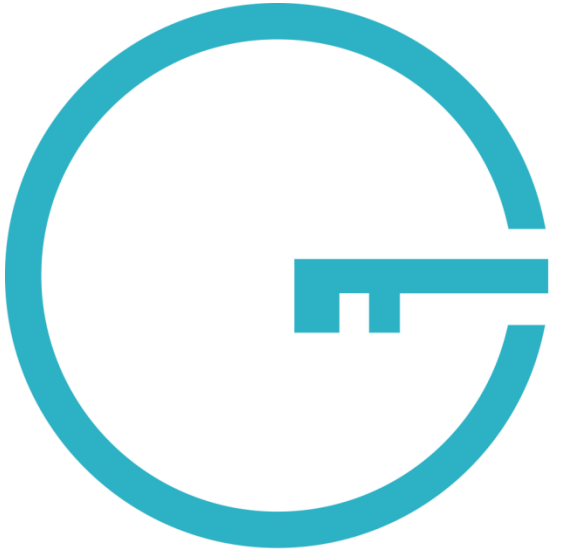
Safe-Guarding Home IoT Enviroments with Personalised Real-time Risk Control



Konstantinos Votis

Partners:

Televes · NTNU · EXUS · KIT Karlsruher Institut für Technologie · kalos Information Systems · Universidad de Genève · iti · Imperial College London · OBRELA Security Industries · Cruz Roja Española

GHOST has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under GA No. 740923

