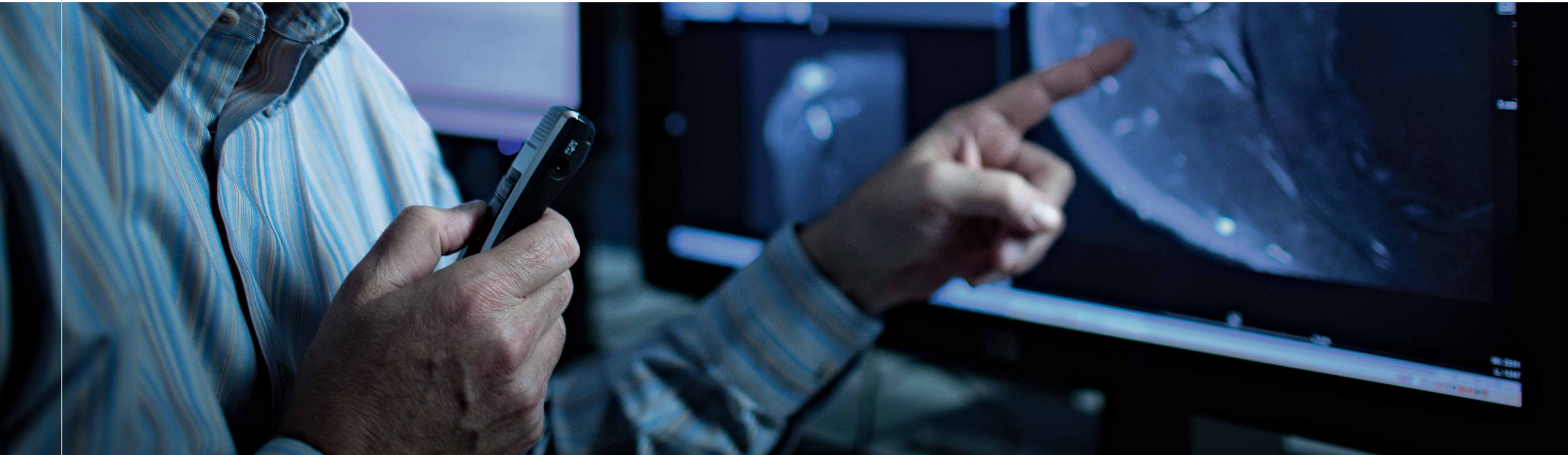
Securing ICS Environments for Rapid Industrial App Development

The rise of the Internet of Things



With the dawn of the Internet, consumer appetite for instant access to information has grown at an explosive rate. Smart phones and other connected devices gave rise to a mobile culture that is connected 24 hours a day, 7 days a week. Now, with a growing desire to further integrate technology with everyday life, the era of the interconnected, smart 'things' is upon us. Better known as the Internet of Things (IoT).

In early 2017, Gartner estimated that over 20 billion 'things' will be connected to the Internet by 2020. While that number includes consumer devices, it also includes the industrial assets necessary to produce them. Excluding consumer devices, business IoT-installed units, including cross-industry and vertical-specific estimates, represent approximately 7.5 billion[1] of that total. Although the Gartner estimate has gained the most favor, other organizations have released estimates, with some running as high as 100 billion 'things'[2]. While there are multiple conflicting estimates, the message is clear: The rapid pace at which devices are being produced and connected provides attractive opportunities for growth for industrial companies.

As a result, business leaders are looking to advanced technology and digital capabilities, including cloud adoption, as a way to get ahead of the curve. The problem is their ability to improve the efficiency and productivity of their operations to capture those opportunities, while maintaining safety of equipment and people, as well as availability of existing systems—24 hours a day, 7 days a week.

The solution rests with the data that exists within the operational environment. Accessing and utilizing that data requires the interconnectivity of machines, controllers, workstations and other devices, giving rise to the Industrial Internet of Things (IIoT).

To ensure success for manufacturers, operators, services providers, and other organizations who adopt the IIoT, purpose-built, industrial-strength platforms and applications are needed.

1. *Gartner Newsroom. Gartner. Feb 2017 http://www.gartner.com/newsroom/id/3598917*
2. *Huawei 100 Billion connected terminals statement with link.*

Cyber-physical systems and the IIoT

At the heart of the Industrial Internet are cyber-physical systems, which the National Institute of Standards and Technology (NIST) defines as co-engineered interacting networks of physical and computational components.[3] According to NIST, “These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, and electric power generation and delivery, as well as in many other areas now just being envisioned.”

