black hat USA 2023

AUGUST 9-10, 2023

BRIEFINGS

A Manufacturer's Post-Shipment Approach to Fend-Off IoT Malware in Home Appliances

Speakers: Yuki Osawa and Satoru Higuchi

Contributors: Satoshi Ito, Manabu Nakano and Takayuki Uchiyama

Email: astira@ml.jp.panasonic.com

Panasonic Holdings Corporation

Agenda

- Background
- ASTIRA - Panasonic IoT Threat Intelligence -
- IoT-specialized self-protection module
- Summary and further discussion

Who are we

Yuki Osawa

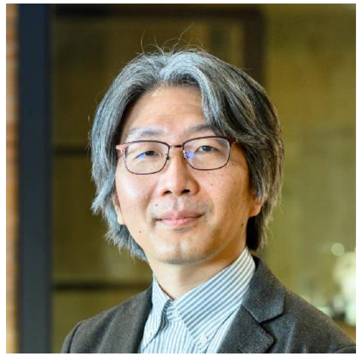
Chief Engineer

Satoru Higuchi

Senior Engineer

Satoshi Ito

Staff Engineer



Manabu Nakano

General Manager

Takayuki Uchiyama

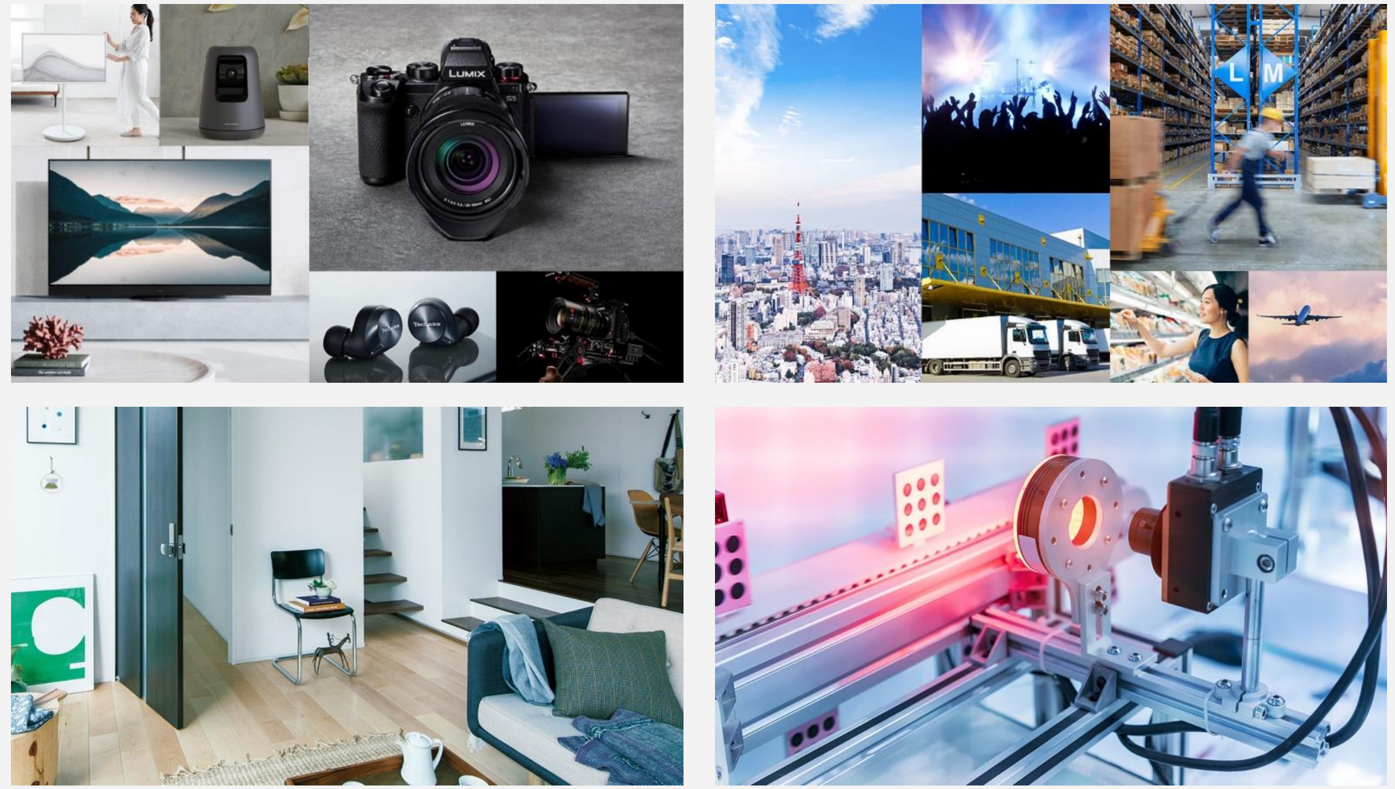
Manager

Product security division that provides business support

Panasonic Holdings Corporation

Support for businesses

Operating Companies



https://holdings.panasonic/global/corporate/about/group-companies.html

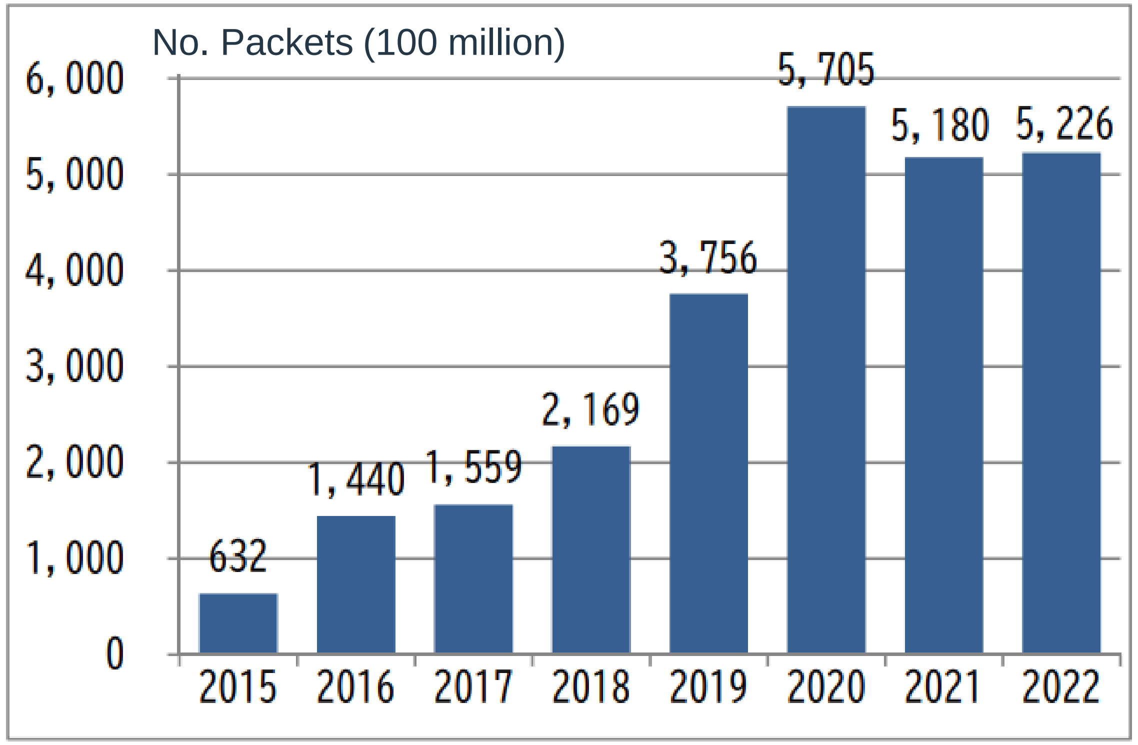
Background

Increase in attacks targeting IoT

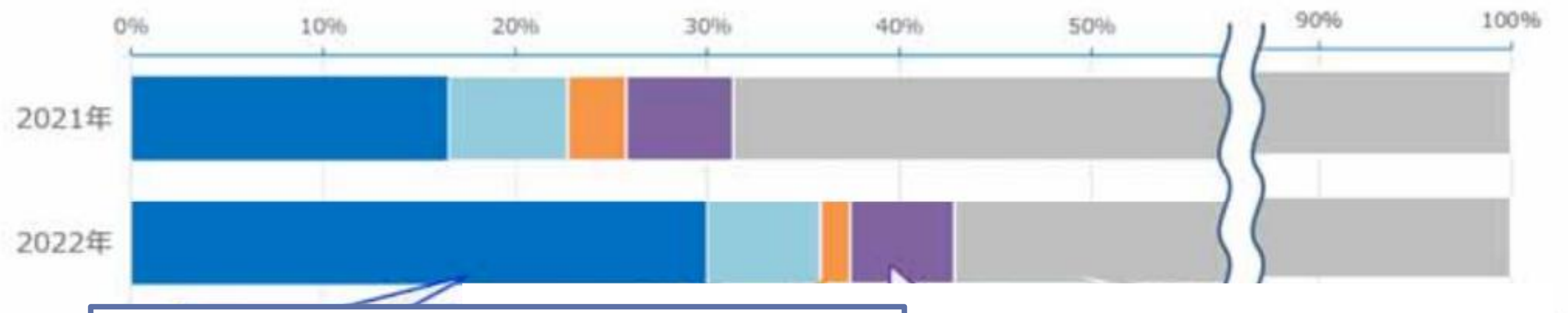
Number of cyber attacks
continue to increase

Sudden increase in attacks targeting IoT since 2021
About one-third of observed attacks targeting IoT

Number of Attacks Observed by NICTER Darknet Sensors



Breakdown of Observed Attacks by NICTER Darknet Sensors (2021, 2022)

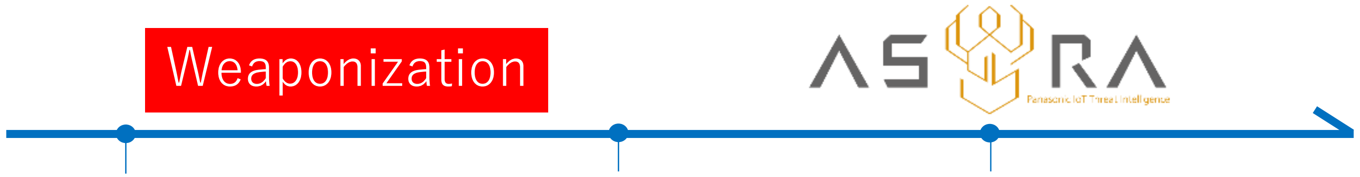


Attacks targeting IoT devices
(Web Cameras, Routers, etc.)

