nquiringminds
Dr Nicholas Allott
nick@nqminds.com

manySECURED

# SECURE IOT GATEWAYS

Highlighting the industry challenges, and identifying the collaborative innovation needed to address them

**Device security good**

**Gateway security better**

complimentary/more practical/future proof


Everything to follow is framed by ManySecured tech stack (open sourced/ emerging standard)

The requirements however standalone and represent good/next practice



## IN THE CROSSHAIRS OF CYBER CRIMINALS AND TARGETED ATTACK GROUPS.

While worms and bots continued to account for the vast majority of Internet of Things (IoT) attacks, in 2018 we saw a new breed of threat emerge as targeted attack actors displayed an interest in IoT as an infection vector.

The overall volume of IoT attacks remained high in 2018 and consistent (-0.2 percent) compared to 2017. Routers and connected cameras were the most infected devices and accounted for 75 and 15 percent of the attacks respectively. It's unsurprising that routers were the most targeted devices given their accessibility from the internet. They're also attractive as they provide an effective jumping-off point for attackers.

The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was the third most common IoT threat in 2018. Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched. The worm also expanded its target scope by going after unpatched Linux servers. Another noticeable trend was the increase in attacks against industrial control systems (ICS). The Thrip group went after satellites, and Triton attacked industrial safety systems, leaving them vulnerable to sabotage or extortion attacks. Any computing device is a potential target.

The emergence of VPNFilter in 2018 represented an evolution of IoT threats. VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove. With an array of potent payloads at its disposal, such as man in the middle (MitM) attacks, data exfiltration, credential theft, and interception of SCADA communications, VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining. It also includes a destructive capability which can "brick," or wipe a device at the attackers' command, should they wish to destroy evidence. VPNFilter is the work of a skilled and well-resourced threat actor and demonstrates how IoT devices are now facing attack from many fronts.

https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

# "ROUTERS ACCOUNT FOR 75% OF INFECTED IOT DEVICES"

manySECURED

# Router Focus

- Attack target
- Low cost scalable
- Geographically remote attack
- Line of defence
- Attack vector
- Visibility of activity
- Ability to impact/contain

# Challenges

What's so difficult

# CHALLENGE 1

Securing intranet for browsers

nquiringminds

## The issue

You cant connect to http://192.168.0.1 securely (or https)

## Which is problematic

Because almost everyone want to configure your IOT device (and your router) that way

## The alternative

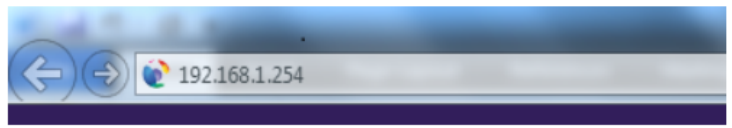
Is a new application for every device which is bad for so many different reasons.

# Learn about the BT Hub Manager

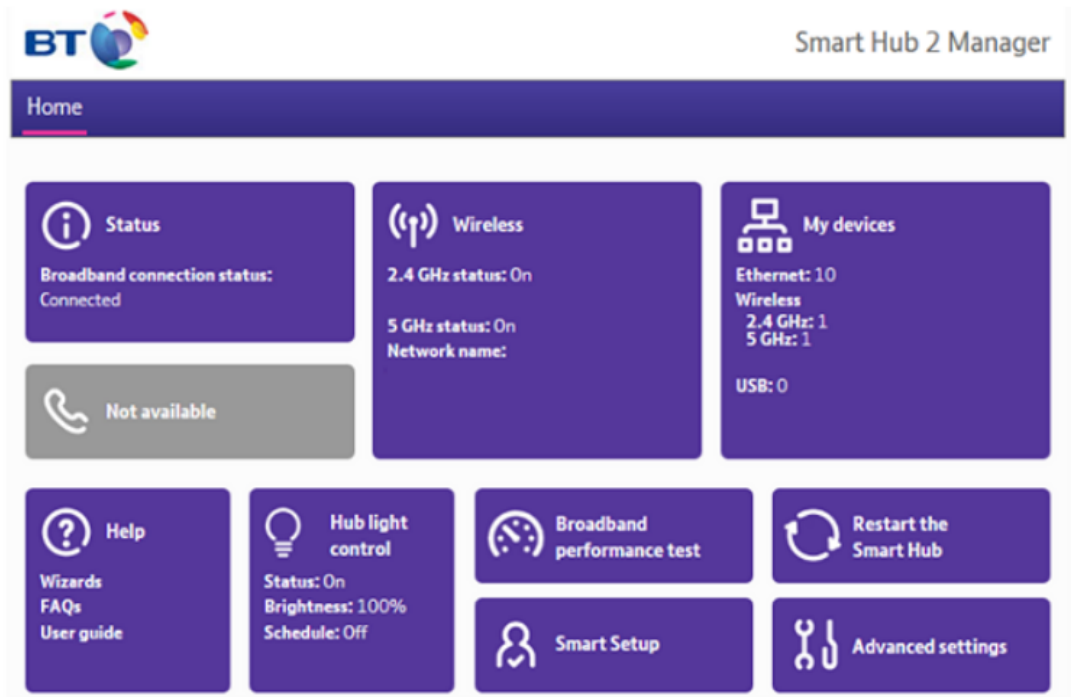
Alongside the launch of our new BT Smart Hub 2, we've redesigned the Hub Manager. It's now even easier to manage the Hub's settings and to get the best wi-fi set-up. It's also easy to see the Hub Manager across all devices.

## How to open the Hub Manager

1. Open a new web browser
2. Type **192.168.1.254** into the address bar




3. This will open the Hub Manager



# CHALLENGE 2

## Evaluating trustworthiness of a device

nquiringminds

### What are you

What's at the end of this IP address ?

