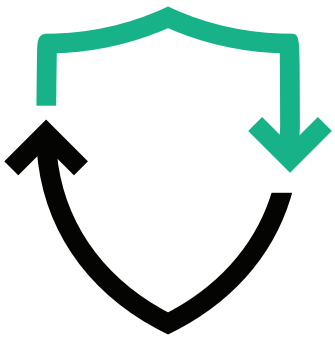
Hewlett Packard Enterprise

Enable secure product delivery

HPE Software Security & Trust Office



Who we are

The mission of the Security & Trust Office is to enable the secure delivery of HPE software products portfolio, increase customers trust, and address security reports.

Integrating security with software development

Three-tier security layers

- Security Lifecycle Management (SLM)
- Software security scanning tools
- Security lab assessment

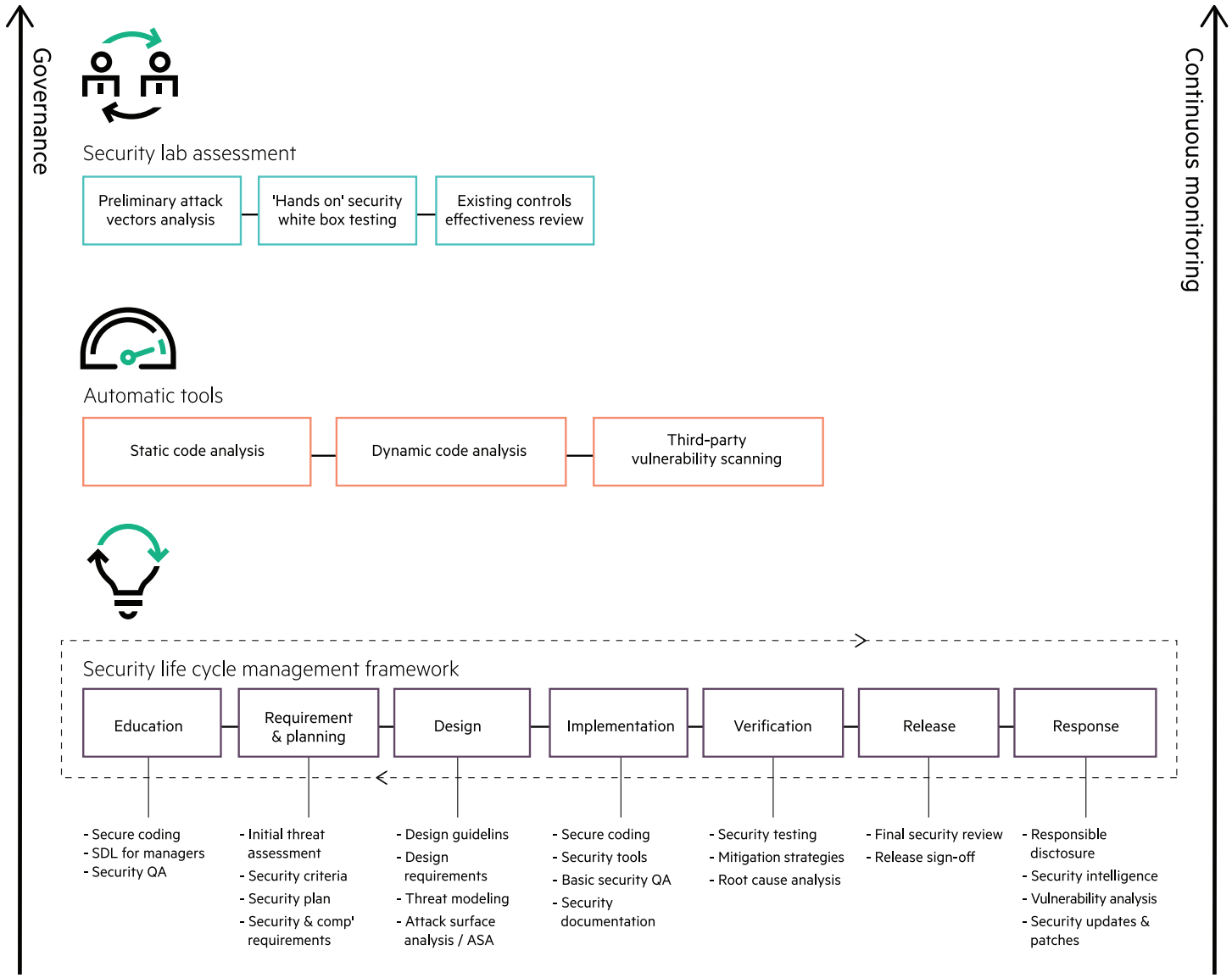
HPE Software is well aware of the responsibility it has to provide the best solutions possible while making sure our products are enhanced to provide our customers the appropriate information protection.

