Scribe

Securing the Future: Delivering Software Products Secure by Design with Scribe Security

INVINCIBLE PRODUCT SECURITY

Additional information is available on scribesecurity.com

Introduction

As the reliance on software continues to grow exponentially, ensuring its security is no longer optional—it's imperative. The traditional approach of addressing vulnerabilities post-deployment has proven insufficient in mitigating the rising tide of cyber threats. Secure by Design principles emphasize integrating security throughout the software development lifecycle (SDLC), shifting responsibility upstream to manufacturers. Achieving this demands not just a commitment to secure practices but robust technological support.

Scribe Security has emerged as a critical enabler of this paradigm, offering transformative capabilities to embed security into every phase of development. This white paper explores why Secure by Design is essential and how Scribe Security empowers organizations to deliver secure software products while maintaining speed and compliance.

The Importance of Secure by Design

The Secure by Design philosophy entails embedding security as a foundational element of product development, ensuring protection against cyber threats from inception to deployment. It is no longer enough to deliver software products and expect users to bear the burden of securing them through manual configurations or frequent updates. Manufacturers must integrate security into the core of their products and processes.

The stakes are particularly high in critical industries such as financial services, healthcare, and infrastructure, where breaches can compromise sensitive information, disrupt services, and undermine trust. Secure by Design practices, supported by robust SDLC policies, provide a way to break the vicious cycle of patch-and-fix by preventing vulnerabilities from reaching production in the first place.

Alignment of Scribe Technology with Secure by Design Principles

The principles outlined in the **Secure by Design** document published by CISA, The NSA, and other commercial and governmental contributors emphasize proactive, built-in security practices that reduce the burden on end-users and ensure robust, reliable products. Scribe Security's technology aligns seamlessly with these principles by embedding policy-as-code capabilities directly into the software development lifecycle (SDLC), enabling automated enforcement of security measures and adherence to secure design standards. Below is a detailed explanation of how Scribe's solutions correspond to the key Secure by Design principles, supported by evidence from the document.

---

1. Taking Ownership of Customer Security Outcomes

The Secure by Design document emphasizes that manufacturers must take ownership of security outcomes rather than leaving the burden on customers. This principle is rooted in proactive application hardening, secure feature design, and default configurations.

Reference from the Secure by Design document: "Manufacturers should take ownership of their customers' security outcomes rather than measuring themselves solely on their efforts and investments".

How Scribe Aligns:

- **Policy-as-Code Enforcement**: Scribe allows organizations to codify security and compliance requirements into their SDLC. By integrating these policies into CI/CD pipelines, Scribe ensures that all builds meet secure configuration and SDLC requirements, effectively taking ownership of security.
- **Breaking the SDLC Process for Non-Compliance**: If a build fails to comply with predefined security policies, Scribe's technology halts the process, ensuring that insecure artifacts are never released. This automated enforcement removes the burden from end-users and ensures consistent application of security standards.

---

2. Embedding Security into the SDLC

The Secure by Design document stresses the importance of embedding security into the SDLC and making it a central component rather than an afterthought.

Reference from the Secure by Design document: "Secure by design development requires the strategic investment of dedicated resources by software manufacturers at each layer of the product design and development process that cannot be 'bolted on' later".

How Scribe Aligns:

- **Integrated DevSecOps Tooling**: Scribe embeds security checks and policy enforcement mechanisms directly into DevOps workflows, ensuring security is an intrinsic part of every development stage.
- **Enforcing Compliance with Frameworks**: Scribe ensures adherence to frameworks like the NIST Secure Software Development Framework (SSDF) and Supply Chain Levels for Software Artifacts (SLSA). This guarantees that security is not an add-on but a built-in feature of the SDLC.

---

3. Automation and Default Security

The principle of “Secure by Default” outlined in the Secure by Design document stresses that products should be secure out of the box, with automation playing a significant role in achieving this.

Reference from the Secure by Design document: "The complexity of security configuration should not be a customer problem. Manufacturers can aid their customers by optimizing secure product configuration".

How Scribe Aligns:

- **Automated Security Compliance**: Scribe’s policy-as-code capabilities automate the enforcement of secure configurations, reducing manual effort and ensuring that products are secure “out of the box.”
- **Preventing Misconfigurations**: Scribe eliminates the need for users to apply hardening guides manually by embedding secure defaults and nudging developers to adopt secure practices during development.

---

4. Transparency and Accountability

Radical transparency is a key pillar of the Secure by Design philosophy, encouraging manufacturers to provide clear documentation and visibility into their security practices.