GHOST vision and mission

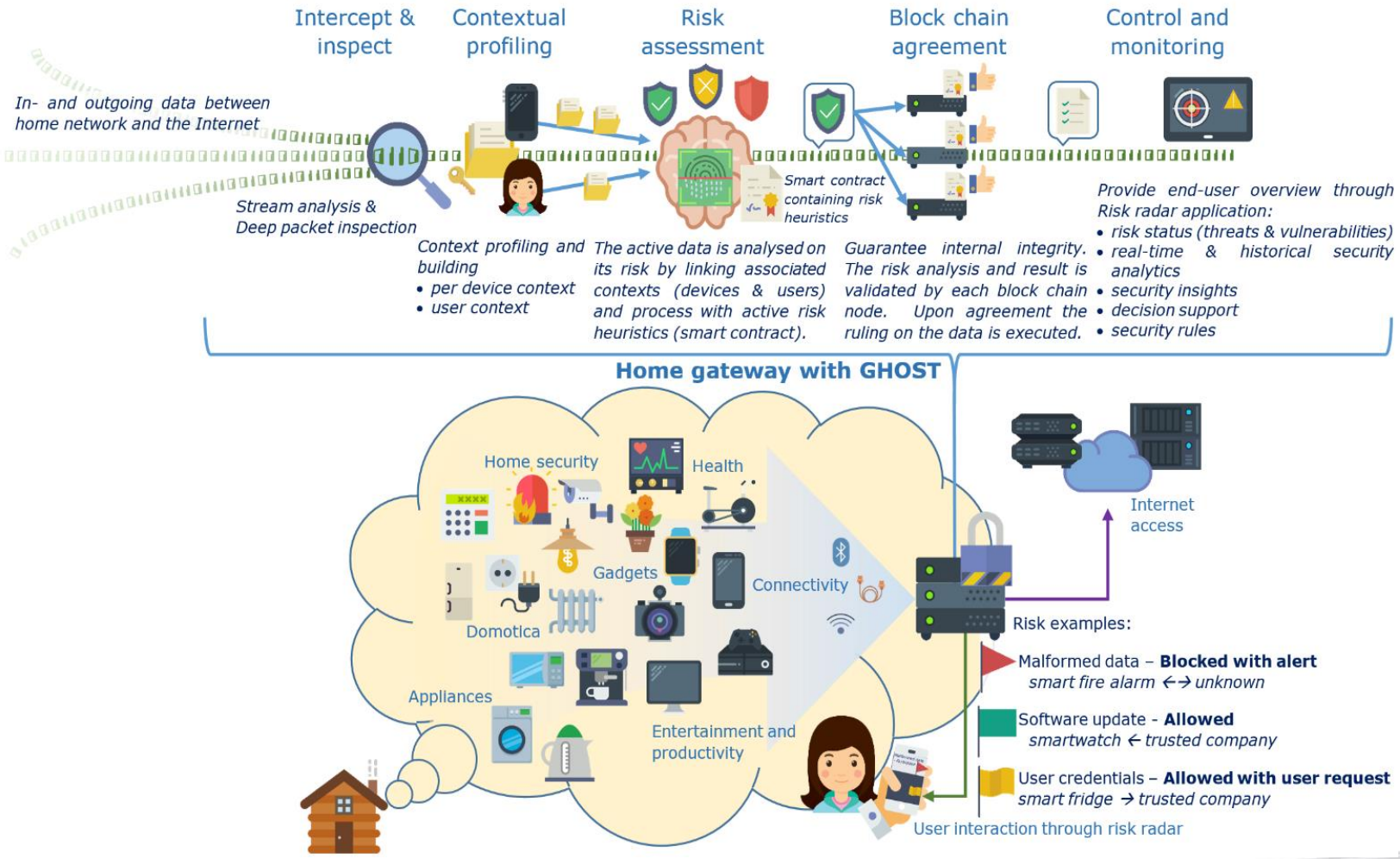
- Vision

  GHOST envisions a **transparent cybersecurity** environment for all Europeans living in a connected world: with minimal effort consumers will become aware and **understand** the cybersecurity risks (threats and vulnerabilities), and will take informative decisions affecting their cyber-physical security and privacy. Cybersecurity technology will transform consumers' decisions into **reliable automated security services** and solutions, will promote **security-friendly end-user habits** through behavioural engineering, and deliver **usable transparency**