Cybersecurity Research Institute - Cyber Security 2023
Appending 6 - Cyber Security Related Data - NICTER Observation Results
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf

Current state of IoT malware

- Attack cycles are becoming faster as IoT malware is in the wild within a few days after a vulnerability is disclosed

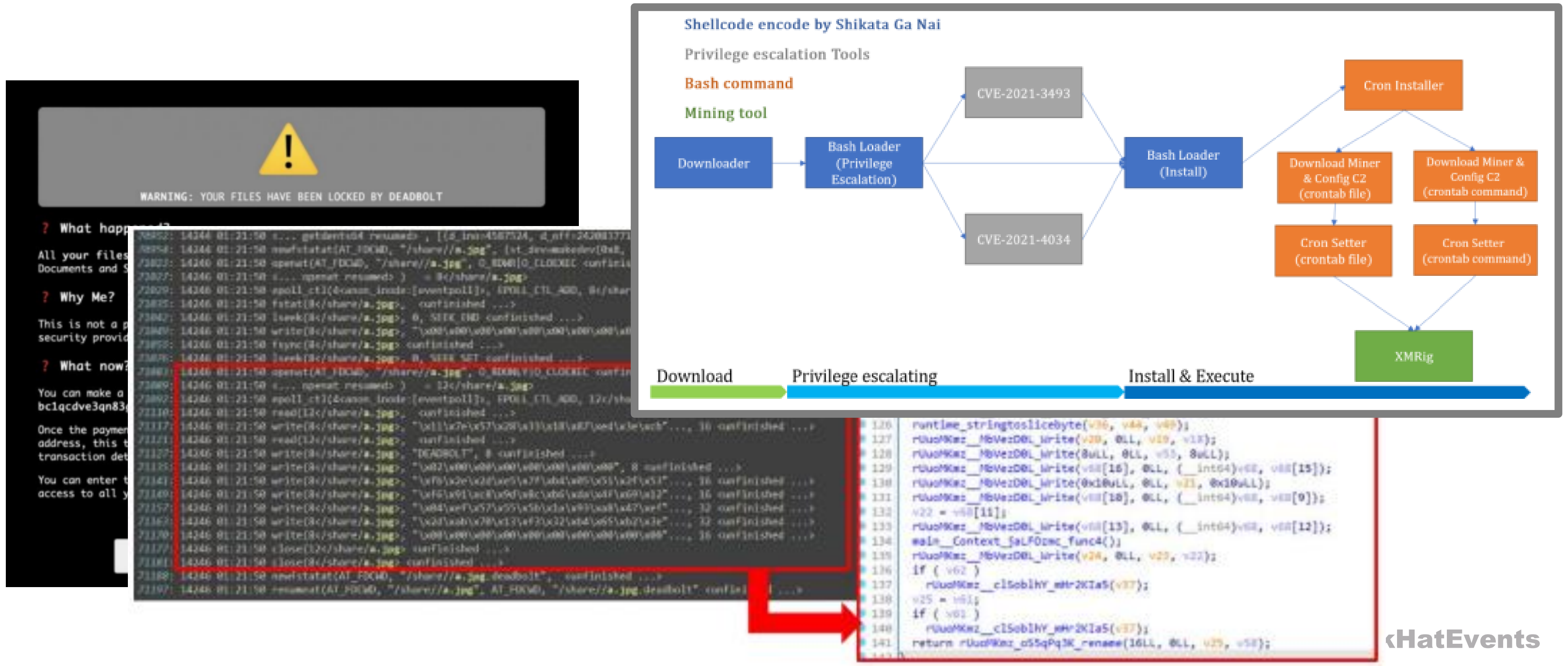


2021/8/16
Vulnerability disclosed

2 days later
IoT malware in the wild

After 8/31
Malware captured by ASTIRA

- Increasingly complex capabilities
  - Ransomware
  - Sophisticated techniques to avoid being detected


WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT

? What happ

All your files
Documents and S

? Why Me?

This is not a p
security provid

? What now?

You can make a
bc1qcdve3qn83

Once the paymen
address, this t
transaction det

You can enter t
access to all y

```
14244 01:21:50 <... getdents64 resumed> , [{d_ino=4587524, d_off=242083771
14244 01:21:50 newfstatat(AT_FDCWD, "/share//a.jpg", {st_dev=makedev(0x8,
14246 01:21:50 openat(AT_FDCWD, "/share//a.jpg", O_RDWR|O_CLOEXEC <unfinis
14246 01:21:50 <... openat resumed> )   = 8</share/a.jpg>
14246 01:21:50 epoll_ctl(4<anon_inode:[eventpoll]>, EPOLL_CTL_ADD, 8</shar
14246 01:21:50 fstat(8</share/a.jpg>, <unfinished ...>
14246 01:21:50 lseek(8</share/a.jpg>, 0, SEEK_END <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x00\x00\x00\x00\x00\x00\x00\x00\x0
14246 01:21:50 fsync(8</share/a.jpg> <unfinished ...>
14246 01:21:50 lseek(8</share/a.jpg>, 0, SEEK_SET <unfinished ...>
14246 01:21:50 openat(AT_FDCWD, "/share//a.jpg", O_RDONLY|O_CLOEXEC <unfin
14246 01:21:50 <... openat resumed> )   = 12</share/a.jpg>
14246 01:21:50 epoll_ctl(4<anon_inode:[eventpoll]>, EPOLL_CTL_ADD, 12</sha
14246 01:21:50 read(12</share/a.jpg>, <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x11\x7e\x57\x28\x13\x18\x87\xed\x3e\xcb"..., 16 <unfinished ...>
14246 01:21:50 read(12</share/a.jpg>, <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "DEADBOLT", 8 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x02\x00\x00\x00\x00\x00\x00\x00", 8 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\xf0\x2e\x2d\xe5\x7f\xb4\x05\x51\x2f\x53"..., 16 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\xf6\x91\xc8\x9d\x8c\xb6\xda\x4f\x69\x12"..., 16 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x84\xef\x57\x55\x5b\x1a\x93\xa8\x47\xef"..., 32 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x2d\xab\x78\x13\xf3\x32\xd4\x65\xb2\x3e"..., 32 <unfinished ...>
14246 01:21:50 write(8</share/a.jpg>, "\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"..., 16 <unfinished ...>
14246 01:21:50 close(12</share/a.jpg> <unfinished ...>
14246 01:21:50 close(8</share/a.jpg> <unfinished ...>
14246 01:21:50 newfstatat(AT_FDCWD, "/share//a.jpg.deadbolt", <unfinished ...>
14246 01:21:50 renameat(AT_FDCWD, "/share//a.jpg", AT_FDCWD, "/share//a.jpg.deadbolt" <unfinished ...>
```

