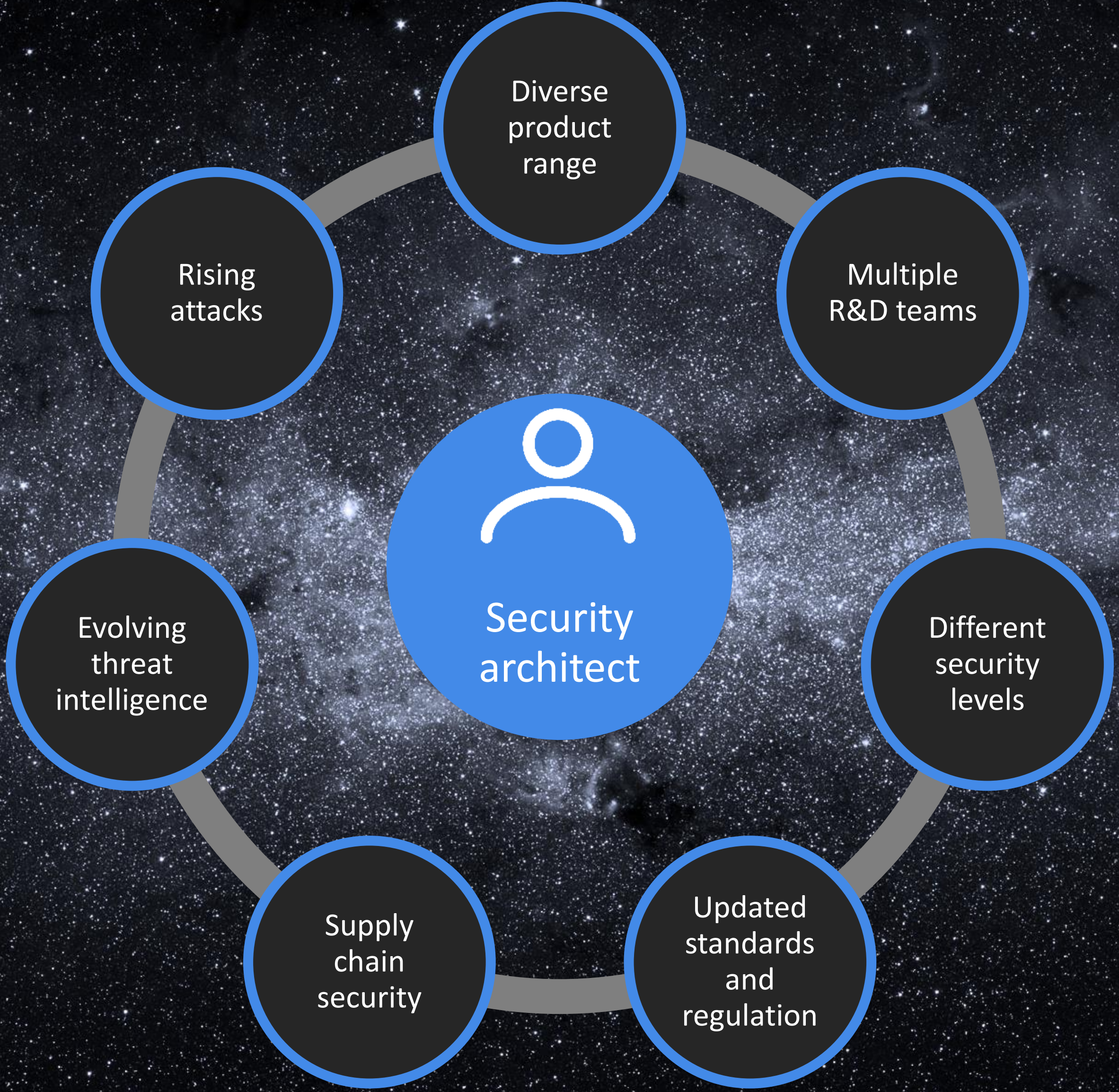
VDOO

SCALING UP IOT SECURITY

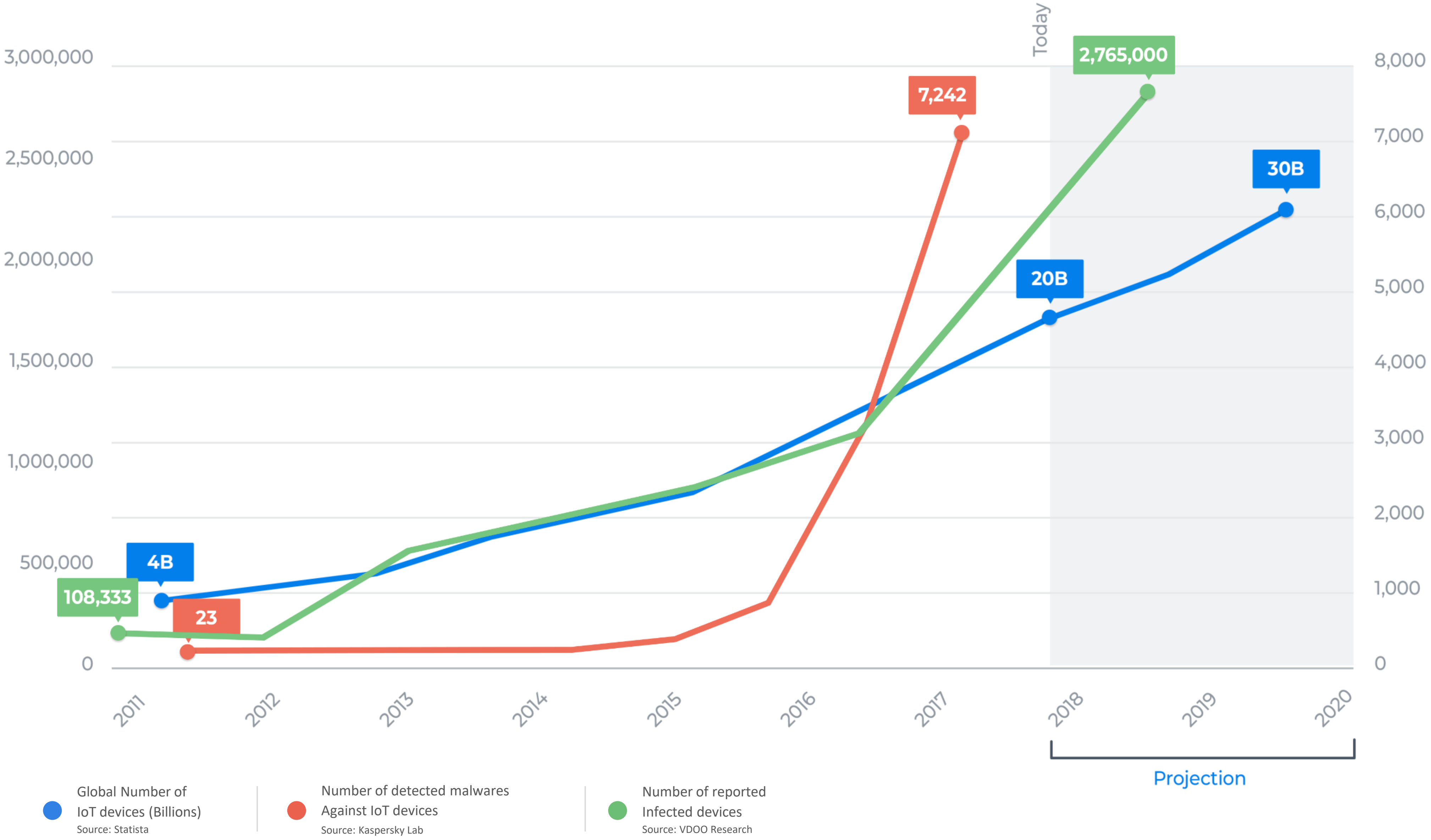
IoT Security Foundation Conference December 2018

