Payatu

Research Powered Cybersecurity

Made with  in Pune

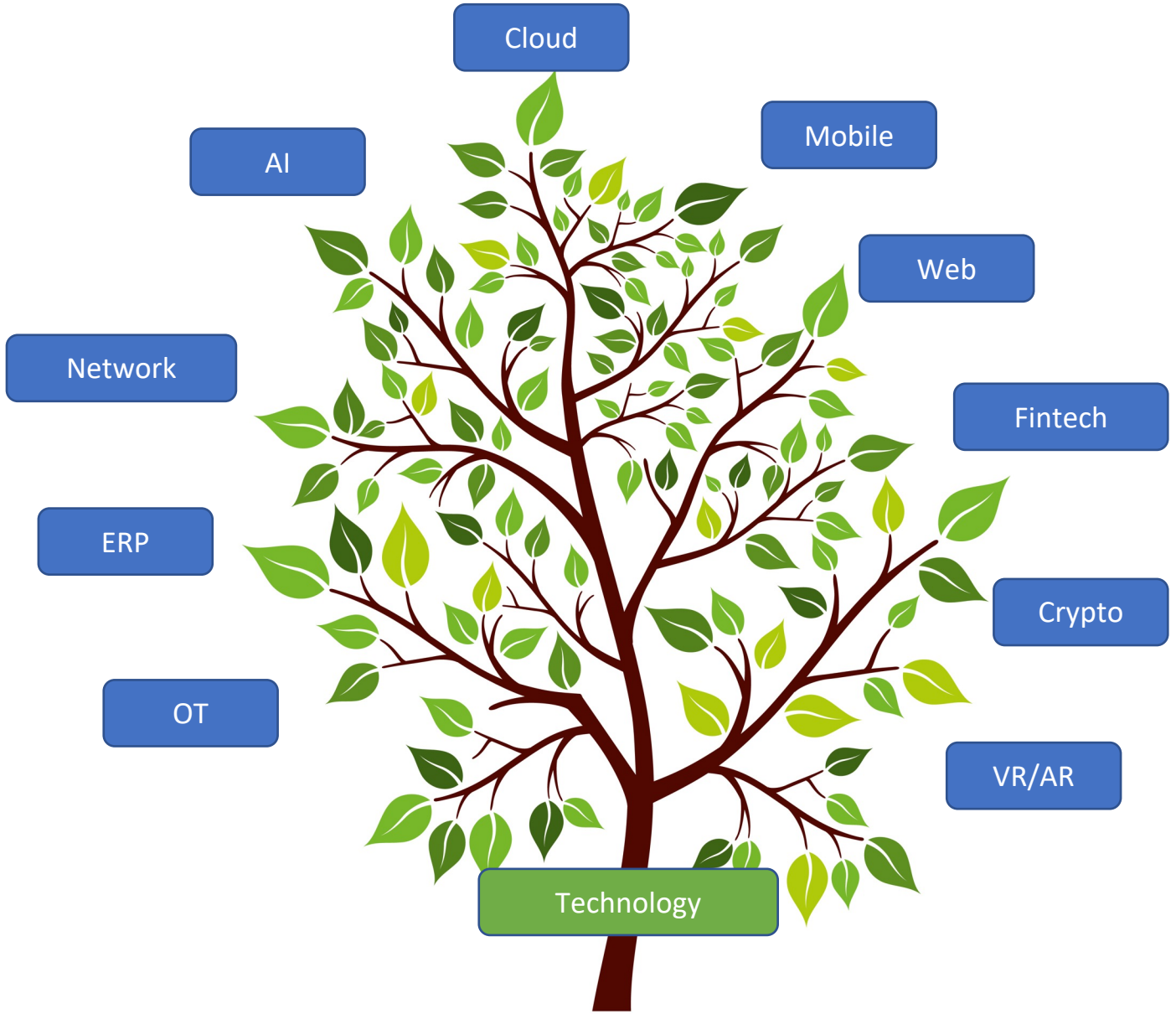


Image Credit: https://www.freepik.com/free-vector/tree-with-roots-green-leaves_13187538.htm#query=tree%20roots&position=0&from_view=keyword&track=ais