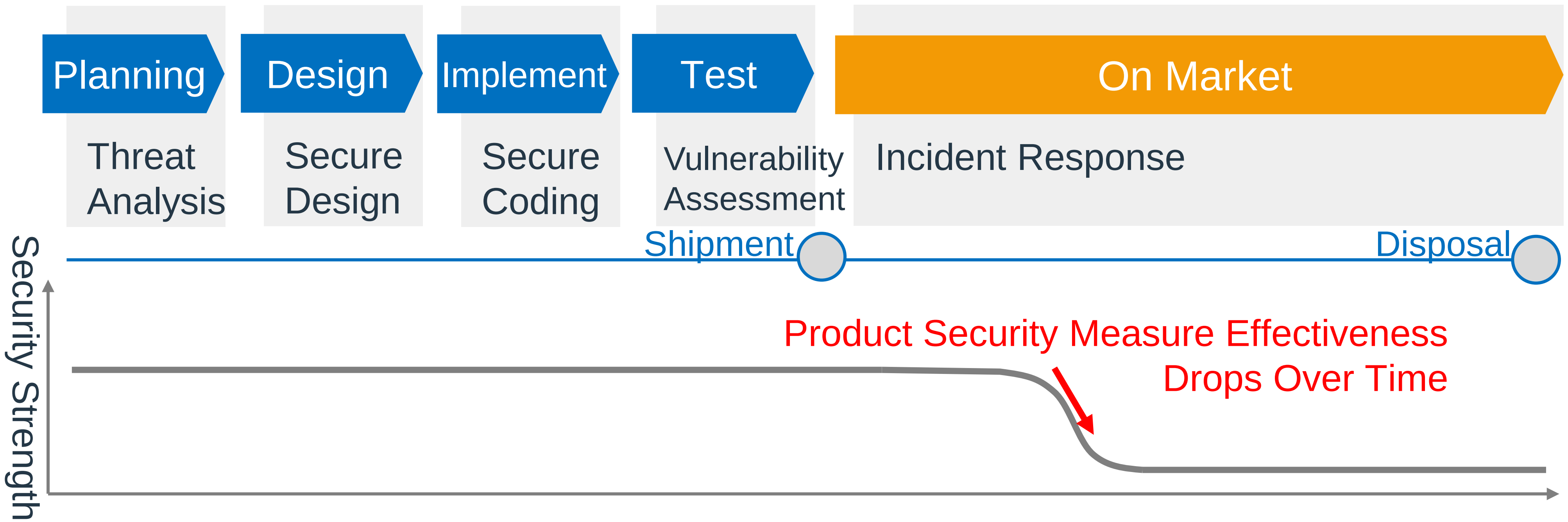
Shellcode encode by Shikata Ga Nai
Privilege escalation Tools
Bash command
Mining tool
Downloader
Bash Loader (Privilege Escalation)
CVE-2021-3493
CVE-2021-4034
Bash Loader (Install)
Cron Installer
Download Miner & Config C2 (crontab file)
Download Miner & Config C2 (crontab command)
Cron Setter (crontab file)
Cron Setter (crontab command)
XMRig
Download
Privilege escalating
Install & Execute

```
runtime_stringtoslicebyte(v36, v44, v49);
rUuoMKmz__MbVezD0L_Write(v20, 0LL, v19, v18);
rUuoMKmz__MbVezD0L_Write(8uLL, 0LL, v55, 8uLL);
rUuoMKmz__MbVezD0L_Write(v68[16], 0LL, (__int64)v68, v68[15]);
rUuoMKmz__MbVezD0L_Write(0x10uLL, 0LL, v21, 0x10uLL);
rUuoMKmz__MbVezD0L_Write(v68[10], 0LL, (__int64)v68, v68[9]);
v22 = v68[11];
rUuoMKmz__MbVezD0L_Write(v68[13], 0LL, (__int64)v68, v68[12]);
main__Context_SaLFOzmc_func4();
rUuoMKmz__MbVezD0L_Write(v24, 0LL, v23, v22);
if ( v62 )
  rUuoMKmz__clSoblhY_mHr2KIa5(v37);
v25 = v61;
if ( v61 )
  rUuoMKmz__clSoblhY_mHr2KIa5(v37);
return rUuoMKmz_o5SqPq3K_rename(16LL, 0LL, v25, v58);
```

Importance of product security after shipment

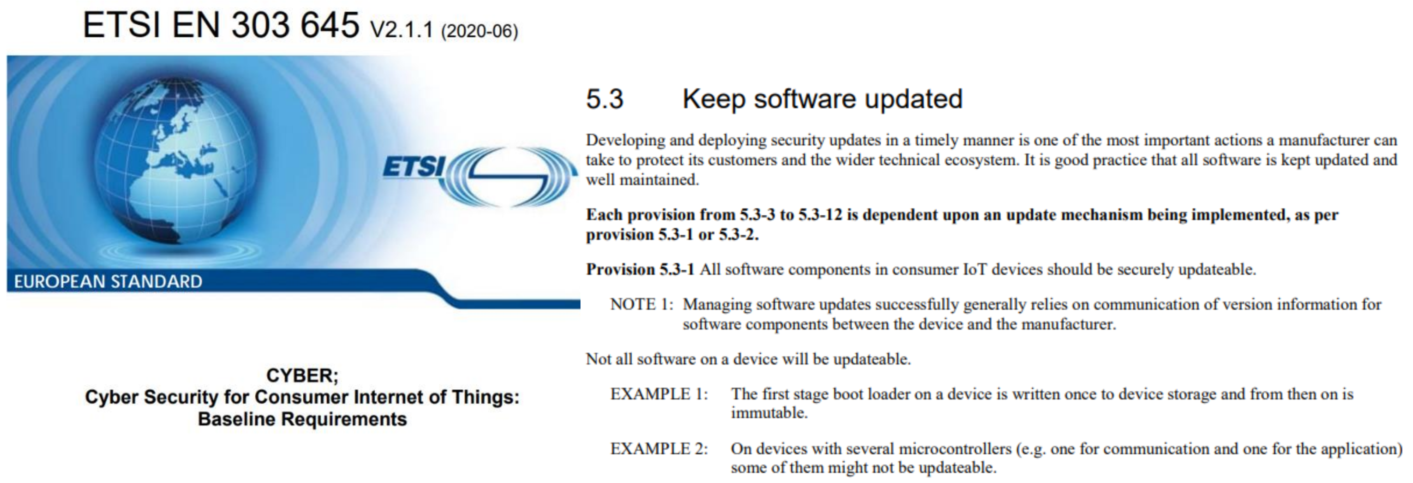
- Security activities that cover the product lifecycle
  - But attack methods continuously evolve

=> Product security measure effectiveness drops over time



Product Security Measure Effectiveness Drops Over Time

- Security updates mandated by standards such as ETSI EN303.645



ETSI EN 303 645 V2.1.1 (2020-06)

EUROPEAN STANDARD

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

5.3 Keep software updated

Developing and deploying security updates in a timely manner is one of the most important actions a manufacturer can take to protect its customers and the wider technical ecosystem. It is good practice that all software is kept updated and well maintained.

Each provision from 5.3-3 to 5.3-12 is dependent upon an update mechanism being implemented, as per provision 5.3-1 or 5.3-2.

Provision 5.3-1 All software components in consumer IoT devices should be securely updateable.

NOTE 1: Managing software updates successfully generally relies on communication of version information for software components between the device and the manufacturer.

Not all software on a device will be updateable.

EXAMPLE 1: The first stage boot loader on a device is written once to device storage and from then on is immutable.

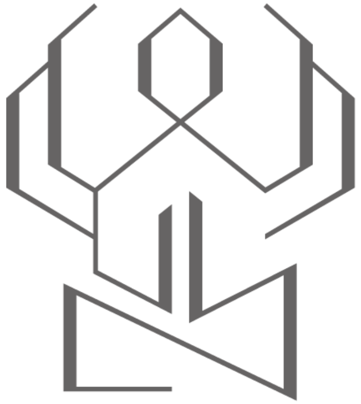
EXAMPLE 2: On devices with several microcontrollers (e.g. one for communication and one for the application) some of them might not be updateable.

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

ASTIRA

Panasonic IoT Threat Intelligence

What is ASTIRA?



阿修羅

ASURA ← Project feature like…

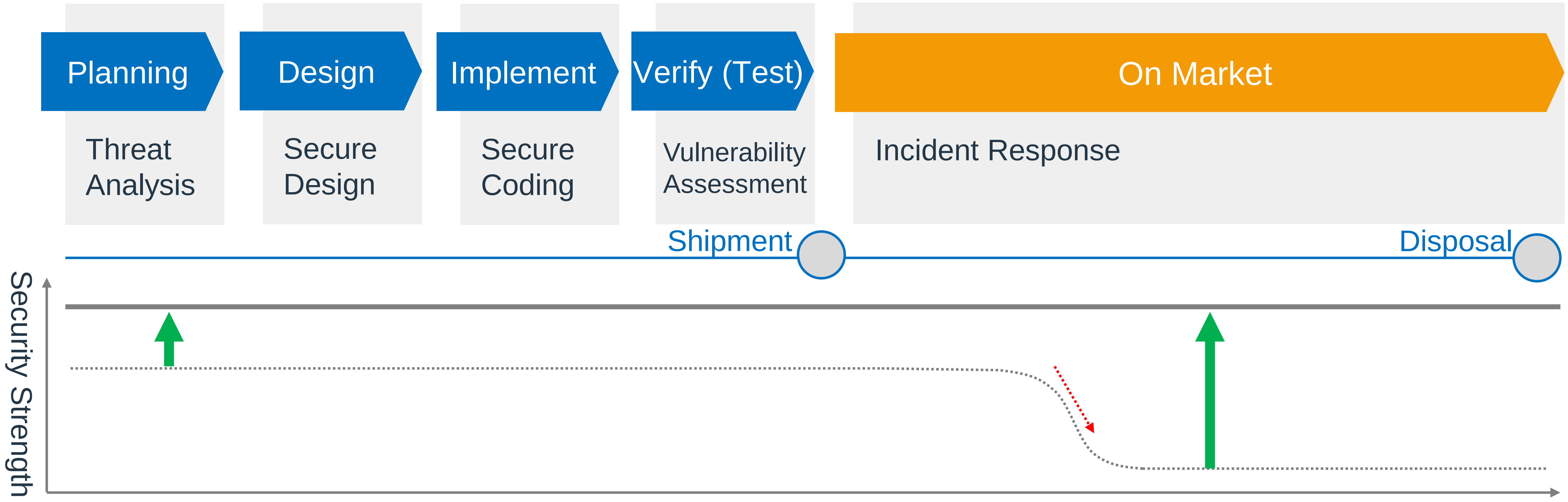
In Buddhism
having 3 heads, 6 eyes and 6 arms
and BATTLE