Large operational environments typically contain numerous cyber-physical systems, commonly known as industrial controls systems (ICS), operating independently. To extract the greatest value, these systems need to be integrated into a broader IIoT system comprising of hardware, software, and networking technologies. This broader connected system then allows data from one cyber-physical system to inform the operation of a related system. Uniting these systems on a common platform allows organizations to begin the digital industrial transformation.

3. *Cyber-Physical Systems. NIST.* https://www.nist.gov/el/cyber-physical-systems

Advantages of IIoT

The practical advantages of interconnected systems are numerous. For instance, by linking intelligent machines, big data analytics, and data-empowered workers, a digital industrial organization can reduce unplanned downtime and open up new opportunities for growth. Sensors can provide real-time performance information that helps identify problems with machinery before they occur, thereby reducing unplanned outages and improving asset performance.

With that insight, workers are able to make informed decisions that improve efficiency and productivity while reducing risk to people and assets. That insight can also lead to broader business decisions that improve performance across the entire enterprise delivering positive influence to the bottom line.

As an example, RasGas, one of the world's premier integrated Liquefied Natural Gas (LNG) enterprises, is using IIoT-powered predictive maintenance to extend the life of its assets and lower operating costs through greater efficiencies. Insights into plant operations are enabling forward-looking decisions that improve business operations.[4]

Using IIoT in this way, more work gets done with less effort and assets run more predictably. Enterprises move from a reactive break-fix approach to predictive problem prevention, thereby decreasing unplanned downtime and increasing asset lifespan. Product-centric business models are extended to or replaced by more lucrative service-based offerings, with the flexibility and responsiveness to meet fluctuating business demands.

Data is the key. Its potential for constructive use by organizations for their own benefit and that of their customers and communities is huge, but so is its potential for misuse in the wrong hands.