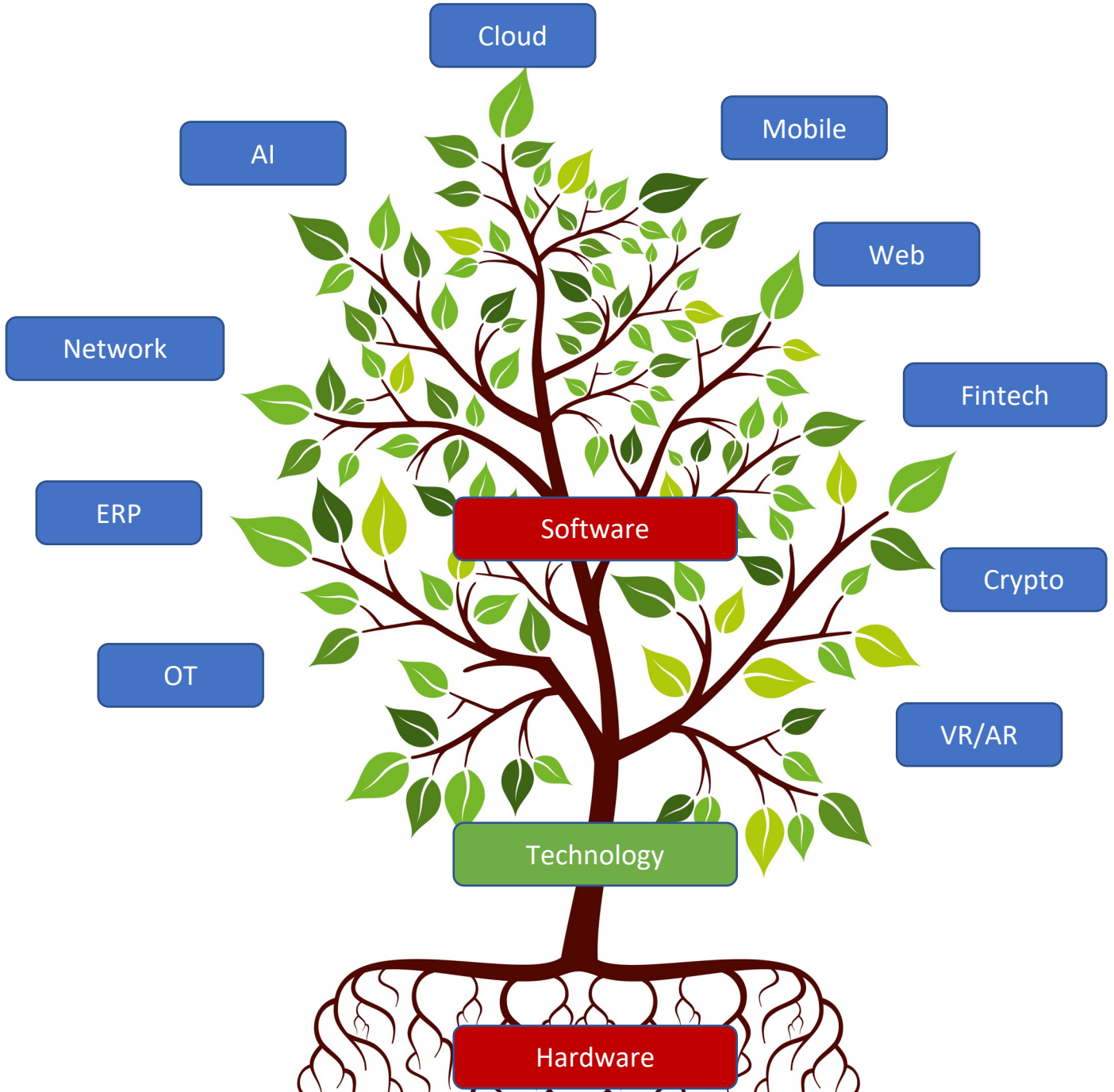