Capturing and analyzing
enormous amount of data day and night
to FIGHT cyber threats

+ TI ← Threat Intelligence

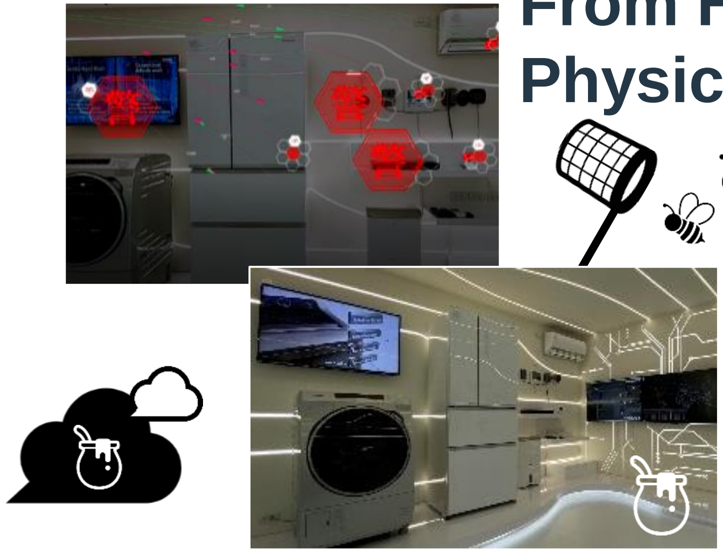
= ASTIRA

Motivations for ASTIRA



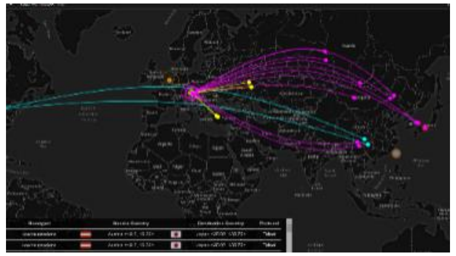
- Activities along the product lifecycle, from threat analysis to incident response for over 15 years.
- Attackers continue to make progress. The security level of the product decreases relative to the level of the product after shipment.
- Aim to continuously improve each security activity in the product lifecycle.

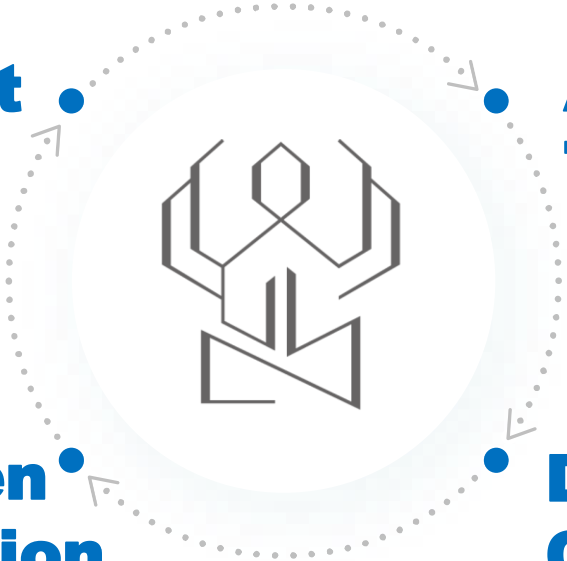
What does ASTIRA do?



From Honeypots in both Physical and Cyber space

Intelligence Platform





Collect Data

Analyze Threat

Develop / Take Countermeasures

Strengthen Organization

Visualize

From Insight to Strategy

To Quickly Alert Entire Group

To Share Results

for *BEFORE* shipment
To Establish DevSecOps

for *AFTER* shipment
To Ensure Service Phase Security

Statistical summary of data collected over 5 years

- Panasonic IoT devices installed as honeypots
- IoT devices are intentionally „loosely" configured to make them vulnerable to attacks
- Automated collection, static and dynamic analysis of IoT malware
- Data collection also performed on products under development that have not been released to the market

[Since November 2017]

Total Attacks	2,205,335,583
Malware	109,276
IoT Malware	32,015

MITRE ATT&CK analysis against some real devices

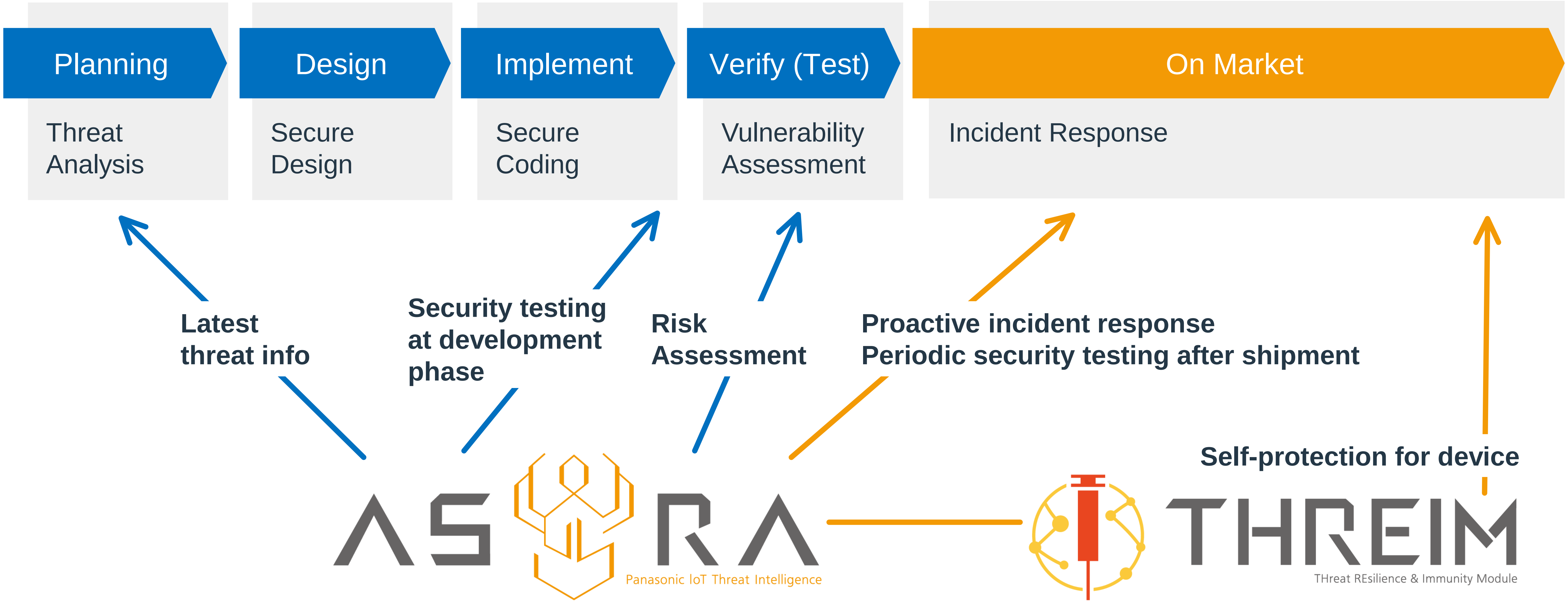
No	Tactics	Technique	Attacks	Cumulative relative frequency
1	Reconnaissance	Active Scanning, Gather Victim Network Information, Gather Victim Host Information, Gather Victim Identity Information	208,487	80.50%
2	Initial Access	Exploit Public-Facing Application, External Remote Services	50,354	99.94%
3	Execution	User Execution, Shared Modules	19	99.95%
4	Persistence	-	0	99.95%
5	Privilege Escalation	-	0	99.95%
6	Defense Evasion	Indicator Removal on Host	6	99.95%
7	Credential Access	-	0	99.95%
8	Discovery	Network Share Discovery, File and Directory Discovery, System Information Discovery	128	99.99%
9	Lateral Movement	-	0	99.99%
10	Collection	Data from Configuration Repository	4	100%
11	C&C	-	0	100%
12	Exfiltration	-	0	100%

Percentages are rounded to 2 decimal places

Collaborate with business units for risk feedback

No compromised devices have been observed so far

Improve each phase of product lifecycle



Planning

Threat Analysis

Design

Secure Design

Implement

Secure Coding

Verify (Test)

