WHITE PAPER

SAS® Product Security Framework

Engineering secure products

Contents

About the framework 1

Governance and participation 2

Secure design 2

Secure implementation 3

Security testing 4

Incident management 5

You can count on SAS 6

About the framework

The SAS Product Security Framework is our conceptual foundation for producing software that is resistant to misuse and cybersecurity threats. It organizes a wide array of security resources and activities into five logical categories. This structure helps ensure that security considerations are identified, prioritized and addressed throughout the software development life cycle (SDLC).

Figure 1 depicts the framework's five categories and selected elements within each category.

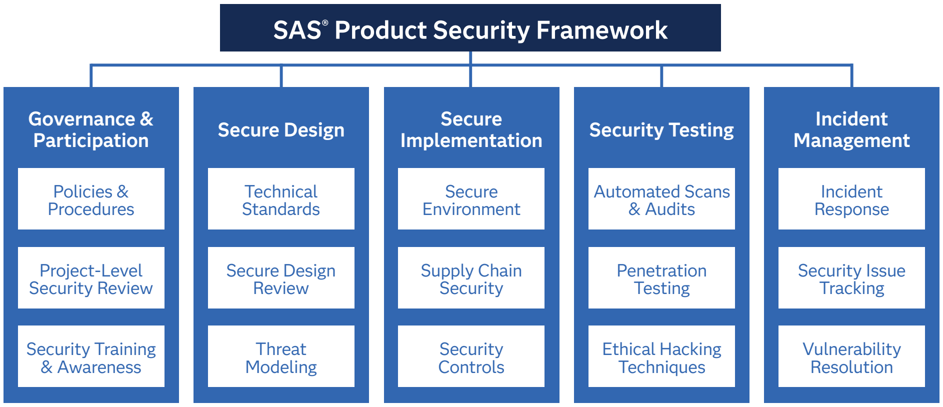

Figure 1: SAS Product Security Framework

Note that the framework does not prescribe a particular sequence of security activities. Instead, the pattern and chronology of security activities adapt to the shape of any SDLC to which the framework is applied. For example, if the framework is applied to the SDLC that is depicted in Figure 2, security activities occur in continuous micro-iterations and are repeated as applicable in each instance of each life-cycle phase.

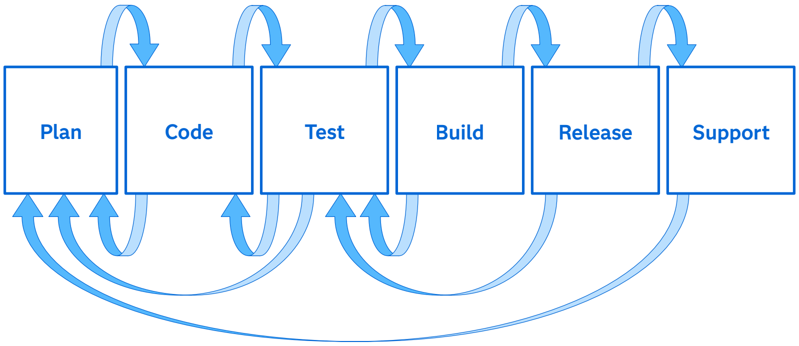

Figure 2: Example of a software development life cycle

The following sections highlight key aspects of each category of the SAS Product Security Framework. For information about the SAS software development life cycle, please refer to the **SAS Quality Imperative** white paper.

Governance and participation

Policy

Our product security policy reflects industry best practices and standards from organizations such as the US National Institute of Standards and Technology (NIST), the International Standards Organization (ISO) and the Open Web Application Security Project (OWASP). All R&D product teams are required to comply with the policy.

PLSR

Our project-level security reviews (PLSRs) provide objective evidence of conformance to SAS product security policy requirements.

People

Key contributors include:

- A centralized team of dedicated product security specialists.
- A matrix organization of divisional product security leads and security champions.
- Project managers that plan, scope and monitor security work for their product teams.

Training

Product security training is delivered through mediums that include:

- Real-time application security coaching within development environments.
- Internal forums and demonstrations on tools and trending topics in application security.
- Formal application security training modules in our corporate learning management system.

Culture

Security engagement is fostered by internal activities such as:

- Retrospectives for major product security incident events.
- Reviews of lessons learned from penetration testing.
- Ethical hacking and cybersecurity awareness events.

Secure design

We implement a secure-by-design philosophy as follows:

- Our product teams are empowered to review their product and platform architectures to identify and address security design flaws and potential security enhancements. These embedded continuous efforts include techniques (such as threat modeling) that can identify security issues not detectable by security scan tools.
- Our secure design review practice uses structured multifaceted analysis to identify and address security design risks. In each secure design review, a product security specialist collaborates with a product team to produce a holistic evaluation of the security design and posture of a particular product or architecture.

Secure implementation

Environment

- Our engineers work in trusted, secure development and build environments that are centrally monitored and maintained.
- Our software build systems and release pipelines are accessible to only those individuals who have a legitimate need for access.
- Automated checks help ensure that shipping code includes required security updates.

