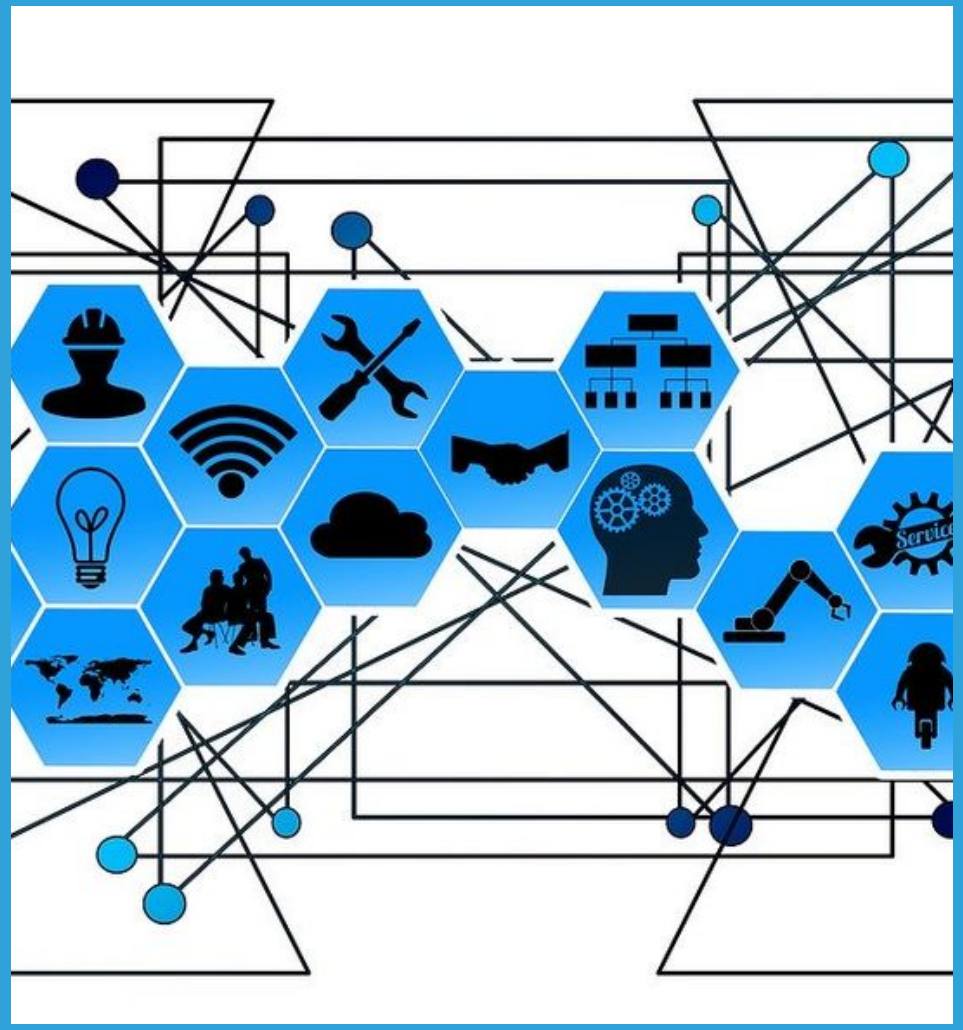
IoT Security Roadmap

Pivot Point SECURITY

Proving Your IoT Is Secure & Compliant...

... is Less Complex Than You Think

Internet of Things (IoT) Defined



- A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction

Wikipedia

The Problem

The scale & complexity of your IoT solution makes proving it is secure and compliant to key stakeholders a daunting task ...

The Only Constant is Change

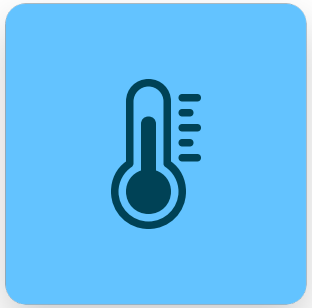
- **For 20+ years we have been helping organizations prove emerging technologies are secure & compliant**

  Yes, IoT is different, but it's fundamentals are less so, and we have a proven approach to share that will get you where you need to be

IoT's Paradox

1. IoT is **More Complex & Very Different** from “Traditional” Computing
2. IoT Security **Isn't Very Different** from “Traditional” Security
3. **We have a proven plan for securing IoT … Let's Dig In!**

IoT is Different From Conventional Computing in 4 Key Ways

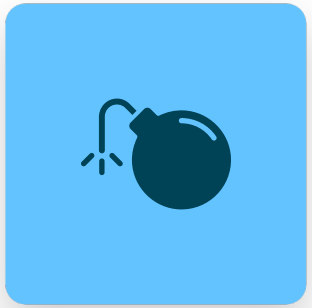


Devices

Shift from human centered to device centered communications

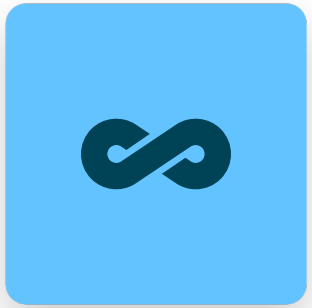
Use Cases

Autonomous decisions for emerging use cases of notable significance



Scale/Complexity

~41.6 billion IOT devices generating 79.4 Zettabytes (ZB) of data per day by 2025



Impact

Devices, use cases, scale & complexity drive impact to a potentially massive scale

IoT Devices (& Communication) are Very Different

- **Non- traditional computing paradigm**

  They ain't people at PCs

- **Often embedded**

  Industrial control systems, medical devices, vehicles, etc.