Leo Dorrendorf

The challenges of IoT security architecture



Rising attacks on IoT



Our research

3,737

Auto-analyzed IoT embedded systems

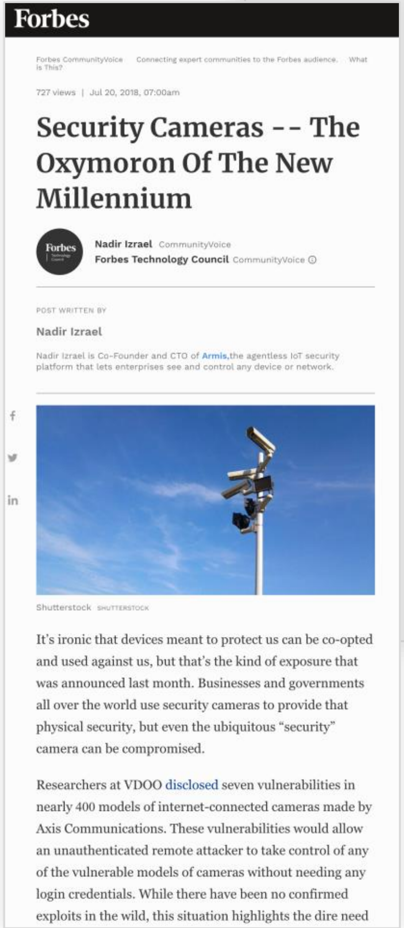
162,151

Aggregated IoT vulnerabilities

50

0-day vulnerabilities

The state of IoT security



Forbes

Forbes CommunityVoice Connecting expert communities to the Forbes audience. What is This?

727 views | Jul 20, 2018, 07:00am

Security Cameras -- The Oxymoron Of The New Millennium

Nadir Izrael CommunityVoice
Forbes Technology Council CommunityVoice

POST WRITTEN BY

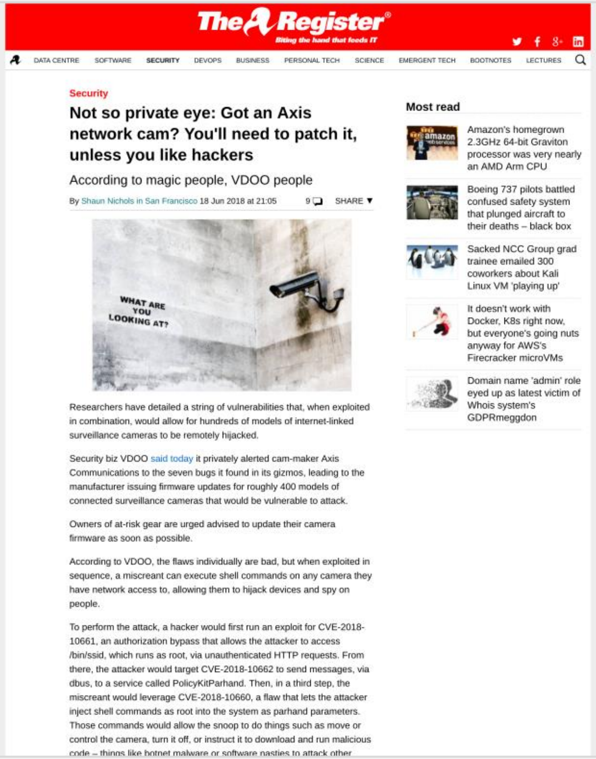
Nadir Izrael

Nadir Izrael is Co-Founder and CTO of Armis,the agentless IoT security platform that lets enterprises see and control any device or network.

Shutterstock SHUTTERSTOCK

It's ironic that devices meant to protect us can be co-opted and used against us, but that's the kind of exposure that was announced last month. Businesses and governments all over the world use security cameras to provide that physical security, but even the ubiquitous "security" camera can be compromised.

Researchers at VDOO disclosed seven vulnerabilities in nearly 400 models of internet-connected cameras made by Axis Communications. These vulnerabilities would allow an unauthenticated remote attacker to take control of any of the vulnerable models of cameras without needing any login credentials. While there have been no confirmed exploits in the wild, this situation highlights the dire need



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Security

Not so private eye: Got an Axis network cam? You'll need to patch it, unless you like hackers

According to magic people, VDOO people

By Shaun Nichols in San Francisco 18 Jun 2018 at 21:05 9 SHARE ▼

Researchers have detailed a string of vulnerabilities that, when exploited in combination, would allow for hundreds of models of internet-linked surveillance cameras to be remotely hijacked.

Security biz VDOO said today it privately alerted cam-maker Axis Communications to the seven bugs it found in its gizmos, leading to the manufacturer issuing firmware updates for roughly 400 models of connected surveillance cameras that would be vulnerable to attack.

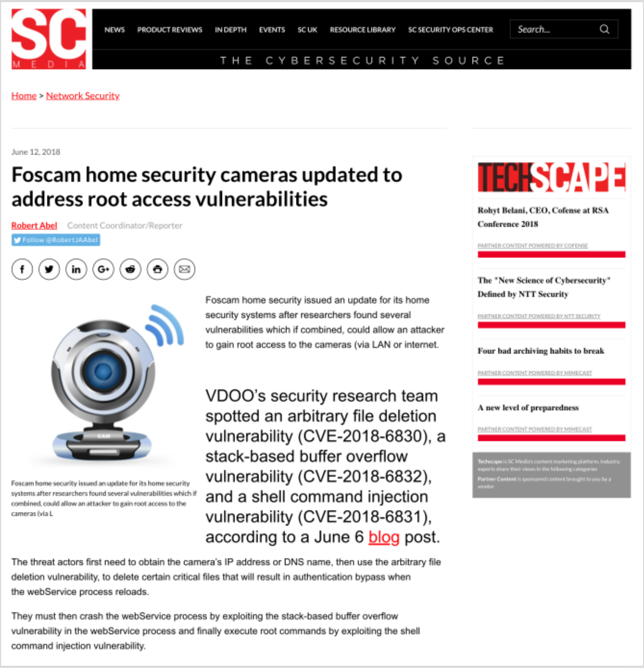
Owners of at-risk gear are urged advised to update their camera firmware as soon as possible.

According to VDOO, the flaws individually are bad, but when exploited in sequence, a miscreant can execute shell commands on any camera they have network access to, allowing them to hijack devices and spy on people.