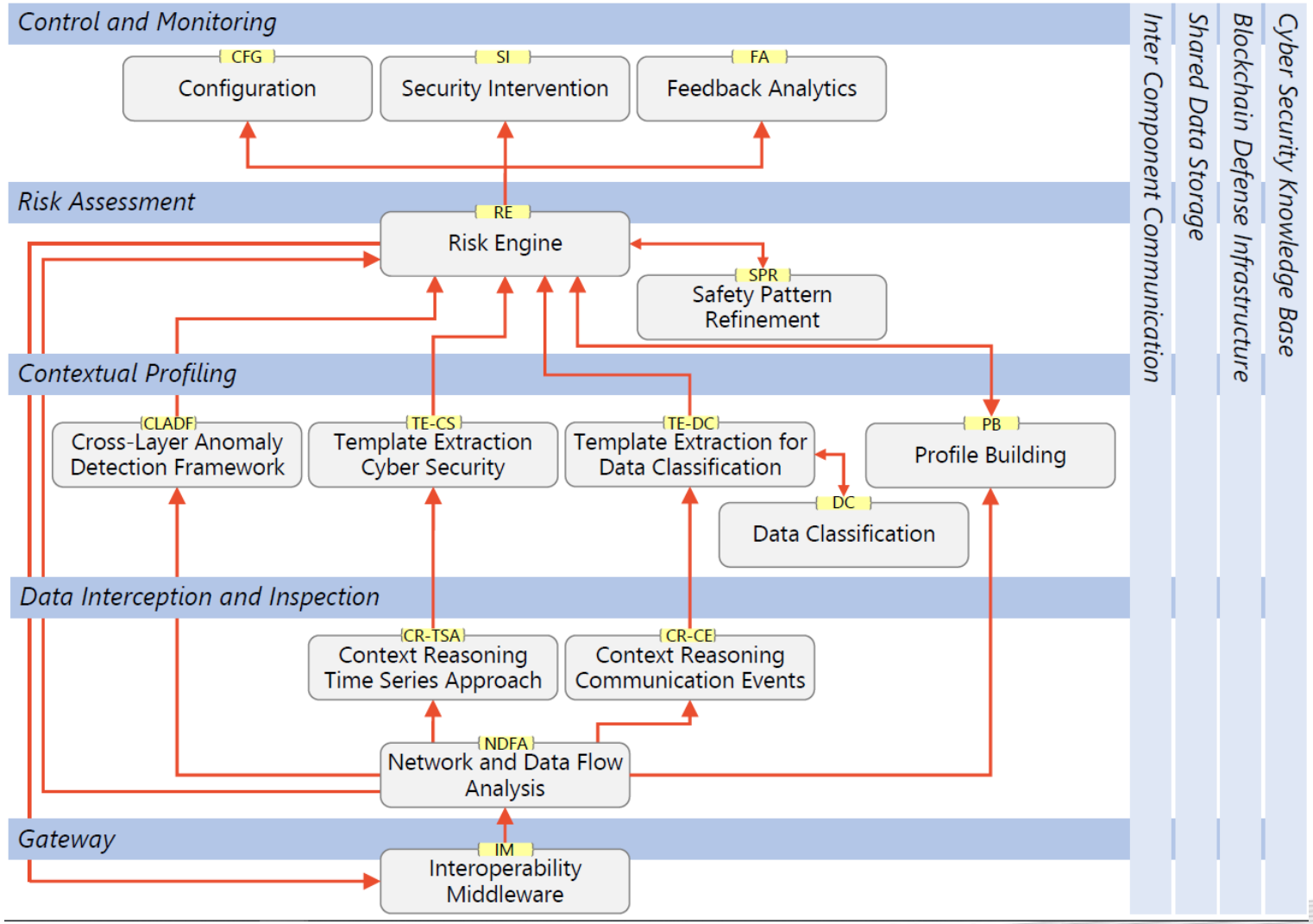
- Mission

  To deliver the first generation of **disruptive software-enabled usable security network solution for smart-home occupants**. GHOST cutting-edge technology will increase the level and the effectiveness of automation of existing cybersecurity services, enhance **system self-defence** and will open up the cybersecurity 'blackbox' to consumers and build **trust** through advanced usable transparency tools derived from end-users' mental models.

GHOST high-level concept



GHOST architecture



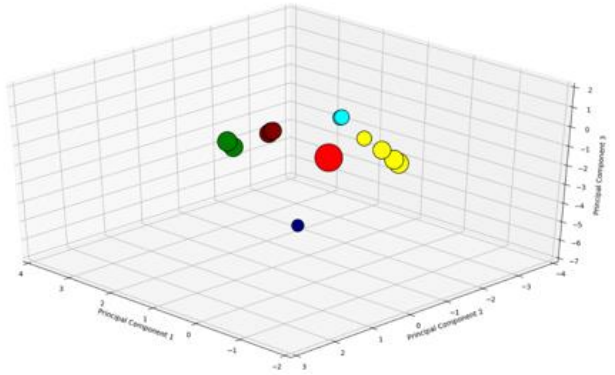
IoT Templates/Profiles

Training Phase

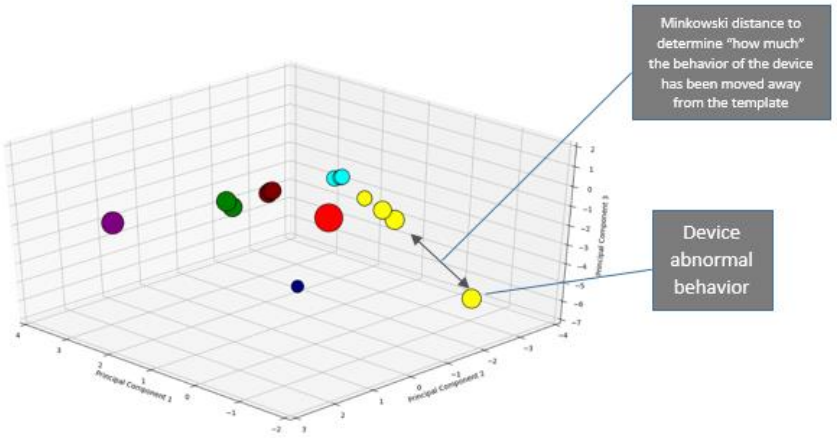
- Iterative procedure that updates the models every night
- Creates templates of the devices by using clustering algorithms

Running Phase

- Detects anomalies in the network traffic by producing a template similarity score for each device