- **Usually sensors and/or actuators**

  Sending streams of data (speed, pressure, glucose) via the internet and taking actions based on data

IoT Use Cases are Very Different: It's About Sense AND Control

- **Autonomous Vehicles**

  Trains, planes, & automobiles :)

- **Industrial Automation**

  Energy, Chemical, & Industry 4.0

- **Smart Battlefields**

  Munitions, vehicles, & robots

- **Building Automation**

  Lighting, security, & environmental

- **Home Automation**

  Smart appliances, video, & energy

- **Internet of Bodies**

  Ingested, implanted, & connected

IoT's Scale & Complexity is Very Different

- **Law of Unintended Consequences**

  Endless permutations of interaction between fixed, autonomous, & proactively integrated new actors can border on chaos

- **Machine Learning/AI**

  Big data allows machine learning models to improve & control processes, products & services

- **Unimaginable Data Volumes**

  40 ZB of data has been generated in the entire history of man, remarkably the IoT will generate 79 ZB per day by 2025

- **Interoperability**

  41.6B devices, big data, AI, and millions of micro-services will need to seamlessly work together

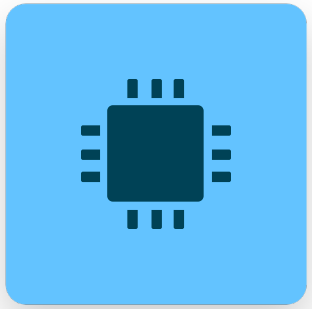
The Impact of an IoT Event Could be VERY, VERY Different

- **With Great Power Comes Great Responsibility**

  The IoT's promise is limitless; its peril is nearly as limitless. Massively connected closed loop systems magnify the potential impact of attacks against critical IoT systems to previously unforeseeable levels (e.g., cripple global companies, topple economies, cause mass suffering/death). The next wave of dystopian novels will surely illuminate the possibilities.

The Good News ... Remarkably, IoT Security Isn't Very Different

For IoT, the Fundamentals Of Information Security Still Directly Apply



Protect the Device

Ensure the physical & logical security of the device

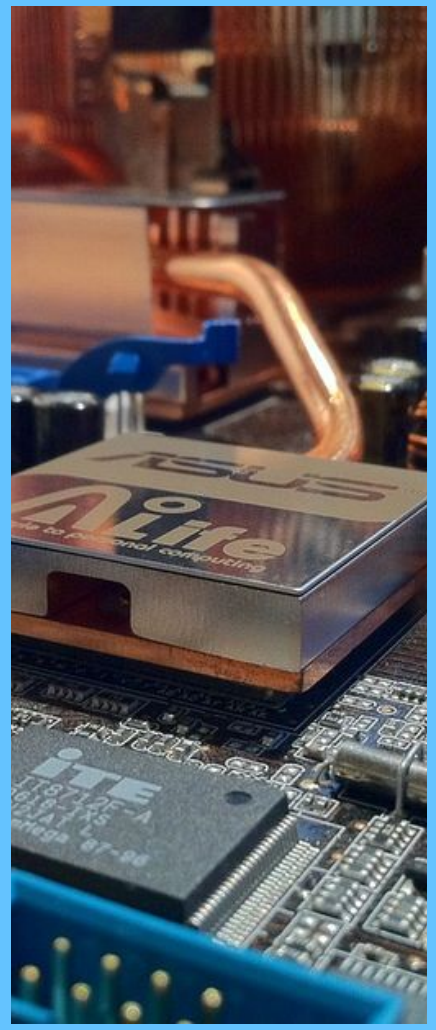
Protect the Communication

Ensure the **Confidentiality**, **Integrity**, & **Availability** of data & communications

Protect the Application(s)

Ensure the Apps & underlying systems are optimally secured against advanced attacks

Protecting the Device is A Bit Different



- **Physical Tampering**

  Protect against device intrusion (UART, JTAG)

- **Exposed Physical Interfaces**

  Protect USB, Ethernet, serial, etc.