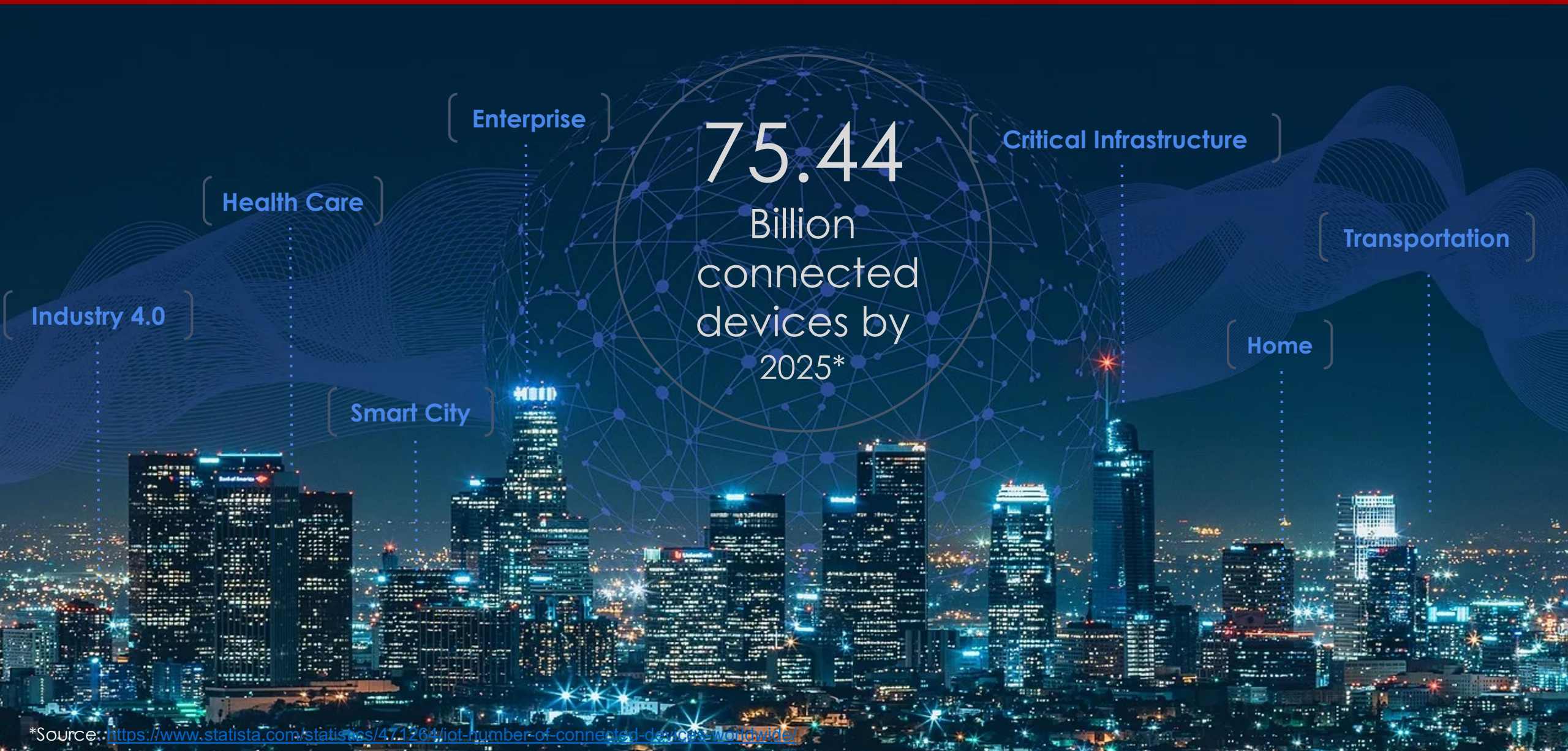


