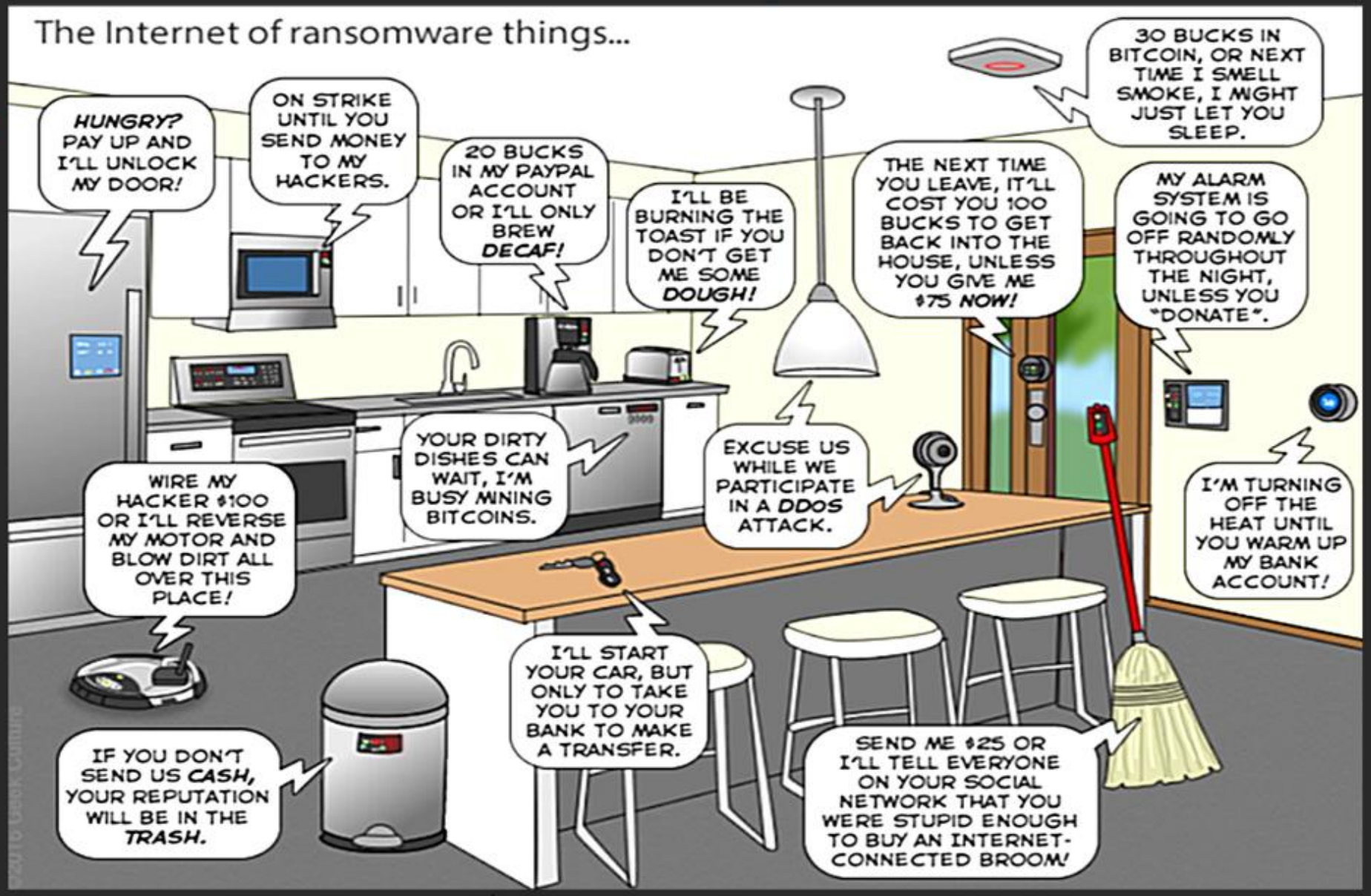
THE FUTURE SHOCK



IoT CYBER SECURITY
ACROSS THE STACK

IoT Solution Elements

User * | Device(s) | Gateway | Connection | Cloud | Applications

Key Generation
Secure Programming
Secure Provisioining

Trusted Platform

Implement Firewall

Whitelisting

Important Security Principles

A. Secure Device (Hardware)

Device identification
Device s/w & f/w config
Data protection
Logical access - Interface
Standardized protocols
Event logging
Decommissioning
Privacy engineering