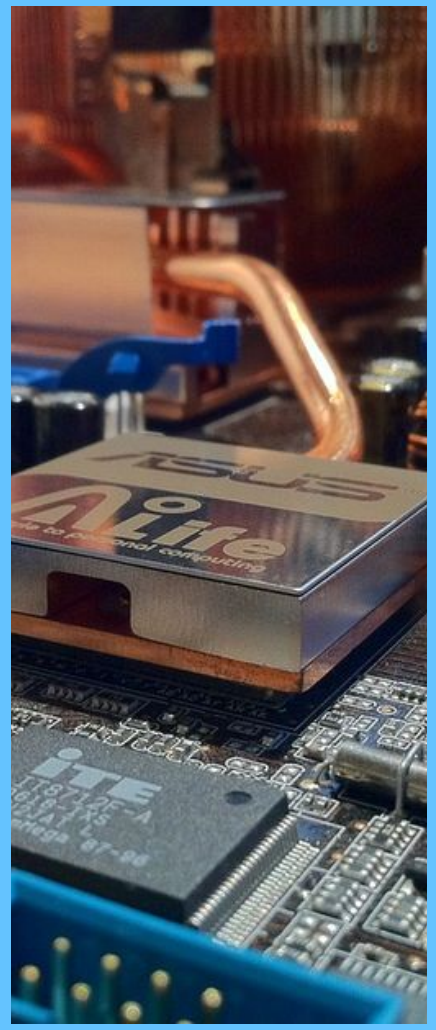
- **Logical Interfaces**

  Protect Zigbee, WiFi, BLE, etc.

- **Firmware**

  Protect the “stack” (embedded web services, OS, etc.)

Protecting Communications is Identical



- **Trust, But Verify**

  Authenticate & Authorize all communications

- **Encrypt**

  Protect data commensurate with its classification/ requirements

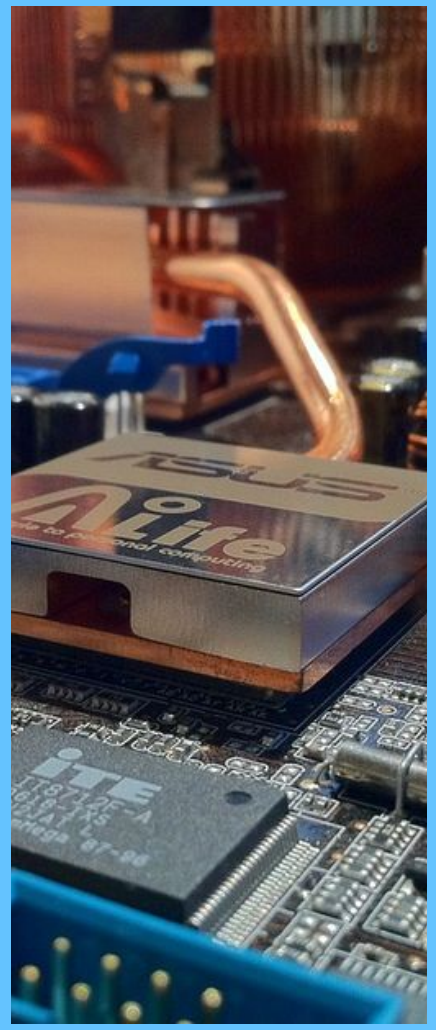
- **Secure Protocols**

  Leverage proven approaches (e.g., TLS, SSH)

- **Log & Monitor**

  In accordance with Security Management objectives

Protecting Applications Is Identical



- **Validate All Input**

  Server side validate all communications

- **Bake Security into SDLC**

  From security requirements to security certification testing

- **Solution Architecture**

  In accordance with regulations, best practice, & risk assessment

- **Address All Modalities**

  API, browser, mobile, agents, & firmware

- **Secure the Base**

  Ensure the network & systems are properly protected

Understanding Risk in IoT Isn't Very Different (but it is notably more important)

- **Greater Impact Requires Stronger Risk Management Processes**

  "Organizations should ensure they are addressing the cybersecurity and privacy risk considerations and challenges throughout the IoT device lifecycle … ", NIST 8228

- **IoT Risks Are Effectively Mitigated by Strong Scoping & Risk Analysis**

  Well characterized risk is essential to determining where to optimally apply critical security controls to mitigate IoT risk to a reasonable, appropriate & acceptable level

Proving Your IoT is Secure & Compliant (the approach is the same; the target/guidance isn't)

Leverage a Proven Information Security/Privacy Framework

Cyber Security/Privacy frameworks like ISO 27001, ISO 27701, & NIST ensure that you take a comprehensive, consistent, & repeatable approach to provably managing IoT security & privacy risks

Leverage a Proven Application Security Framework

IoT is only as secure as the software that drives it; leveraging an Application Security Framework like OWASP ASVS to take a comprehensive approach to validating IoT applications is essential to demonstrable IoT Security