To perform the attack, a hacker would first run an exploit for CVE-2018-10661, an authorization bypass that allows the attacker to access /bin/ssid, which runs as root, via unauthenticated HTTP requests. From there, the attacker would target CVE-2018-10662 to send messages, via dbus, to a service called PolicyKitParhand. Then, in a third step, the miscreant would leverage CVE-2018-10660, a flaw that lets the attacker inject shell commands as root into the system as parhand parameters. Those commands would allow the snoop to do things such as move or control the camera, turn it off, or instruct it to download and run malicious code – things like botnet malware or software nasties to attack other

Most read

- Amazon's homegrown 2.3GHz 64-bit Graviton processor was very nearly an AMD Arm CPU
- Boeing 737 pilots battled confused safety system that plunged aircraft to their deaths – black box
- Sacked NCC Group grad trainee emailed 300 coworkers about Kali Linux VM 'playing up'
- It doesn't work with Docker, K8s right now, but everyone's going nuts anyway for AWS's Firecracker microVMs
- Domain name 'admin' role eyed up as latest victim of Whois system's GDPRmeggdon



SC MEDIA

NEWS PRODUCT REVIEWS IN DEPTH EVENTS SC UK RESOURCE LIBRARY SC SECURITY OPS CENTER Search...

THE CYBERSECURITY SOURCE

Home > Network Security

June 12, 2018

Foscam home security cameras updated to address root access vulnerabilities

Robert Abel Content Coordinator/Reporter
Follow @RobertJAAbel

Foscam home security issued an update for its home security systems after researchers found several vulnerabilities which if combined, could allow an attacker to gain root access to the cameras (via LAN or internet.

Foscam home security issued an update for its home security systems after researchers found several vulnerabilities which if combined, could allow an attacker to gain root access to the cameras (via L

VDOO's security research team spotted an arbitrary file deletion vulnerability (CVE-2018-6830), a stack-based buffer overflow vulnerability (CVE-2018-6832), and a shell command injection vulnerability (CVE-2018-6831), according to a June 6 blog post.

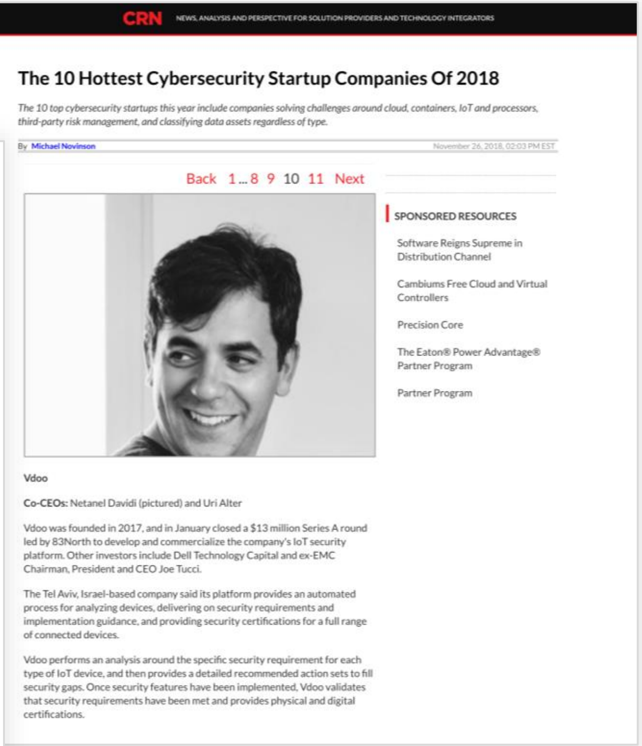
The threat actors first need to obtain the camera's IP address or DNS name, then use the arbitrary file deletion vulnerability, to delete certain critical files that will result in authentication bypass when the webService process reloads.

They must then crash the webService process by exploiting the stack-based buffer overflow vulnerability in the webService process and finally execute root commands by exploiting the shell command injection vulnerability.

TECHSCAPE

- Rohyt Belani, CEO, Cofense at RSA Conference 2018
  PARTNER CONTENT POWERED BY COFENSE
- The "New Science of Cybersecurity" Defined by NTT Security
  PARTNER CONTENT POWERED BY NTT SECURITY
- Four bad archiving habits to break
  PARTNER CONTENT POWERED BY MIMECAST
- A new level of preparedness
  PARTNER CONTENT POWERED BY MIMECAST

Techscape is SC Media's content marketing platform. Industry experts share their views in the following categories
Partner Content is sponsored content brought to you by a vendor



CRN NEWS, ANALYSIS AND PERSPECTIVE FOR SOLUTION PROVIDERS AND TECHNOLOGY INTEGRATORS

The 10 Hottest Cybersecurity Startup Companies Of 2018

The 10 top cybersecurity startups this year include companies solving challenges around cloud, containers, IoT and processors, third-party risk management, and classifying data assets regardless of type.

By Michael Novinson November 26, 2018, 02:03 PM EST

Back 1 ... 8 9 10 11 Next

Vdoo

Co-CEOs: Netanel Davidi (pictured) and Uri Alter

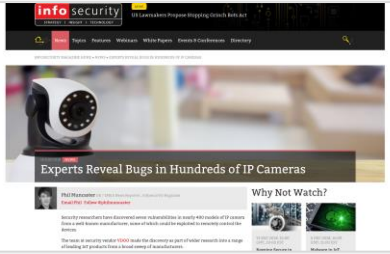
Vdoo was founded in 2017, and in January closed a $13 million Series A round led by 83North to develop and commercialize the company's IoT security platform. Other investors include Dell Technology Capital and ex-EMC Chairman, President and CEO Joe Tucci.

The Tel Aviv, Israel-based company said its platform provides an automated process for analyzing devices, delivering on security requirements and implementation guidance, and providing security certifications for a full range of connected devices.

Vdoo performs an analysis around the specific security requirement for each type of IoT device, and then provides a detailed recommended action sets to fill security gaps. Once security features have been implemented, Vdoo validates that security requirements have been met and provides physical and digital certifications.

SPONSORED RESOURCES

- Software Reigns Supreme in Distribution Channel
- Cambiums Free Cloud and Virtual Controllers
- Precision Core
- The Eaton® Power Advantage® Partner Program
- Partner Program



info security STRATEGY | INSIGHT | TECHNOLOGY

US Lawmakers Propose Stopping Grinch Bots Act

News Topics Features Webinars White Papers Events & Conferences Directory

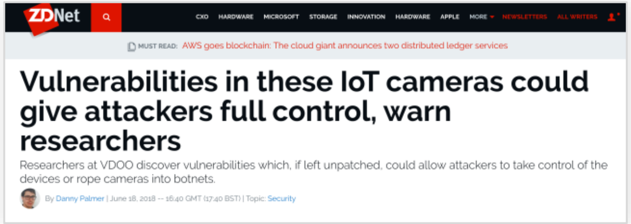
Experts Reveal Bugs in Hundreds of IP Cameras

Phil Muncaster

Security researchers have discovered seven vulnerabilities in nearly 400 models of IP camera from a well-known manufacturer, some of which could be exploited to remotely control the devices.

The team at security vendor VDOO made the discovery as part of wider research into a range of leading IoT products from a broad sweep of manufacturers.

Why Not Watch?



ZDNet

CXO HARDWARE MICROSOFT STORAGE INNOVATION HARDWARE APPLE MORE NEWSLETTERS ALL WRITERS

MUST READ: AWS goes blockchain: The cloud giant announces two distributed ledger services

Vulnerabilities in these IoT cameras could give attackers full control, warn researchers

Researchers at VDOO discover vulnerabilities which, if left unpatched, could allow attackers to take control of the devices or rope cameras into botnets.