Secure Dev Lifecycle
3rd Party Sourcing
Code review
Secure Key Storage
Root of Trust
Secure Boot
Pentest

B. Secure Communications

Industry standards
Data protection - In motion
Messaging Control
Device initiated connection

C. Secure Cloud

Authentication and Authorization
End-to-End Encryption
Risk & Behavior Analytics

D. Secure Lifecycle Management

Key Management System
Device Identity and Authorization
Secure Update

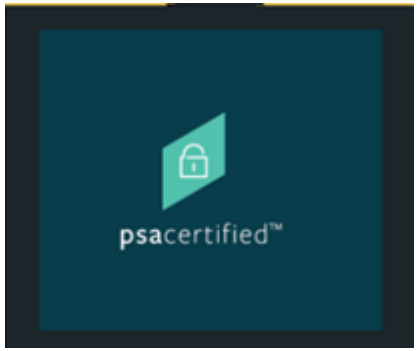
Real Time Monitoring
Audit
Manage End-of-Life


The role of standards in IoT security


THE STANDARDS INSTITUTION OF ISRAEL
Cyber Israel
Prime Minister's Office
National Cyber Directorate
ISO
IEC
Ministry of Economy and Industry
Foreign Trade Administration
ISO/IEC JTC 1/SC 27 IT Security techniques
WELCOME
ISO 27005... ISO 27001, ISO 27002, ISO 27003, ISO 27004

IOT Security | Guidance & Frameworks

IOT Security | Certification & Labeling



ARM
Platform Security Architecture

IOT Security Foundation
Best Security Mark

Cellular Telecommunications
Industry Association

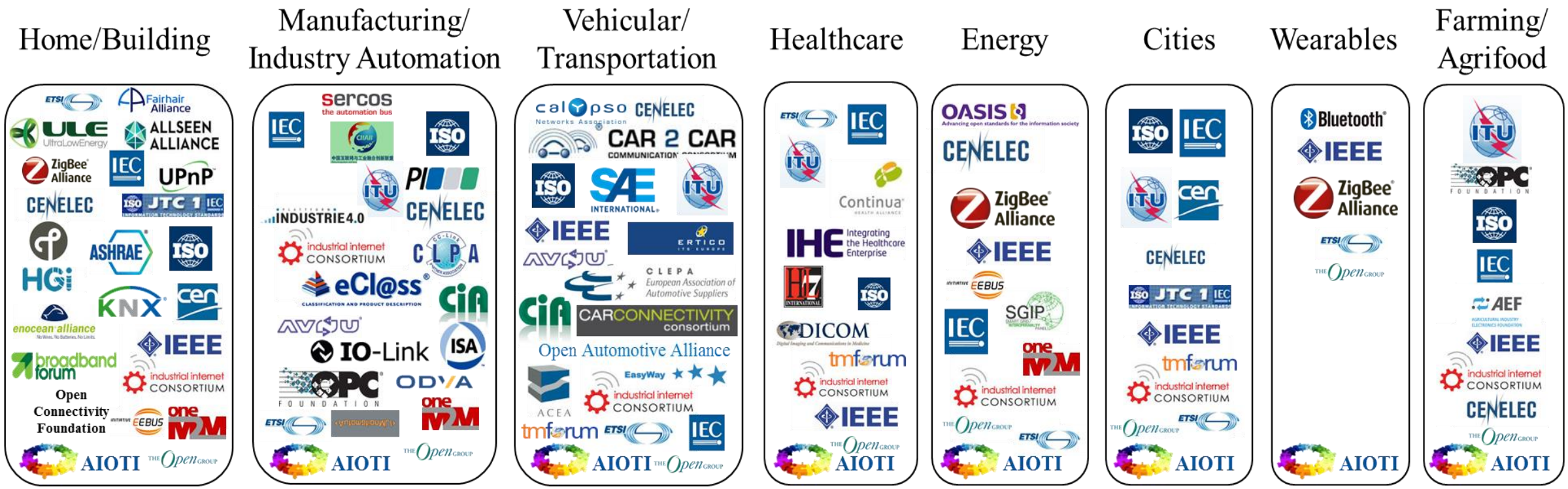
UL
IOT Security Rating

ioXt
Compliance Mark

IoT SDO & Alliances | Technology & Marketing Dimension

Source: AIOTI WG3 (IoT Standardisation) – Release 2.0

IOT SDO & Alliances | Landscape by Vertical



AIOTI WG3 (IoT Standardization)