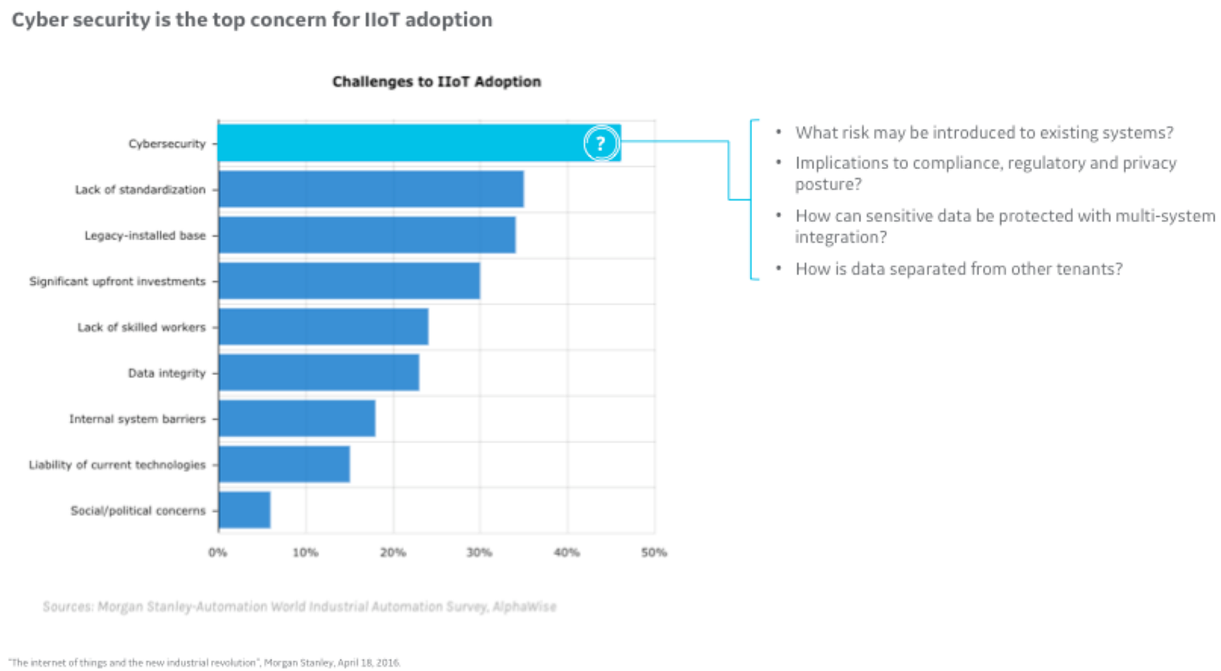


Fig. 1.0 – Morgan Stanley: Cyber security is top concern impeding IIoT adoption

The advent of IIoT renews concern for cyber security. Despite the allure of digital industrial transformation, many hold reservations about exposing their critical infrastructure to the global Internet. With critical industrial equipment and services at stake, the need for excellence and robustness in data and asset security is obvious.

While adoption of IIoT is quickly gaining favor, it should come as no surprise that security of the data is one of the biggest questions when it comes to it. In fact, cyber security concerns are often cited as the biggest barrier to IIoT adoption[5].

4. https://industrial-iot.com/2015/11/the-importance-of-ge-predix-pilot-for-rasgas-and-gcc/

5. *"The internet of things and the new industrial revolution", Morgan Stanley, April 18, 2016*

Where there's technology, there's risk

Over the years, industrial networks were typically designed to be isolated. Today, with the proliferation of the Internet, mobile technologies, and ubiquitous connectivity, isolation is rarely the case.

In a bid to seize big opportunities, many industrial organizations are pursuing the digital industrial evolution by adopting new technology and connecting their operational technology (OT) network with existing enterprise IT networks and applications. In doing so, data from a once closed OT network is now available for use in data-driven decision making, but it is also exposed to the well known threats to the IT network.

The security of data that flows across and between these networks is of paramount concern and cannot be overlooked.

This is why GE's Predix, the platform for the Industrial Internet, was designed with cyber resilience and data security as its core tenants.

Connected assets and a solid IIoT platform increase the value of industrial data for both the enterprise and potential adversaries. To ensure the security of that data, Predix was built with security in mind, contemplating not just the hardware, networking, and programming components, but also the importance of compliance and regulatory concerns, vulnerability management, and the security capabilities of the cloud providers. The result is a securely structured platform that is flexible, scalable, and sustainable.

Securing Predix at its core

According to a report from UBM Technology, only 42% of organizations follow a secure software development lifecycle as part of their development process[6]. From day one, developers of the Predix platform followed the Predix Secure Development Lifecycle (PSDL), a set of best practices based on existing models with the addition of Predix specific requirements. PSDL ensures security is embedded at every layer including infrastructure, platform, data, and application services. This PSDL includes secure design and architecture, threat modeling, risk assessment, software and system security development, and security testing. Embedding security into the development lifecycle ensures that security is built in, not bolted on afterwards.

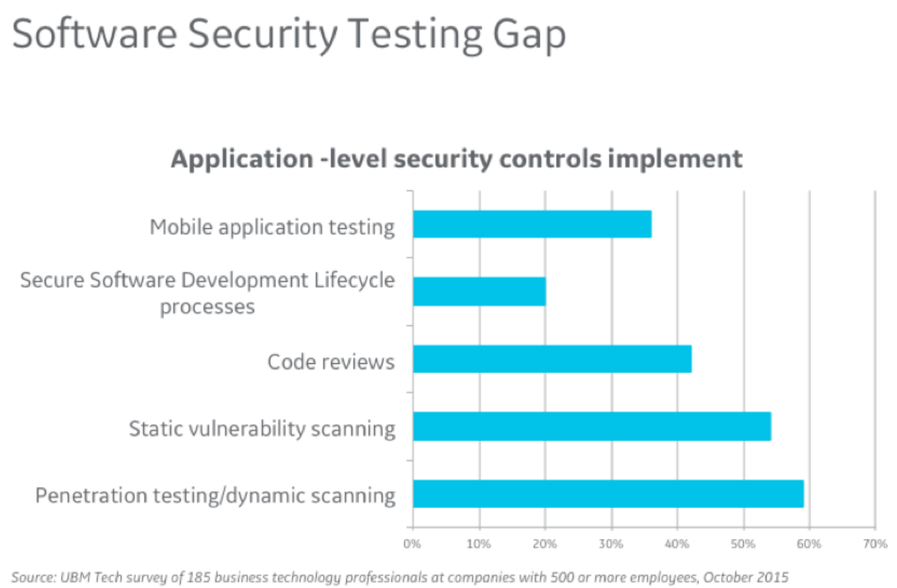


Fig. 2.0 – Software security testing is a critical gap, presenting a significant risk to IIoT adoption

6. *UBM Tech. December 2015. "Application security trends"*

Generally, the PSDL includes careful security considerations at every stage of building the Predix platform:

Requirements gathering and analysis: Assesses the standards, policies, and compliance requirements that the software must follow. This approach ensures that audit requirements are more easily met and allows easier mapping of compliance requirements to security controls.