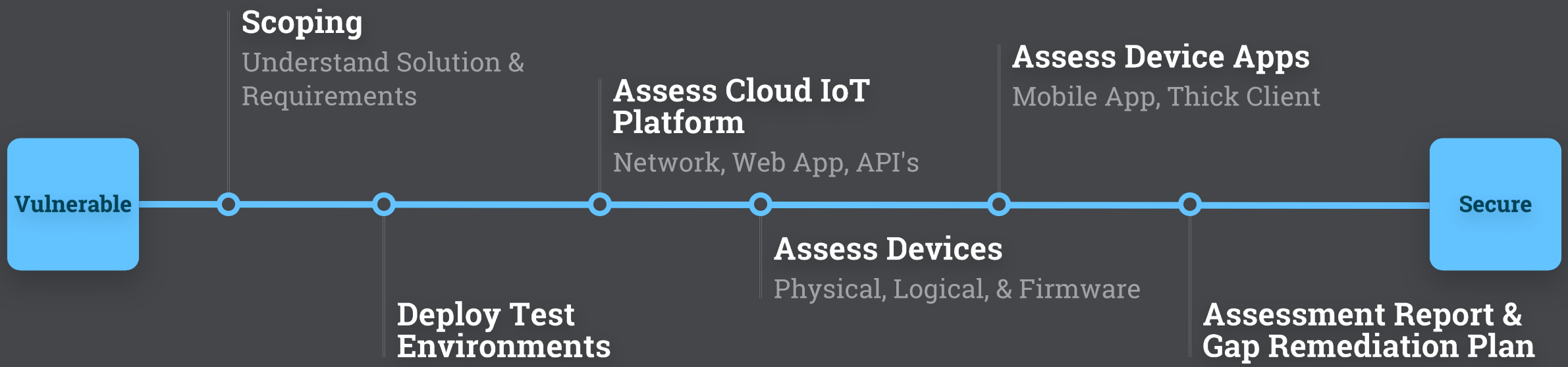
Leverage Open Trusted IoT Guidance

IoT specific regulations/frameworks like NIST-8259, CA-327, ENISA, & CIS, provide insight into understanding technology/use case specific risks and in proving your IoT security conforms with best practice and key regulations

Proving Your IoT is Secure & Compliant

- **The challenge is notable, but so are the rewards**
  - Shortens sales cycles & time to revenue
  - Reduces the burden and/or challenge of dealing with Security Questionnaires and customer audits
  - Provable conformance with security frameworks significantly reduces your overall information related risk
  - Provable conformance with security & privacy regulations reduces your legal risk
  - A good nights sleep