IOT Security | SDOs, National Bodies, Forums

International Standards Organisations

ISO

IEC

ISO/IEC JTC 1

ETSI

CEN

CENELEC

ISA

SAE

ITU-T

IEEE

National Standards Bodies

NIST

ENISA

BSI

Forum, Consortia etc

IETF

TCG

Global Platform

OASIS

AIOTI

FIDO

Eurosmart

IOT Security | Consumer

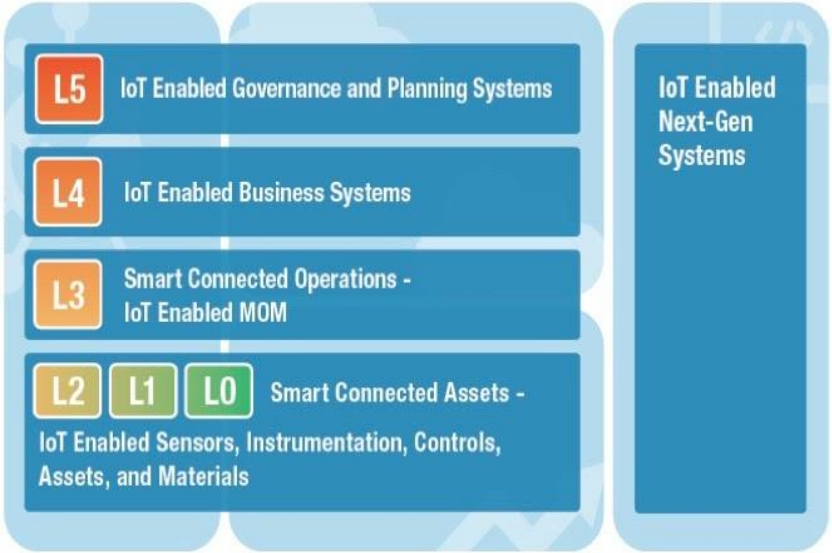
Standards

- **ETSI EN 303645 :** Cybersecurity for Consumer IoT
- **ETSI TS 103 701 :** Guidance on EN 303645 assessment
- **ISO/IEC 27403.6 :** IoT Domotics Security & Privacy
- **ETSI WI-00598 :** Residential Smart Door Locking System

References

- **NIST(IR) 8267** : Security Review of Consumer Home IoT Products.