Vulnerability Assessment

On Market

Incident Response

Latest threat info

Security testing at development phase

Risk Assessment

Proactive incident response
Periodic security testing after shipment

Self-protection for device

ASTRA

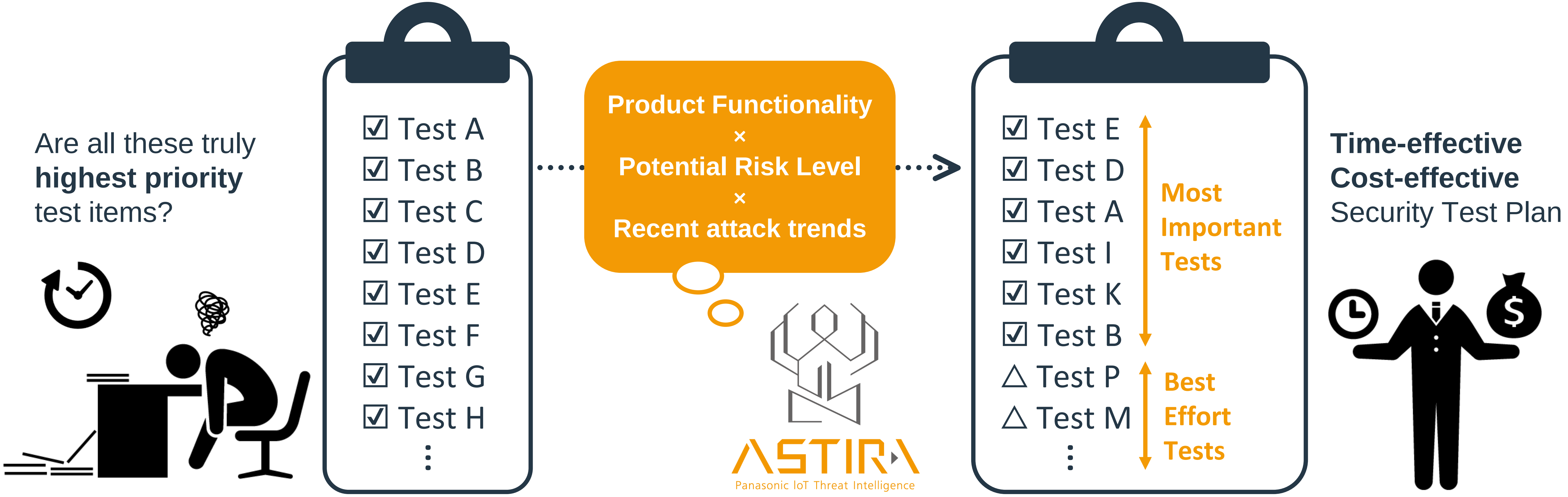
Panasonic IoT Threat Intelligence

THREIM

THreat REsilience & Immunity Module

Example of Product Lifecycle Enhancement Initiatives

Periodic security testing after shipment



Are all these truly **highest priority** test items?

☑ Test A
☑ Test B
☑ Test C
☑ Test D
☑ Test E
☑ Test F
☑ Test G
☑ Test H
⋮

Product Functionality
×
Potential Risk Level
×
Recent attack trends

☑ Test E
☑ Test D
☑ Test A
☑ Test I
☑ Test K
☑ Test B
△ Test P
△ Test M
⋮

Most Important Tests

Best Effort Tests

Time-effective
Cost-effective
Security Test Plan

IoT-specialized self-protection module

THREIM

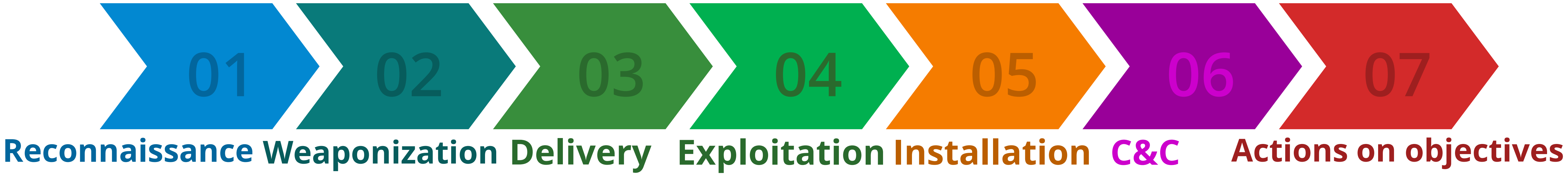
THreat REsilience & Immunity Module

THreat REsilience & Immunity Module

for IoT device

Preventing a device from being taken over and abused

Cyber Kill Chain (The framework developed by Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)



01 Reconnaissance

02 Weaponization

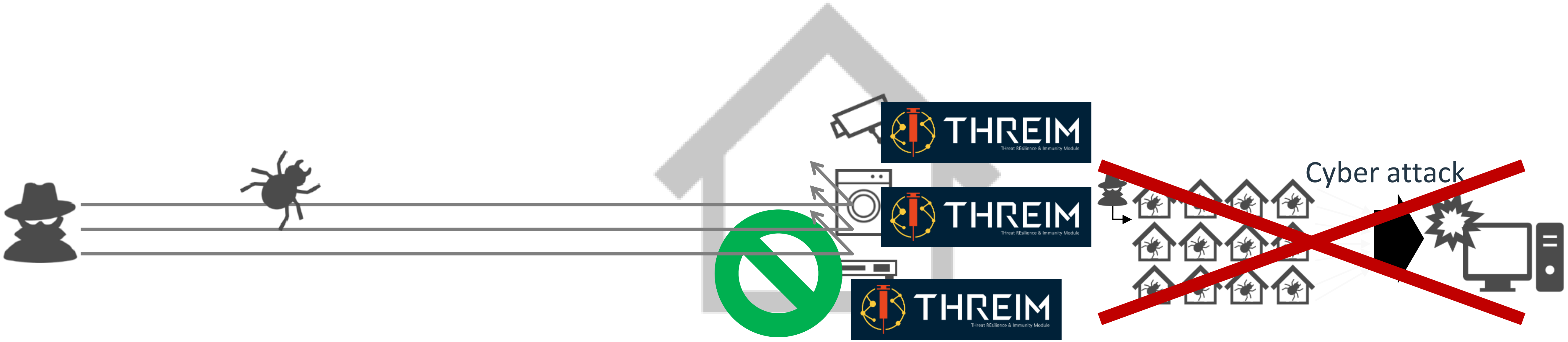
03 Delivery

04 Exploitation

05 Installation

06 C&C

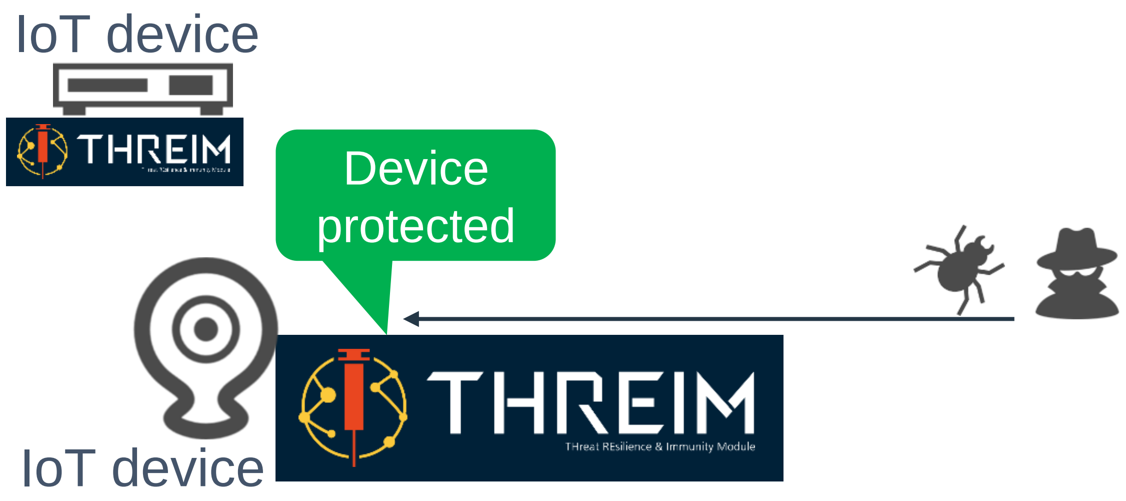
07 Actions on objectives


THREIM
Threat REsilience & Immunity Module
THREIM
Threat REsilience & Immunity Module
THREIM
Threat REsilience & Immunity Module
Cyber attack

THREIM key features

- Built-in anti-malware with no required installation by a user
- Lightweight and minimum operational impact to an IoT product
- Linux based IoT device supported

- Capable to enhance device's security
  - Mitigation until firmware update is applied