To achieve this, HPE Software has adopted security industry best practices and adapted those to our own products and business processes. We have established industry-leading software secure design and coding techniques and a comprehensive Security Lifecycle Management (SLM) framework to support an end-to-end product secure development and shipment.

Product secure delivery model

Multi-stage security phase in the development lifecycle

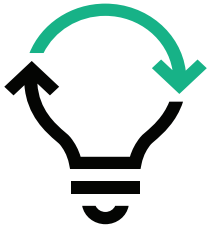
HPE Software incorporates three-tier security layers in our development lifecycle, allowing us to incorporate security from the early development stage to a proactive test of efficiency of the security controls as the development moves on, with a static code analysis and hands-on security penetration test provided by industry-leading security experts.



Security Lifecycle Management (SLM) framework

HPE Software has established a secure development framework to enable the proactive integration of security into its products lifecycle. The integration of comprehensive security controls such as design review, threat modeling, security testing, and more into the product lifecycle makes sure the risks are identified and appropriate mitigation is provided prior to the product release.

Framework components



Security Lifecycle Management (SLM)

– Proactively integrating security controls throughout development process, direct and indirect. Empowering our developers with knowledge in secure development, identifying in early stage potential risks and including proper measures to address incident when occurring.

Education (Security experience)

Our product security lifecycle is built from the ground up to make sure that all key personnel involved in the product lifecycle are equipped with a comprehensive set of tools to deal with today's threat landscape.

The objective of the education phase in the HP Software products lifecycle management framework is to provide the different functions in our product teams (executives, product management, development, QA, and operational staff) with the necessary competencies required to handle related security threats they encounter in their daily jobs.

All of that is provided through a comprehensive educational security experience framework, which enables the relevant vulnerability management tools to the product teams.

Requirements and planning

The objective of this phase is to define, conduct an initial assessment, and prepare toward the future release of the products. The requirements and planning phase includes:

– Performing an initial threat assessment for planned features and enhancements

– Define product security release criteria

– Create a product security plan that will serve as a baseline for all related security activities

– Define security and compliance requirements

Design

Through this phase, the Security & Trust Office will work with the R&D team to perform a threat modeling and design review to build a secure product architecture and design with appropriate mitigation in place. This stage will include the following activities:

– Perform a threat modeling and design review for planned features and enhancement (including an assessment for usage of third parties)

– Define secure design requirements

– Perform attack surface analysis or reduction

Implementation

The security controls through the code implementation phase will assist in risk reduction before later phases and assist the product teams in identifying risks independently. The stage will include the following activities:

– Develop code using secure coding guidelines

– Run automatic tools during code implementation and QA phases

– Perform basic security testing by the QA teams

– Fix detected vulnerabilities according to acceptance criteria

– Create secure deployment guidelines

Verification

The verification phase objective will provide a comprehensive product risk status to make sure risks are identified before release. The stage will include the following activities:

– Perform comprehensive product security testing

– Validate mitigation strategies and root cause analysis

– Fix detected vulnerabilities

– Validate security fixes

Release

Through the release phase, the team will perform final security validations execute a mitigation plan, and approve product version for release. The stage will include the following activities:

- Perform final security review to enable mitigation of design risks and identified security vulnerabilities
- Perform necessary mitigations
- Approve product version release

Response

The response phase objective is to maintain a secure product according to evolving attack trends and customers' feedback, address security threat, and work with the R&D teams for resolution following a comprehensive disclosure to customers.

Software security scanning tools

To provide our engineers' community with secure development tools to identify risks independently, HPE Software Security & Trust Office has deployed a comprehensive multi-tier security scanning platform.

