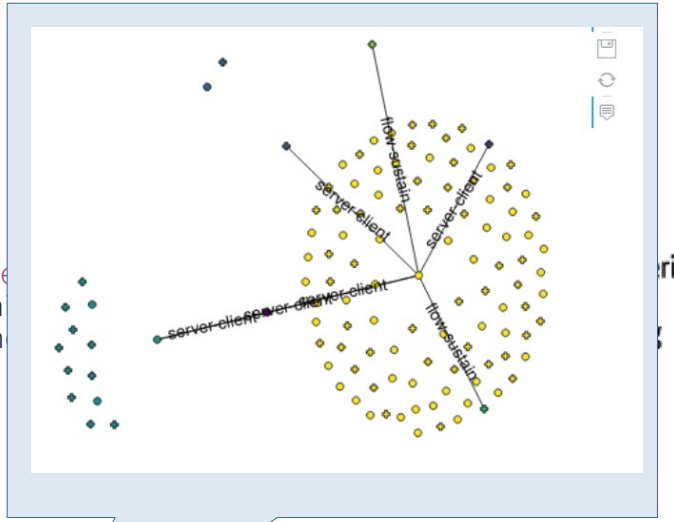
Policys

Firewalls

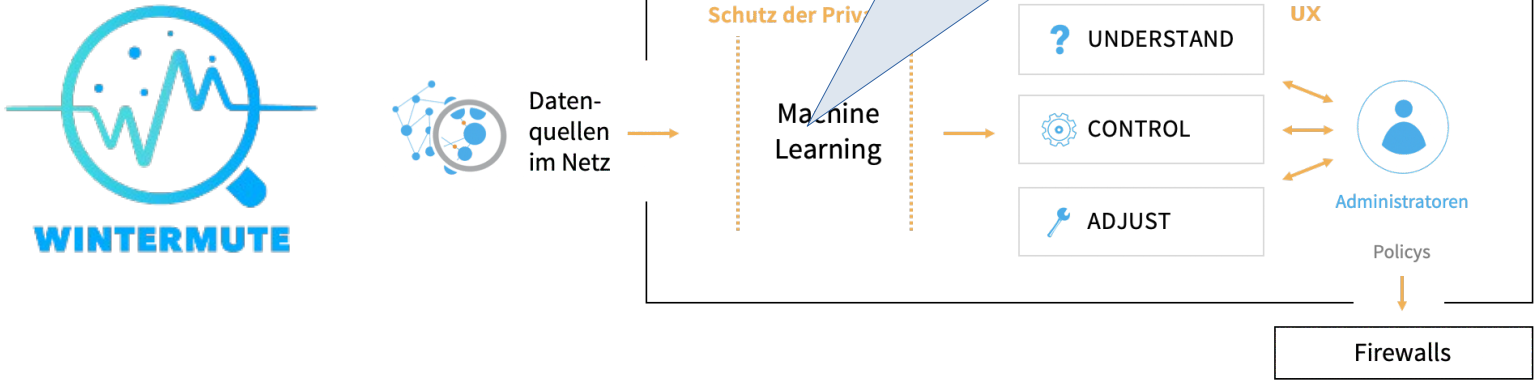
genua.

Wintermute 101

„Within the research project Wintermute, an interactive
usable system will be developed, that will enable adm
istrators to control the data traffic even in complex an
dynamic networks by close-meshed policies.“