Our Proven Process for Assessing IoT Security



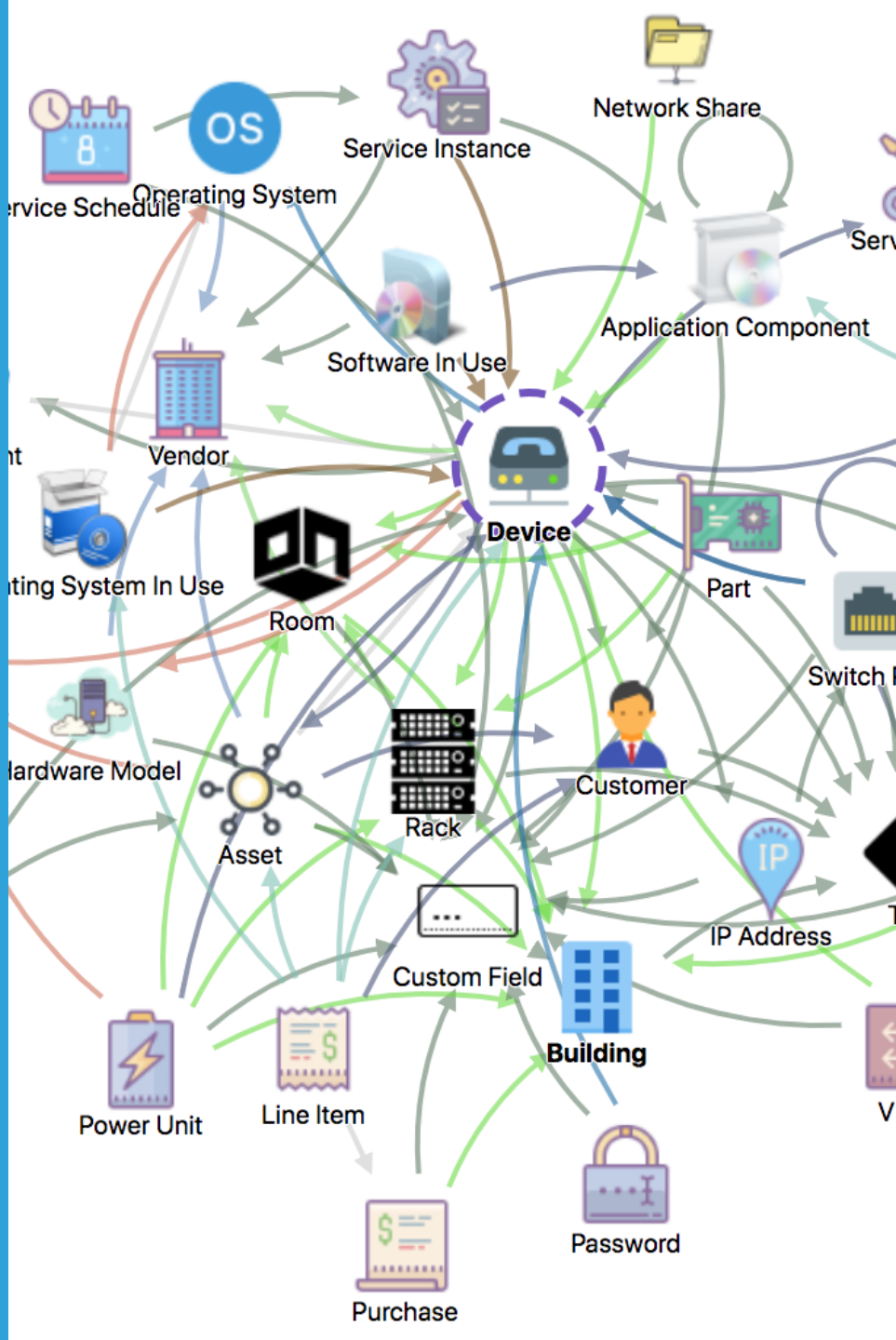
Scoping

Understand Your Solution & Requirements

IoT testing requires that you have a thorough understanding of your solution as a whole. We do this via; interviews with product specialists, artifact review (e.g., manuals, specifications, data flow diagrams), initial device installation/use, and any additional required research (e.g., communication protocols, published vulnerabilities).

GOAL OF THIS STEP

Understand the solution architecture & data flows within.



Deploy Test Environments

Whether its 900 Mhz spread spectrum frequency hopping radios, Alexa enabled consumer devices, or intelligent vehicles; IoT testing generally requires the tester (& testee) to construct a testing environment aligned with the test objectives.

GOAL OF THIS STEP

Create a safe and controlled environment to test the entire IoT ecosystem (from physical device through Cloud infrastructure and 3rd Party solution partners.

Assess Cloud IoT Platform(s)

Network, Web App, API's

Best practice is to ensure the security of the core platform and then extend outwards to the additional elements in your IoT ecosystem. We recommend conducting a CREST Penetration test to ensure the security of your underlying systems/network infrastructure. We recommend conducting an Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) compliant test against key web apps & API's. This is an industry leading, comprehensive approach, that provides a high degree of assurance the solution as a whole is secure while at the same time addressing key requirements of other leading IoT standards including SB 327 & NISTIR 8259.

GOAL OF THIS STEP

Understand the security of your cloud (network) infrastructure, platform, and underlying API's and discover any gaps you will want to address.

Assess Devices

Physical, Logical & Firmware

- Are all physical ports (e.g., ethernet, serial, USB) properly secured?
- Can the device be deconstructed to expose other modes of access (JTAG, UART)?
- Are all wired and wireless modes of communication (e.g., Ethernet, WiFi, ZigBee, Bluetooth, 6Low) properly secured?
- Are all supporting systems (e.g., IoT platform, Certificate Authorities, Authentication, configuration/management/monitoring, API's) and associated communications properly secured? Is the device's firmware secure?
- Is the devices firmware stack (e.g., embedded Linux, local web services) secured against direct attack, decompilation, unauthorized updates, and other attacks?
- Does the device conform with security/privacy requirements (e.g., California SB-327, CIS CSC, TISX, NISTIR 8228, CCPA)?

GOAL OF THIS STEP

Understand the security of your physical devices and discover any gaps you will want to address.