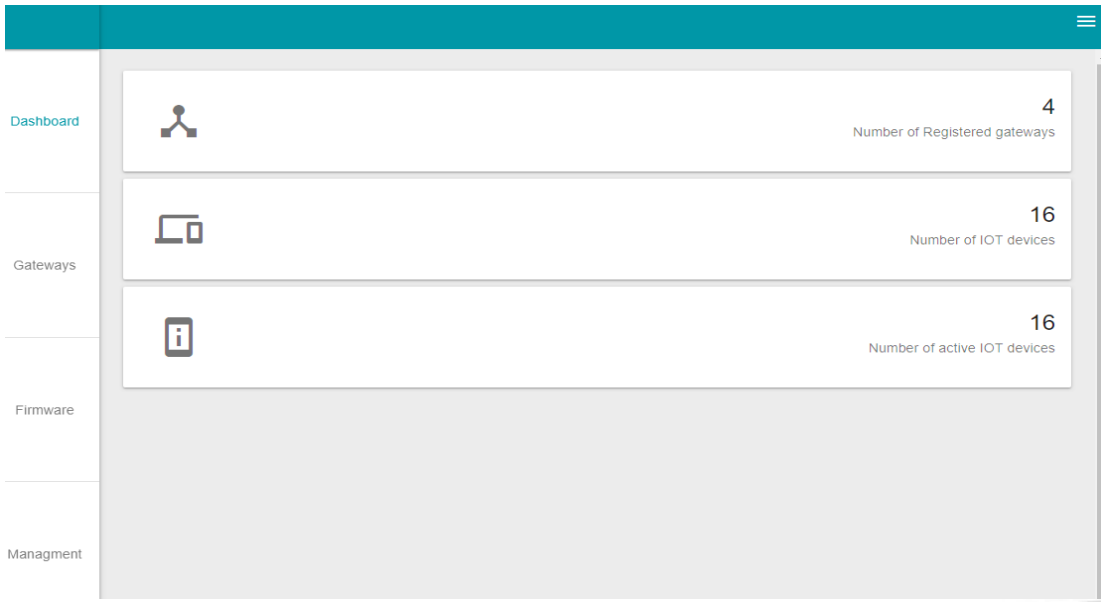
Normal behavior



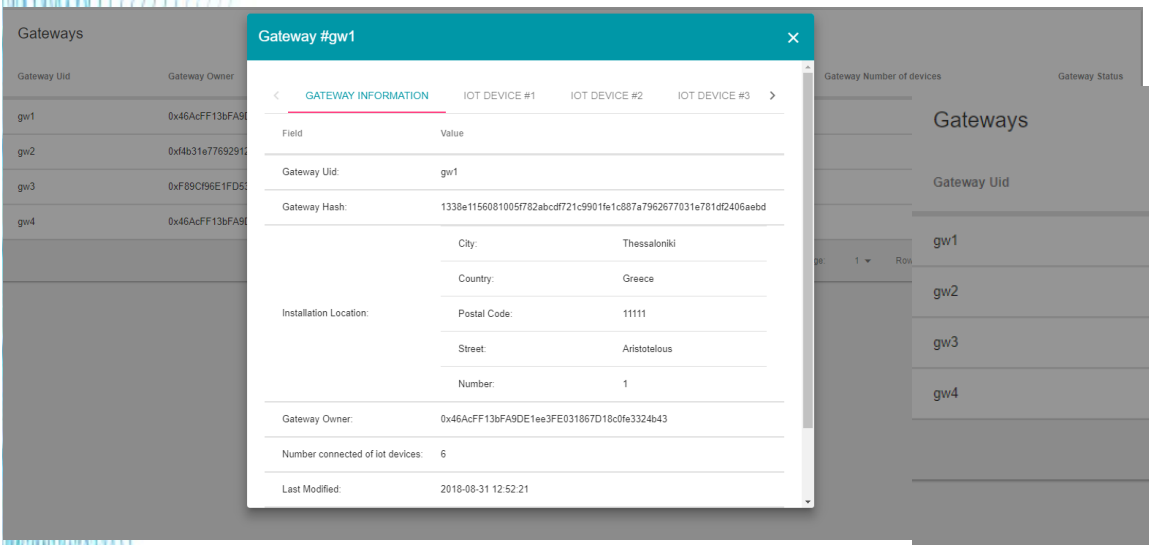
Abnormal Behavior

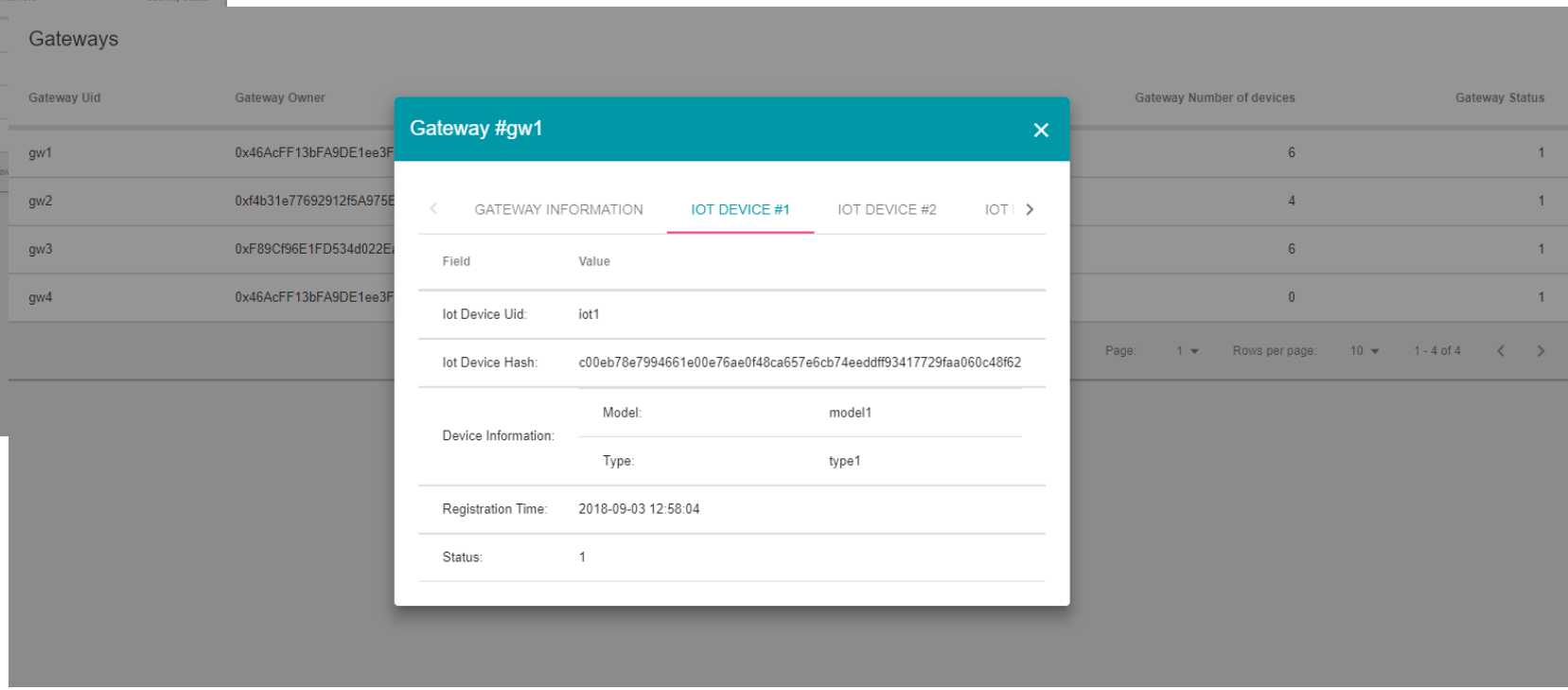
Decentralized solutions

- Extensible and transparent Blockchain framework for supporting the following actions/use cases
  - Registration of GWs into the GHOST system
  - Registration of IoT devices into the GHOST system
  - Consent form
  - Software integrity at
    - GHOST software GW installation level
    - IoT device level