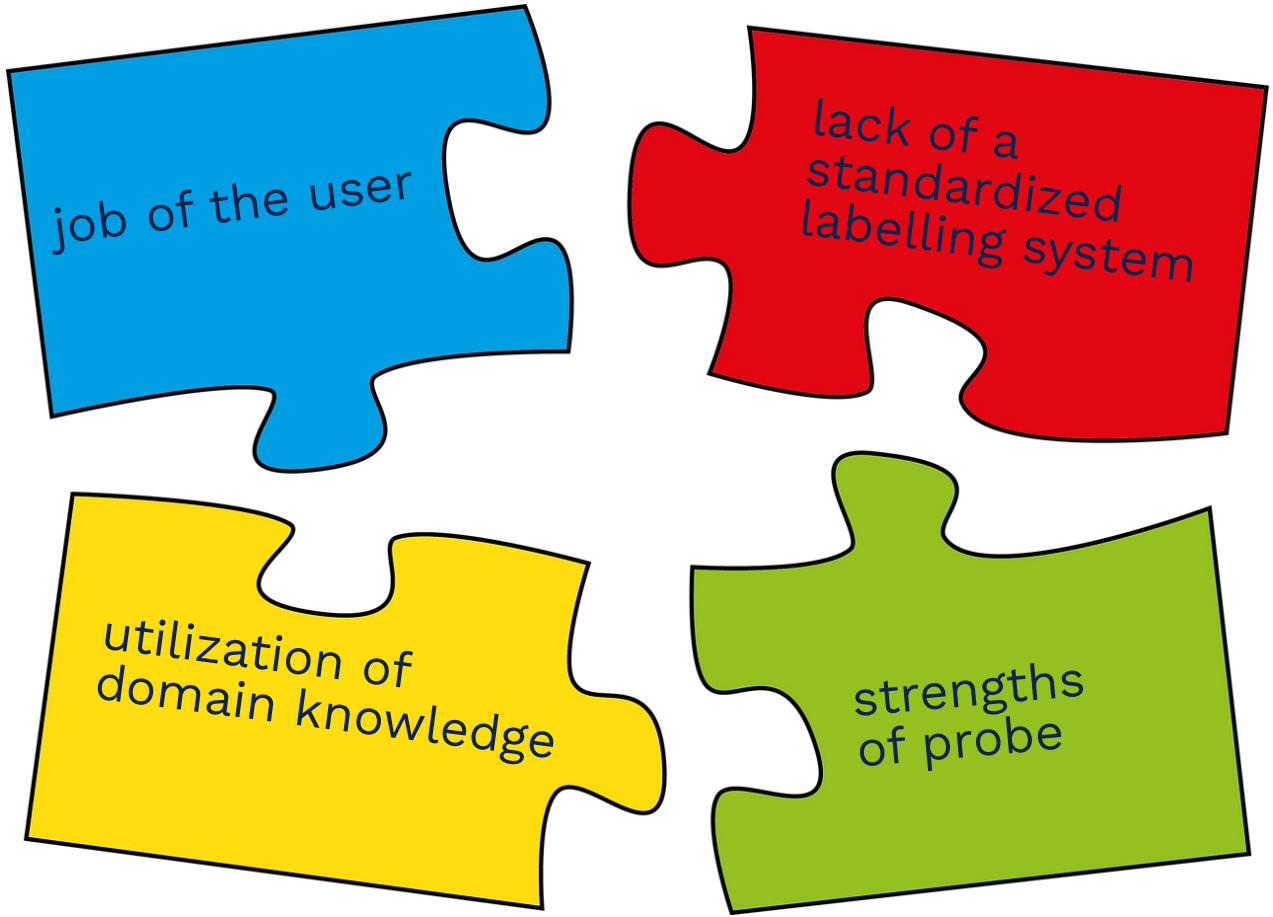
rium

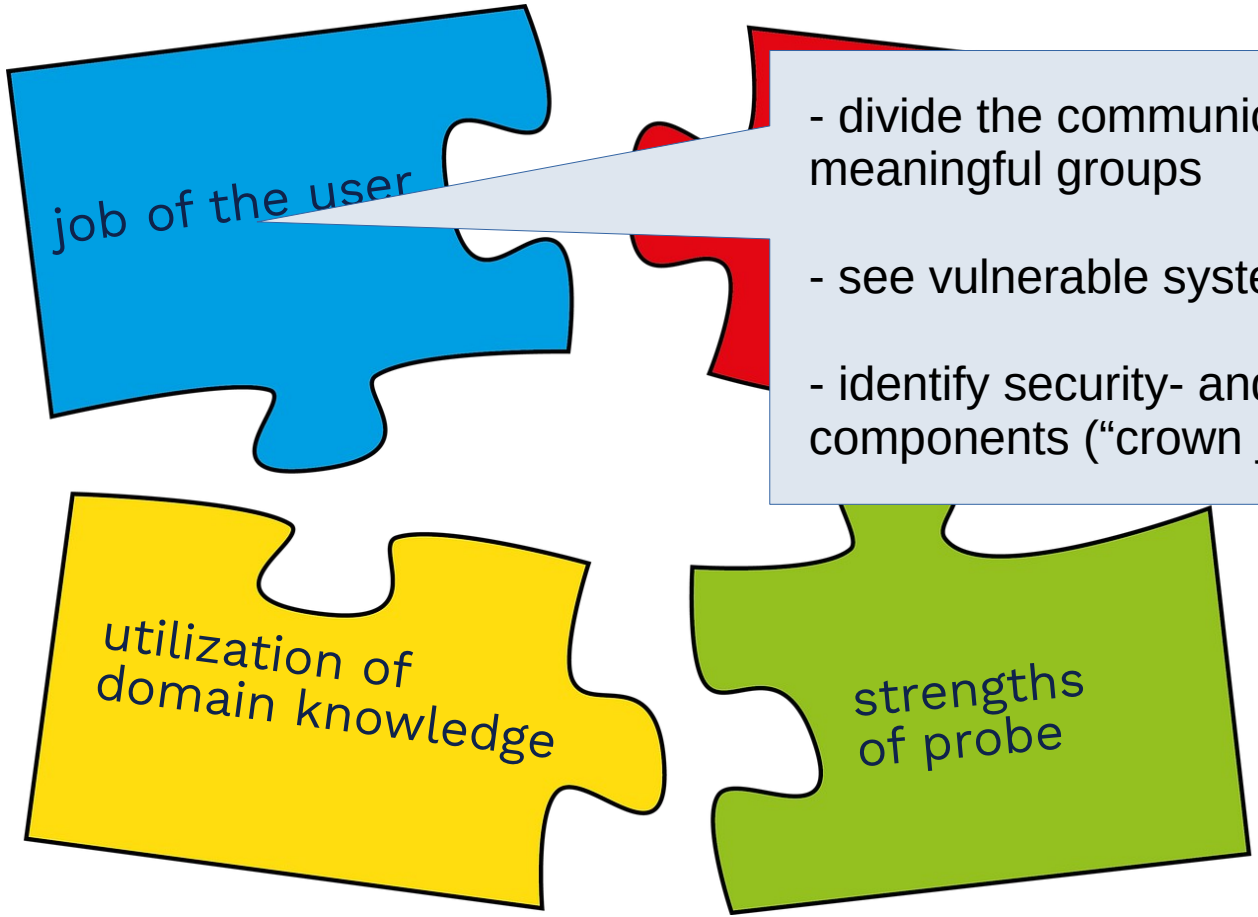


Four Noble Truths

genua.

genua.


job of the user
lack of a standardized labelling system
utilization of domain knowledge
strengths of probe