Design: Threat assessment and modeling tests the software blueprint against numerous threat scenarios and assesses security robustness to ensure the software is resilient by design.

Coding: Developers are trained to understand where technical and business logic vulnerabilities can originate at the coding stage. Secure coding guidelines are enforced and reviews of source code are regularly conducted to meet GE security and quality standards.

Quality Assurance: Vulnerability assessment is conducted using leading-edge testing tools and third-party assessors. Potential human actions and errors are also considered at this stage to assess the potential for insider threat.

Deployment: The platform is configured to strict standards for available services and privileges. Deployment is further protected with security controls and supporting technology, including intrusion detection and prevention systems, firewalls, and encryption.

Embedding security into the development lifecycle

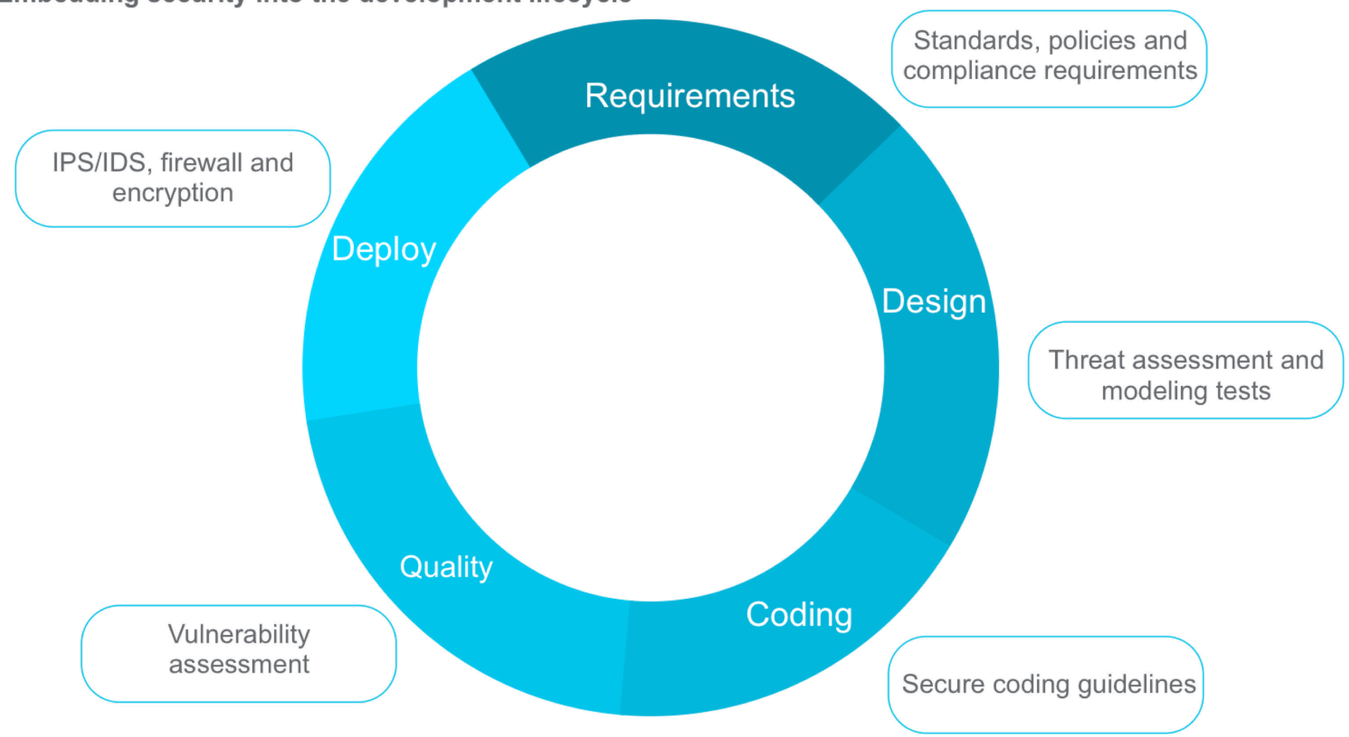


Fig. 3.0 - Predix Secure Software Development

As part of the ongoing release cycle of Predix, these and other best practices are in use throughout the Security Development Operations (SecDevOps) cycle. For example, a design and architecture review, including threat modeling and attack surface analysis, occurs with each new version of Predix. Also, every release must include automated Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) to ensure the code is free of vulnerabilities. Through automated Open Source Software (OSS) vulnerability assessment, as well as an assessment of license compliance requirements, Predix limits the risk of open source conflicts and vulnerabilities. It also includes a red team penetration test to ensure resilience. This approach is integral to the release and updates of the software, and provides confidence that the platform code itself remains secure.