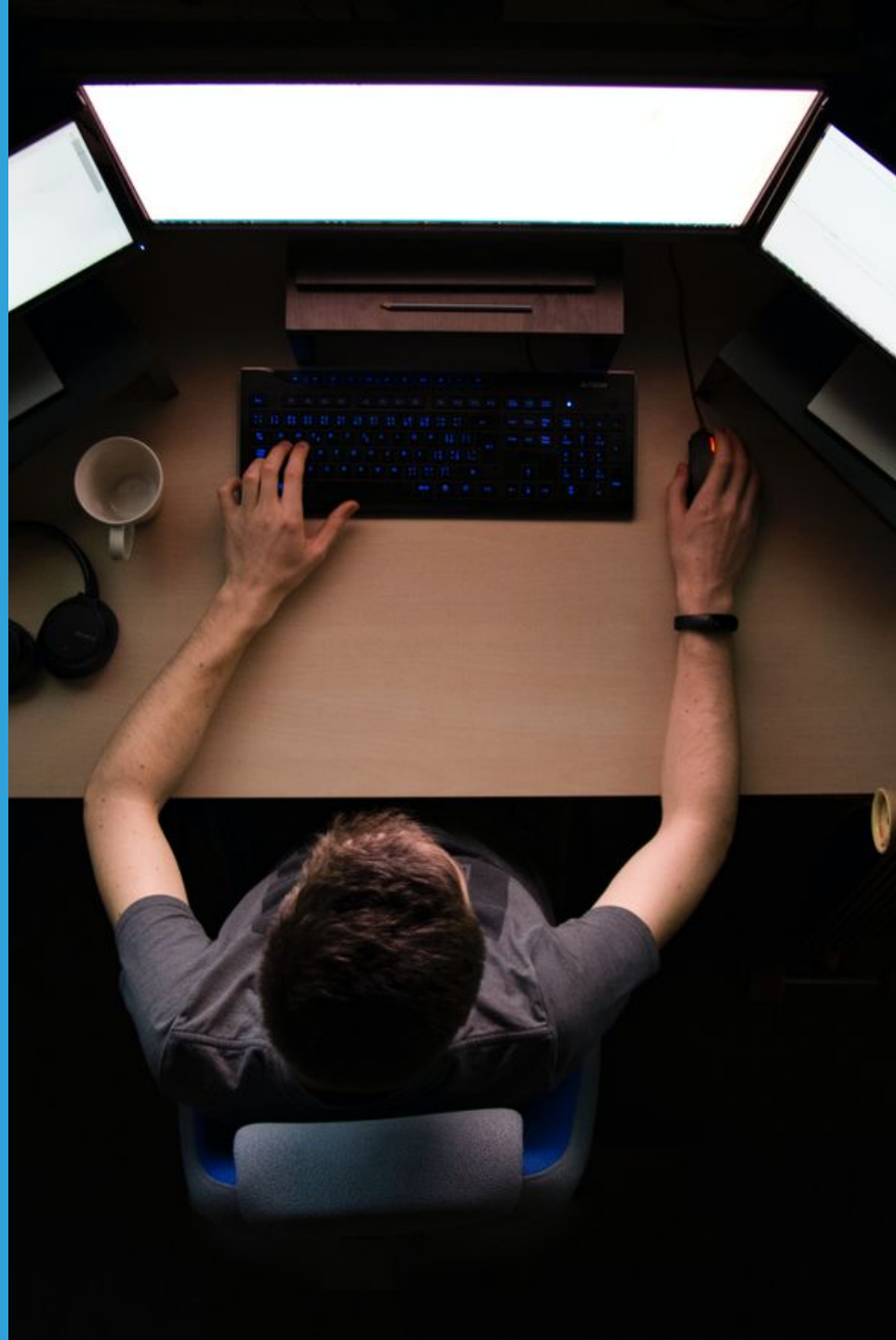
Assess Device Applications

Mobile App, Thick Client

Integral to ensuring device security is ensuring the applications you use to authenticate, configure, deploy, manage, & operate your devices are secure as well. We recommend using the Mobile OWASP Application Verification Standard (MASVS) for mobile application testing. It is an open and trusted framework that provides the highest possible degree of assurance by incorporating a combination of application architecture assessment, code review, vulnerability assessment, and penetration testing.

GOAL OF THIS STEP

Understand the security of your device applications and discover any gaps you will want to address.



Assessment Report & Gap Remediation Plan

It is crucial your assessment efforts turn into actionable guidance. Our work isn't done until the findings have been communicated and you have a clear and actionable plan to get you where you need to go. Our reports include:

Executive Summary of your testing and findings to ensure your work is understood by the “C-Suite”.