Image Credit: https://www.freepik.com/free-vector/tree-with-roots-green-leaves_13187528.htm#query=tree%20roots&position=0&from_view=keyword&track=ais

Next-Gen Tech



*Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Next-Gen Tech

Next-Gen Hacking!

Stranger hacks family's baby monitor and talks to child at night

By CHANTE OWENS August 4, 2016

A family living in Washington is speaking out about the horrors they experienced while operating a baby monitor inside their 3-year-old son's bedroom. The couple Jay and Sarah were alarmed to discover that a stranger had hacked into their baby monitor and was spying on their toddler, sometimes speaking disturbing messages into the device, as CBS News describes.

Internet of things will 'aggravate' data privacy compliance problems, Ofcom-commissioned study finds

States scramble to get ahe

The increasing connectivity of devices and flow of data that it brings will aggravate existing difficulties companies face in complying with data privacy laws, a report commissioned by Ofcom has concluded.

08 Jul 2015

REVEALED: Security expert who 'hacked a commercial flight and made it fly sideways' bragged that he also hacked the International Space Station

Hacker Chris Roberts told FBI he took control of United plane, FBI claims

By Just[illegible]m. Moyer May 18, 2015

Lessons From The Ukraine Ele[illegible] Grid Hack

New SANS analysis on how the attackers broke in and took cc[illegible] the industrial control systems at three regional power firms in Ukraine and shut off the lights.

Most Read

ANDY GREENBERG SECURITY 06.16.2020 09:00 AM

A Legion of Bugs Puts Hundreds of Millions of IoT Devices at Risk

The so-called Ripple20 vulnerabilities affect equipment found in data centers, power grids, and more.

Israeli security firm JSOF revealed on Tuesday a collection of vulnerabilities it's calling Ripple20, a total of 19 hackable bugs it has identified in code sold by a little known Ohio-based software company called Treck, a provider of software used in internet-of-things devices. JSOF's researchers found one bug-ridden part of Treck's code, built to handle the ubiquitous TCP-IP protocol that connects devices to networks and the internet, in the

Hackers Remotely Kill a Jeep on the Highway—With Me in It

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Researchers hack a pacemaker, kill a man(nequin)

MORE LIKE THIS


10 terrifying extreme hacks


MEDJACK: Hackers hijacking medical devices to create backdoors in hospital...


Anonymous insiders reveal real hacking risks to nuclear power plants, report

on IDG Answers
Why is my Asus wireless router not working?

GET CLOUD

Medical Device Security Gets Intensive Care

FDA draft cybersecurity guidance for medical device-makers and a new 'Hippocratic Oath' for the industry debut amid growing concerns of patient safety.

Israel facing 'up to two million' critical infrastructure hacking attempts daily

By Jason Murdock

June 16, 2016 17:38 BST

30

About Us

Our Journey

- Over a Decade of impact
- Known worldwide for research, advisories and quality

Community & Conference

n|u
https://null.co.in

NULLCON

hardwear.io
Hardware Security Conference and Training

Consulting

Payatu
Securing The Future

Products

CLOUDFUZZ

EXPLIOT
www.expliot.io

Challenges

Zero Days

- Simple Fuzz Testing, Inefficient and rarely conducted

Regulation and Compliance

- Manual Verification, rarely conducted as most guidelines are recent

Huge Attack Surface

- Separate Assessments, multiple tools, manual integration of results and chances of missing vulnerabilities

Security Testing

- Manual effort for different interfaces, increases timeline due to learning to use new tech

Supply Chain

- Rarely conducted, assessment adds extra effort to the security testing

Zero Days (Unknown bugs)