By Danny Palmer | June 18, 2018 -- 16:40 GMT (17:40 BST) | Topic: Security

The problems with the manual approach

Quick ✗

Scalable ✗

Reusable ✗

Standardized ✗

The advantages of the automated approach

Quick

✓

Scalable

✓

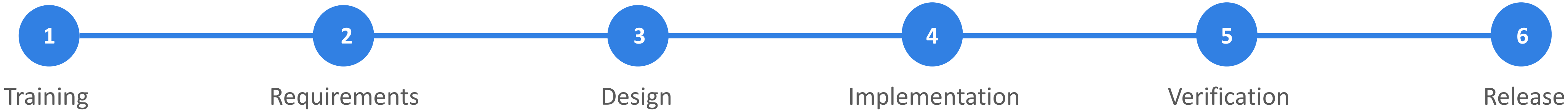
Reusable

✓

Standardized

✓

The IoT security process



1 Training

2 Requirements

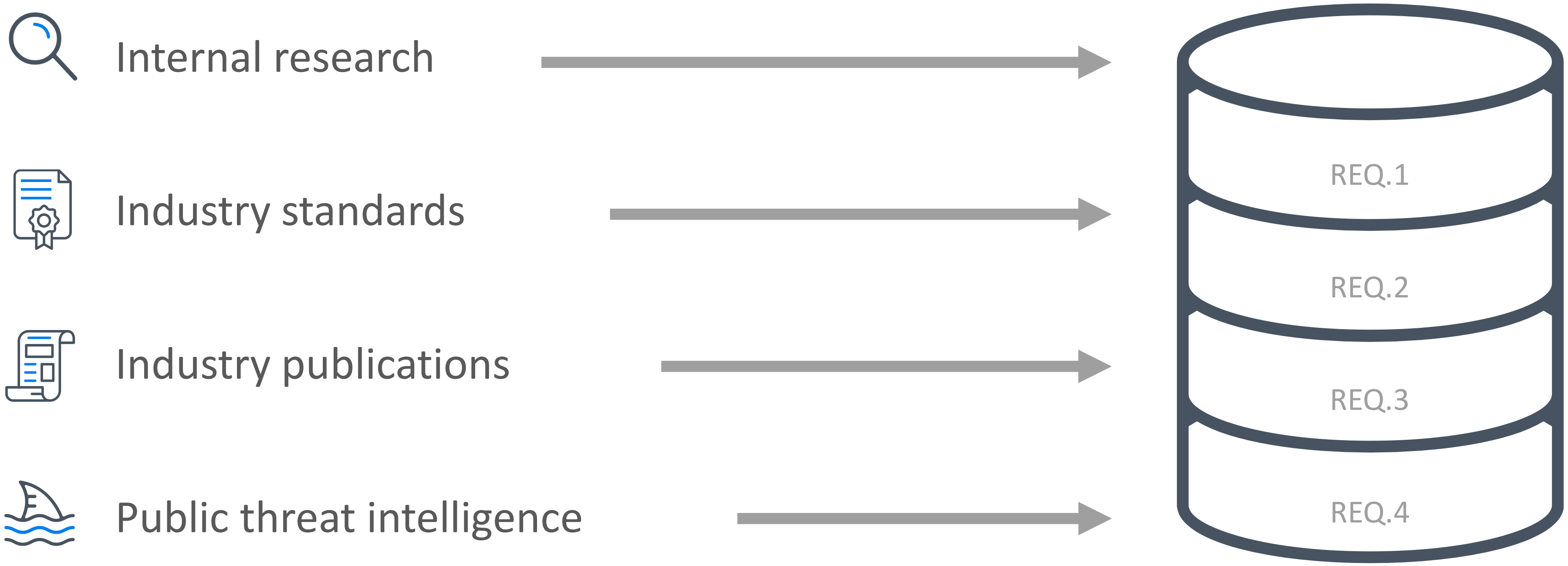
3 Design

4 Implementation

5 Verification

6 Release

Creating a requirements database



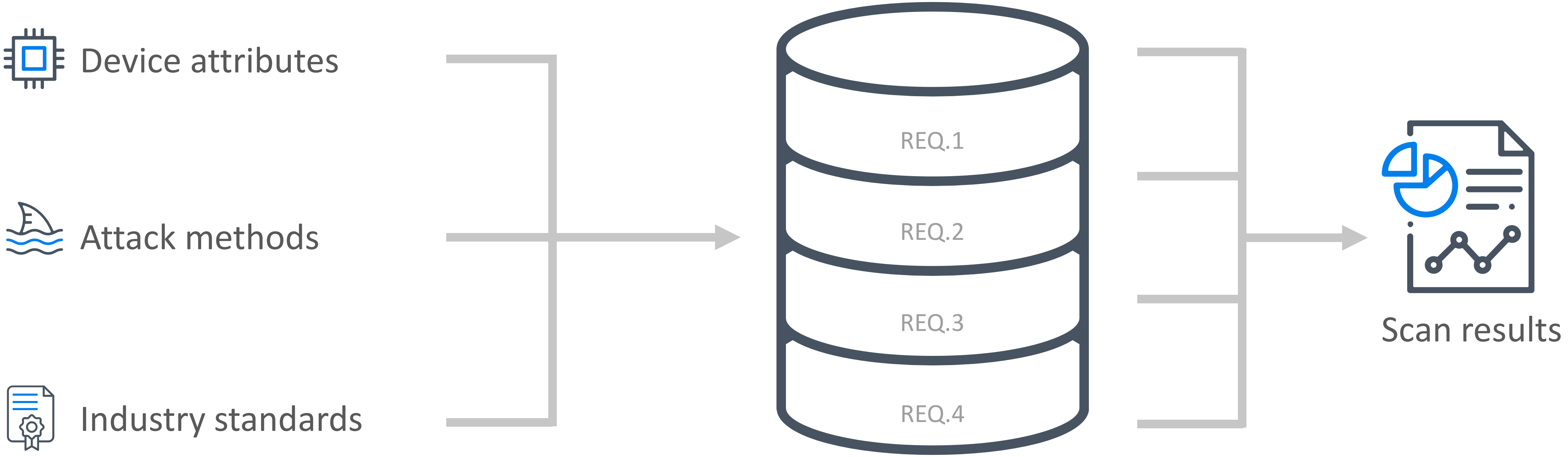
Internal research

Industry standards

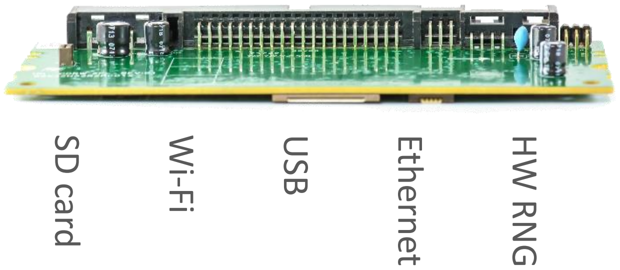
Industry publications