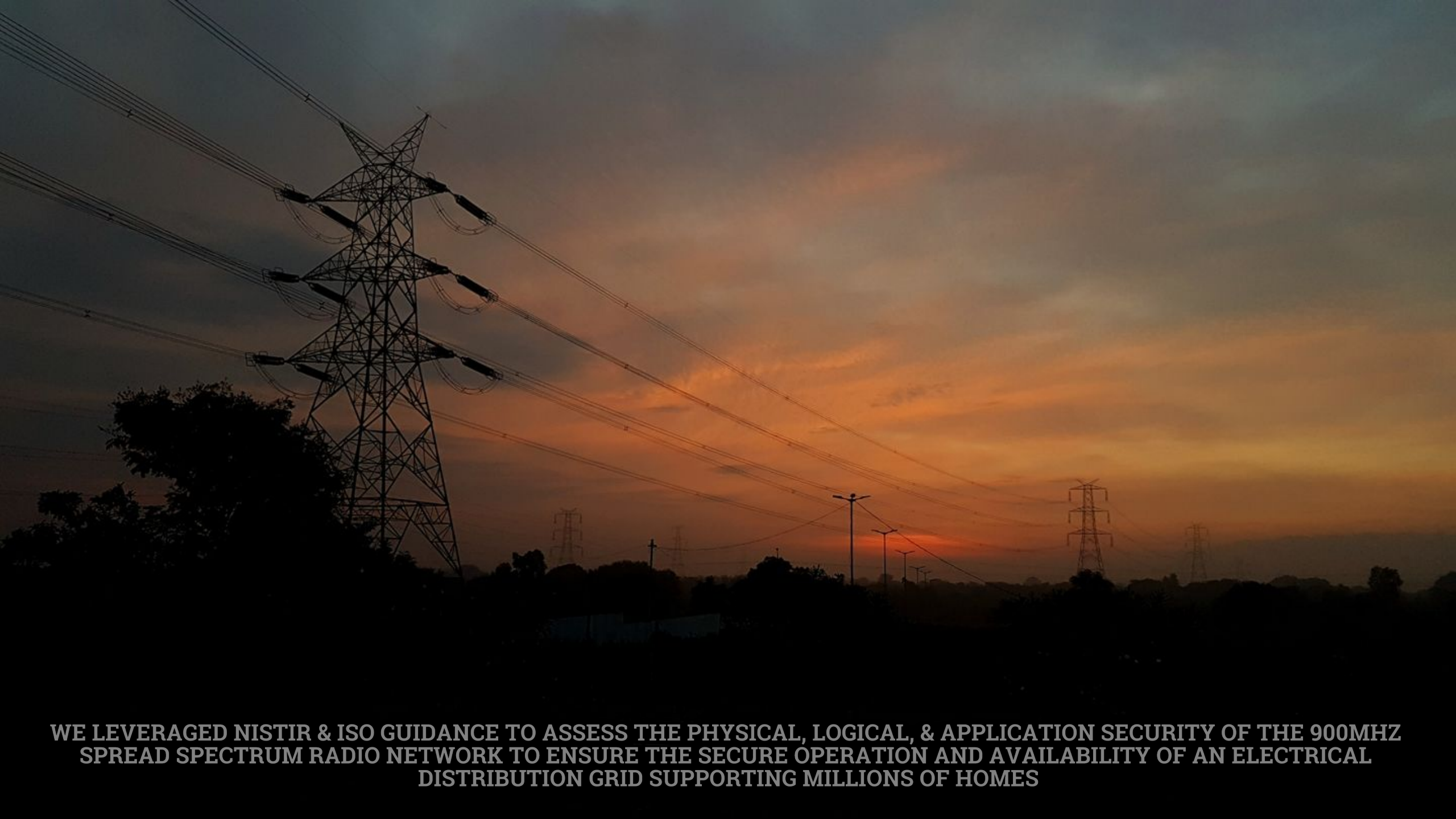
Technical Summary of your testing and findings to ensure your work is understood by IT, IS, and developers.

Gap Remediation Plan because findings without actionable guidance are as useless as ejection seats on a helicopter.

GOAL OF THIS STEP

Summarize assessment work into an actionable plan to bring your IoT security from where it is to where you want it to be.

Not our first IoT Rodeo...



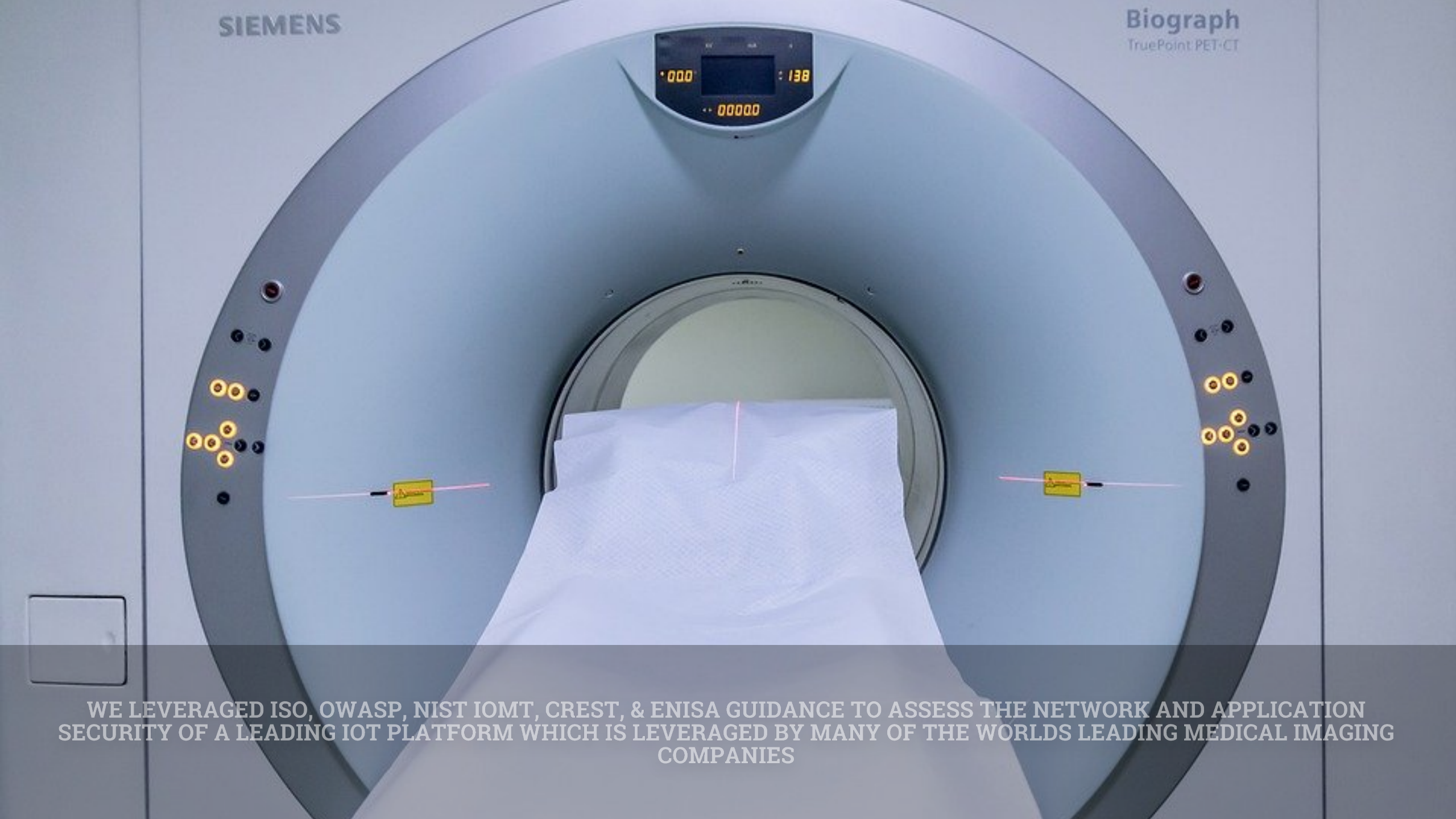
WE LEVERAGED NISTIR & ISO GUIDANCE TO ASSESS THE PHYSICAL, LOGICAL, & APPLICATION SECURITY OF THE 900MHZ SPREAD SPECTRUM RADIO NETWORK TO ENSURE THE SECURE OPERATION AND AVAILABILITY OF AN ELECTRICAL DISTRIBUTION GRID SUPPORTING MILLIONS OF HOMES