Requirements

- Throughout the software development life cycle, we prioritize security requirements, both functional and nonfunctional.
- We build software according to industry best practices for secure coding and open protocol standards for secure authentication and network communication.

Controls and configuration

- Examples of application security controls that are incorporated into our products include allowable encryption algorithm and cipher suite specification, authentication and authorization mechanisms, audit controls, error handling and session management.
- To ensure that our products are secure in deployment, we identify secure default configuration settings and provide guidance to customers on the risks of altering those defaults.

Supply chain

- Digital signatures ensure the integrity of SAS software. All SAS components that interact with the operating system (or that otherwise require digital signatures to work properly) are signed using a trusted SAS certificate. Windows executables, installation files, Outlook plug-ins and extensions, various Java files and other pieces are signed as required.
- Software components, including third-party components, are required to be scanned against Common Vulnerabilities and Exposures published in the National Vulnerability Database, maintained by NIST.

Security testing

Our multidimensional approach to security testing strengthens the resilience of SAS products to external threats. Trained engineers triage findings to identify, confirm and analyze potential weaknesses. Confirmed issues are captured in an industry-standard tracking system and addressed in accordance with our product security policy.

Test techniques and targets vary by software type and can include:

- Industry-recognized security scanning to flag known vulnerabilities such as those described in OWASP, Common Weakness Enumeration (CWE), Common Architecture Weakness Enumeration (CAWE) and Common Attack Pattern Enumeration and Classification (CAPEC). We make extensive use of commercial and open source tools for:
    - Software composition analysis (SCA).
    - Static application security testing (SAST).
    - Dynamic application security testing (DAST).
    - Open Container Initiative (OCI) testing.
- Testing with users of different role-based security access to make sure that each user has the appropriate access levels.
- Data access, based on row-level permissions, to confirm that data authorization is applied appropriately for each user.
- Password and encryption security.
- Correct behavior with Transport Layer Security enabled protocol (HTTPS).
- Validated credential protection when using SAS/ACCESS® engines to connect to data sources (e.g., user ID and password).
- Product-specific security tests for appropriate user authorization and error testing.
- Integration testing of security features and controls.

Enhanced test and verification activities include the following:

- Within our SAS® Viya® release pipeline, we use automation to capture audit records of security scan results in real time and generate corresponding security issue tickets as applicable. This enhances our ability to discover and address any vulnerabilities or flaws early in the software development cycle and secure our latest releases against common vulnerabilities and exposures (CVEs).
- We monitor the quality of our code as it moves from development to build to release environments. We work to continuously refine and automate that monitoring process.
- We use ethical hacking techniques during our internal bug bounties and bug bashes. Those techniques exercise business logic and workflows that might not be captured by security scanning tools.
- We engage third parties to perform independent security assessments and penetration testing on our software products to determine their resiliency to attack and misuse. Specially constructed virtual environments are used to simulate customer deployments in the cloud and on-site.
- We respond to our customers' security and internal audit teams to verify the results of their own security testing. SAS technical support (**support.sas.com**) works with organizations to understand the significance and impact on environments pertaining to any findings.

By policy, SAS does not share tests or individual results. SAS product security testing tools, methods, models and results are company confidential.

Incident management

Commitment	SAS is committed to responsible reporting of security incidents and managing vulnerabilities identified in our software and integrated third-party components. We are a proud member of the **Forum of Incident Response and Security Teams (FIRST)**.
Approach	Our product security incident response team works with SAS technical support, customers and industry partners to create an informed understanding of the applicability, severity and impact that a security finding may have. The team uses a structured approach to investigating, scoring and responding to vulnerabilities.
Information from SAS	• **SAS security bulletins** are official SAS statements and advisories on the applicability of major CVE announcements and our recommended resolution. • To empower you to determine the status of security findings that may be identified in your own scans, SAS provides data about security vulnerabilities that are addressed in each cadence version of SAS Viya. Licensed customers may request access to this data by contacting **SAS technical support**. • **SAS Notes with security vulnerabilities** and **Communities: SAS Hot Fix Announcements** are for products on the SAS 9.4 and SAS Viya 3.x platforms. • Products on the SAS Viya platform receive **patch updates** instead of hot fixes. • Products on other platforms access hot fixes from the **downloads and hot fixes** page.
How to contact SAS	• Customers who have a valid SAS support contract should report suspected security issues by opening a track with **SAS technical support**. • Security researchers or others who do not have a support contract can contact the SAS product security incident response team directly by emailing psirt@sas.com. Information about security vulnerabilities should be encrypted by using our **PGP public key**.

You can count on SAS

SAS is committed to delivering and maintaining secure analytics solutions. Our solutions and their deployments are highly adaptable to the security configuration requirements of our customers. We have integrated industry best practices for software vulnerability detection throughout each phase of our software development life cycle. We continuously analyze and improve the resiliency of our software against today's emerging cybersecurity threats.

To learn more, please visit **sas.com/trust**.

For more information, please visit sas.com/trust.