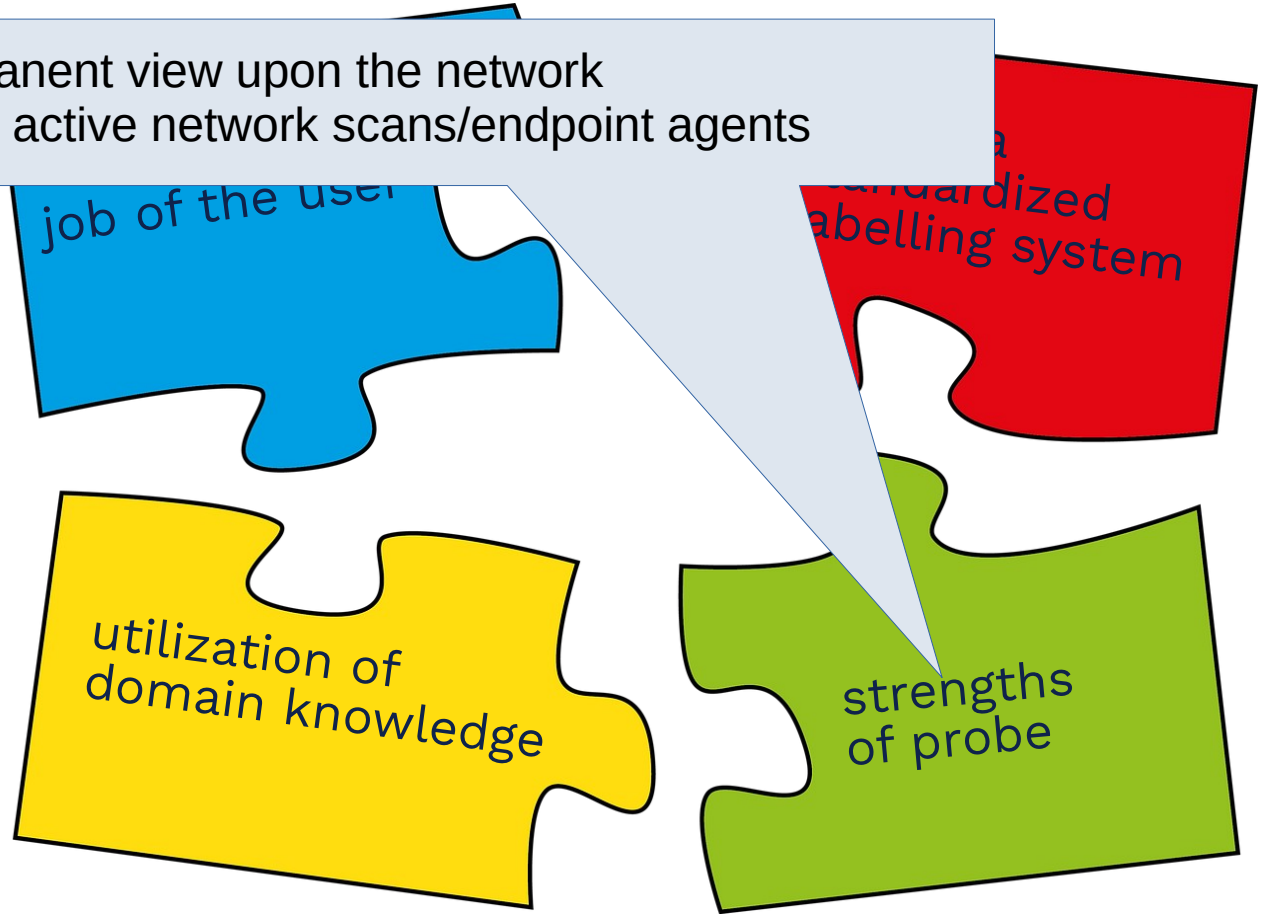


- divide the communicating devices into meaningful groups

- see vulnerable systems

- identify security- and business process-critical components (“crown jewels")

- permanent view upon the network
- avoid active network scans/endpoint agents



"**netflow**" : {

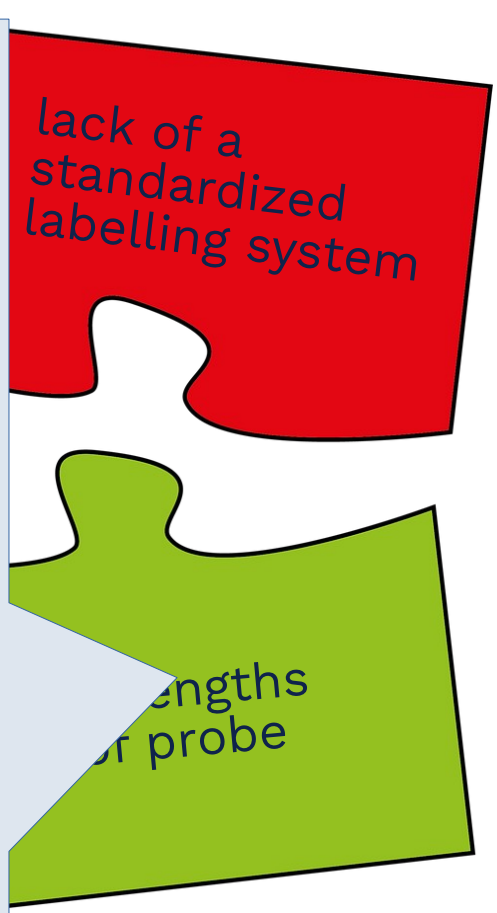
"firewall_event" : 2,
"flow_id" : 36028797034806996,
"flow_start_milliseconds" : "2020-XX-XXT23:59:53.976Z",
"flow_end_milliseconds" : "2020-XX-XXT23:59:53.992Z",

"source_mac_address" : "f4:f2:6d:XX:XX:XX",
"source_ipv4_address" : "10.10.1.X",
"source_transport_port" : 45230
"source_country" : "ZZ",
"source_asset_id" : "0005a4e7-558a-63ae-0016-f4f26d94ab2b",

"destination_mac_address" : "00:1a:8c:XX:XX:XX",
"destination_ipv4_address" : "212.X.X.X",
"destination_transport_port" : 80,
"destination_country" : "DE",
"destination_asset_id" : "",

"application_name" : "ip.tcp.http",
"domain" : "www.example.com",

"octet_total_count" : 90,
"packet_total_count" : 1,
"reverse_octet_total_count" : 90,
"reverse_packet_total_count" : 1 }



Reasons for labelling devices

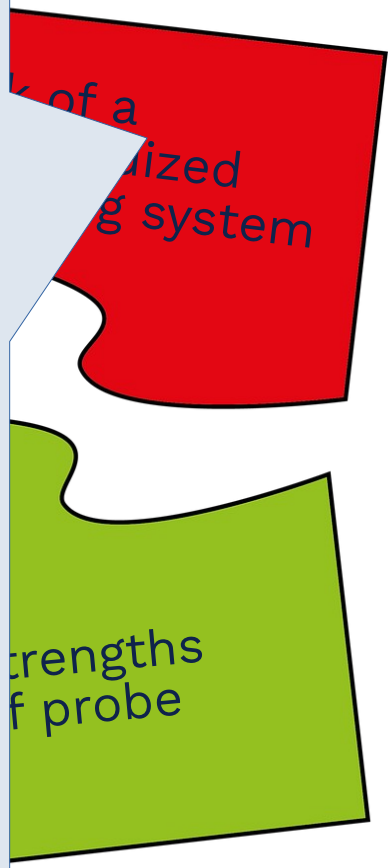
1. Inventory

2. Filtering for reporting

3. Usage in firewall rule
   - Precondition for flow action
   - Policy Override

   Example – `mqttallow:`
   device is allowed to access internet although it is using mqtt
   → *overrides a No-mqtt-Policy*

4. localization
   - Building/Floor/geo localisation
   - Subnet
   - Working group

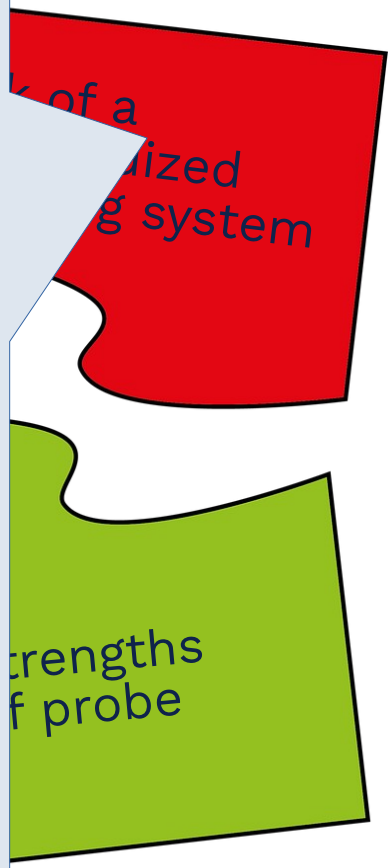


Grouping of Systems according to IT-Basic-Protection-Taxonomy

…

APP.3 Netbased Services
- APP.3.1 Web Applications
- APP.3.2 Web Server
- APP.3.3 File Server
- APP.3.4 Samba
- APP.3.6 DNS Server