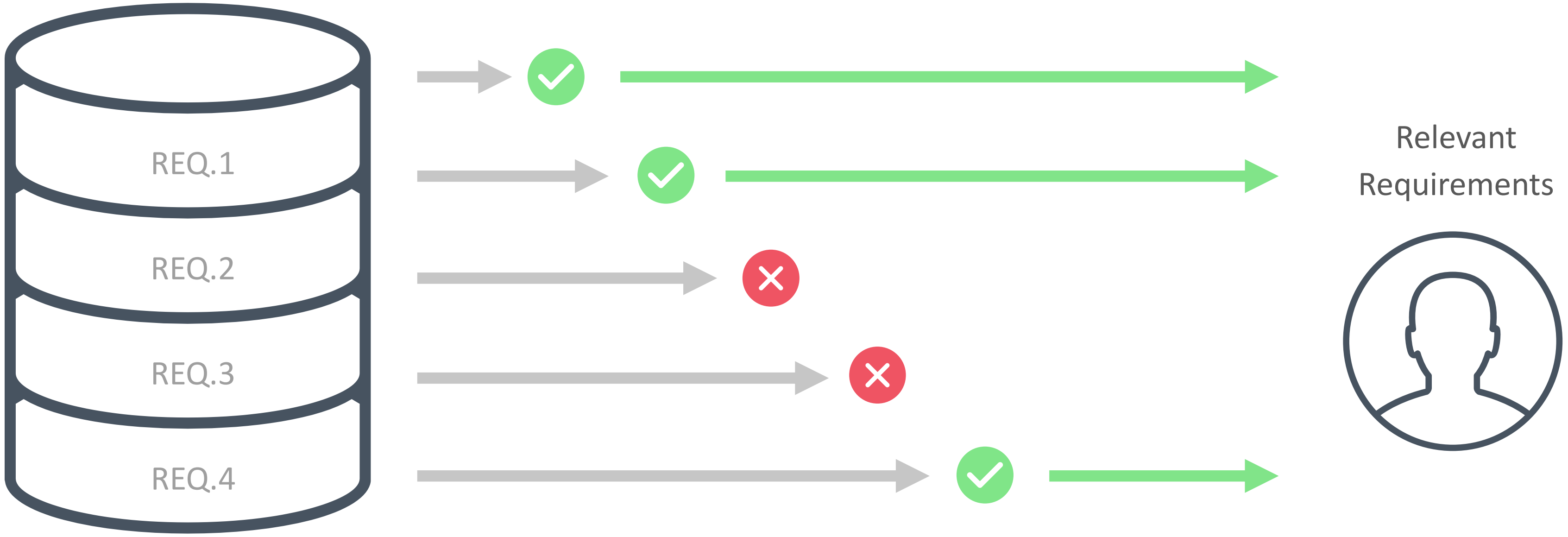
Public threat intelligence

Linking related objects

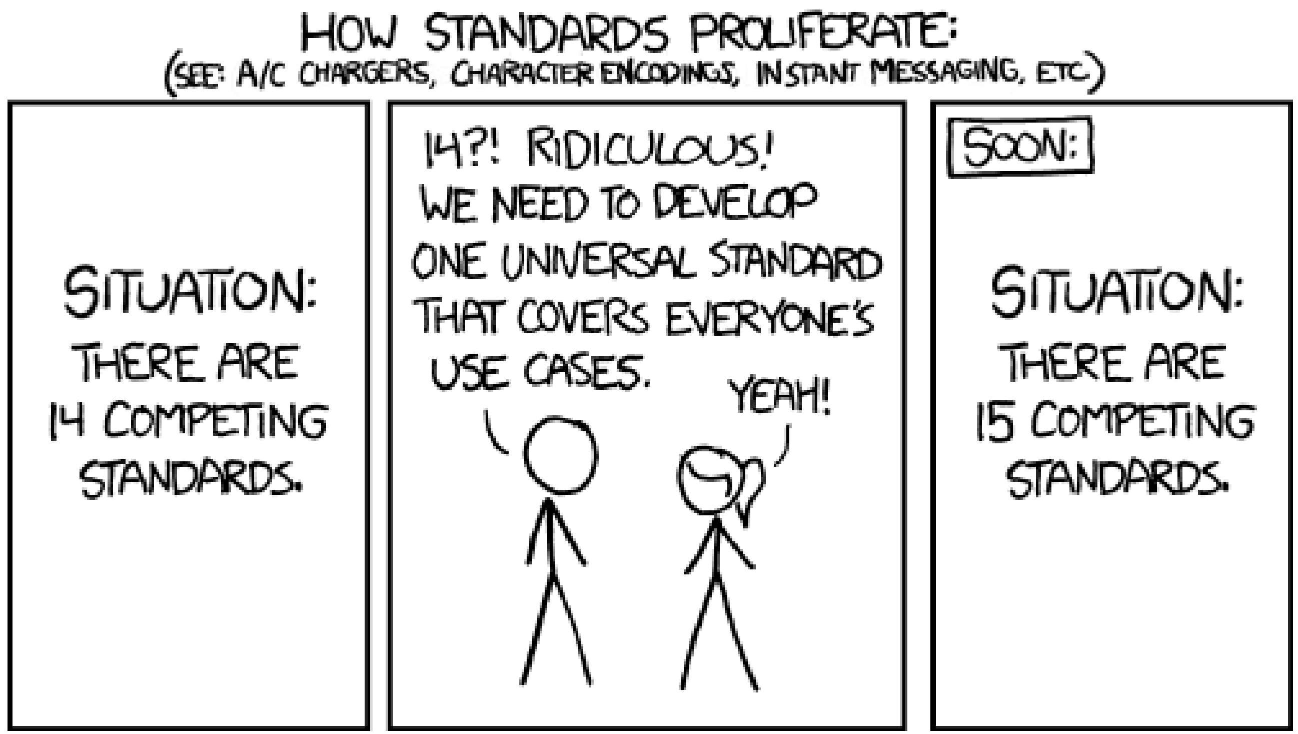


Filtering relevant requirements





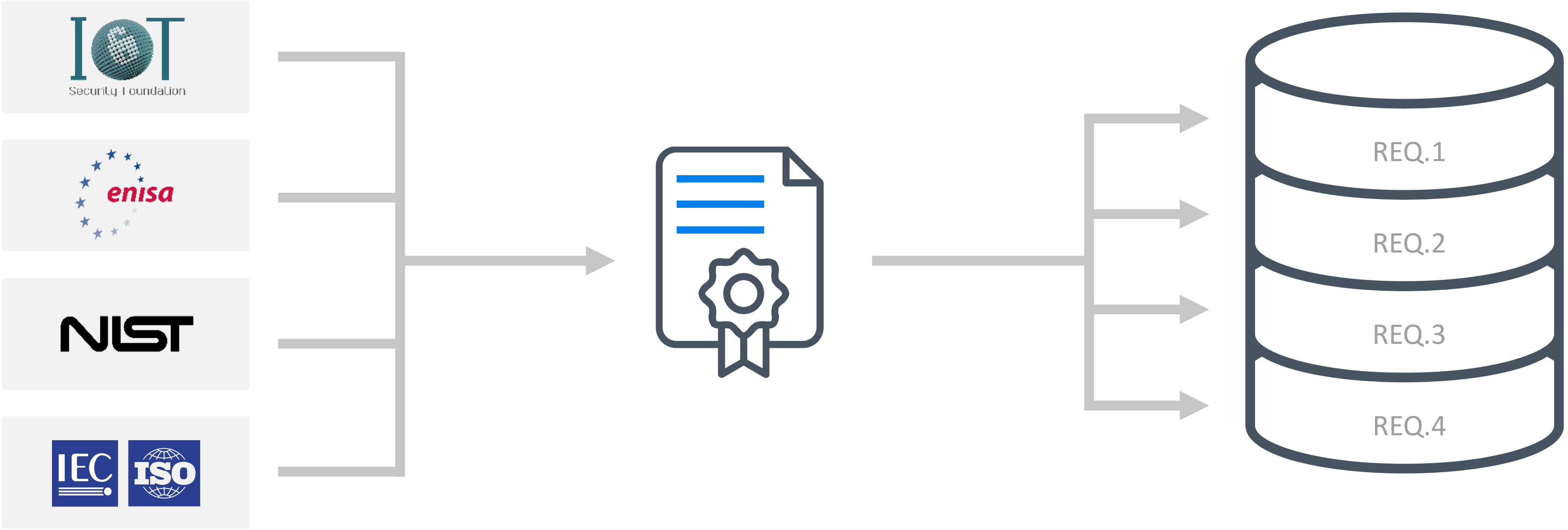
Integrating existing standards


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

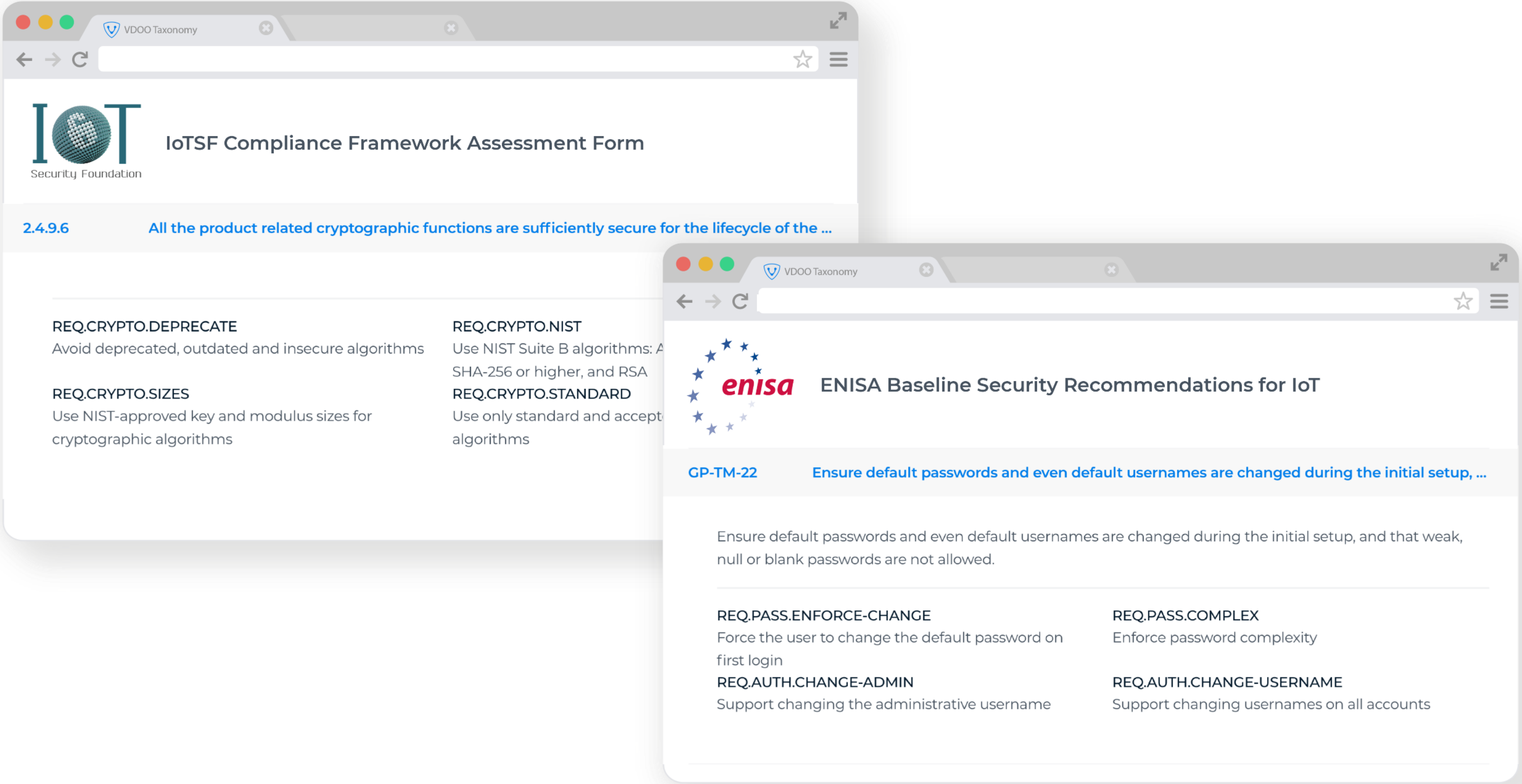
https://xkcd.com/927

shared under the Creative Commons license by its author

Integrating existing standards



Mapping requirements



IoTSF Compliance Framework Assessment Form

2.4.9.6 All the product related cryptographic functions are sufficiently secure for the lifecycle of the ...