### Are you behaving

Is the device doing what it should do

### What can I do about it

Containment and intervention

# CHALLENGE N++

Everything else

nquiringminds

## Heterogenous networks

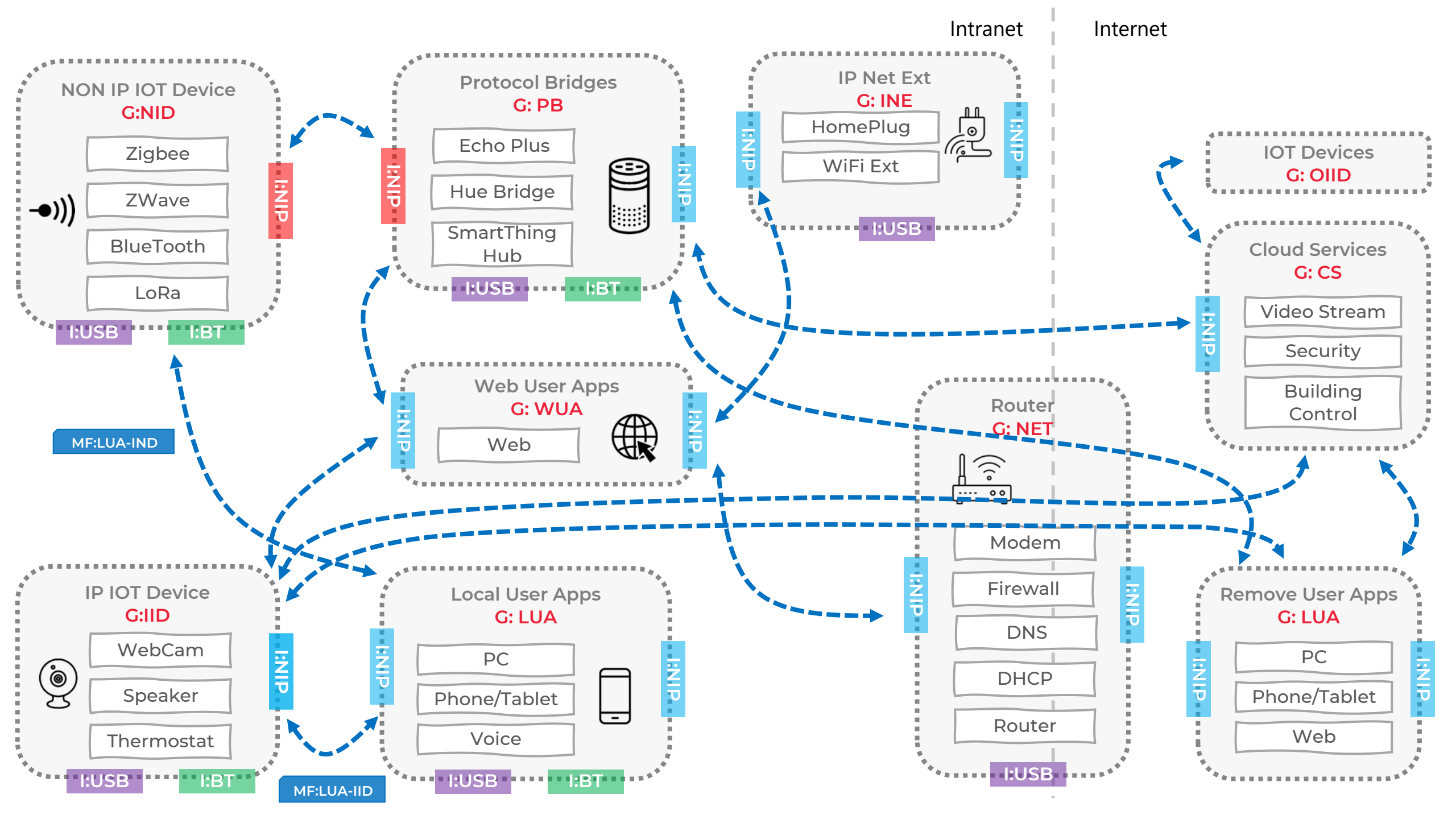
IOT networks are evolving and diverse

## No single source of truth

Ability to reason under uncertainty

## Devices live longer then manufactures

Legacy support and operational issues


Intranet
Internet
NON IP IOT Device
G:NID
Zigbee
ZWave
BlueTooth
LoRa
I:NIP
I:USB
I:BT
Protocol Bridges
G: PB
Echo Plus
Hue Bridge
SmartThing Hub
I:NIP
I:USB
I:BT
IP Net Ext
G: INE
HomePlug
WiFi Ext
I:NIP
I:USB
IOT Devices
G: OIID
Cloud Services
G: CS
Video Stream
Security
Building Control
I:NIP
Web User Apps
G: WUA
Web
I:NIP
MF:LUA-IND
Router
G: NET
Modem
Firewall
DNS
DHCP
Router
I:NIP
I:USB
IP IOT Device
G:IID
WebCam
Speaker
Thermostat
I:NIP
I:USB
I:BT
Local User Apps
G: LUA
PC
Phone/Tablet
Voice
I:NIP
I:USB
I:BT
MF:LUA-IID
Remove User Apps
G: LUA
PC
Phone/Tablet
Web
I:NIP