WE LEVERAGED AMAZON, CREST, & OWASP-ASVS GUIDANCE TO GAIN “ALEXA” CERTIFICATION FOR A LINE OF SOUND BARS FOR ONE OF THE WORLDS PREMIER AUDIO COMPANIES


WE ARE USING ISO-27001 TO PROVABLY SECURE AN ARTIFICIAL INTELLIGENCE PLATFORM OPERATING GLOBALLY IN 250 MILLION AUTOMOBILES
120
140
160
km/h


WE LEVERAGED NISTIR-7628, ISO-27002, AND IEEE-802 ZIGBEE GUIDANCE TO ASSESS THE PHYSICAL, LOGICAL, AND APPLICATION SECURITY OF THE “SMART GRID” (INCLUDING METER, THERMOSTAT, AND DEMAND RESPONSE PLATFORM) FOR A MIDWESTERN UTILITY
0000C150F1
FCC ID:SK9AMI5,IC:8644G-AMI5,MODEL:AMI5
CL200 240V 3W TYPE C2S0D 30TA 1.0Kh
9122702
HW3
DE
*1NF
9122702 1858*


WE LEVERAGED CA-327, NISTIR-8228, OWASP-ASVS, & VENDOR SPECIFIC GUIDANCE FROM MULTIPLE STREAMING MEDIA SERVICES TO VALIDATE THE IOT POSTURE OF A LEADING SMART SPEAKER PRODUCT LINE



WE LEVERAGED ISO, OWASP, NIST IOMT, CREST, & ENISA GUIDANCE TO ASSESS THE NETWORK AND APPLICATION SECURITY OF A LEADING IOT PLATFORM WHICH IS LEVERAGED BY MANY OF THE WORLDS LEADING MEDICAL IMAGING COMPANIES

WE ARE LEVERAGING ISO-27001 & OWASP GUIDANCE TO ENSURE FOOD SAFETY & SUPPLY CHAIN TRANSPARENCY UTILIZING THE IOT & BLOCKCHAIN

WE ARE LEVERAGING OWASP-ASVS GUIDANCE TO ENSURE THE SECURITY OF HUNDREDS OF IOT CONNECTED HOSPITAL PHARMACY MEDICATION & CONTROLLED SUBSTANCE DISPENSARY MANAGEMENT SYSTEMS

COMPREHENSIVE TECHNICAL TESTING FOR DIGITAL LIGHTING, HEATING, ENERGY, NETWORK, & PHYSICAL ACCESS MANAGEMENT SYSTEMS DEPLOYED TO MILLIONS OF BUILDINGS WORLDWIDE


WHAT IOT CHALLENGE CAN WE HELP YOU SOLVE TODAY?

Pivot Point SECURITY

Any questions? Reach out!

609-581-4600

info@pivotpointsecurity.com