…



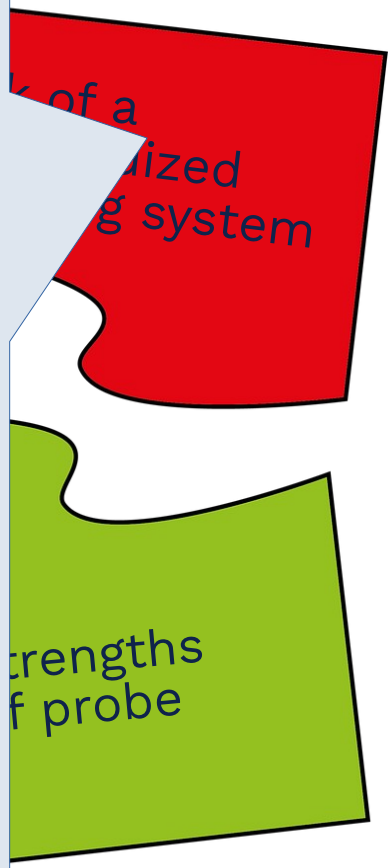
Grouping of Systems according to IT-Basic-Protection-Taxonomy

…

APP.3 Netbased Services
- APP.3.1 Web Applications
- APP.3.2 Web Server
- APP.3.3 File Server
- APP.3.4 Samba
- APP.3.6 DNS Server

…

ORP.3 Awareness Raising and Training regarding Information Security



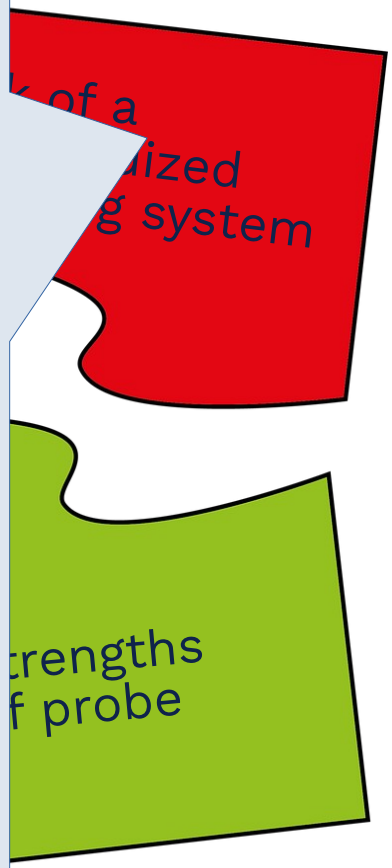
Grouping of Systems according to IT-Basic-Protection-Taxonomy

…

APP.3 Netbased Services
- APP.3.1 Web Applications
- APP.3.2 Web Server
- APP.3.3 File Server
- APP.3.4 Samba
- APP.3.6 DNS Server

…

~~ORP.3 Awareness Raising and Training regarding Information Security~~



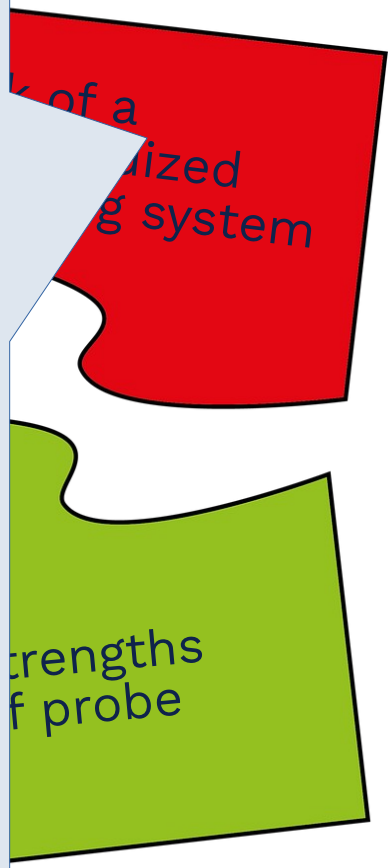
Grouping of Systems according to IT-Basic-Protection-Taxonomy

- Overview of type and properties of the devices communicating within the network

- Information for compliance / certification

- micro segmentation of the network

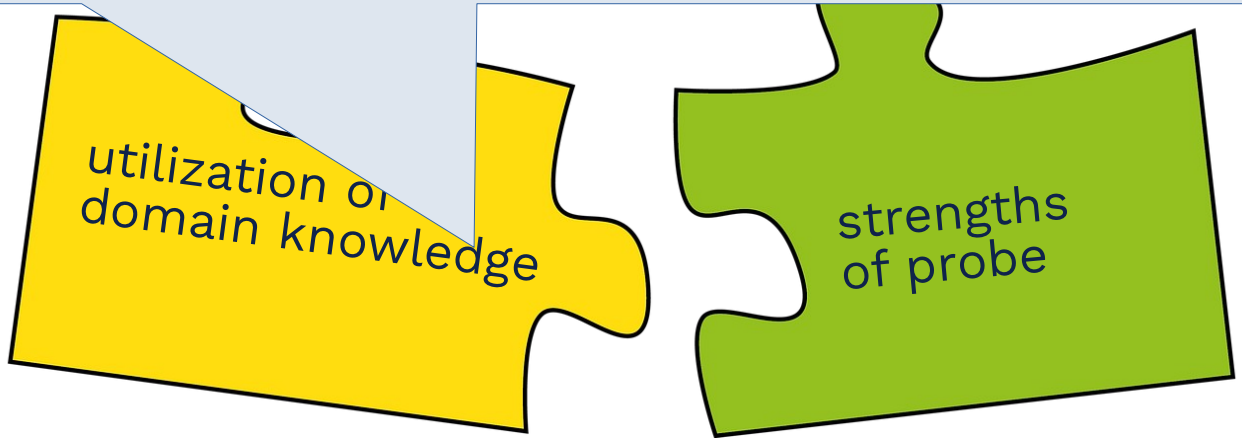
→ enforcing security policies for the communication utilizing user-defined tags



Usually: „abstract (numeric) features derived from network data“

intention of the features is described – Example *Jakalan*

- *number of communication partners: popularity of the IP node, differentiate one-to-one-/one-to-several/one-to-many-communication*
- *mean packet size: signaling traffic vs data exchangea*