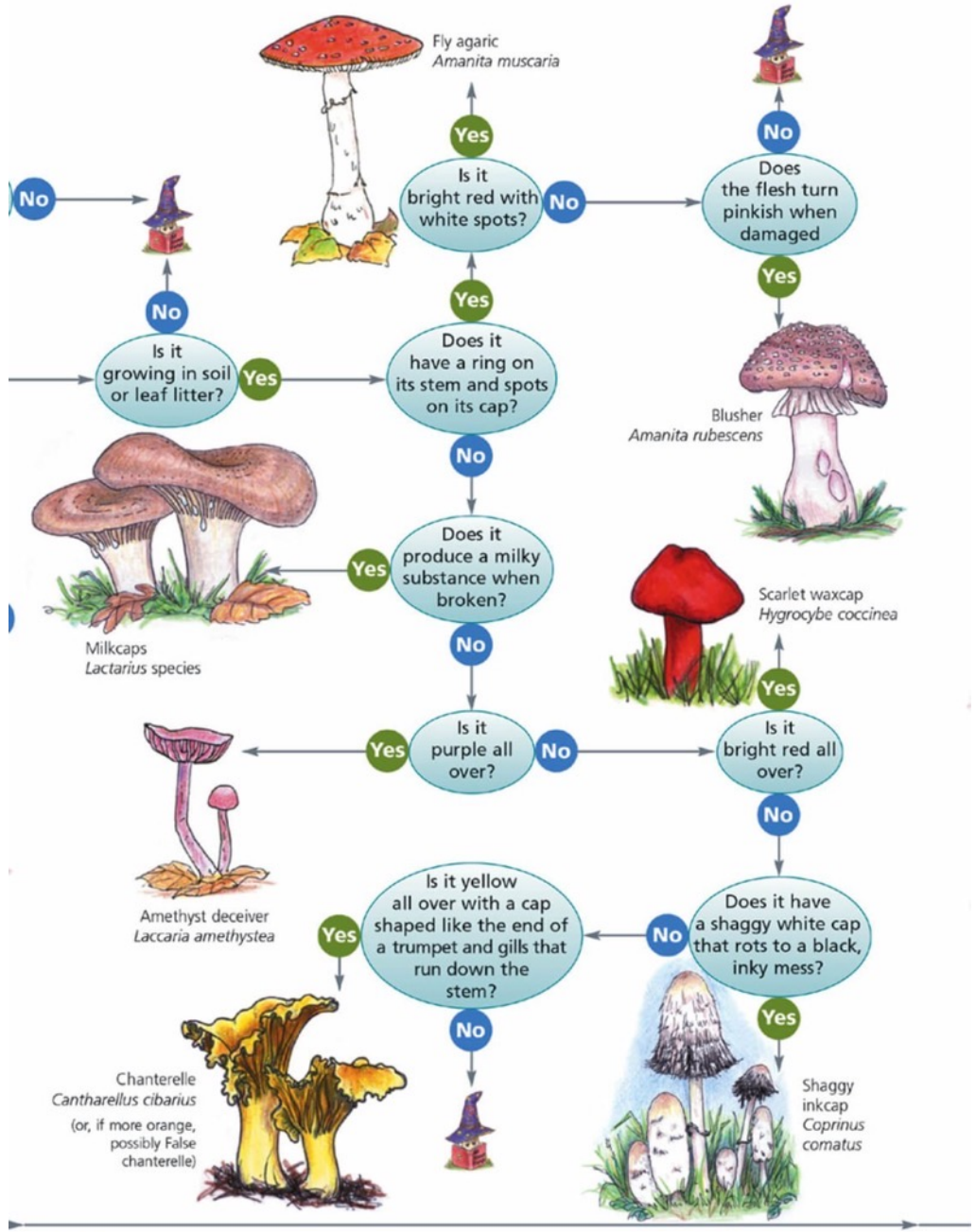
# A Theory of types

## Creating the glue

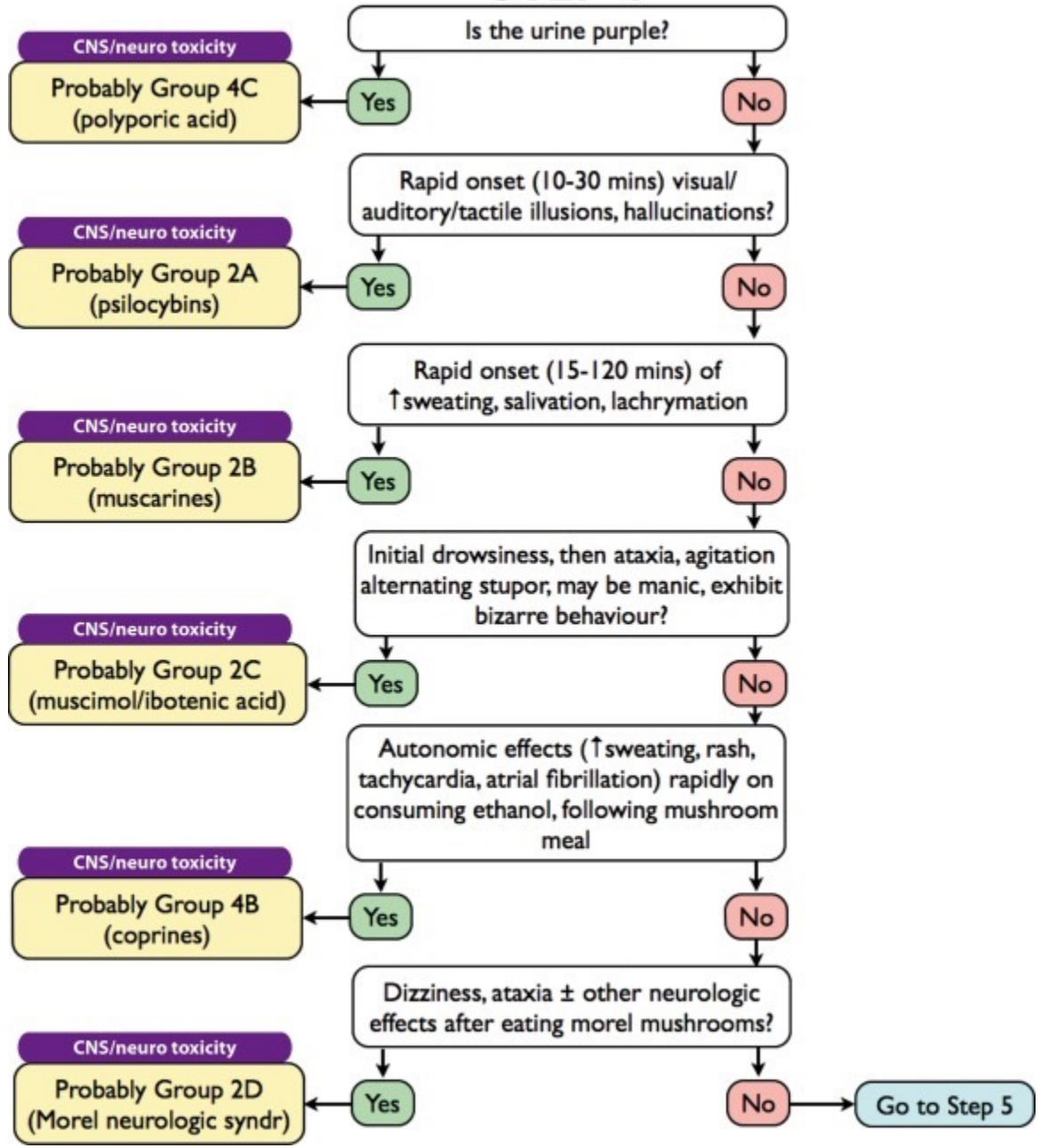
(database foreign key)


How to survive in the woods?


Comparisons Between Similar Species
TRICHOLOMA ALLIES
Porcelain Mushroom
Rooting Shank
Fairy Ring Champignon
St George's Mushroom
Plums and Custard
Broad Gill
Changeable Melanoleuca
Wood Blewit
Field Blewit
Heath Naval
Spruceone Cap
The Goblet
Giant Funnel
Bitter Oysterling
Velvet Shank
SHIELDS
Deer Shield
Goldleaf Shield
Velvet Shield
Veined Shield
ROUNDHEADS
Dung Roundhead
Vendigris Toadstool
PSILOCYBE
Magic Mushroom
MUSHROOMS
Yellow-staining Mushroom
Field Mushroom
The Prince
Wood Mushroom
Horse Mushroom
Macro Mushroom
Scaly Wood Mushroom
Pavement Mushroom
OYSTERS
Branched Oyster
Oyster Mushroom
INKCAPS
Shaggy Inkcap
Common Inkcap
Fairy Inkcap
Glistening Inkcap
CHANTERELLES
Chanterelle
Trumpet Chanterelle
Horn of Plenty
Sinuous Chanterelle
FALSE CHANTERELLE
False Chanterelle
BRACKET FUNGI
Hen of the Woods
Chicken of the Woods
Beefsteak Fungus
Dryad's Saddle
Many-zoned Polypore
Birch Polypore
Lumpy Bracket
Blushing Bracket
Hoof Fungus
CLUBS & CORALS
Antler Fungus
White Spindles
Yellow Club
Field Club
Giant Club
Wrinkled Coral
Grey Coral Fungus
White Coral
CORALS
Upright Coral
Clustered Coral
PUFFBALLS
Grey Puffball
Brown Puffball
Giant Puffball
Stalked Puffball
Mosaic Puffball
Common Puffball
Stump Puffball
Meadow Puffball
NOTE Not to scale


Fly agaric
Amanita muscaria
Yes
Is it bright red with white spots?
No
Does the flesh turn pinkish when damaged
No
Yes
No
Is it growing in soil or leaf litter?
Yes
Does it have a ring on its stem and spots on its cap?
Yes
No
Blusher
Amanita rubescens
Milkcaps
Lactarius species
Yes
Does it produce a milky substance when broken?
No
Scarlet waxcap
Hygrocybe coccinea
Yes
Yes
Is it purple all over?
No
Is it bright red all over?
No
Amethyst deceiver
Laccaria amethystea
Yes
Is it yellow all over with a cap shaped like the end of a trumpet and gills that run down the stem?
No
Does it have a shaggy white cap that rots to a black, inky mess?
Yes
Chanterelle
Cantharellus cibarius
(or, if more orange, possibly False chanterelle)
Shaggy inkcap
Coprinus comatus