1. Weaponized Malware
2. Product recall
3. Network breach

Regulations and Compliance

1. Privacy - GDPR
2. IoT - California IoT security, ETSI, IoTSF...
   Domain - IEC 62443, PCI, HIPAA...

Security Testing

1. Open source hobbyist tools
2. Individual protocol analysers
3. Limited attack surface coverage tools

Huge Attack Surface

1. Cloud
2. Mobile
3. Hardware
4. Firmware
5. Radio
6. IoT Protocols

Supply Chain

1. Multiple hardware components
2. Third party software and hardware
3. Less visibility into security

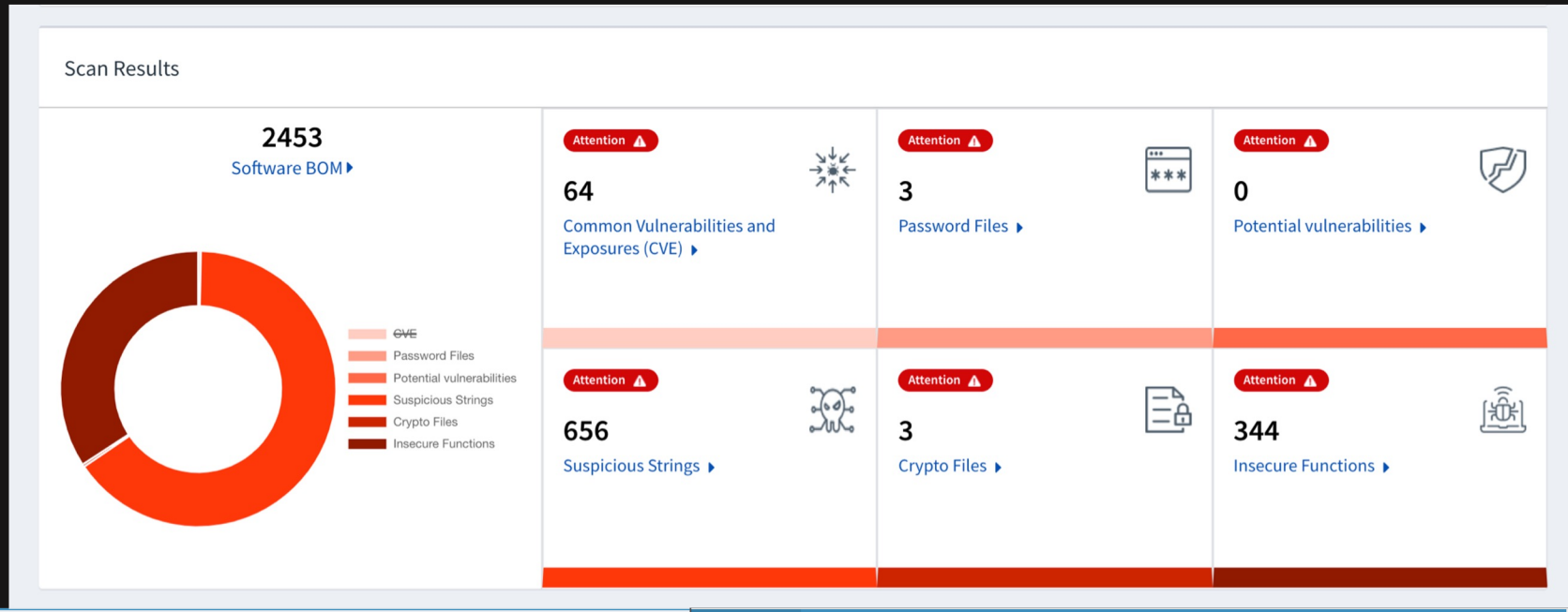
*Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-

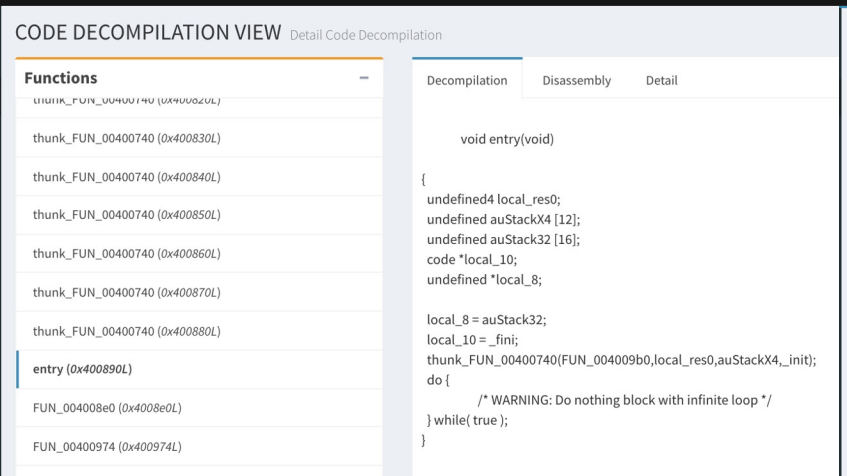
Product - IoT Auditor Platform

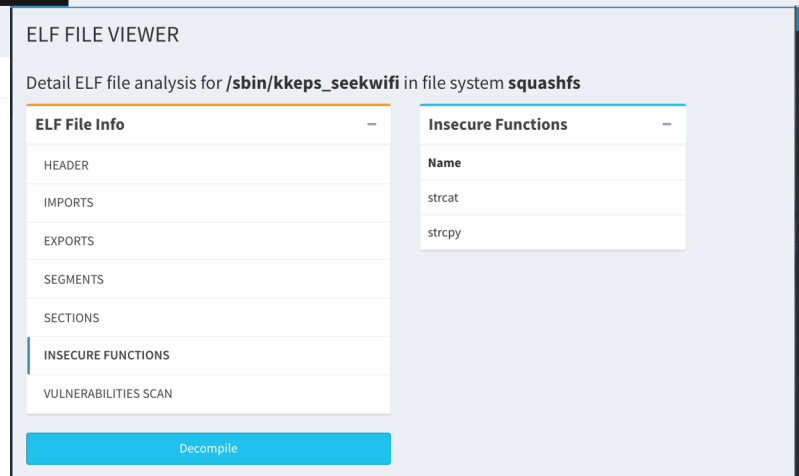
Zero Days • Simple Fuzz Testing, Inefficient and rarely conducted	**Highly Scalable Fuzz Testing** • Continuous, scalable and intelligent fuzz testing for native Applications/SDKs.
Regulation and Compliance • Manual Verification, rarely conducted as most guidelines are recent	**Vulnerability Dashboard with Compliance Mapping** • Mapping vulnerabilities with compliance violations and providing an assessment dashboard
Huge Attack Surface • Separate Assessments, multiple tools, manual integration of results and chances of missing vulnerabilities	**Comprehensive coverage** • Ability to analyse firmware, hardware, radio and cloud.
Security Testing • Manual effort for different interfaces, increases timeline due to learning to use new tech	**Automated Tests and Attacks** • Ability to run simple to complex test cases and attacks from a single dashboad.
Supply Chain • Rarely conducted, assessment adds extra effort to the security testing	**Blackbox Assessment** • Ability to analyse blackbox components