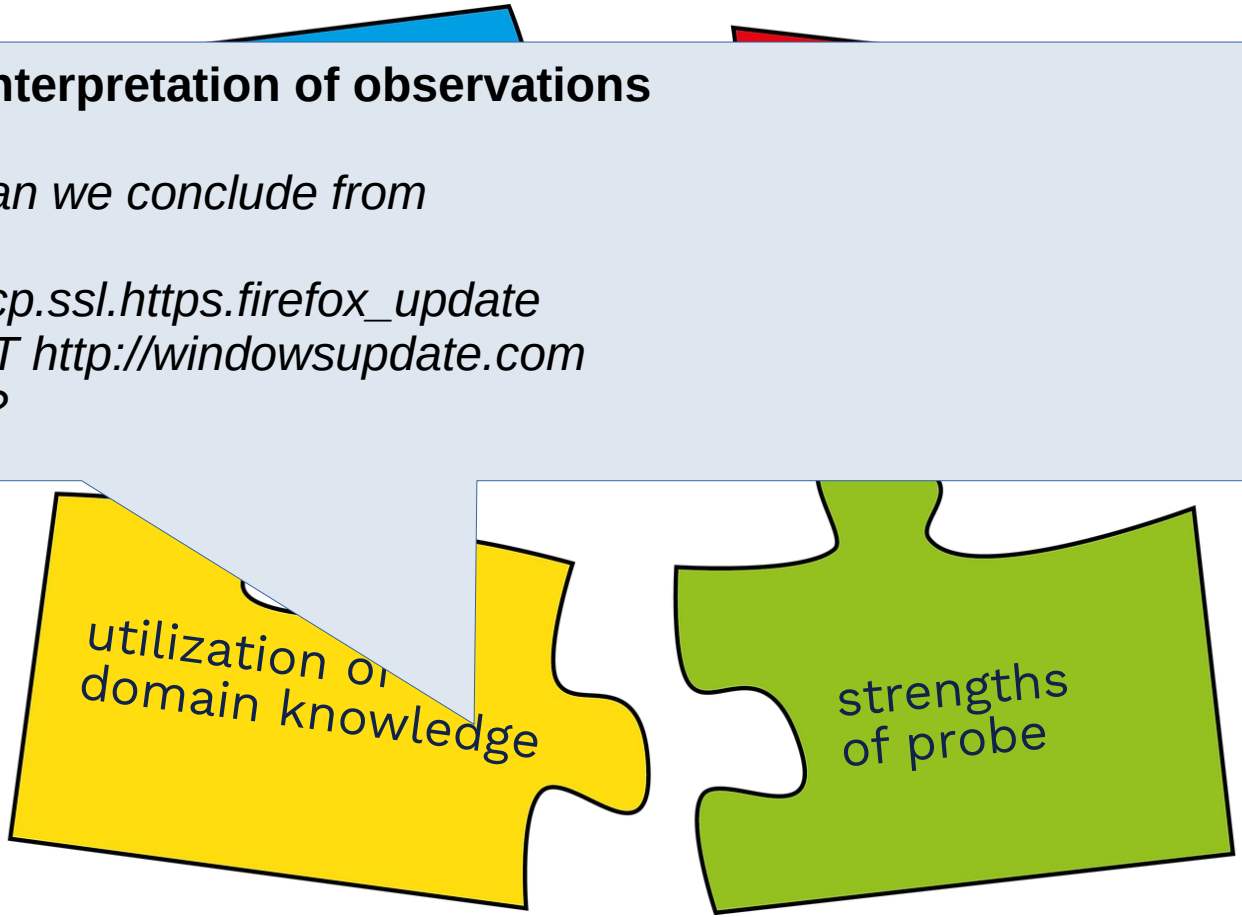


genua.

Here: Interpretation of observations

What can we conclude from

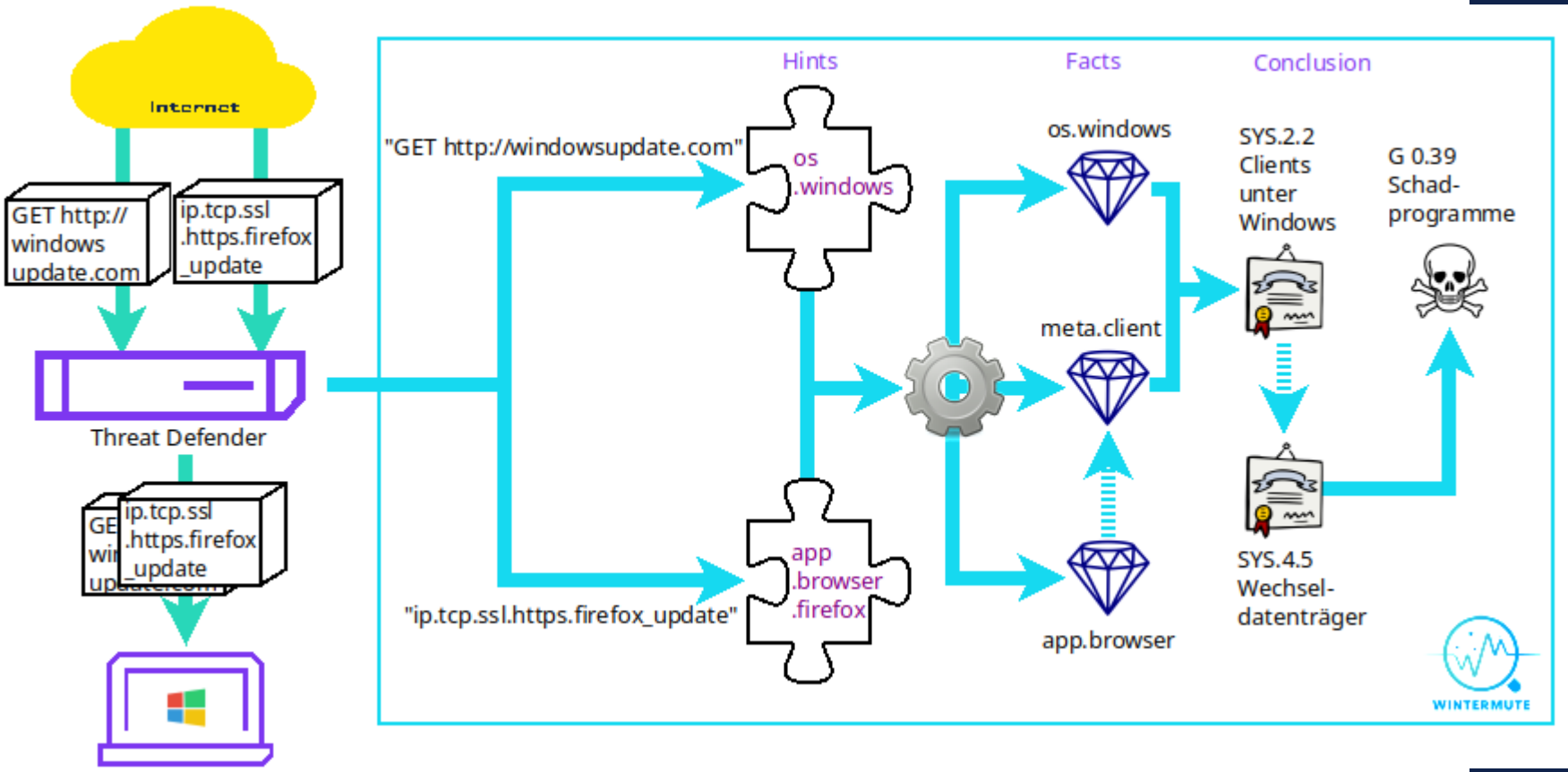
- *ip.tcp.ssl.https.firefox_update*
- *GET http://windowsupdate.com*
- *… ?*



