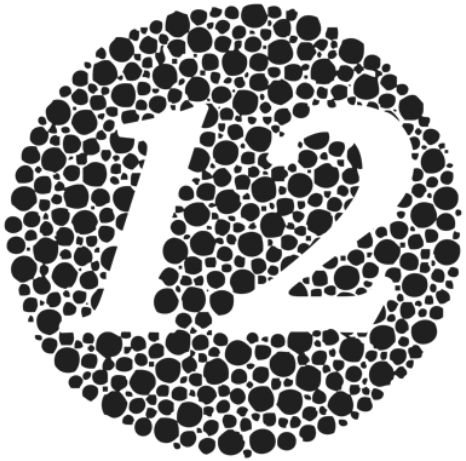
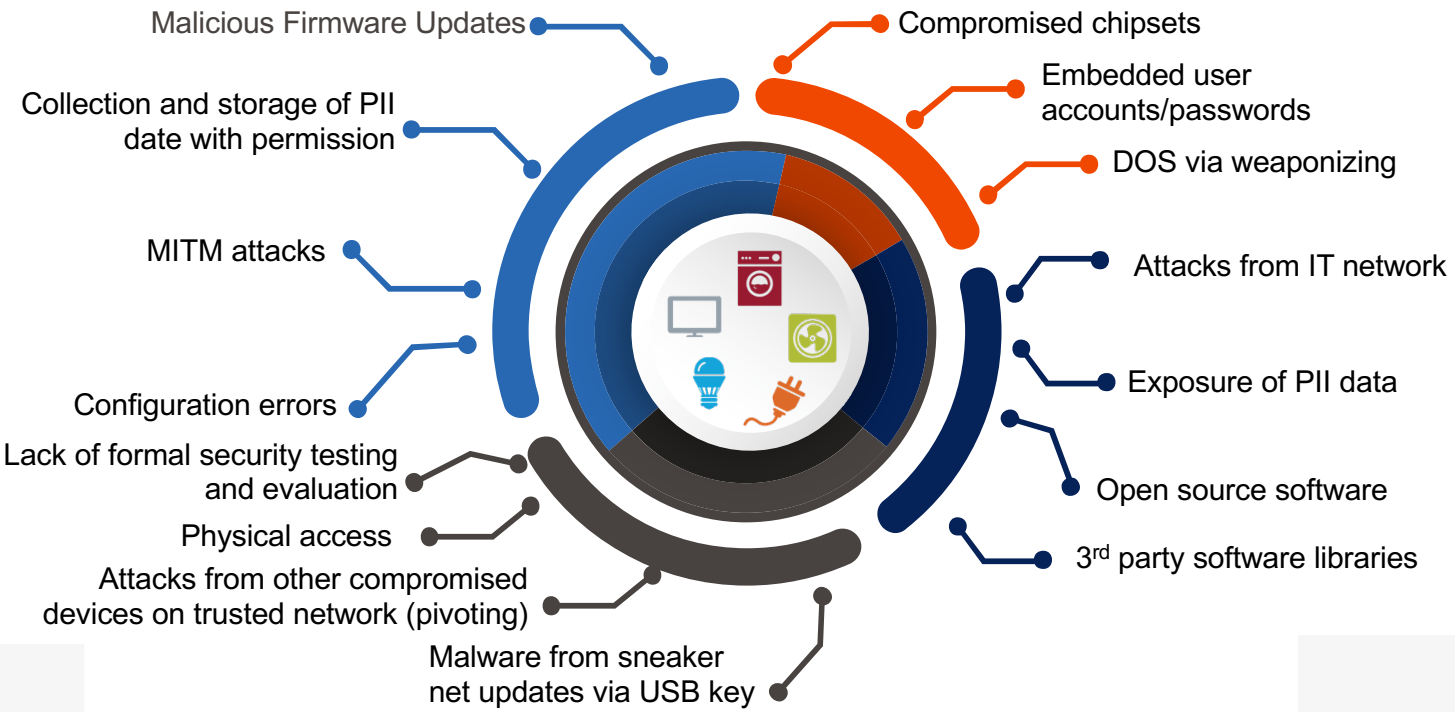