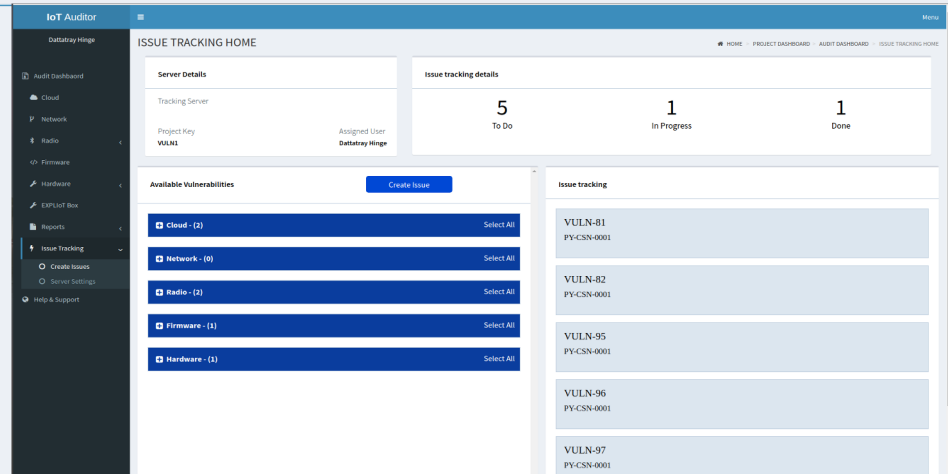
Product - IoT Auditor Platform

- Vulnerability Dashboard
- Potential Vulnerabilities
- Known Vulnerabilities (CVE)
- IoT Compliance Mapping
- Hardware Scans
- Firmware Scans
- Radio Scans









Security Services

- Security Training
- Penetration Testing
- Secure SDLC
- Advisory
- Red Teaming
- Source Code Audit

- Fintech / BFSI
- Telecom
- Medical
- Industrial Control Systems
- Automotive
- E-Commerce
- Manufacturing

ISO 17025 Certified - IoT/Hardware Security Lab






Case Studies

Bypassed **Android MDM u**sing **Electromagnetic Fault Injection** by a USD $1.5 Electric Lighter

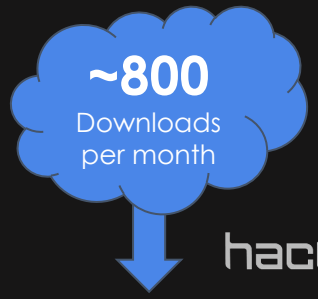
Complete takeover of a **Smart Facility Management Product** focused on data center, building energy management, by combining hardware and cloud bug.

- Firmware Extraction
- Infra Red Command Injection

by eavesdropping Device Firmware Upgrade of an X-Ray Machine

Traction

- Winners – IoT Security Foundation Global Champion Award 2021
- 1st Runner-up – MEITY/DSCI Cybersecurity Grand Challenge 2021
- Open-Source Downloads (pypi only) ~ 800 Per month
- Talks, Workshops delivered at Premier events
- Contributing Member of ISO, BIS, TEC – DOT, IoXt Alliance, IoTSF
  - ISO – 27400, 27402
  - TEC, DOT – Code of Practice for Securing IoT



Aseem Jakhar (Co-Founder)

Email: info@payatu.io

Website: https://payatu.io