# STEP 4


Is the urine purple?
Yes
CNS/neuro toxicity
Probably Group 4C (polyporic acid)
No
Rapid onset (10-30 mins) visual/ auditory/tactile illusions, hallucinations?
Yes
CNS/neuro toxicity
Probably Group 2A (psilocybins)
No
Rapid onset (15-120 mins) of ↑sweating, salivation, lachrymation
Yes
CNS/neuro toxicity
Probably Group 2B (muscarines)
No
Initial drowsiness, then ataxia, agitation alternating stupor, may be manic, exhibit bizarre behaviour?
Yes
CNS/neuro toxicity
Probably Group 2C (muscimol/ibotenic acid)
No
Autonomic effects (↑sweating, rash, tachycardia, atrial fibrillation) rapidly on consuming ethanol, following mushroom meal
Yes
CNS/neuro toxicity
Probably Group 4B (coprines)
No
Dizziness, ataxia ± other neurologic effects after eating morel mushrooms?
Yes
CNS/neuro toxicity
Probably Group 2D (Morel neurologic syndr)
No
Go to Step 5

## Device instance

Physical
Observable evets
Ephemeral

## Device type

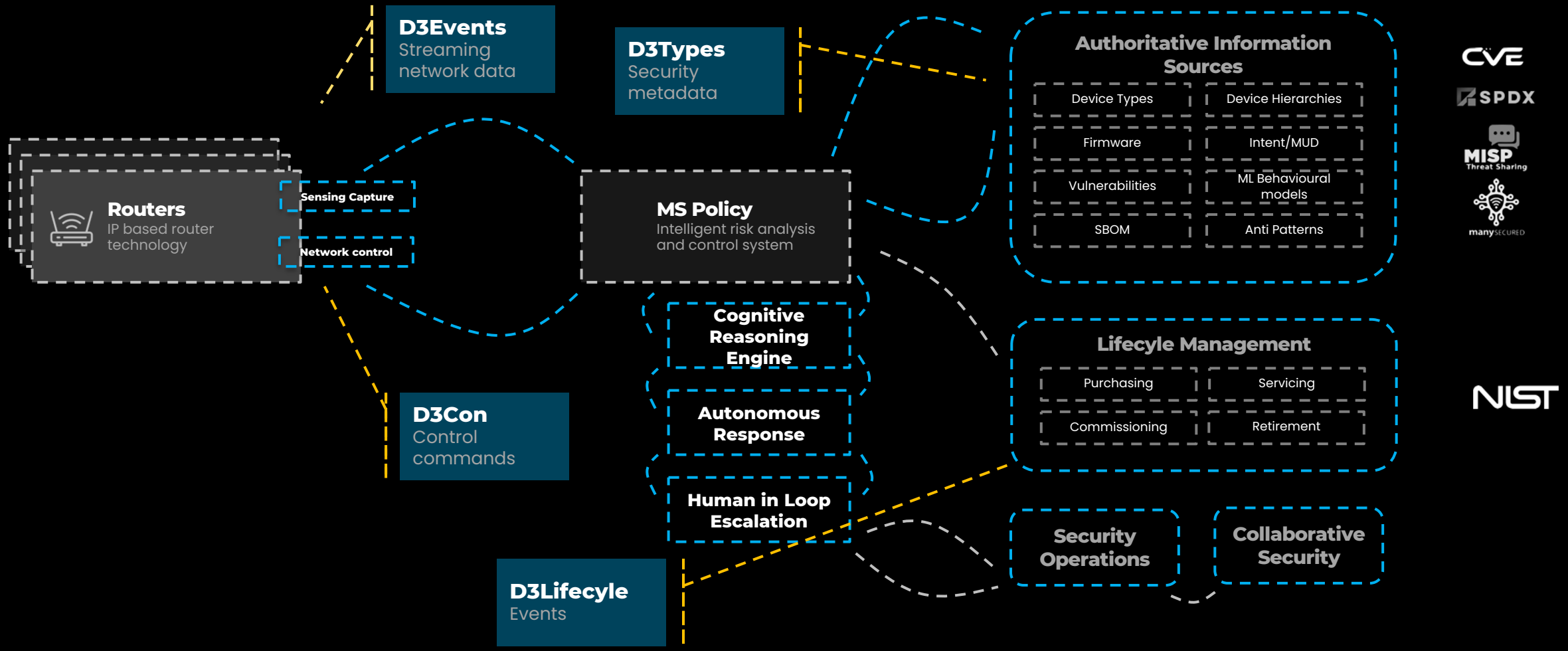
Conceptual
Statistical descriptors
Perpetual

# ManySecured Architecture

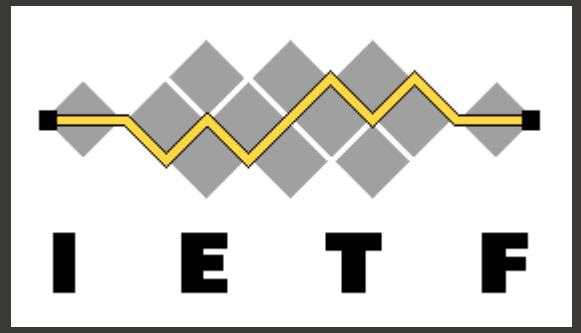
A candidate blueprint

# HOW IT WORKS

## Operational Deployment




# What's already out there ...




manySECURED

# Manufacturer Usage Description

## What is it

Method of describing different device types and there expected “least privilege  behaviour.
Method of security publishing, discovering and binding these descriptions to induvial devices.
Can be used to enforce constraints on a router

## Considerations

- Insecure when using DHCP (can be spoofed)
- Bootstrap problem (fax machine) when creating community
- Designed for new (compliant) devices

nquiringminds



# MATTER

## What is it

Zigbee focussed method of creating interoperable IOT devices/services with a strongg notion of device commissioning

## Considerations

- How truly interoperable are the interfaces
- Where does “user” authorisation sit
- Potential source of type identifiers and instance identifies

nquiringminds



# FIDO

## What is it

Device onboarding protocol
Has strong device type identity

## Considerations

- A solution for

nquiringminds




# Software Bill of Materials

## What is it

Device onboarding protocol

## Considerations

- Needs a VEX to be useful

manySECURED

# NVD Vulnerability Databases

## What is it

List of publicly disclosed vulnerabilities
There are many such databases

## Considerations

- What is the granularity

nquiringminds


manySECURED

# Threat sharing

## What is it

Behaviourally defined threat sharing
List of suspicious destination points

## Considerations

- False positives

nquiringminds

# Building blocks

What's so difficult

# D3: IMPLEMENTATION

Flexible secure data structures

manySECURED

Signed by

| **DevType ID** | Unique ID for device type |
|---|---|
| Manufacturer | Domain name of originating manufacturer |
| Model number | Finest grained, unique model number |
| Model number extra | Secondary model number |
| ID Link | Unique persistent URI (hosting descriptor) |
| Manufacture link | Usable model link for end users |
| Parent type | (optional) parent type (**DevType ID**) |
| Terminal type | Is this terminal type |
| Description | Friendly description of type |

Signed by

| **TAG ID** | Tag ID |
|---|---|
| Friendly name | name |
| Description | Link to download firmware |
| DevType ID | Link to **(DevType ID)** |