IOT SECURITY - DESIGN AND TESTING CONSIDERATIONS

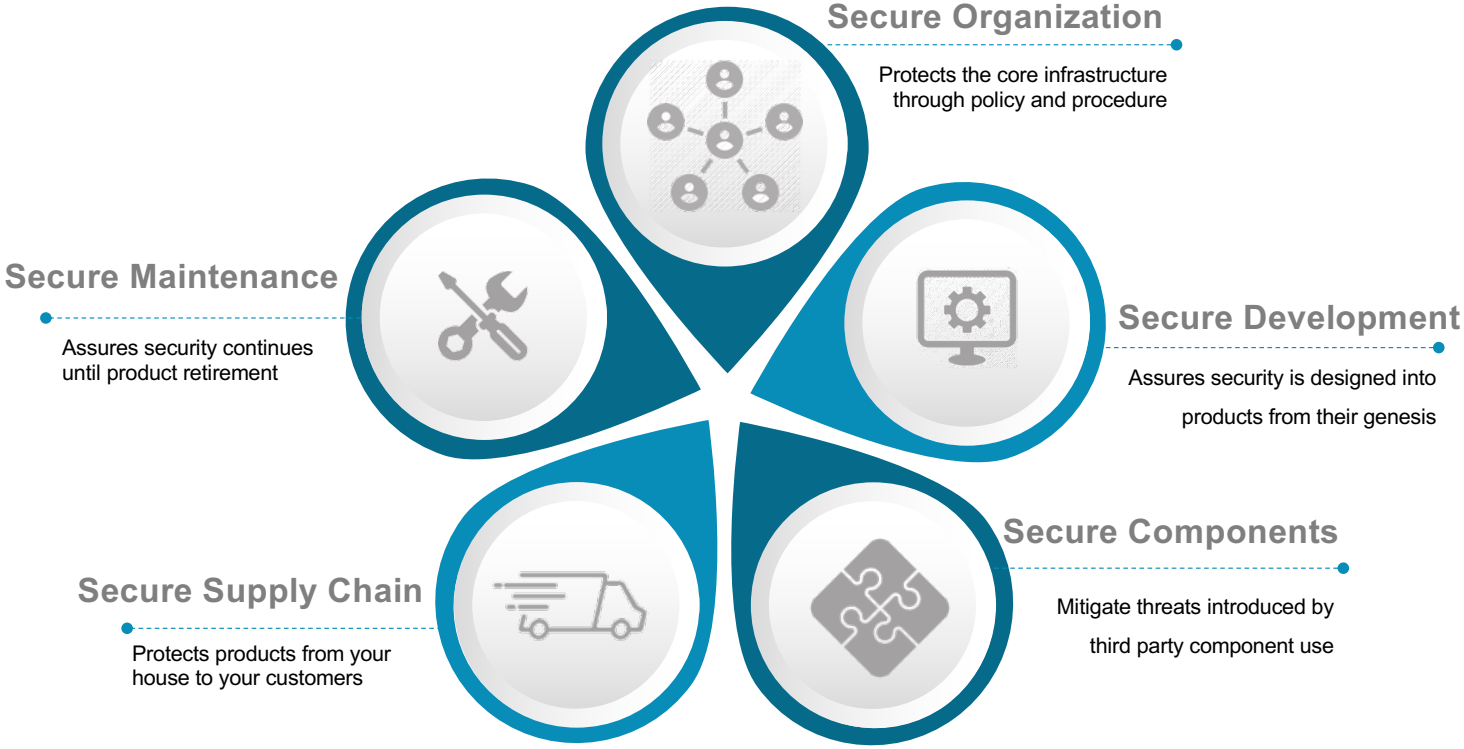
ATTACK SURFACE



HOW DID WE GET HERE?

- Vendors do not have a SDLC (design, testing, evaluation of cyber)
- Lack of awareness for buyers on security risks
- Lack of formal testing and evaluation in the marketplace
- Foreign actors (and others) are looking for attack surface and data
- Configuration errors (users)

ESSENTIAL CYBERSECURITY ACTIVITIES



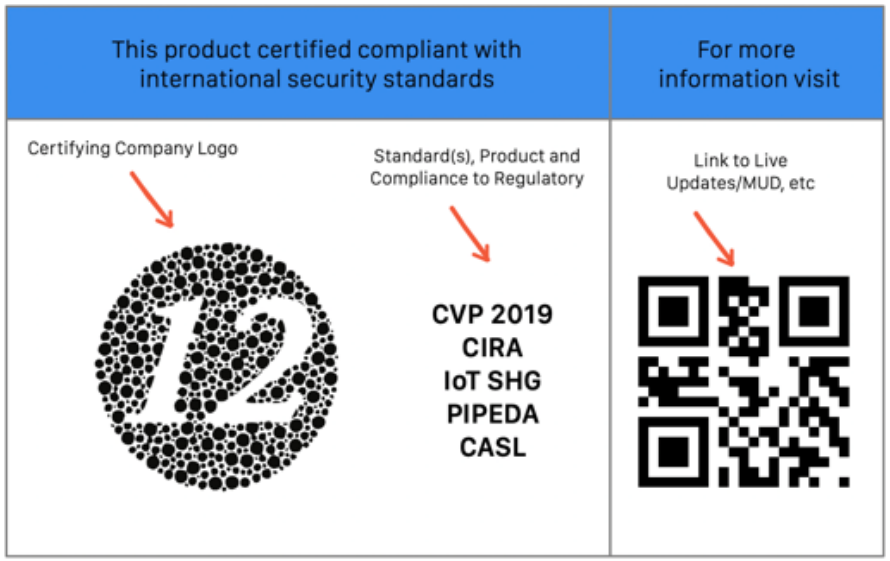
VENDOR IMPROVEMENTS

- Need to create a governance function – Culture of Security
- Secure Development Lifecycle (SDLC) – Secure by Design, Privacy by Design principles
- Formal Testing and Evaluation by a 3rd party – Accredited
- Public policies on privacy and security – Openness to their practices
- Create awareness to how your products are designed, built and tested securely

CONDUCTING AN EVALUATION

- How does your organization implement – Governance, SDLC, Threat Data, Deployment, Secure by Design
- Audit your organization against these aspects
- Conduct a vulnerability/penetration test against the end-to-end solution including cloud, middleware, 3rd party libraries, device and all communication channels
- Vendor needs to improve maturity in company && develop processes

FUTURE – SECURITY LABEL



Reference Sample ONLY

RECOMMENDATIONS

- Create a web site with detailed product/security information
- MUD will be your friend in the future
- Does the vendor sign up for programs such as IoXT commitment?
- International Standards are coming – ISO/IEC 27030 Privacy and Security for IoT, IEC 30149 Framework for Trustworthiness
- Bi-National Standards are coming - T200 in Canada/US

A securely managed company will develop a secure product

DESIGN. BUILD. SECURE

security@twelvedot.com

@encrypto99

www.twelvedot.com