Where some organizations overlook the importance of following a secure development lifecycle, or save security testing to the end, Predix engineers and developers embed security testing and assessment at every stage throughout development.

GE Digital's significant investment in this level of cyber security assurance is unique in the industry and informed by GE's own experiences with cyber security for its operations. The result is a defense-in-depth approach specific to the unique demands of industrial environments.

Secure environment for application development

Industrial environments generate enormous amounts of complex data, but that data often lacks context and common syntax. Extracting insight to enhance operations requires applications that can ingest and analyze this type of unstructured data. Existing IT applications are not ideal for this task. To drive cost savings, efficiency improvements, and process enhancements, new industrial applications are needed.

But, given the unique cyber security vulnerabilities inherent in industrial environments, application developers must understand and adhere to industrial security standards. Without alignment, developers could unwittingly introduce cyber threats to the platform that could lead to disruption.

Industrial applications must address data privacy and security while continuously delivering value added functionality.

With Predix, application security is a fundamental requirement. In order to ensure the security of the Predix ecosystem, the applications on the platform, and the data that flows through those applications, GE Digital provides security-related guidelines, processes, and tools for software development.

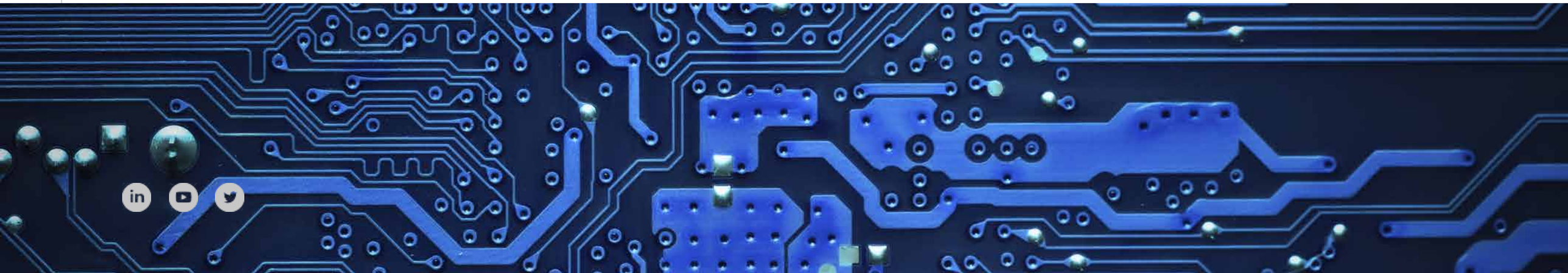
In order to successfully deploy applications to Predix, successful developers will address three key points in the process:

