GE Digital

Information Security & Compliance

Software Development Lifecycle | Secure Development

THE CYBER SECURITY POSTURE OF GE DIGITAL PRODUCTS

GE Digital's SDLC process aligns to industry-published secure development standards such as the Microsoft SDL[1], OWASP[2], NIST 800-53[3] and others.
By focusing on best practices, we improve our security posture while still meeting the spirit and intent of broad requirements.

BUSINESS CHALLENGE

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then, I have my doubts" – Gene "Spaf" Spafford

Clearly, such a system would not be terribly useful to an organization operating critical infrastructure in today's world.

Technology vendors and their customers form a symbiotic relationship and must work together to continuously maintain the balance between timeliness-to-market based on demand at an appropriate price point, versus the effort and time spent securing those products based on potential risk and regulatory requirements.

This interdependence continues even after product release. Customers need to deploy, operate, and patch/update/upgrade products in an environment with defense-in-depth and over-time security controls commensurate with risk, while vendors need to respond appropriately when a security weakness is identified.

OVERVIEW

Balancing time-to-market and value with security

All development efforts are based on the following foundational principles:

- **Governance** in accordance with our 9001 Quality and 27001 Information Security Management Systems, associated internal and external audit program(s), and corresponding independent certifications
- Role-based **Secure Development Training** for developers
- **Software Change and Revision Control**, enforcing role-based access control and authorization to modify product code
- Utilizing **Continuous Integration / Continuous Deployment** to detect potential security issues when code changes are made

Our SDLC process mandates that development programs for new product versions or entirely new products undertake the following:

- The Product Manager and engineering team write **security requirements as user stories**, e.g. "As a system admin, I want to be able to enable MFA for specific user-groups to protect against password attacks"
- **Manage use of 3rd party software** by consolidating functionality and versions, inventorying, updating, and performing license and vulnerability scans
- **Threat Modeling** to identify risks early so critical concerns can be mitigated through design decisions
- Performing a **Privacy by Design** assessment to ensure Personal Data / PII can be appropriately protected
- Deriving **Technical Requirements** from user stories and putting them into actionable change or enhancement requests for developers
- Leveraging **Automated Code Analysis** (static and/or dynamic) to automatically detect and report on potential bugs before new code is released
- **Peer Code Reviews** with a security focus are performed since tools may not be able to identify well-written malicious code
- Drafting a **Secure Deployment Guide** to instruct the end user on controlling residual risk
- **Security Release Review and Sign Off** which ensures the appropriate steps outlined above were taken
- Periodically commissioning **Independent Assessments or Penetration Testing**, based on factors such as a product's risk rating or major changes

GE Digital

Information Security & Compliance

Software Development Lifecycle | Secure Development

VALUE DELIVERED

Independent InfoSec Certificate

Rely on the work of an independent, accredited auditor who has verified GE Digital not only has secure development policies and procedures in place in accordance with ISO27001's "A14.2 Security in Development and Support Processes" requirements, but also samples evidence for those controls to ensure they are being adhered to

Evolves with the Times

GE Digital is committed to continuous improvement, which necessarily includes our Secure Development Lifecycle processes and controls. For example, with the introduction of GDPR we added requirements to assess and document any privacy impacts.

Leverage Industry Expertise

Using publicly available Secure Coding standards and guidelines eases GE Digital's ability to share those practices with customers, onboard personnel coming from other development companies, and stay up to date as best-practices change.
Such public standards also make the use of off-the-shelf analysis tools easier too, as custom rules don't need to be maintained for scanning.

"Shift Left" Mentality

We've implemented a number of measures to put information about code security at developers' fingertips so potential new issues can potentially be caught early. Static code analysis tooling enables code scanning and a display of findings; the continual CI/CD pipeline builds can integrate with both dynamic and OSS CVE scanning to generate finding reports early & often rather than waiting until the end of the release cycle.

Partnering on Pen Tests

GE Digital has specialized teams perform internal penetration testing and also partners with independent, 3rd-party organizations to perform penetration testing & vulnerability assessments on a rotating basis. Testing considers factors such as likelihood and impact of compromise in the real world, recent architectural changes affecting technical risk, amount of time since last assessment and more

OTHER KEY INFORMATION SECURITY & COMPLIANCE OFFERINGS

Personnel & Training

Partner with GE knowing its experts are up-to-date with trainings in cyber security areas.

Open Source Software Security

GE's Digital OSS Security strategy is largely meant to cover the four OSS practices recommended by Microsoft and address the risks raised in other industry guidelines.

Secure Product Delivery

The SDLC process is not complete until the software is securely in the hands of the intended customers.

Supply Chain Risk Management

GE takes its role as a supplier of systems seriously, and has pre-populated questionnaires, model procurement language, and information to assist Entities with their supply chain risk assessments

GE Digital continues to evolve its established Secure Development Lifecycle policies, procedures, and processes to continually improve software security while balancing other KPIs such as usability, time to market, and cost.

Footnotes

[1] https://www.microsoft.com/en-us/securityengineering/sdl
[2] https://owaspsamm.org/model/
[3] https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/

Contact Us

ge.com/digital/sales-contact-me