REQ.CRYPTO.DEPRECATE
Avoid deprecated, outdated and insecure algorithms

REQ.CRYPTO.NIST
Use NIST Suite B algorithms: A
SHA-256 or higher, and RSA

REQ.CRYPTO.SIZES
Use NIST-approved key and modulus sizes for cryptographic algorithms

REQ.CRYPTO.STANDARD
Use only standard and accept
algorithms

ENISA Baseline Security Recommendations for IoT

GP-TM-22 Ensure default passwords and even default usernames are changed during the initial setup, ...

Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.

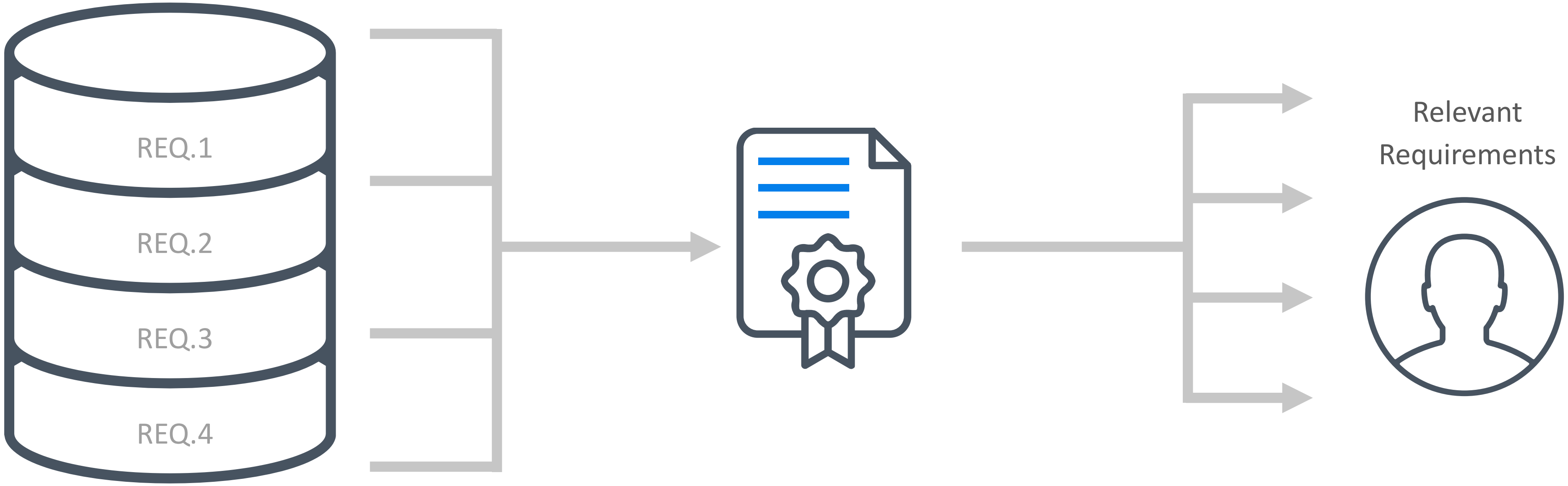
REQ.PASS.ENFORCE-CHANGE
Force the user to change the default password on first login