Current Approach

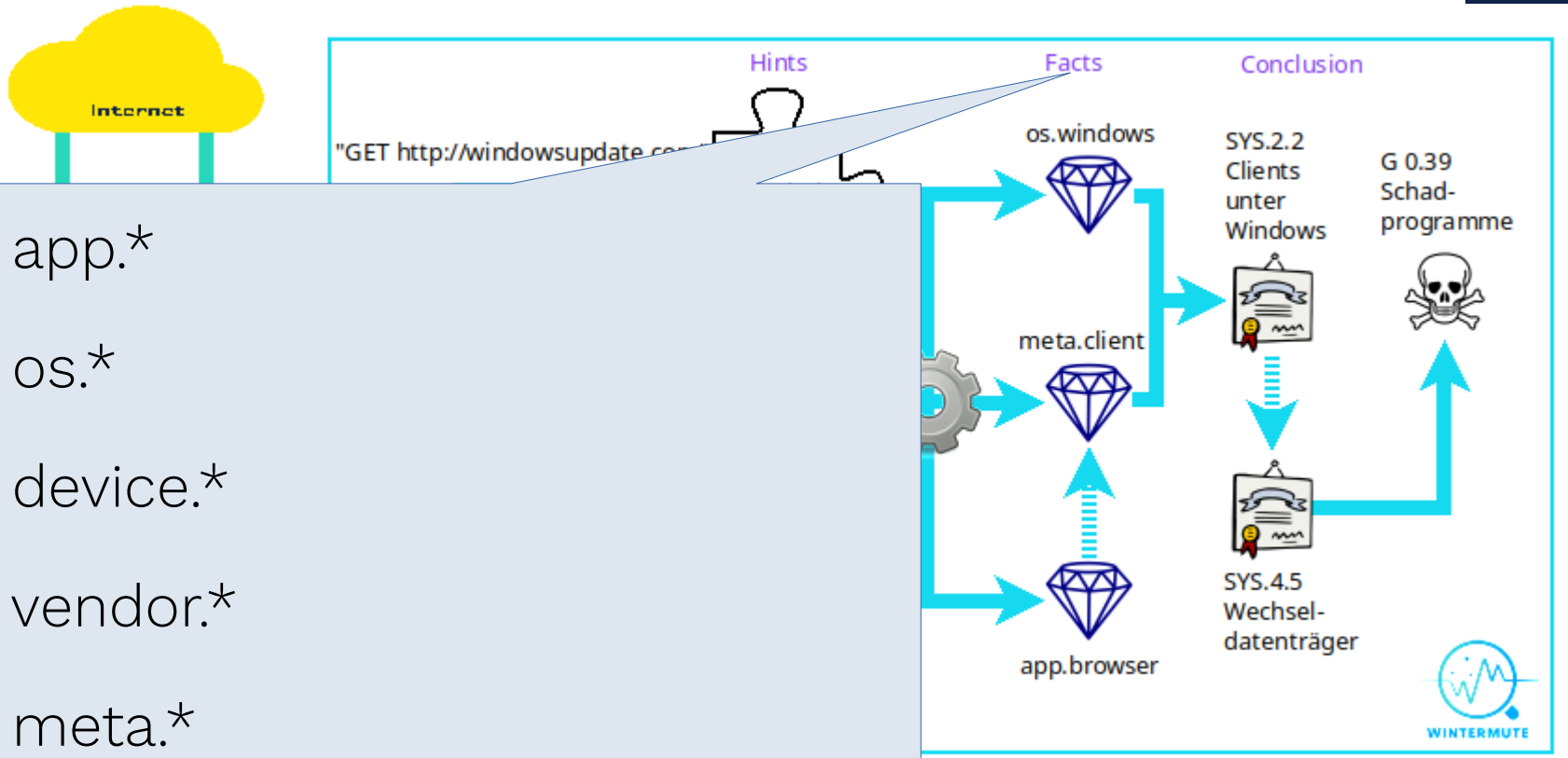
genua.

Passive Asset Discovery



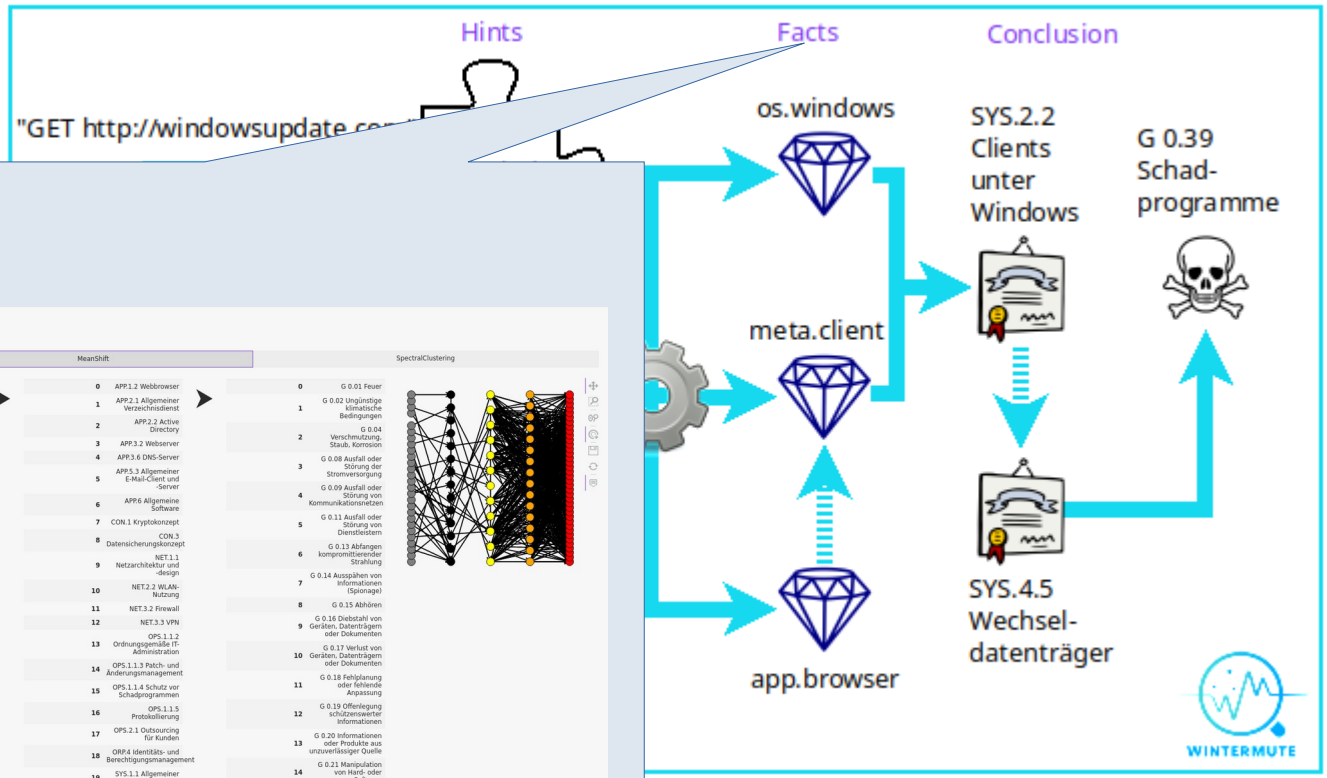
genua.