Signed by

| **Firmware ID** | Unique ID for firmware |
|---|---|
| Version no | Version number for firmware |
| Link | Link to download firmware |
| Hash | Hash of firmware content |
| Previous firmware | Which firmware this supersedes |
| DevType ID | Link to **(DevType ID)** |
| Parent type | (optional) parent type |
| Description | Friendly description of firmware |

Signed by

| **Behaviour ID** | Tag ID |
|---|---|
| Friendly name | name |
| Behaviour | List of allowed network behaviours TBD |
| DevType ID | Link to **(DevType ID)** |

**Verifiable Credentials Data Model 1.0**

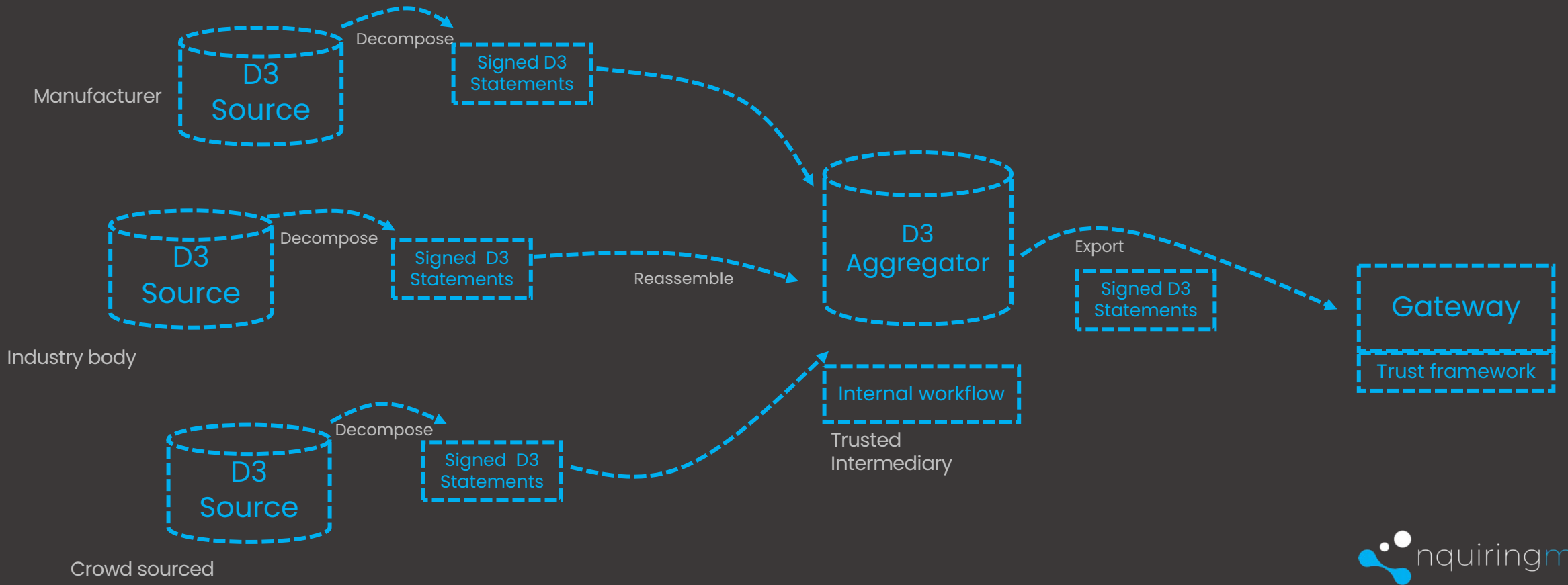
https://www.w3.org/TR/vc-data-model/

nquiringminds

# D3: IMPLEMENTATION

## Anticipated workflow

manySECURED




nquiringminds

# D3: USE CASES

Establishing a real need

manySECURED

## UC1: Type Assertion & hierarchy

Assemble a model of types to reason from

## UC2: Recognise a type

Bind instance to a type: hard methods (certificates), soft methods (recognisers), human methods (people doing stuff)

## UC3: Define least privilege behaviour

Use the MUD stuff

## UC4: Infer stochastic behaviour

Observe an instance of assemble all behaviours of declared types

## UC4: Infer risk from type

Using bindings of type to CVEs to triage risk. And use other information sources

## UC5: Infer risk from instance behaviour

User MISP (or other) to infer risk on the single instance
What does this tell you by type? Possible vulnerability

## UC6: Onboard a device

Auto enrol a device if “sufficient” evidence presented

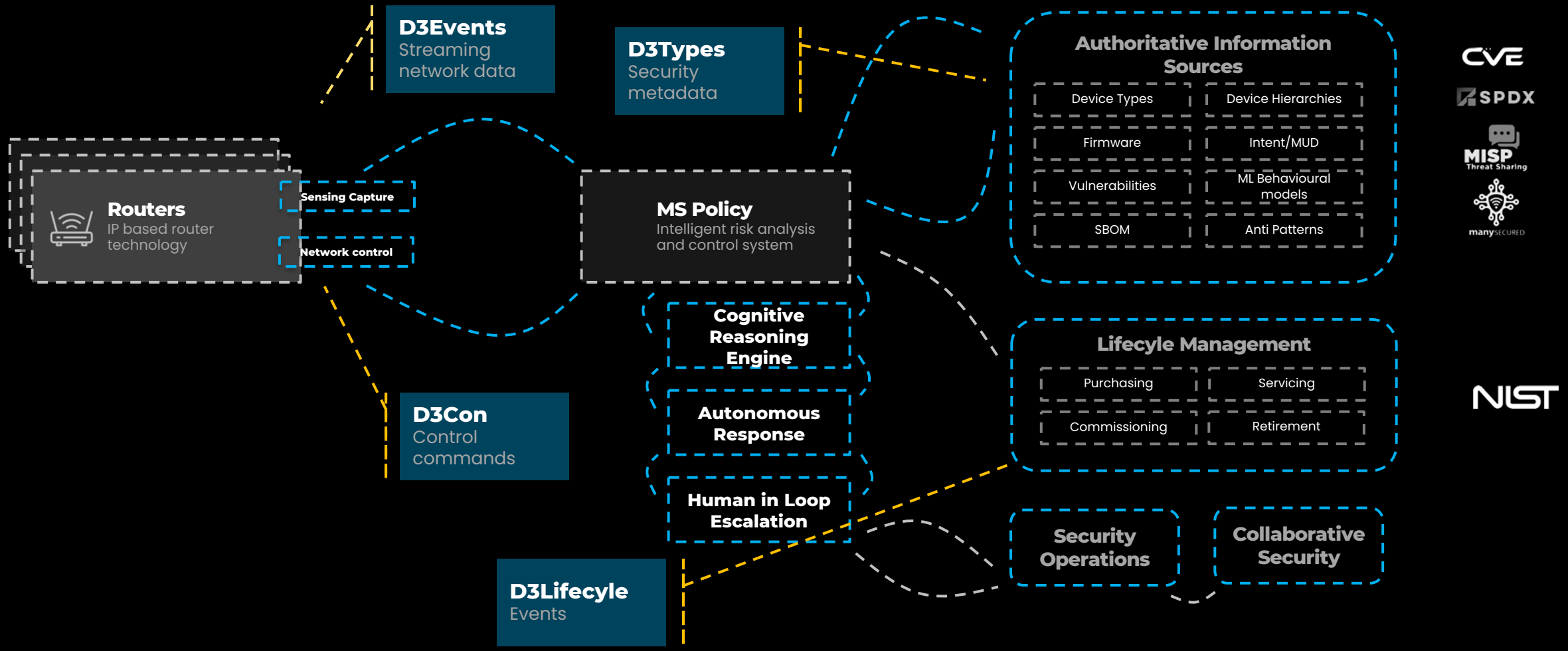
## UC7: On board a browser

Enrol a device certificate to a browser for a more secure experience

nquiringminds

# HOW IT WORKS

## Operational Deployment



# Summary

Secure Gateway Next Steps

nquiringminds

## Status

Good next practice for gateway security

Integrated existing systems in a useful way

Foundation for “useful” collaboration

Practical and concrete

## Get involved

Specifications

Implementations

Data gathering/sharing:

**Virtual IOT Cyber Lab**

Website: https://manysecured.net/

Specifications:

https://specs.manysecured.net/

Specification source:

https://github.com/TechWorksHub/ManySecured-WGs

Open source gateway reference:

https://github.com/nqminds/edgesec/issues

Email:

info@manysecured.net

nquiringminds

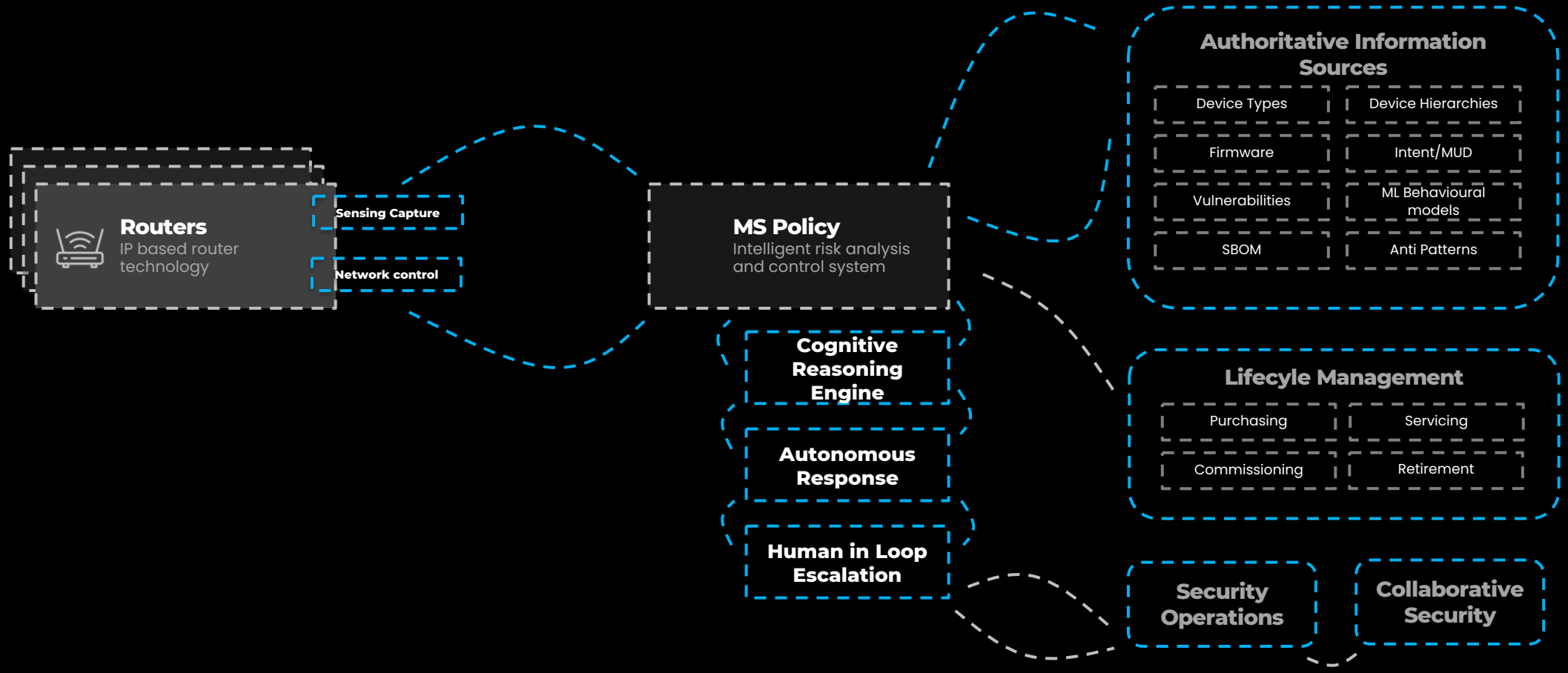
manySECURED

Dr Nicholas Allott
nick@nqminds.com

# Backup slides

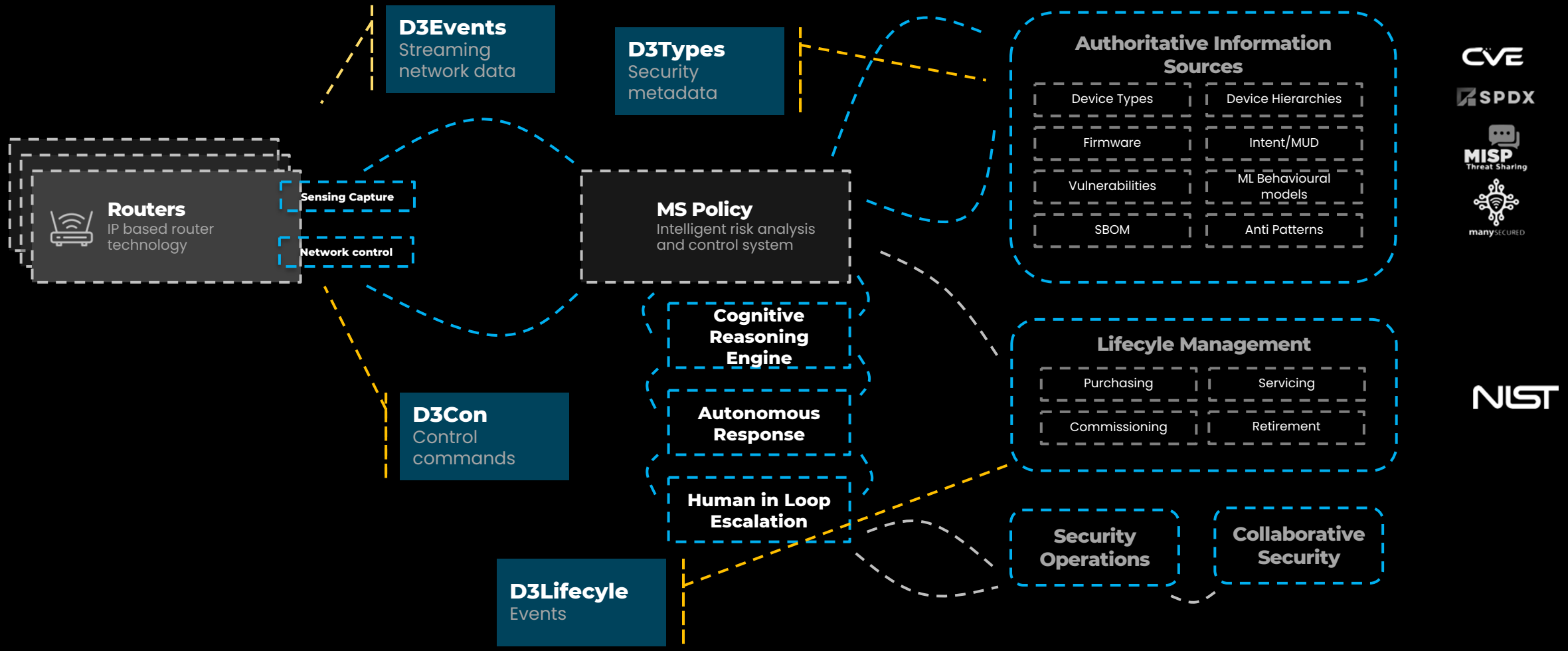
# HOW IT WORKS

## Operational Deployment



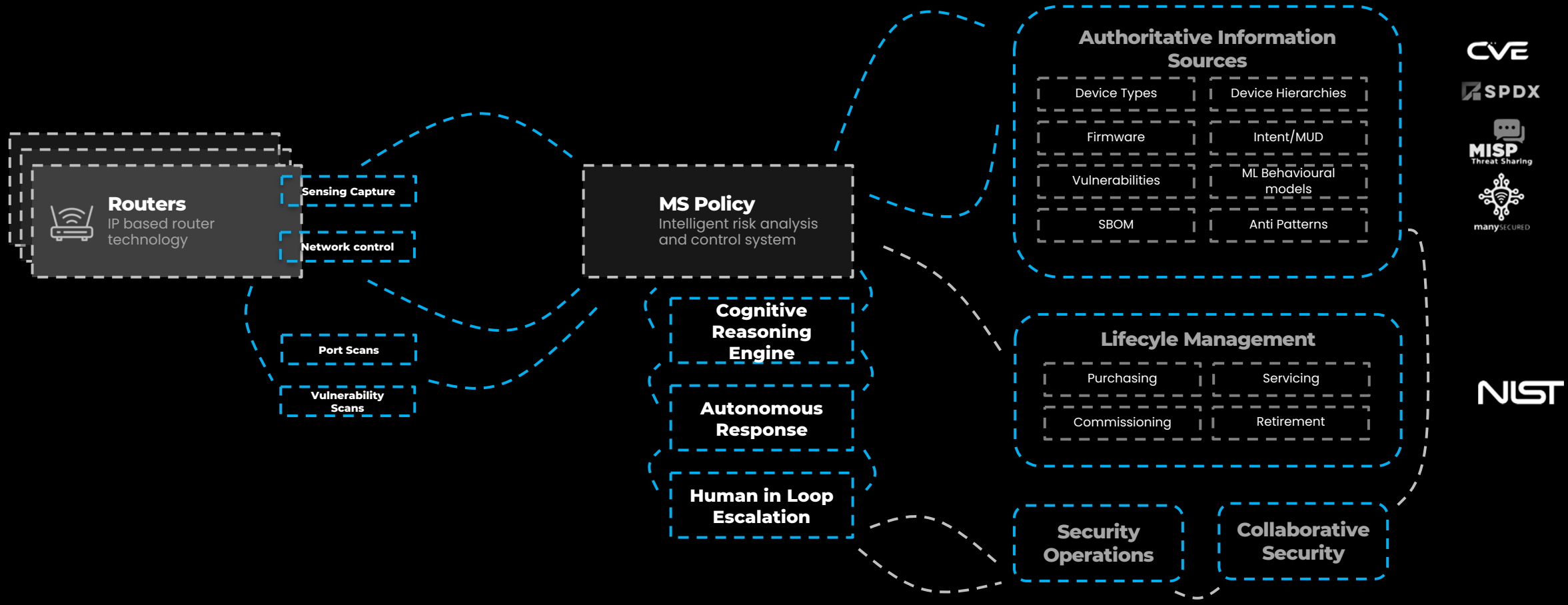
# HOW IT WORKS

## Operational Deployment



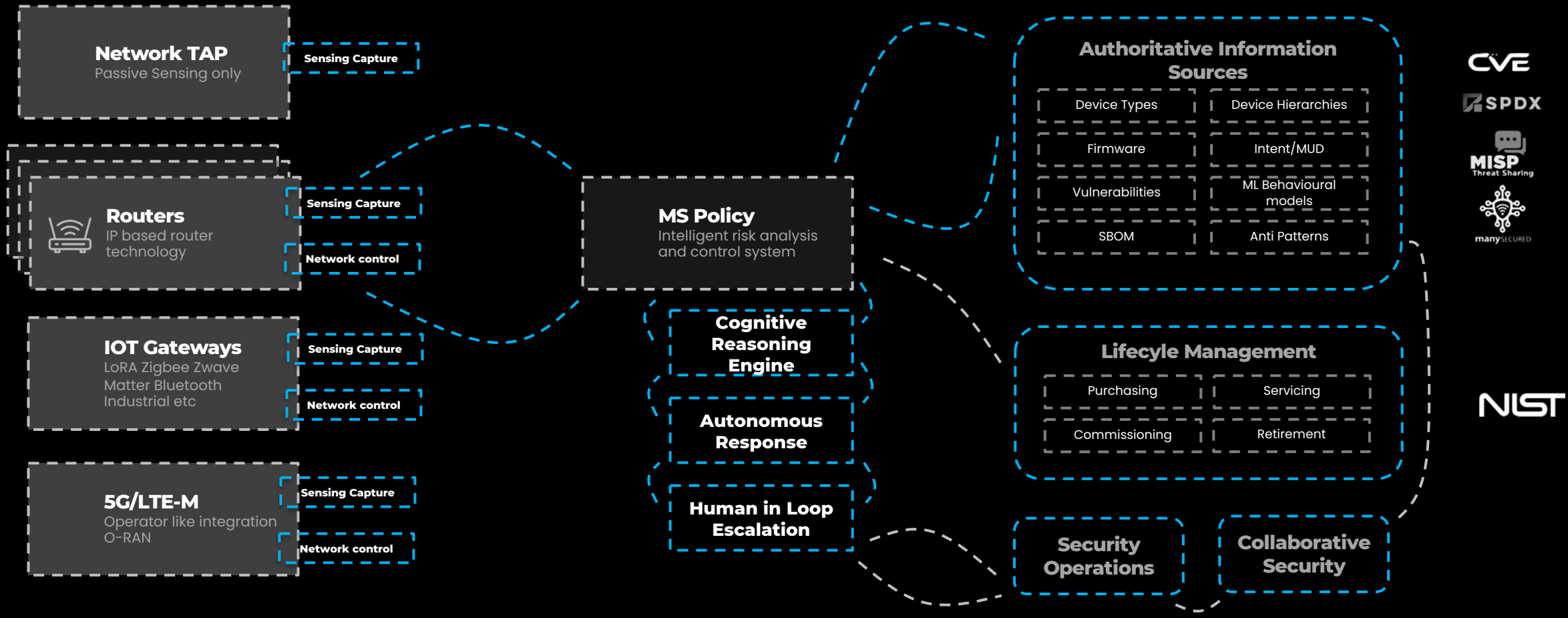
# HOW IT WORKS

## Additional Information

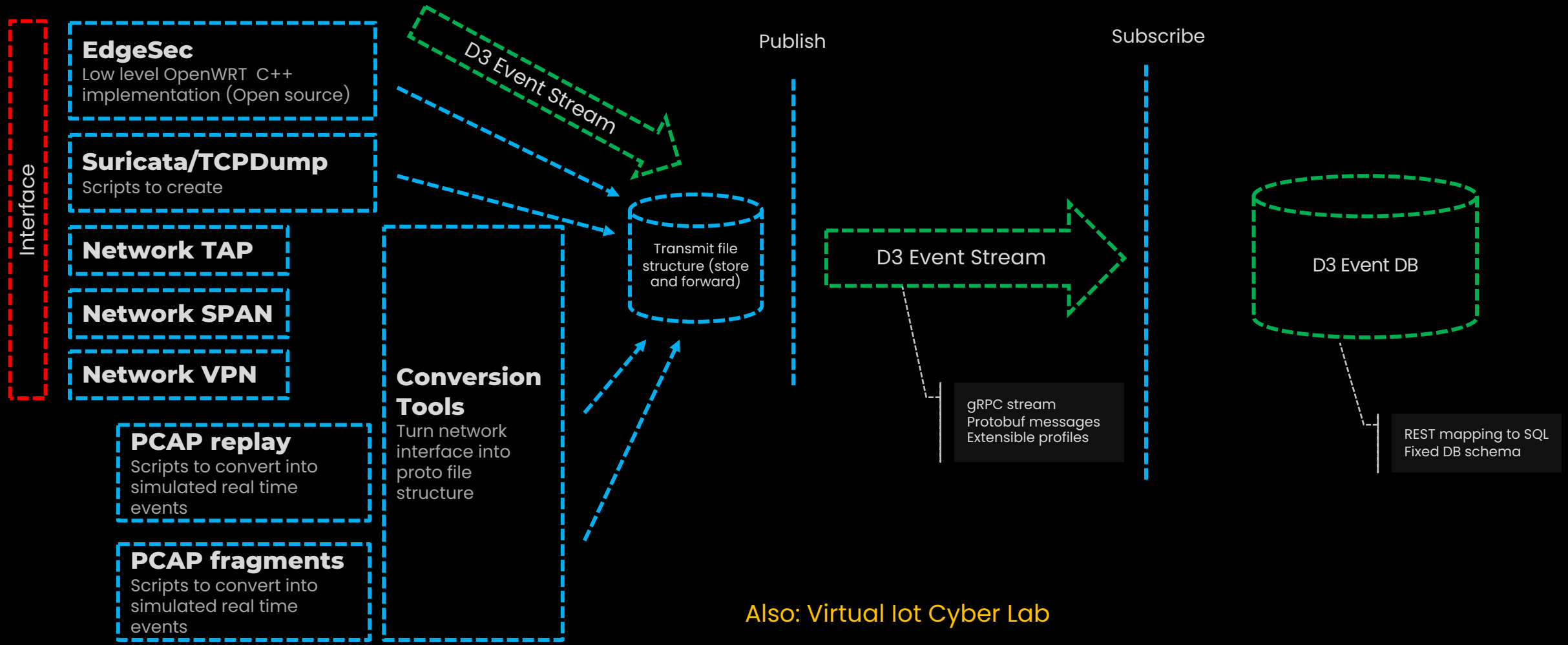


# HOW IT WORKS

## Different Deployments



# How to integrate




Also: Virtual Iot Cyber Lab

# Practical use cases

Value added router features

nquiringminds

# Counterfeiting

Stop device spoofing

## How it works

Spotting a device register in two places or to two organisations at the same time.

More than MAC address or IP address, looks at deeper identity can check with an authorise source

## Integration points

With either manufacturer or some point in the purchasing/provisioning chain (lifecycle)

nquiringminds

# Updating

Ensure devices are updated

## How it works

The gateway determines current firmware on this device instance, and compares against available firmware for this device type

## Integration points

Infer current firmware (auto scan, provisioning event, RATS, SBOM)

Declaration of official device type to firmware bindings

Integrity checks

nquiringminds

# Onboarding

Ensure devices are updated

## How it works

Automatically provision network credentials

Selectively on board:

- Recognised device ID
- Purchase device