REQ.PASS.COMPLEX
Enforce password complexity

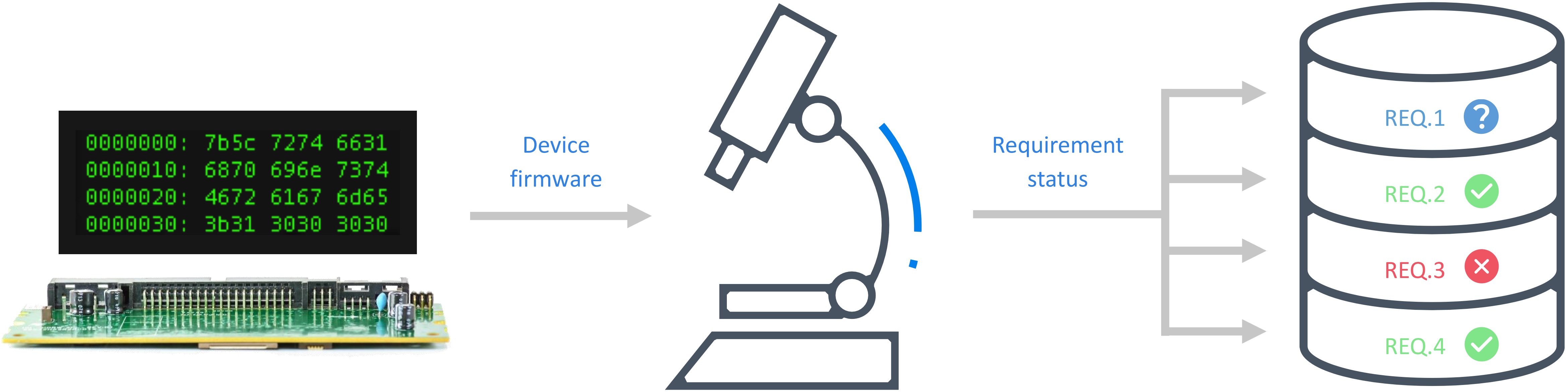
REQ.AUTH.CHANGE-ADMIN
Support changing the administrative username

REQ.AUTH.CHANGE-USERNAME
Support changing usernames on all accounts

Filtering to a selected standard



Automatic scanning for requirement status



```
0000000: 7b5c 7274 6631
0000010: 6870 696e 7374
0000020: 4672 6167 6d65
0000030: 3b31 3030 3030
```

Device firmware

Requirement status

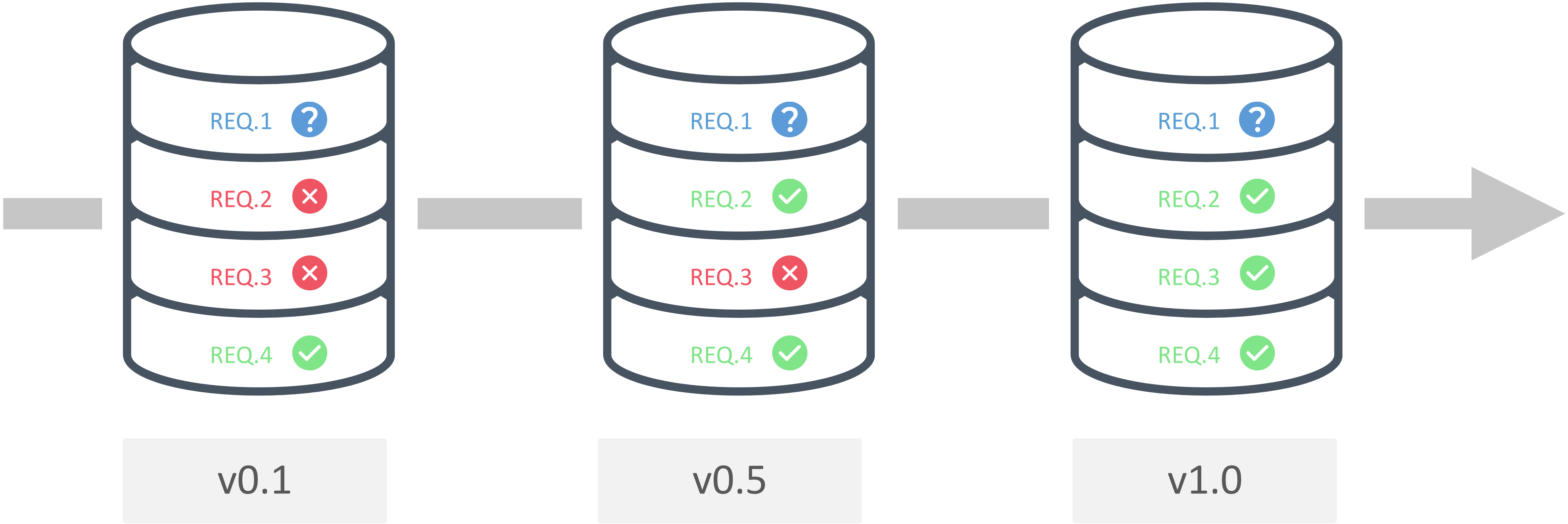
REQ.1 ?