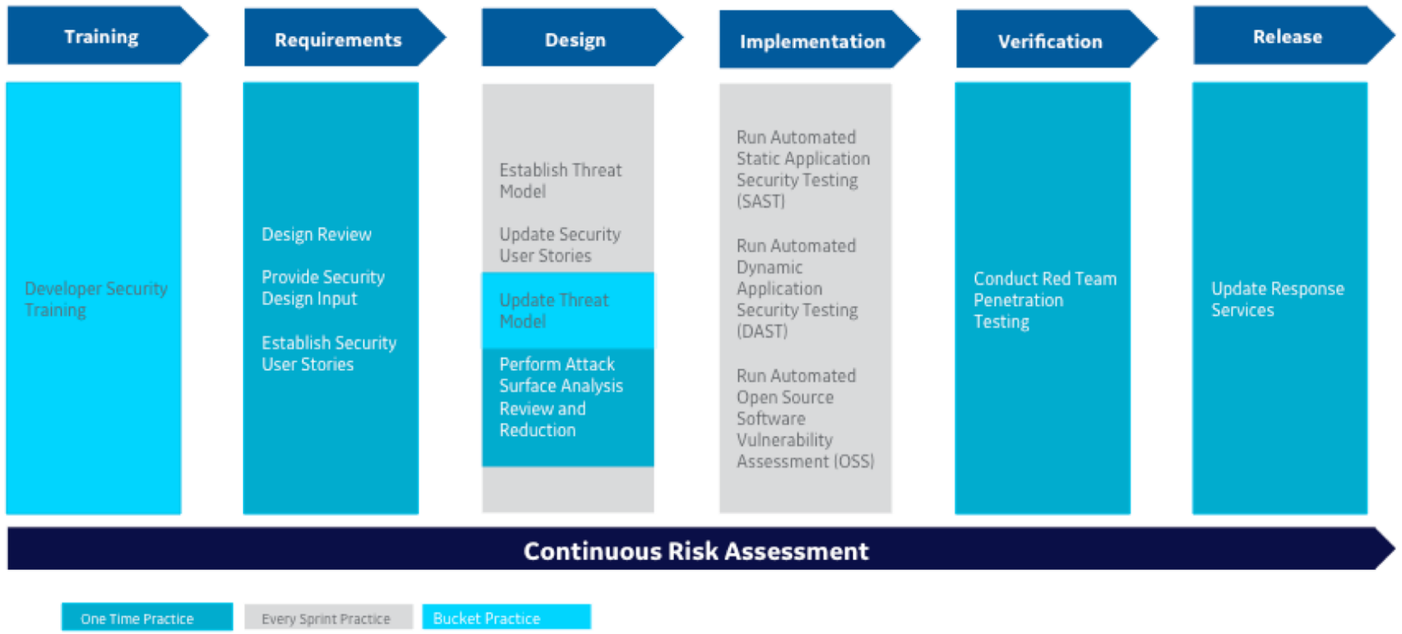
- Consider security of the application during the design and development stage through the PSDL.
- Leverage existing security microservices to speed the development process.
- Submit the programming code and necessary documentation for security review.

Developers have access to a robust and expanding library of microservices that support the migration of existing applications, while also providing an ideal dev/ops environment for the creation of innovative tools and services. Use of microservices can accelerate the deployment of applications, thereby increasing developers' speed to market and helping industrial companies see benefits more quickly.

Predix secure development lifecycle

Ensuring a secure application starts by considering the potential for vulnerabilities during the design and development process. In doing so, application developers can address potential risks before release, thereby reducing costly reprogramming if a vulnerability is found. This approach also ensures that user data is not exposed through exploit of a programming bug.





As applications are designed, the following items are integral to secure development lifecycle (SDL) implementation:

Developer security training: Creating secure applications starts with understanding potential vulnerabilities and the techniques needed to avoid them. Ongoing courses help to improve understanding of techniques for identifying and mitigating security vulnerabilities. Training focuses on topics including threat modeling, SAST, DAST, and OSS testing, and coding techniques to prevent common defects such as SQL injection.

Design/architecture review: Assesses and develops application design patterns that mitigate risk to the platform and associated applications and services.

Threat modeling: A structured approach for analyzing the security of an application with special consideration for boundaries between logical system components, which often communicate across one or more networks.

Security user stories/security requirements: A description of functional and non-functional attributes of a software product and its environment that must be in place to prevent security vulnerabilities.

Automated dynamic application security testing (DAST): A process of testing an application or software product in an operating state, implemented by a web application security scanner.

Automated static application security testing (SAST): A process of testing an application or software product in a non-operating state, analyzing the source code for common security vulnerabilities.

Red team penetration testing: Hands-on security testing of a runtime system. This sort of testing uncovers more complex security flaws that may not be caught by DAST or SAST tools.

Through the PSDL, developers have a streamlined process to speed time to market, without compromising security of the applications.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology, and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-800-322-3616 or 1-434-978-5100
Global regional phone numbers are available on our web site.

www.ge.com/digital