IOT Security | Industrial



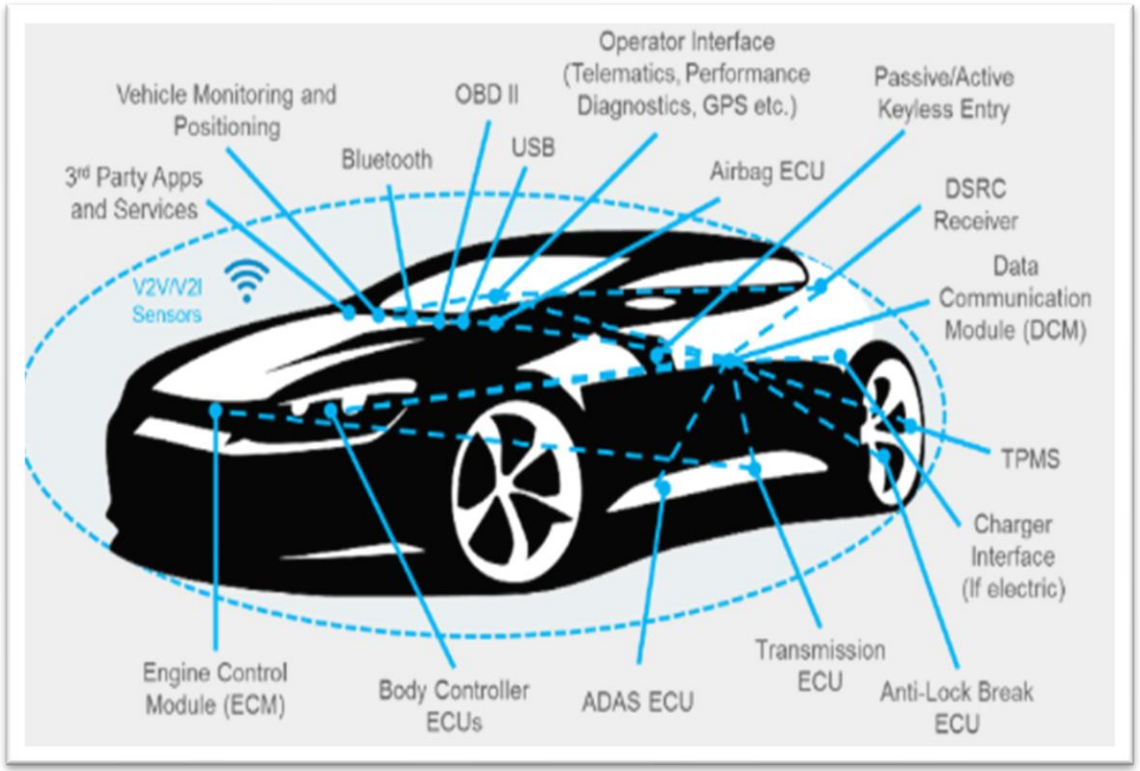
Standards

- **ISA/IEC 62443 Series :** Cybersecurity for Industrial Automations & Control Systems

References

- **NIST SP 800-82** : Guide to Industrial Control Systems (ICS) Security.
- **IIC CSF**: Industrial Internet Consortium's Security Framework
- **UL 2900-2-2** : Software Cybersecurity for Industrial control systems
- **UL2900-2-3 :** Security and life safety signaling systems
- **ENISA** : Good Practices for Security of the Internet of Things in the context of Smart Manufacturing

IOT Security | Automotive



Standards

UNECE WP.29 Cybersecurity Regulation(UN155) ***:*** Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

ISO /SAE 21434 : Road Vehicle Cybersecurity Engineering

ISO PAS 5112 : Road Vehicles – Guidelines for auditing cybersecurity engineering

ISO/CD 24089 : Road vehicles — Software update engineering

References

SAE J3601 : Providing basic Guiding Principles on Cybersecurity for Automotive Systems

IOT Security | Medical & Healthcare

Standards

UL 2900-1: Standard for Software Cybersecurity Network-Connectable Products, General Requirements.

UL 2900-2-1 : Software Cybersecurity for network connected components of Healthcare and Wellness Systems.

ISO 62304 : Secure development of medical device software.

ISO 60601-4-5 : Safety-related technical security specifications for Medical Electrical Equipment.

IEC 80001 : Application of risk management for IT-networks incorporating medical devices.

References

IMDRF : Principles and Practices for Medical Device Cybersecurity

US FDA: Content of Premarket & post Market Submissions for Management of Cybersecurity in Medical Devices

OWASP : Medical Attack Surfaces project

SAFE Framework

IOT Security | Reference Standards

ISO/IEC 27001 : Information Security & Management Systems

ISO/IEC 15408 : Security techniques -- Evaluation criteria for IT security.

ECN PP : CC Protection Profile for Edge (Edge Compute Node)

FIPS140-2 / FIPS140-3 / ISO/IEC 19790: Security Requirements for Cryptographic Modules