- Provisioned device
- Attestable device instance (integrity)
- Tested device instance (compliance)
- Tested device type (type compliance)
- etc

## Integration points

All....

nquiringminds

# Offboarding

Ensure devices are updated

## How it works

Remove the device when evidence, implies that no longer suitable

- Resold
- Counterfeit
- Irregular activity

## Integration points

Purchase voucher system

Remote “assurance” tests

nquiringminds

# Vuln Inferencing

Auto detect vulnerabilities on connected devices

## How it works

From this device instance determine the device type and from that device type identify disclosed vulnerabilities

## Integration points

Device type identification process(es)

CVE database sources (with device type reference)

nquiringminds

# Vuln Inferencing2

Use SBOM to infer vulnerabilities

## How it works

Like version 1 – but using SBOM declarations to harvest larger vulnerability list

## Integration points

Device type->SBOM packages

SBOM packages ->CVE

nquiringminds

# Vuln Reporting

Declare new vulnerability against a device type

## How it works

Using automated or manual methods identify a vulnerability against an instance. If found register against the device type

## Integration points

Device instance to device type recogniser

CVE with device type references

nquiringminds

# Suspicious activity inferencing

Flag a device based on its suspicious activity

## How it works

Monitor device activity and pattern match againstt known “bad patterns” or “bad destinations”.

Suspicious activity frequently register against a type may help identify a system vulnerability

## Integration points

MISP database or similar

nquiringminds

# Least Privilege Behaviour Reporting

Create an allowed list description of permissible network behaviour