IoT device

THREIM

Device protected

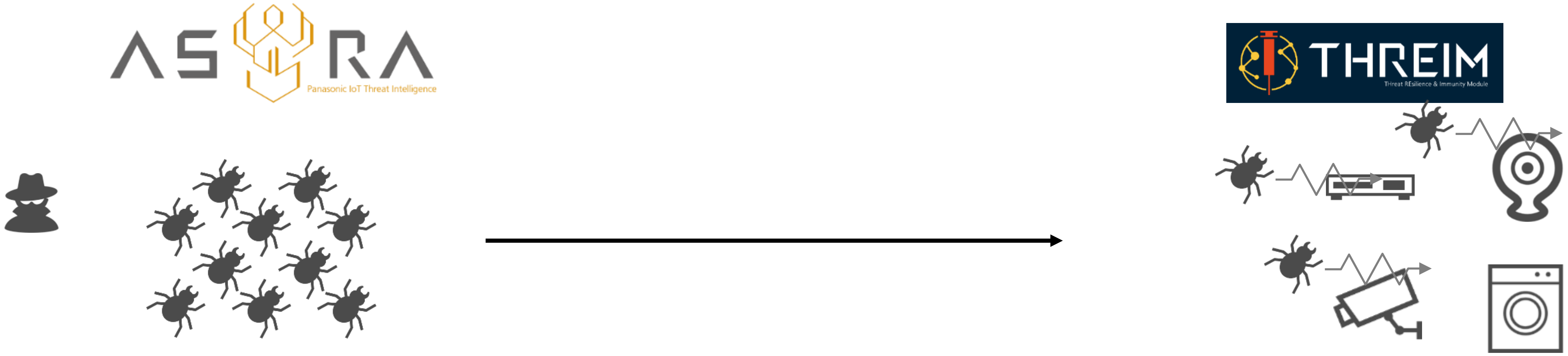
IoT device

THREIM

THreat REsilience & Immunity Module

Strategy of how to evaluate THREIM’s performance

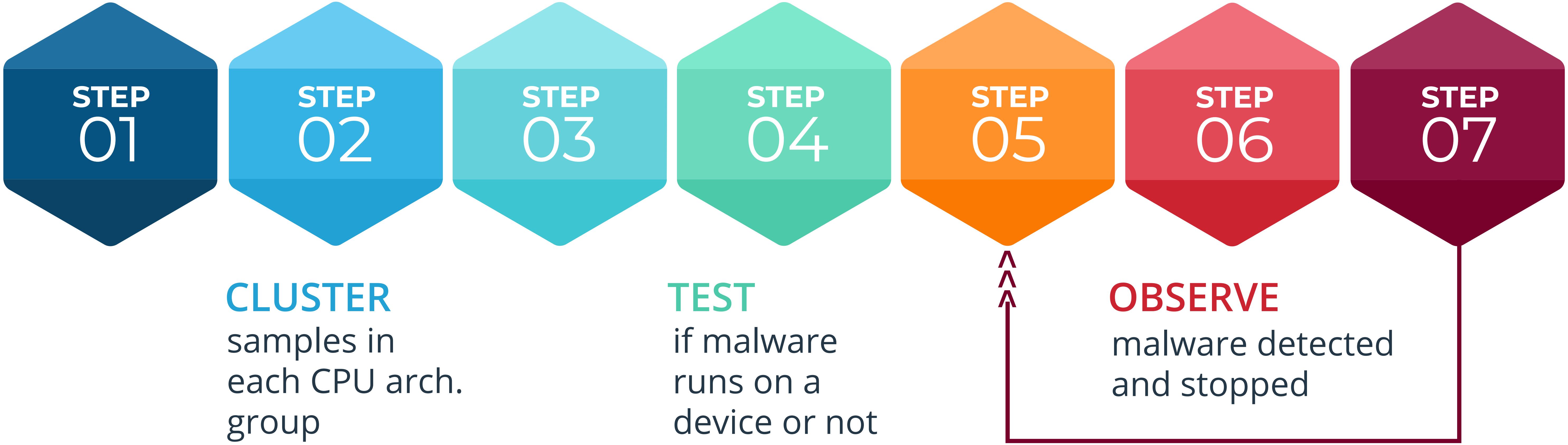
- Using all malware collected by ASTIRA
- Put malware inside IoT products and run it


ASTIRA
Panasonic IoT Threat Intelligence
THREIM
THreat REsilience & Immunity Module

Over 30,000 samples of IoT malware

Run IoT malware inside devices

Evaluation flow



STEP 01 – LIST all malware based on CPU architecture

STEP 02 – CLUSTER samples in each CPU arch. group

STEP 03 – PICK samples from clustered malware

STEP 04 – TEST if malware runs on a device or not

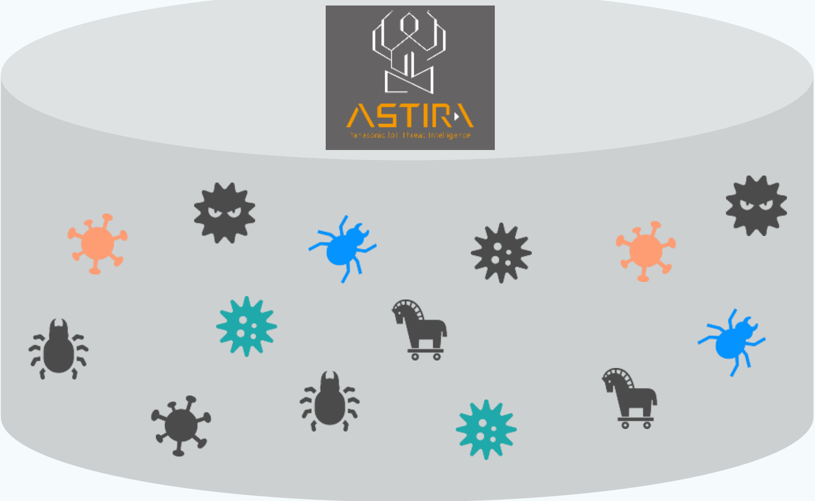
STEP 05 – RUN malware on a device

STEP 06 – OBSERVE malware detected and stopped

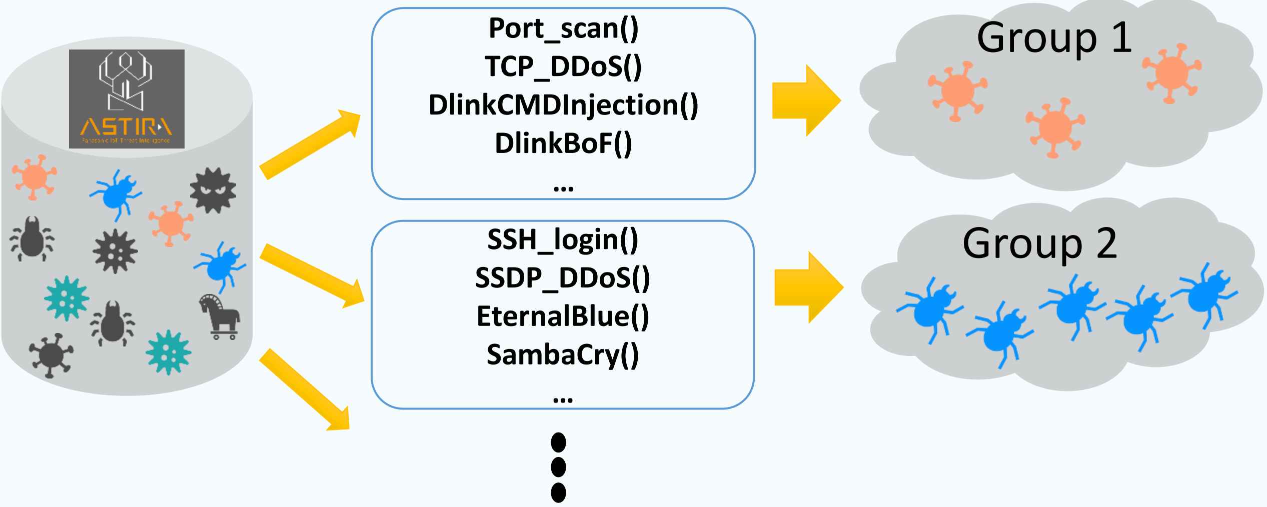
STEP 07 – INITIALIZE a device for next test

Clustering and sampling of malware for efficiency

01 More than 30,000 IoT malware collected



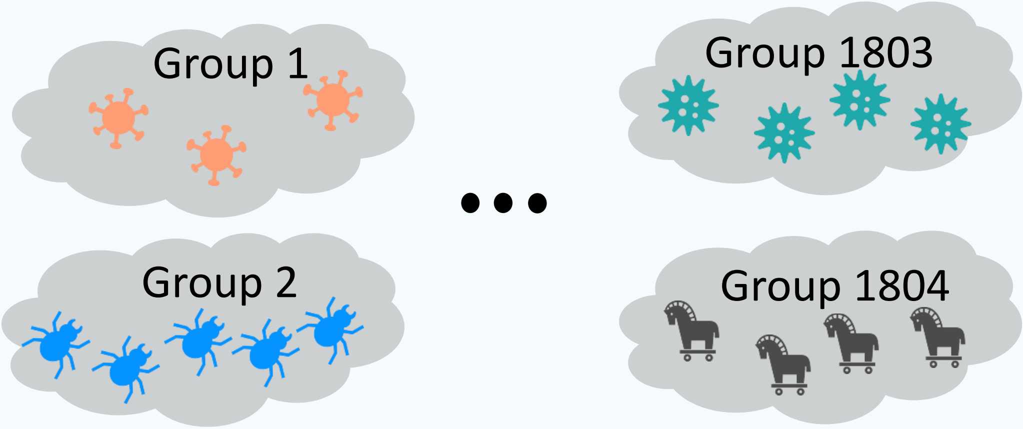
02 Similar malware are classified into the same group



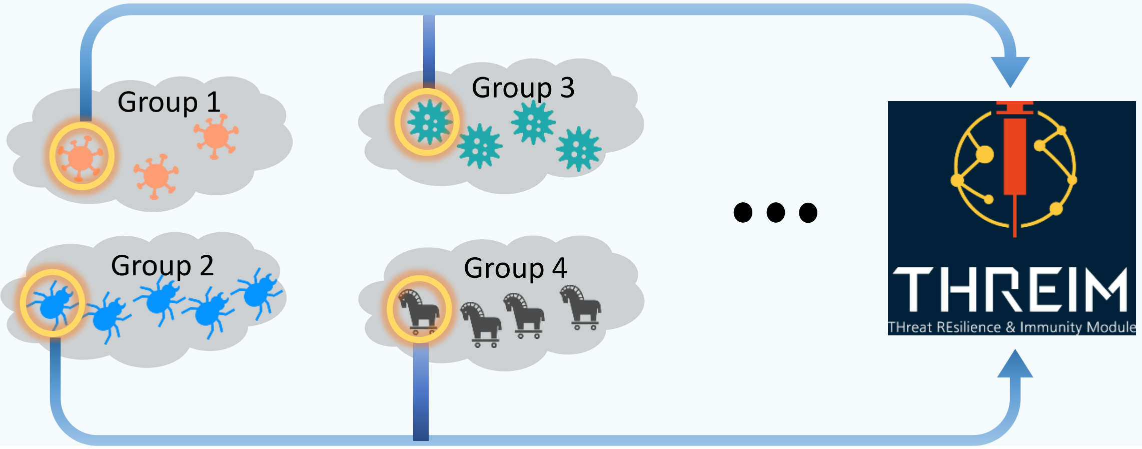
Port_scan()
TCP_DDoS()
DlinkCMDInjection()
DlinkBoF()
…