NIST SP 800-30 / ISO/IEC 31010 : Guide for conducting Risk Assessment

ISO/IEC 27005: Information security risk management

FIDO : Device Onboarding Standard

ISO/IEC 30141: IoT - Reference Architecture

ISO/IEC 29192 : Lightweight cryptography

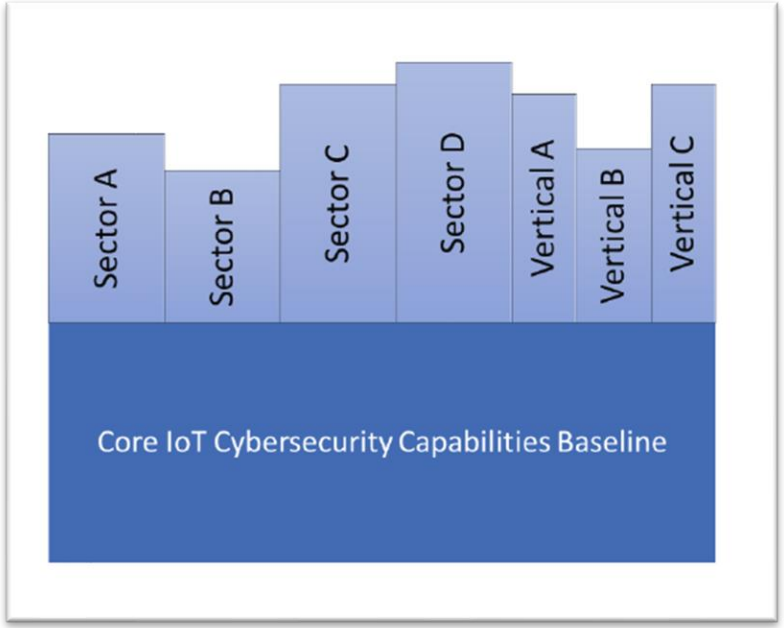
IEEE 1451-99 : Harmonization and security of IoT

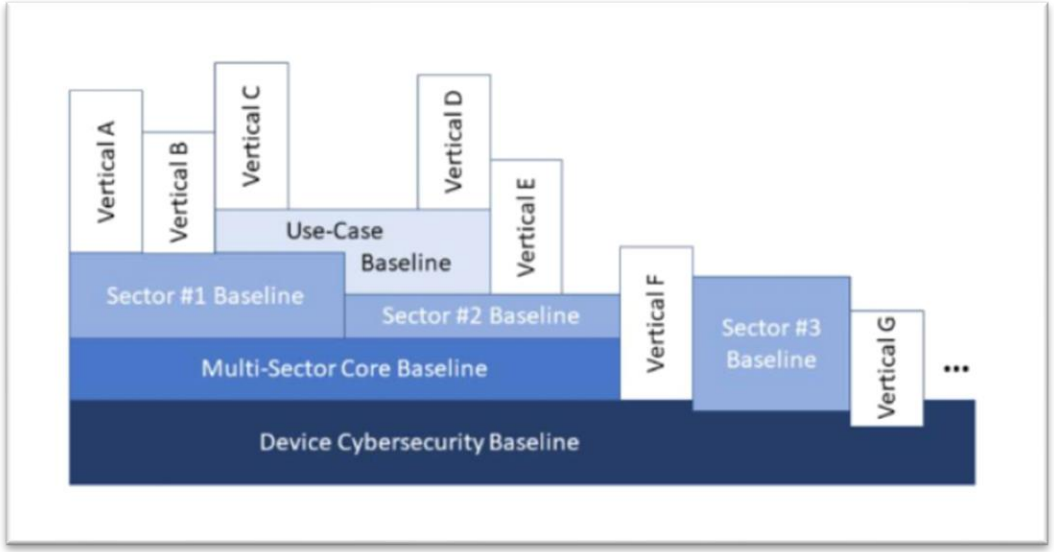
IETF RFC 8520 : Manufacturer Usage Descriptions (MUDs)

NTIA SBOM : Software Bill of Material

ISO/IEC 30111: Vulnerability handling processes

IOT Security | Horizontal Standards





Standards

ISO/IEC 27400 : Guidelines for security and privacy in IoT

ISO/IEC 27402 : IoT security and privacy - Device baseline requirements

ISO/IEC AWI 30149 : IoT - Trustworthiness framework (& 30147 ; methodology)

ANSI/UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products

References

NISTIR 8228 : Considerations for Managing IoT Cybersecurity and Privacy Risks

NIST SP 800-213 (Draft) : IoT Device Cybersecurity Guidance for the Federal Government

NISTIR 8259 : Foundational Cybersecurity Activities for IoT Device Manufacturers

NISTIR 8259A : IoT Device Cybersecurity Capability Core Baseline.

ENISA : Baseline Security Recommendations for IoT

IOT Security | Futureproofing Standards

- **Privacy Engineering**
- **Trustworthiness**
- **Zero Trust Architecture**
- **Quantum Cryptography**
- **Blockchain**