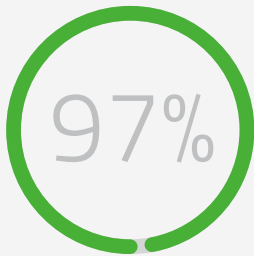


Benefits

- Identify potential security risks in embedded devices
- Ensure proper safeguards are in place to reduce the risk of device failure due to a cyber attack
- Reduce operational costs by discovering and addressing device weaknesses during the development lifecycle
- Improve customer confidence by improving device robustness and reliability
- Reduce liability exposure by adhering to industry best practices for risk mitigation



Percentage of respondents that say a cyber attack on unsecured IoT devices could be catastrophic for the organization.

Source: Ponemon Institute, Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party

Embedded products are expanding our ability to communicate and share information. The rapid growth in the interconnectedness of these devices has also been accompanied by an increase in security threats. Cyber criminals can perform a DDoS attack through the backdoor of these IoT devices. Developers of embedded devices need to consider security issues at every layer – from hardware platforms, virtualization technologies, operating systems, network and communications middleware, and the applications required to support device functionality.

Cylance® Consulting's Embedded System Security Assessment helps development teams cut costs and time frames while decreasing overall security risks. Cylance's dedicated team of IoT and Embedded Systems experts helps to **assess vulnerabilities and develop a plan for responding to them**, starting with the design phase.

Service Overview

Cylance Consulting will perform a black-box assessment of the embedded device, including both manual and automated testing techniques. The in-depth analysis of embedded vulnerabilities will be covered at a technical level, focusing on the common vulnerability types that can be found in embedded applications.

Specific areas of the assessment include:

- **Data Flow Analysis** — Trace data points from input to output, including storage and destruction, to identify potential weaknesses
- **Control Flow Analysis** — Identify threats by stepping through logical conditions and identify all possible paths through which code may traverse
- **Structural Analysis** — Evaluate the security of high-level architecture at multiple-tiers and the composition of the application and its subsystems, including physical deployment characteristics
- **Configure Analysis** — Assess the security configuration of all relevant components to identify vulnerabilities
- **Semantic Analysis** — Analyze the code base within the application's context to identify vulnerabilities unique to the application and environment

The analysis will allow organizations to gain full-spectrum visibility into their security ecosystem with the objective of moving the environment into a state of prevention.

About Cylance Consulting

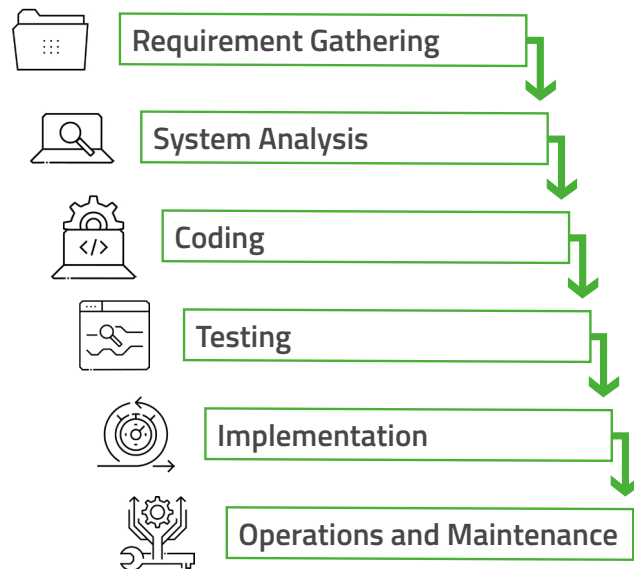
- World-renowned experts work synergistically across practice areas to deliver consistent, fast, and effective services around the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to *prevent* attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Forensics, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, Strategic Services, and Education

Deliverables

As part of the security assessment, Cylance Consulting will provide a comprehensive report detailing:

- Our findings with any potential indicators of compromise
- Graphical summary of testing results
- A strategic remediation roadmap, including:
 - Operational requirements
 - Tactical requirements
 - Governance requirements

EDLC Waterfall Model



Address security challenges in your embedded products before they become pervasive security problems. Contact Cylance Consulting or your technology provider to discuss your needs.