REQ.2 ✓

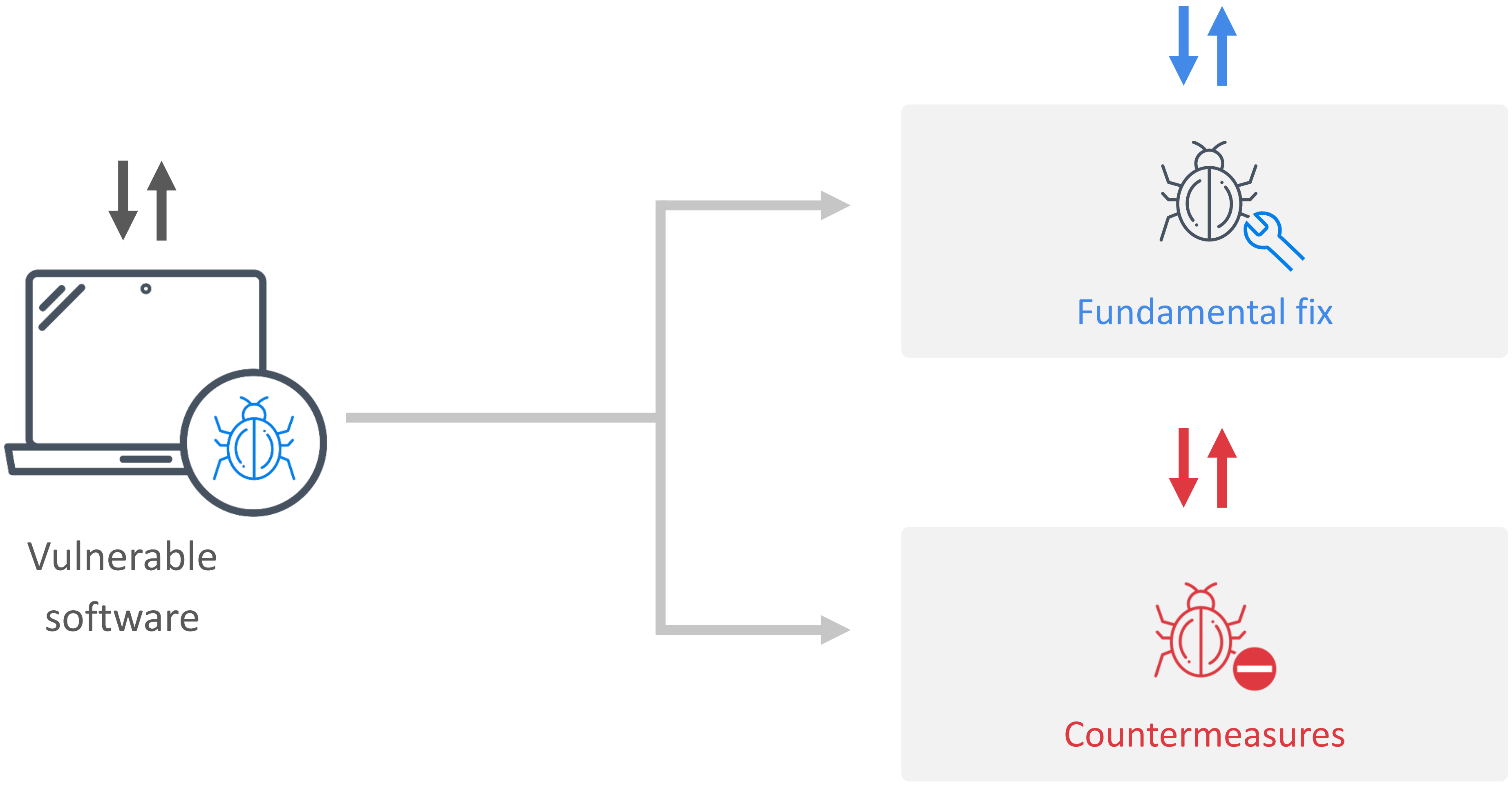
REQ.3 ✗

REQ.4 ✓

Security as part of continuous integration



Post-release protection



Conclusion

01 What is the right security level for my product?

02 What do I already have in my product?

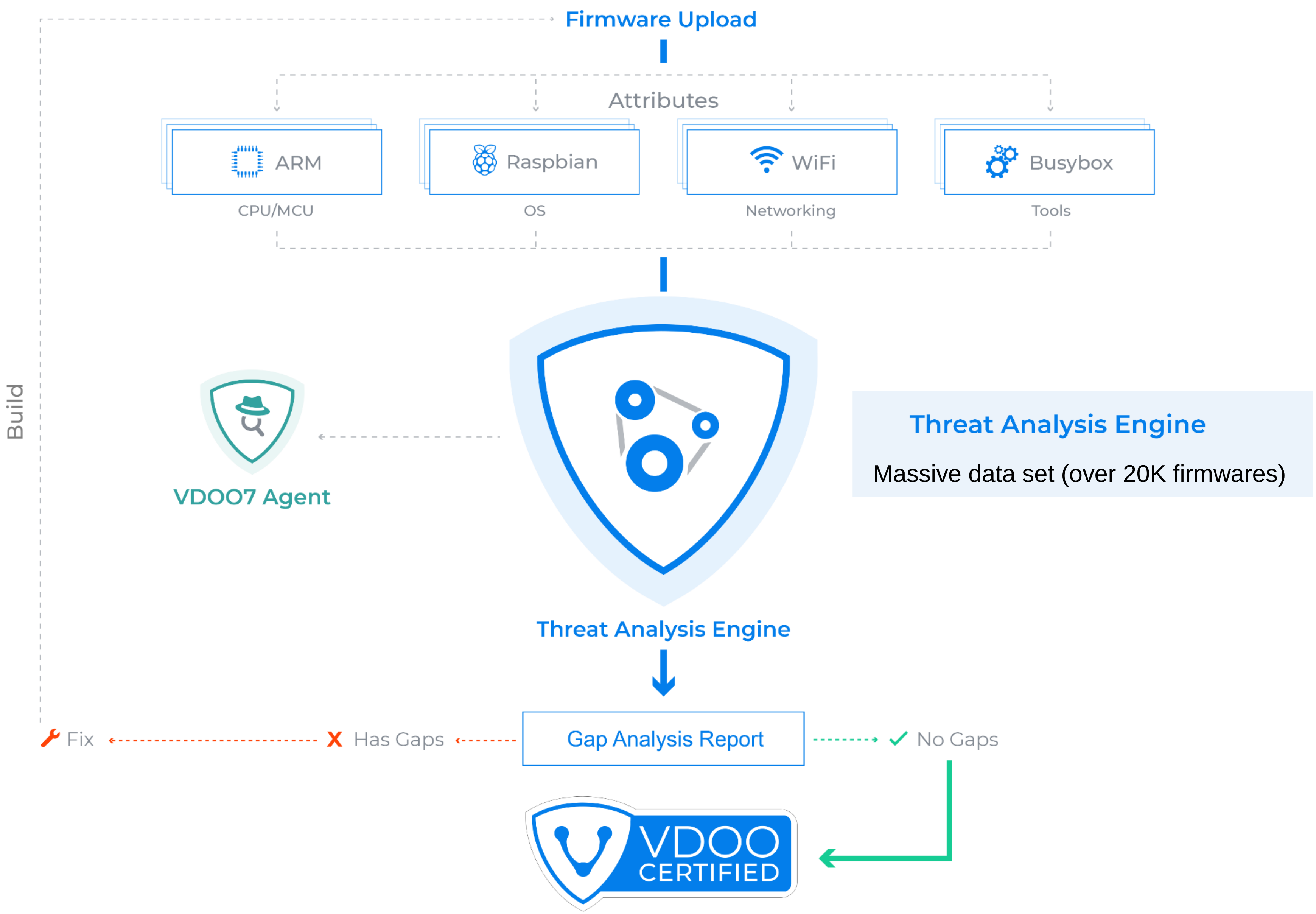
03 What gaps do I have?

04 How to bridge the gaps?

05 How can I be trusted by my customers?

06 How can I maintain trust and security?

Conclusion



Threat Analysis Engine

Massive data set (over 20K firmwares)

THANK YOU

leo@vdoo.com | @leodorrendorf

VDOO