Registration of GWs/IoT devices





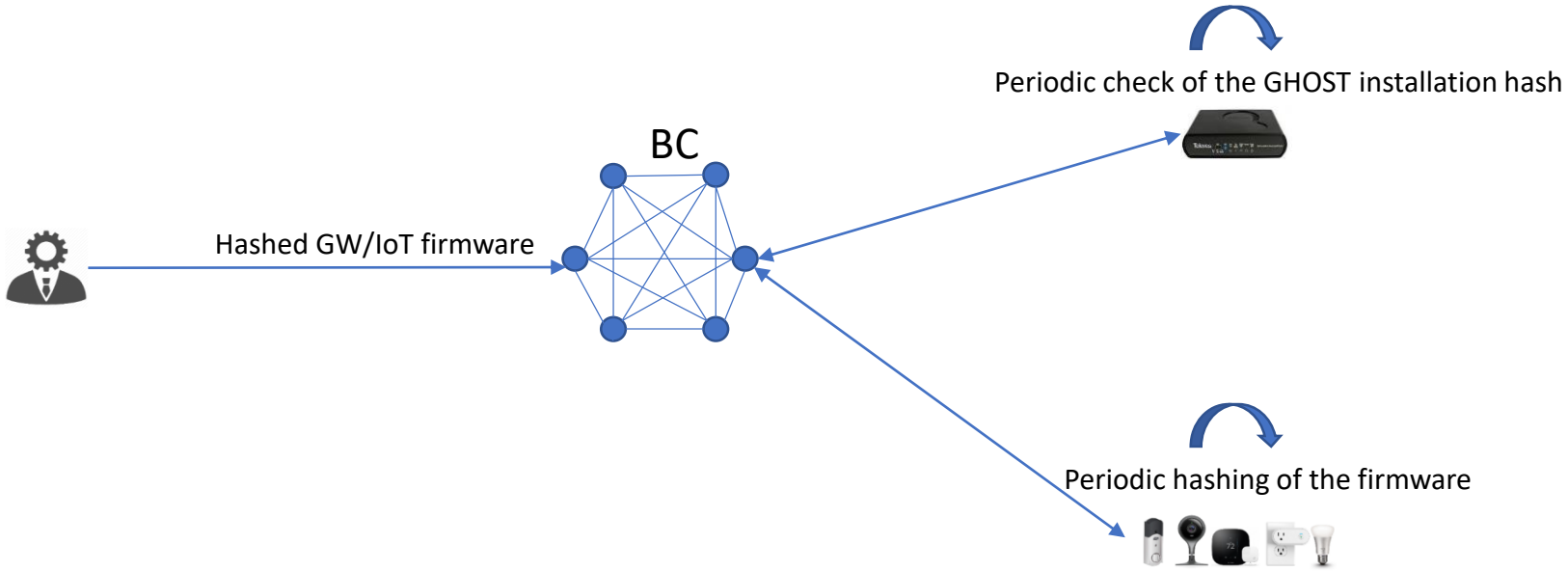
Hashed GW id + user address

BC

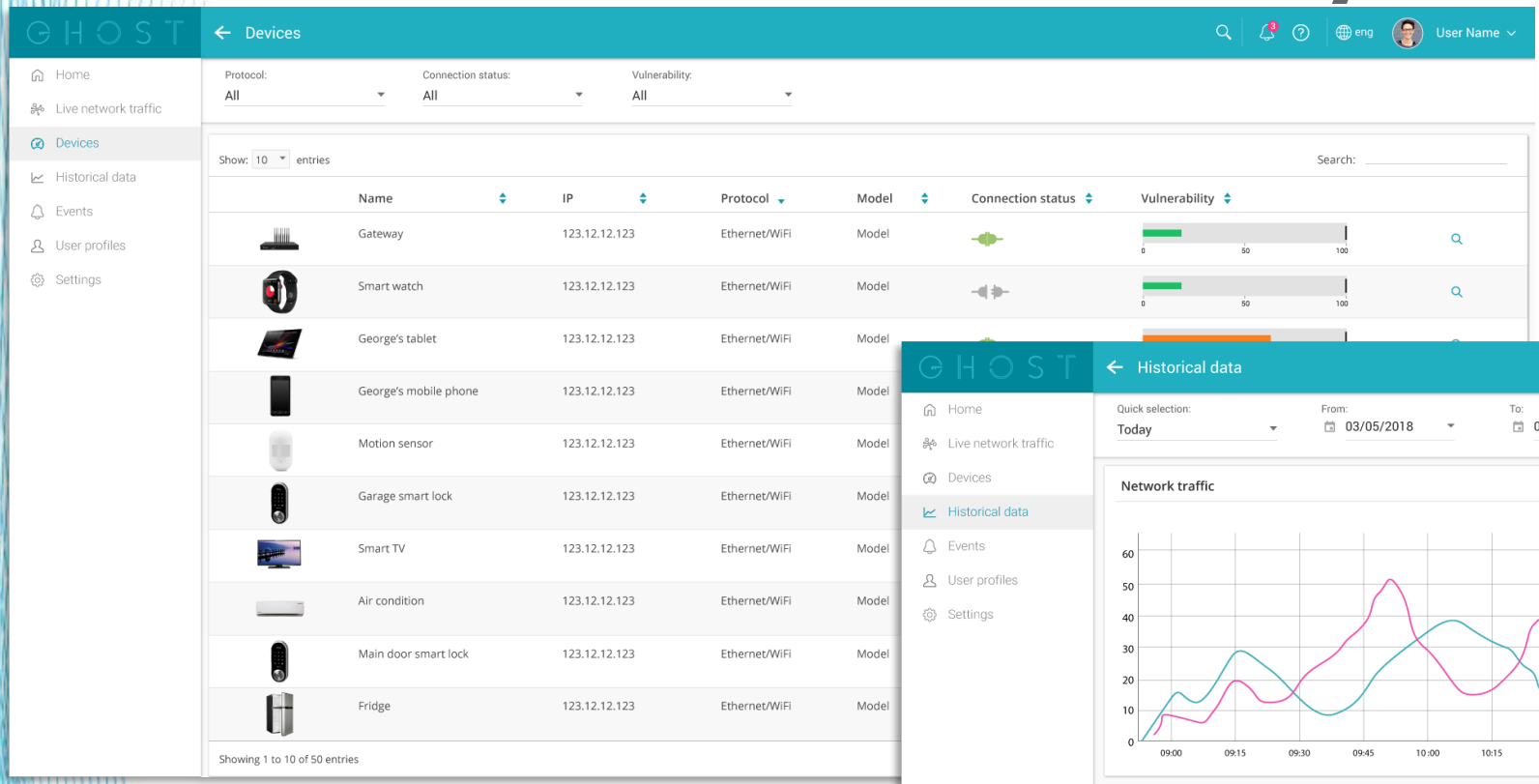
Hashed IoT id + GW id

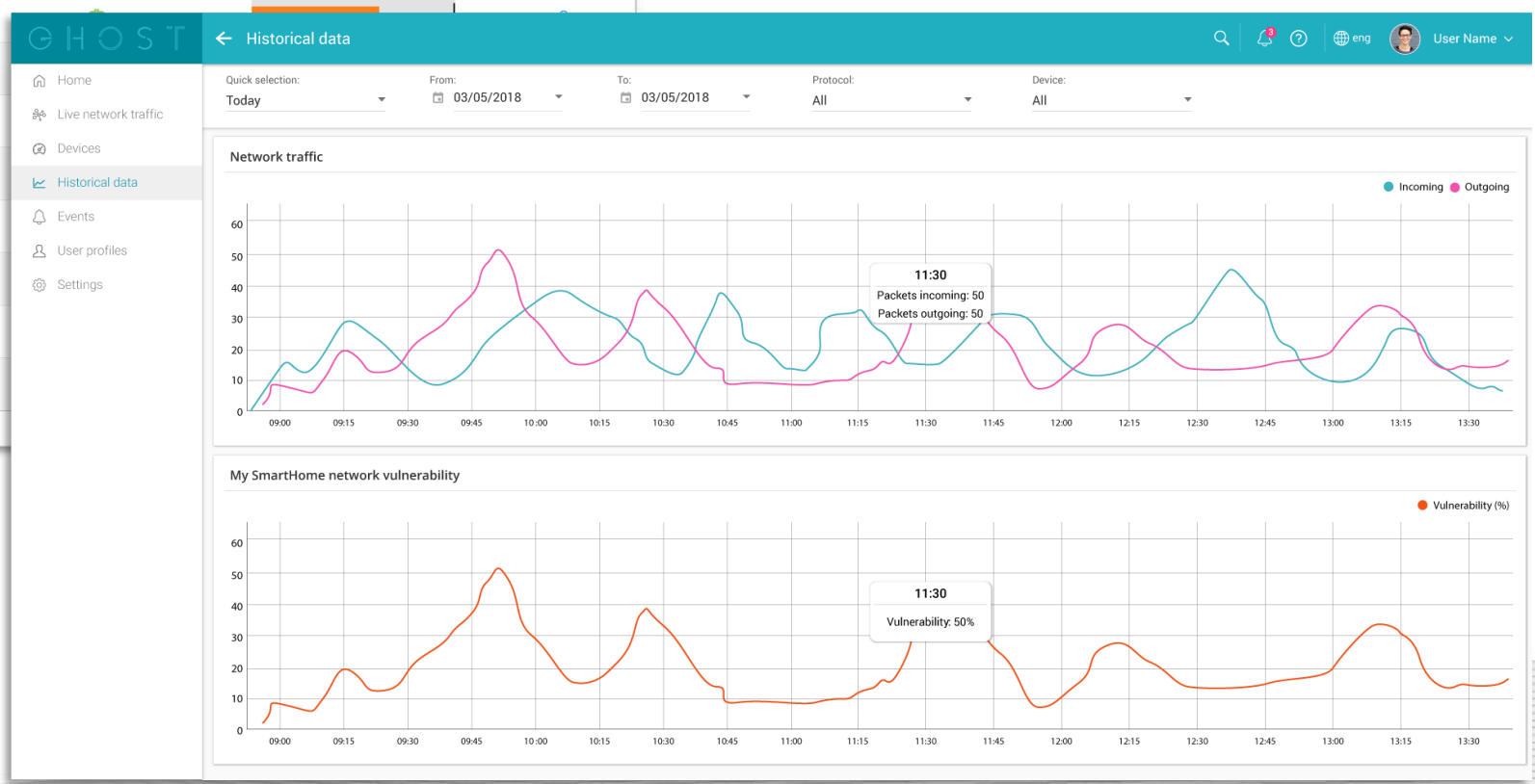
Software Integrity

- Ensure that GW and IoT firmware/software has not been compromised



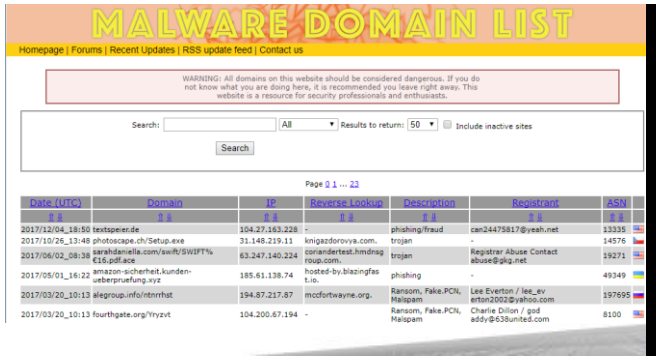
Analytics

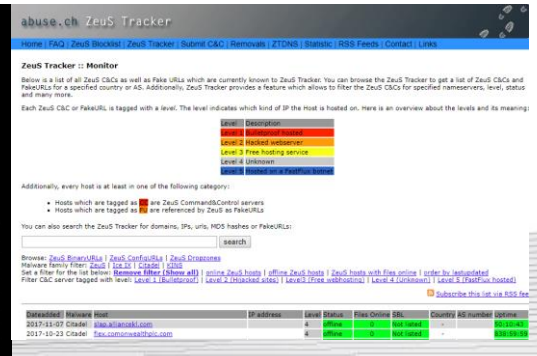

GHOST
Devices
eng
User Name
Home
Live network traffic
Devices
Historical data
Events
User profiles
Settings
Protocol:
All
Connection status:
All
Vulnerability:
All
Show: 10 entries
Search:
Name
IP
Protocol
Model
Connection status
Vulnerability
Gateway 123.12.12.123 Ethernet/WiFi Model