Passive Asset Discovery



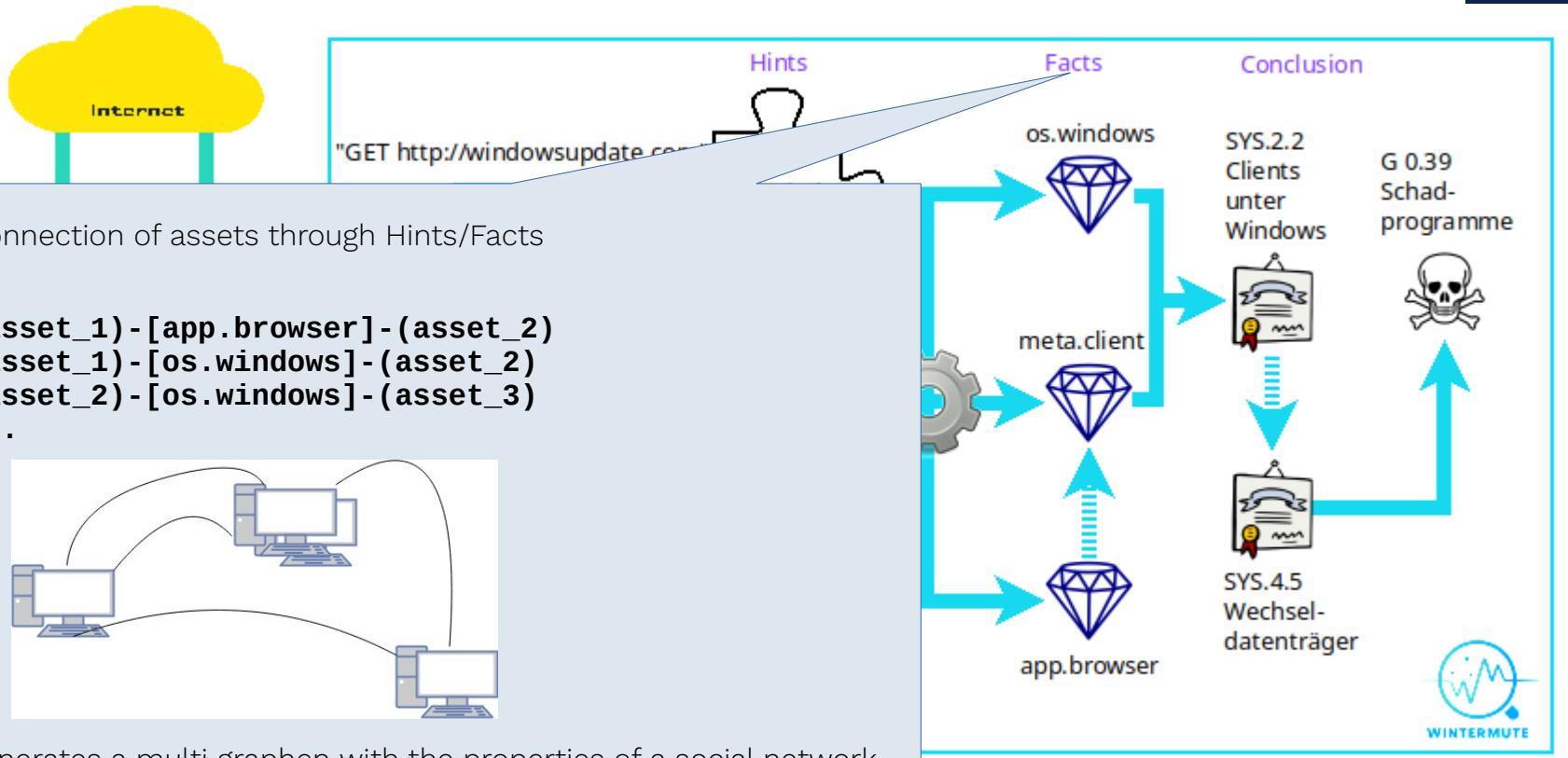
- app.*
- os.*
- device.*
- vendor.*
- meta.*