SSH_login()
SSDP_DDoS()
EternalBlue()
SambaCry()
…

03 Classification result
e.g. ARM: 1,804 groups

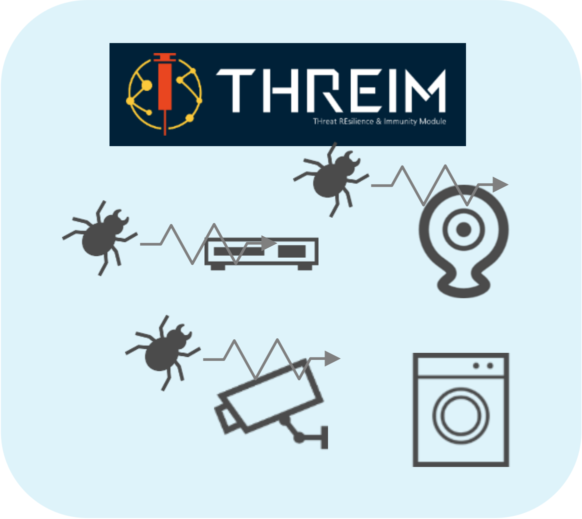


04 Pick a sample from each group

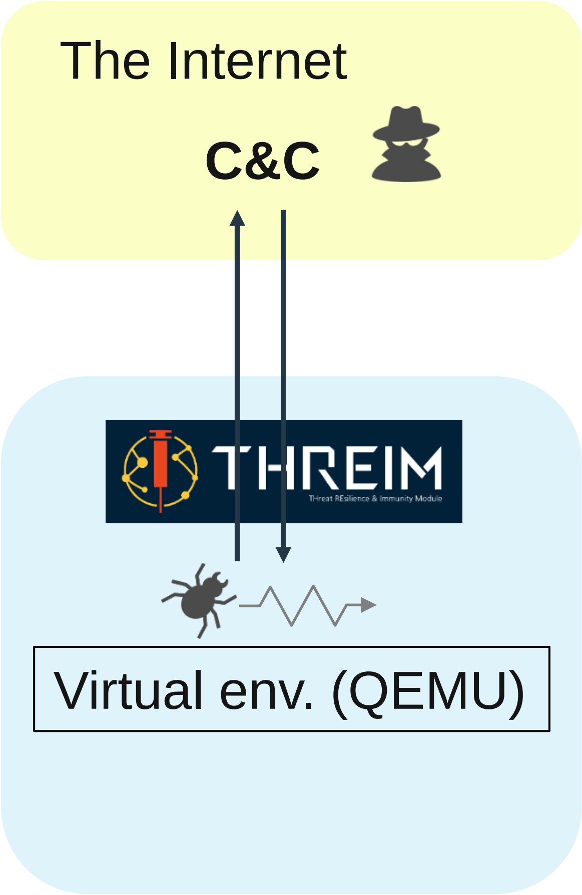


Environment setup

- IoT devices in an isolated network
  - To avoid unnecessary trouble with development environment
- Virtual environment with the Internet
  - For additional evaluation because most malware connect to a C&C via the Internet



Evaluation on real devices
Isolated network



Additional evaluation on virtual env.
With the Internet

Evaluation results

- Maximum 86.1% of samples detected
- About half of samples ran on a device and the other half failed to run
- No big impact on resource consumption of device

Product	CPU	Detection rate	Malware ran on device	Malware tested (total)	CPU usage increased	Mem usage increased
Device A	ARM	**86.1%**	275	1804	+0.3%	+0.9%
Device B	ARM	57.7%	759	1804	+3.2%	+0.1%
Device C	MIPS	66.1%	348	689	+5%	+0.7%
Device D	AMD64	59.5%	742	1102	+2.1%	+0.1%

Notes: Excluded cases that a C2 server was not alive from detection rate calculation.
CPU and Memory usage compared between when THREIM was enabled and disabled.

The project achievements were made possible with the steady collaboration by the business units

Developers from business unit must be involved

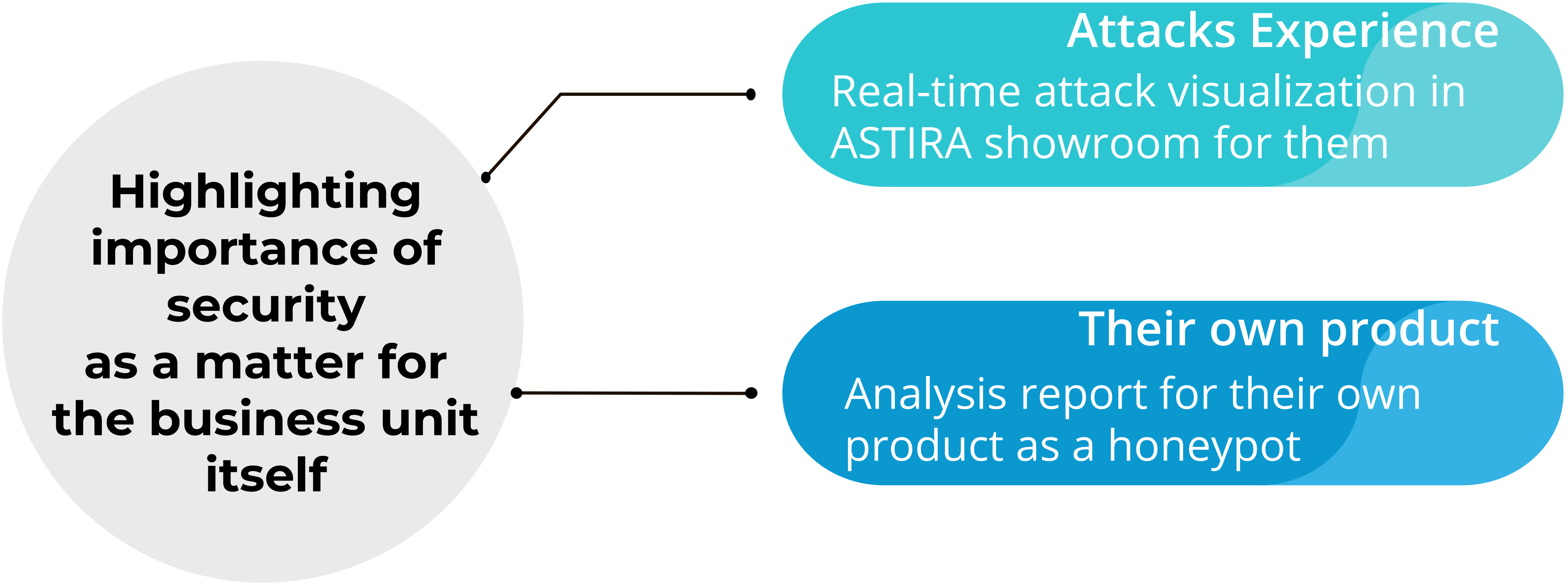
- IoT device is specially customized for each product
  - Unique knowledge is necessary to understand inside, even though Linux-based system

- Functions such as login shell is removed from products on market to prevent abuse
  - We cannot independently install THREIM or run malware inside a device

- Product's functionality is most important, which must not be interrupted
  - Showing TV program, playing music and video, refrigerate, air conditioning, etc.
  - Need to understand how these functionalities are implemented to keep them running properly

Key to successful collaboration 1/2

- The first step is the business unit gain an understanding on the importance of product security
  - Because security such as anti-malware is not popular in IoT devices yet