Smart watch 123.12.12.123 Ethernet/WiFi Model
George's tablet 123.12.12.123 Ethernet/WiFi Model
George's mobile phone 123.12.12.123 Ethernet/WiFi Model
Motion sensor 123.12.12.123 Ethernet/WiFi Model
Garage smart lock 123.12.12.123 Ethernet/WiFi Model
Smart TV 123.12.12.123 Ethernet/WiFi Model
Air condition 123.12.12.123 Ethernet/WiFi Model
Main door smart lock 123.12.12.123 Ethernet/WiFi Model
Fridge 123.12.12.123 Ethernet/WiFi Model
Showing 1 to 10 of 50 entries


GHOST
Historical data
eng
User Name
Home
Live network traffic
Devices
Historical data
Events
User profiles
Settings
Quick selection:
Today
From:
03/05/2018
To:
03/05/2018
Protocol:
All
Device:
All
Network traffic
Incoming
Outgoing
11:30
Packets incoming: 50
Packets outgoing: 50
My SmartHome network vulnerability
Vulnerability (%)
11:30
Vulnerability: 50%

Knowledge Base

- Cloud-based repository for maintaining threat information from:
  - External Web Sources
  - Threat Intelligence repository
    - Honeypots, Darknets, Manually analysis, Forensics, Malware Analysis, Identified Attacks, Corporate sources from Security Opsecs, SIEM correlated incidents
  - Smart homes
- Backend manipulation
  - Based on Unified-Cybersecurity-Ontology (UCO)
  - Semantic annotations of external and user reported threats





Konstantinos Votis

kvotis@iti.gr