Passive Asset Discovery



Clustering on Facts

Passive Asset Discovery



Connection of assets through Hints/Facts

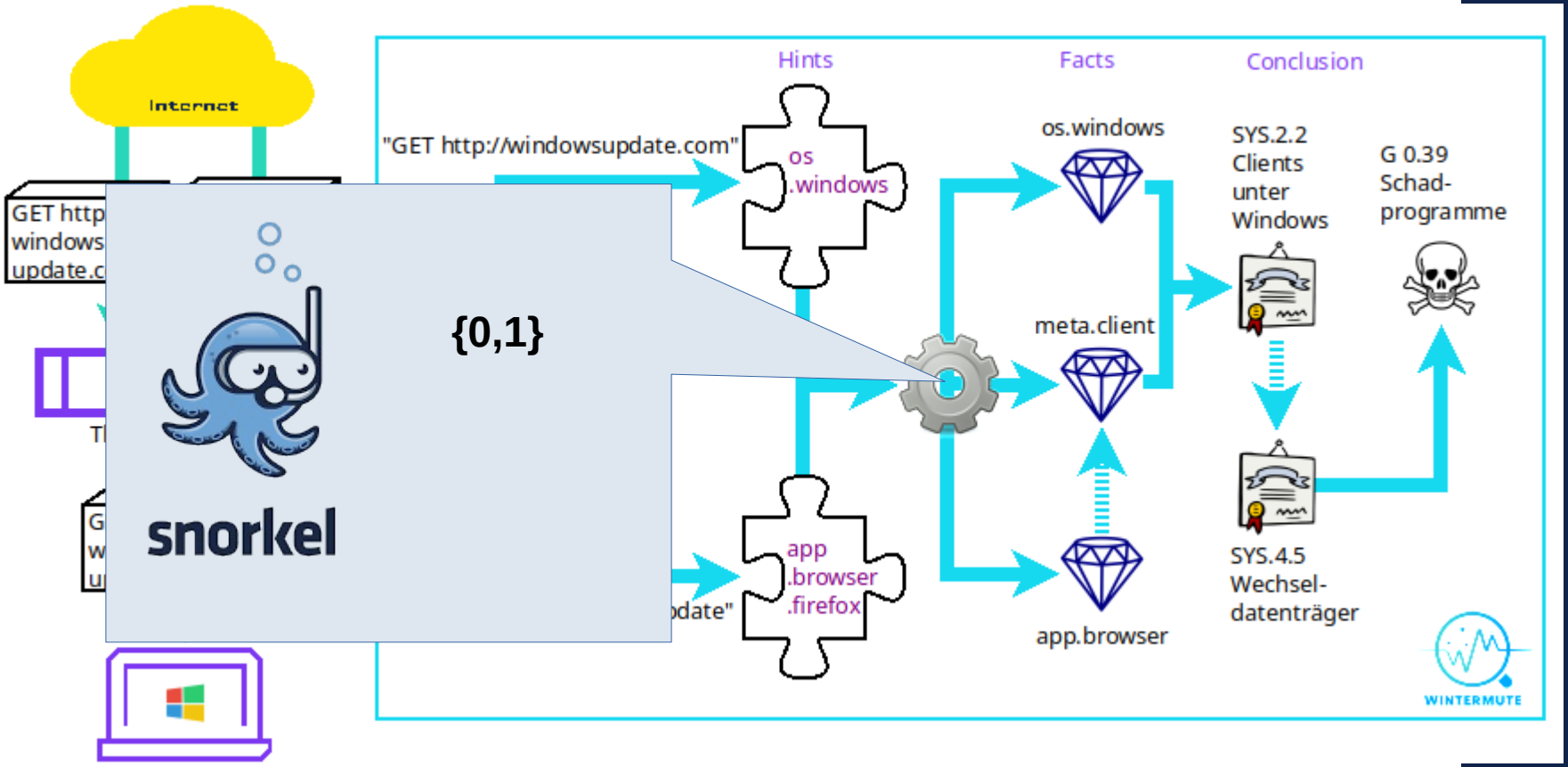
```
(asset_1)-[app.browser]-(asset_2)
(asset_1)-[os.windows]-(asset_2)
(asset_2)-[os.windows]-(asset_3)
...
```


generates a multi graphen with the properties of a social network.

→ classical methods of graph analysis (e.g. computation of cliques)

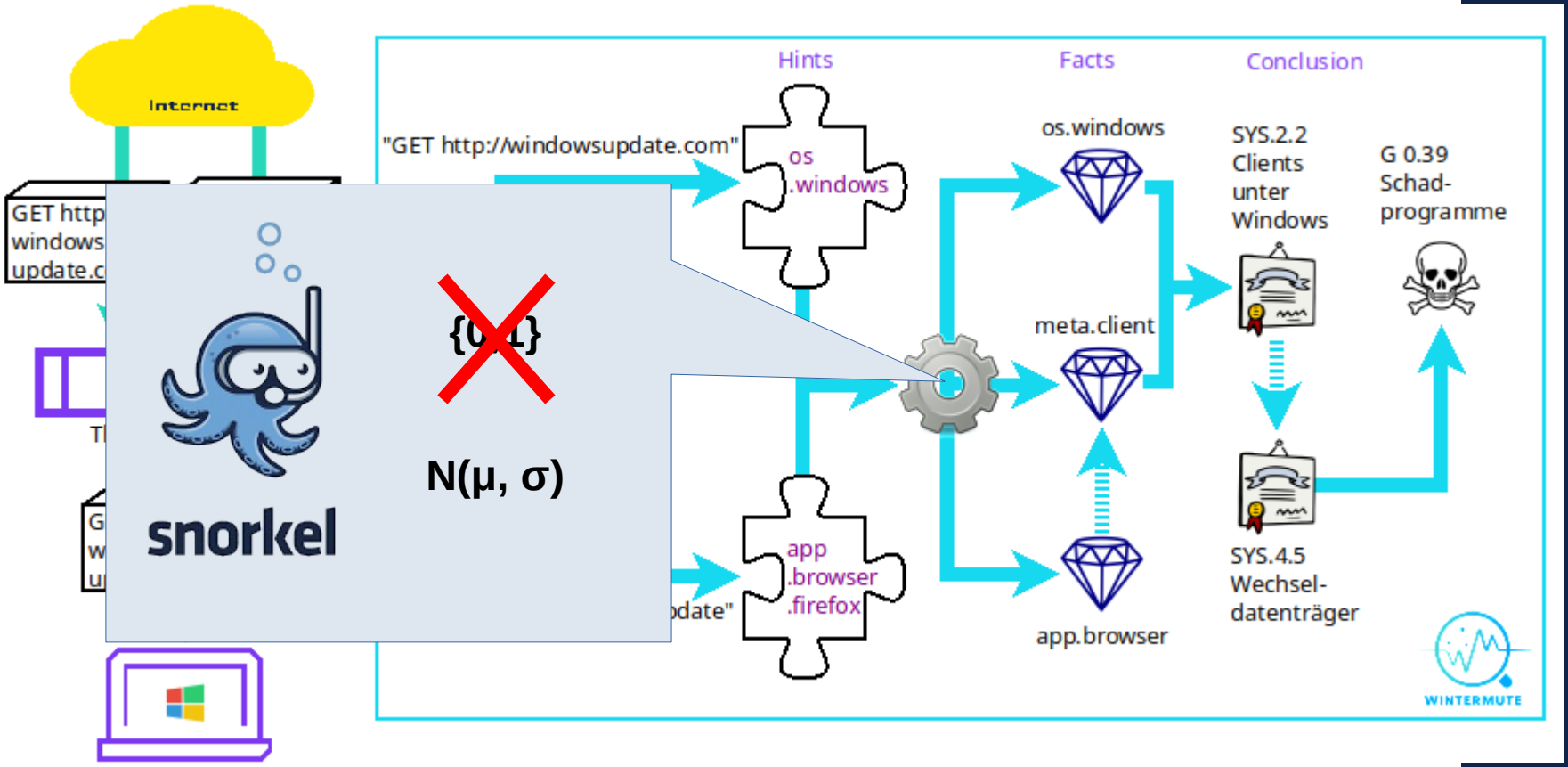
genua.

Passive Asset Discovery



genua.

Passive Asset Discovery



Yes, we sacrificed privacy for explainability.

Q & A