Software security scanning tools

- Utilizing the benefits of security scanning automation. Providing better efficient security coverage and allowing our team of developers to play major role in conducting the scans, running the analysis and assuring proper mitigation.

Static code analysis—using HP Fortify

HPE Fortify Static Code Analyzer uses multiple algorithms and a vast knowledge base of secure coding rules to analyze an application's source code for vulnerabilities that can be exploited in deployed applications.

Early identification of risks allows efficient and timely mitigation and enables secure product release.

Aligning the Security & Trust Office knowledge and expertise with HPE Fortify high quality security code scanning techniques provides an efficient secure development solution to HPE Software product teams.

HP Software developers can now identify risks independently, during code implementation phase without the need for an intensive security professional background.

To learn more: Fortify static code analyzer

Dynamic analysis—using HP WebInspect

HPE WebInspect is an automated and configurable Web application security and penetration testing tool that mimics real-world hacking techniques and attacks.

Aligning the Security & Trust Office knowledge and expertise with HP WebInspect creates an efficient solution for HPE Software product teams and their engineering workforce.

HPE Software quality assurance engineers, with the guidance of HPE Software Security & Trust Office can now simulate known hacking and penetration techniques as part of their ongoing software testing process, and address them in early stages.

To learn more: WebInspect

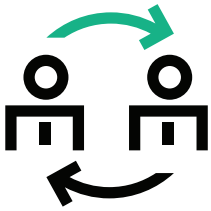
Third-party vulnerability scanner

As part of the ongoing security scans, the Security & Trust Office incorporates automatic security scans for third-party components embedded in our software.

Addressing security vulnerabilities found in third-party components is an integral part of detecting any potential security vulnerabilities that may pose potential threats; risks identified are analyzed, addressed, and resolved either by applying the vendor resolution or by a workaround (if possible) provided by the product engineers and Security & Trust Office software security experts.

Security lab assessment

Comprehensive software security assessments are performed by a team consisting of application security researchers to make sure vulnerabilities are identified before release at all product layers. The assessments consist of these vulnerability activities and testing techniques:



Security lab assessment

– 'Hands on' security analysis and penetration testing provides critical inputs on potential risks not identified on early stages. Security lab assessment provides the last cycle of security analysis prior to product release.

Activities:

1. Information gathering from various sources—human and technological. This includes communicating with technical people.
2. Analysis of the product structure, interfaces, data flow, sensitive modules, infrastructure and architectural aspects, and reliance on third-party products or interfaces, and identifying classes of vulnerabilities.
3. Hands-on testing of the product in various scenarios, with respect to previously obtained knowledge of the product and its data flow scenarios.
4. Analysis of gathered data and results from the previous security assessments. The analysis includes categorizing the detected vulnerabilities and prioritizing them according to the business and technical context of the application.
5. A final and comprehensive report of the security review activity, summarizing the entire review process, the methodology, and the detailed findings.

The security assessment is performed in light of the related risks involved (evaluated based on an unauthorized activity of both a legitimate user and a non-legitimate user).

The following product areas and mechanisms are assessed:

1. Authentication mechanisms of both machine-to-machine and man-machine interfaces (e.g., process, scope, enforcement point, standards, strengths, session management, impersonation, delegation, trust relations, single sign-on usage, and more).
2. Authorization mechanism of both machine-to-machine and man-machine interfaces (e.g., scope, enforcement points, security profiles, privilege elevation, users' privileges profiles, segregation, and compartmentalization) of human and code entities.
3. Auditing mechanism (e.g., log quality, log protection, sensitive information handling, alert mechanisms).
4. Users' management mechanisms (login processes, revoke, audit).
5. Password management mechanisms (policy, minimum requirements) of human and code entities.
6. Cryptography usage and implementation (e.g., standards, algorithm usage, key management, digital signature usage, secure hashing, secure random number generation, and so on).
7. Secure transport mechanisms (confidentiality and integrity protection mechanism implementation related to each transport).
8. Protection mechanisms against denial-of-service attacks (e.g., users locking buffer overflows, request flooding).
9. Secure configuration.
10. Robust review of secure architecture and design.

4AA5-3485ENW, January 2016, Rev.1