Highlighting importance of security as a matter for the business unit itself

Attacks Experience

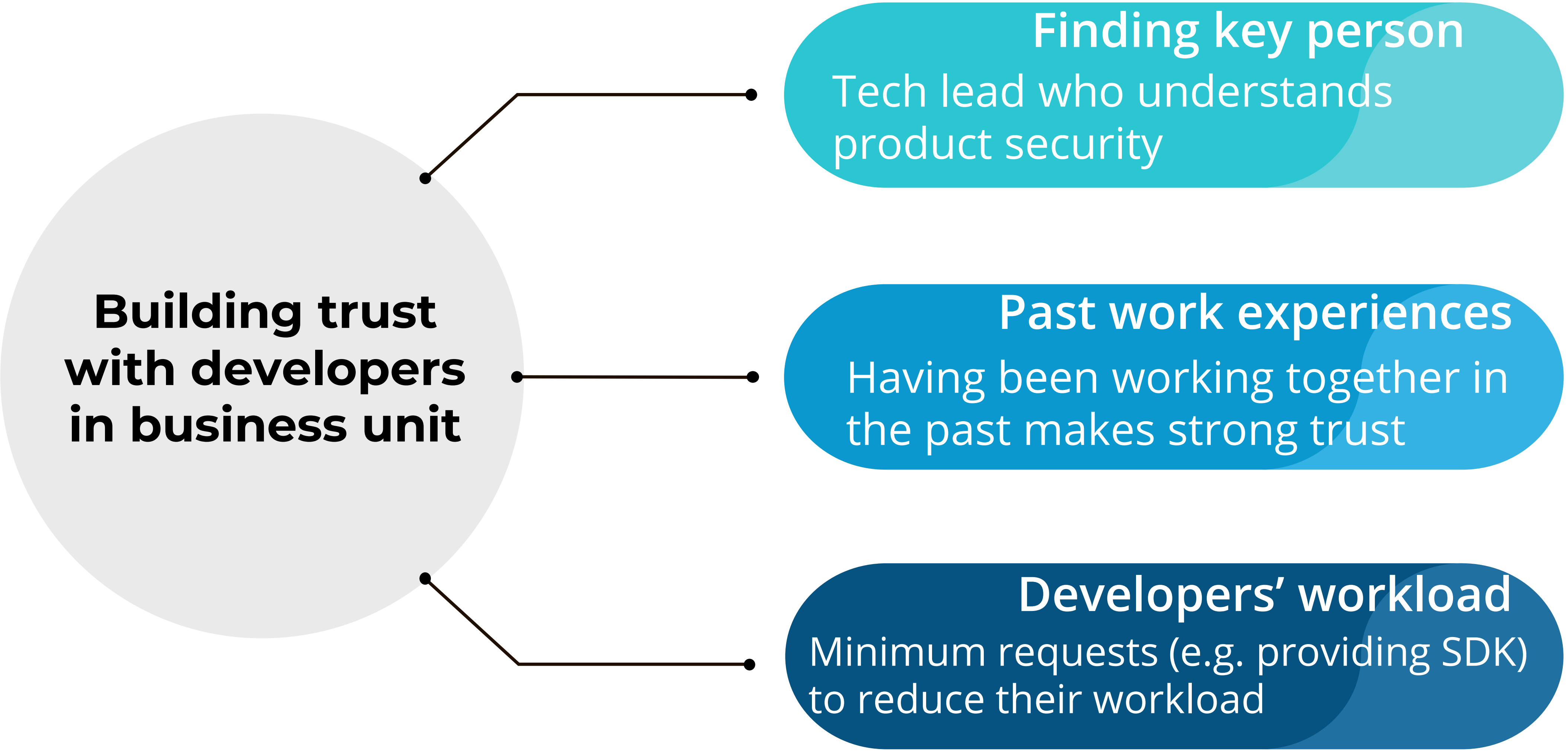
Real-time attack visualization in ASTIRA showroom for them

Their own product

Analysis report for their own product as a honeypot

Key to successful collaboration 2/2

- Trust relationship before engaging and during the collaboration



Building trust with developers in business unit

Finding key person
Tech lead who understands product security

Past work experiences
Having been working together in the past makes strong trust

Developers' workload
Minimum requests (e.g. providing SDK) to reduce their workload

Why manufacturer implements by itself?

Enabled upon powering on

- Self-protection in products need to be implemented in a product before its shipment

Highly trusted partner for BU

- May need to share products' confidential information and know-how
- Prefer not to pay license fee outside the company

Controlled by ourselves

- Achieving perfect security is not necessarily the correct answer
- Need to consider suitable security levels for both industry and our own business

Summary and further discussion

What’s “reasonable” security?

All of us already understand the importance of product security

On the other hand, however, nobody can ensure “perfect” security...

Will there be “reasonable” security for IoT products required in the future?

“Reasonable” from the point of view of stakeholders

Manufacturers

Focus here

- Comply with laws / Certified to standards
- Reduce the risks caused by vulnerabilities
- Accountable explanations to users
- Cost of product security

Users

- A product can be used without concern
- Minimal user effort required

Governments / Auditors

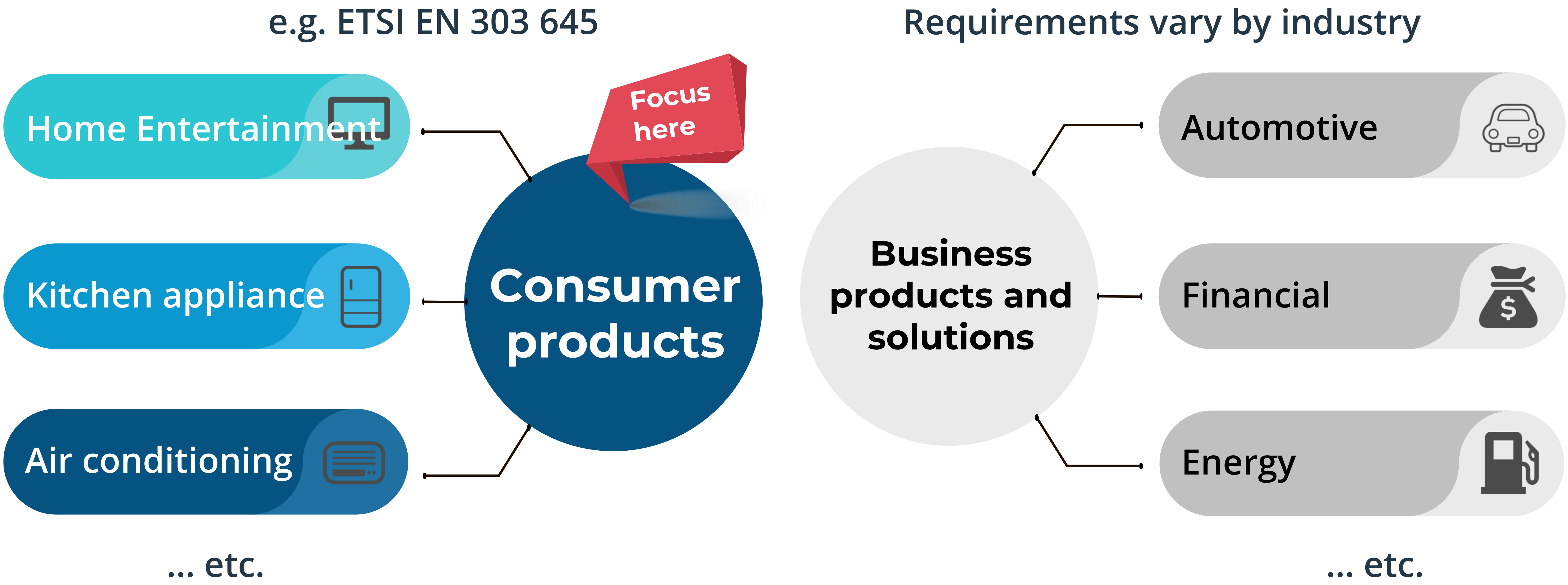
- Establish laws and enforce compliance
- Compliance testing by audit agencies

Researchers / Academia

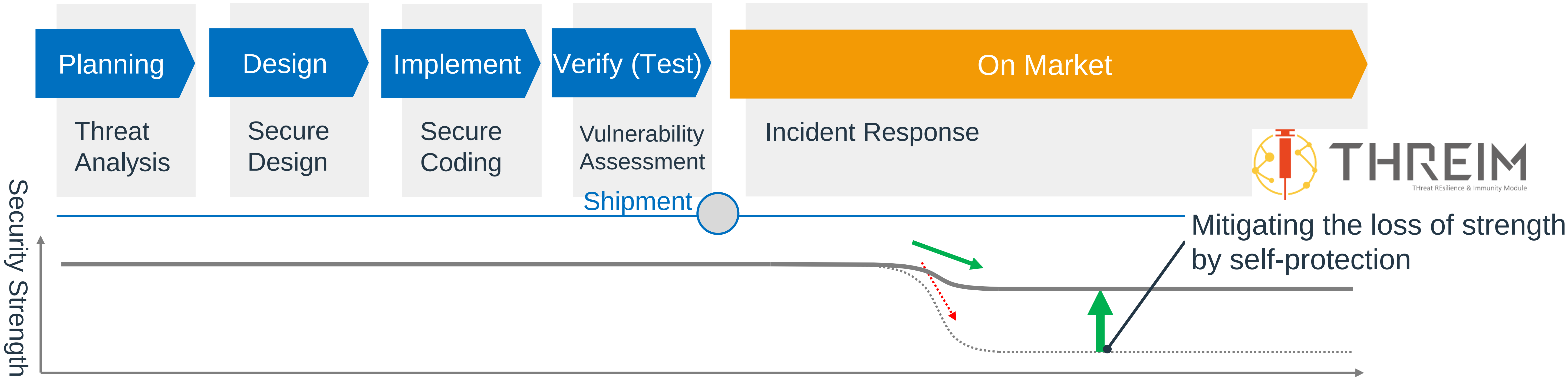
- Protected against all potential threats in theory

(Cost-effectiveness and feasibility may not be a consideration)

Industry requirements



Could self-protection be a “reasonable” option?



1st Priority

Firmware update is the best option

… but not always possible

2nd Priority

Self-protection as a “reasonable” option

Takeaways

- Efforts to continuously improve product security are required for manufacturers
  - Incorporating threat data and its analysis into phases of product lifecycles
  - Self-protection capability of IoT device is proposed to reduce risks after product shipment
- Insights on why and how manufacturers can improve their product security
  - Key is collaboration effort between product security division and business units
  - Carefully consider and control their product security levels
- Potential ideas for industry to better define “reasonable” product security
  - Self-protection as an example for consumer products from manufacturer’s perspective
  - But still need further discussion in each industry

AS
RA
Panasonic IoT Threat Intelligence

THREIM
THreat REsilience & Immunity Module