## How it works

Manufacture, third party of monitoring system builds an “allowed list” model

## Integration points

Publish point for behaviours

MUD specification

nquiringminds

# Least Privilege Behaviour Enforcement

Contain (or flag) a device based on its usual behaviour

## How it works

From device instance determine device type

From device type download behaviour

Enforce/flag behaviour at gateway

## Integration points

MUD publisher

nquiringminds

# Stochastic Behaviour Reporting

Create a statistical /ML model of behaviour

## How it works

Observe individual device instances and aggregate instance bedsores across device type

(its also possible to benchmark and untyped single instance)

## Integration points

Reliable publisher of models

nquiringminds

# Stochastic Behaviour Enforcement

Contain/flag device based on anomalous behaviour

## How it works

Download model from type database.

Enforce model at the gateway (gateway controller)

## Integration points

Trusted published of models

nquiringminds

# Declare Gateway Security Features

Make remotely attestable claims of gateway security features

## How it works

Allow connected IOT device and connecting networking equipment to react to discernible security features

## Integration points

IETF RATS

Secure boot

CHERI/Morello

Rust Kernel

SBOM

GCERT

nquiringminds

# Infer IOT device Security Features

Help gateway determine security features of connected IOT devices

## How it works

Gateway probes each device and asks it to declare its security credentials.

This information can inform how the gateway treats the device.

## Integration points

IETF RATS

Secure boot

CHERI/Morello

Rust Kernel

SBOM

IOTSF Assurance