Reference from the Secure by Design document: "Publish data on unused privileges… and ensure the security of software by providing transparency and accountability across the lifecycle".

How Scribe Aligns:

- **Software Bills of Materials (SBOMs)**: Scribe generates and manages SBOMs, providing end-to-end traceability of software components. This aligns with the Secure by Design emphasis on transparency and the need to provide visibility into the software supply chain.
- **Continuous Attestations**: Scribe generates cryptographically signed attestations, ensuring traceability and accountability throughout the software lifecycle. These attestations give stakeholders confidence in the integrity and compliance of software artifacts.

---

5. Accelerating Time-to-Market Without Compromising Security

One of the core challenges for manufacturers is balancing security with the need to deliver products quickly. The Secure by Design document encourages investments in automation and secure practices that do not hinder speed.

Reference from the Secure by Design document: "Over time, engineering teams will be able to establish a new steady-state rhythm where security is truly designed-in and takes less effort to maintain".

How Scribe Aligns:

- **Policy Integration in CI/CD Pipelines**: By stopping security problems early in the development cycle, Scribe's technology prevents delays caused by addressing vulnerabilities post-deployment.
- **Real-Time Feedback**: Scribe provides immediate feedback to developers, enabling rapid remediation and reducing the time required to address security concerns.

A Closer Look: Empowering Secure by Design Development

Scribe Security's technology enables organizations to operationalize Secure by Design principles effectively. By embedding policy-as-code capabilities into the SDLC and DevOps toolchain, Scribe offers unparalleled power to enforce compliance, ensure consistency, and build confidence in the security of the final product.

Policy as Code: Enforcing Security Throughout the SDLC

One of Scribe's most critical capabilities is its advanced **policy-as-code framework**, which empowers organizations to codify security and SDLC requirements as executable policies. This integration ensures that security and compliance checks are no longer subjective or manually enforced but are embedded into the CI/CD pipelines. By operationalizing these policies, Scribe enables organizations to:

- **Break the SDLC Process if Mandatory Security Requirements Are Unmet**: Scribe's policy-as-code capabilities ensure that deviation from mandatory secure SDLC requirements halts the development process (in the Admission Controller or even earlier in the build process). This enforces a rigorous adherence to security frameworks such as the NIST Secure Software Development Framework (SSDF) and others. The decision to break the SDLC process or just get the alert on a violation and deal with it later depends on the company's security policy and can differ from one product to another.
- **Prevent Vulnerabilities from Reaching Production**: By embedding mandatory security checks early in the process, Scribe stops issues at their root before they can grow into costly and critical vulnerabilities.
- **Automate Compliance with Secure SDLC Frameworks**: Policies can be written, tested, and updated dynamically to reflect evolving security needs, ensuring that every release complies with organizational and regulatory standards.

Integrating Security Directly into CI/CD Pipelines

By integrating security policies directly into CI/CD pipelines, Scribe accelerates time-to-market without compromising security. This approach enables:

1. **Immediate Detection of Non-Compliance**: Security problems are identified at their inception, preventing downstream delays and avoiding the need for extensive rework after development.
2. **Faster Iterations**: Developers receive real-time feedback on compliance issues, enabling rapid remediation and seamless alignment with organizational policies.
3. **Enhanced Reliability**: Automated enforcement of policies ensures consistent application of security standards, reducing human error and subjectivity.

By catching potential issues early, Scribe's policy-as-code integration minimizes the impact of security problems, enabling teams to maintain velocity without compromising integrity.

Use Case: Compliance with SLSA and SDLC Enforcement

A major financial services company faced challenges in securing its software supply chain and ensuring compliance with industry frameworks such as the Supply Chain Levels for Software Artifacts (SLSA). With increasing regulatory scrutiny, maintaining the chain of custody and preventing unauthorized or insecure software releases became paramount.

Challenges:

- Ensuring every build met mandatory SDLC security requirements.
- Maintaining a complete chain of custody for software components.
- Automating compliance with SLSA to meet regulatory and audit requirements.

Solution:

By deploying Scribe Security, the company achieved the following:

1. **Policy Enforcement**: Scribe’s policy-as-code framework was integrated into their CI/CD pipelines, ensuring that any software artifact failing to meet SDLC requirements was blocked from progressing to production.
2. **Chain of Custody**: Scribe's platform provided end-to-end traceability of software artifacts, enabling the company to maintain a comprehensive chain of custody.
3. **Automated Compliance with SLSA**: Scribe automated the validation of SLSA compliance for every build, generating cryptographically secure attestations and verifying artifact integrity at every stage.
4. **Release Assurance**: Only artifacts that met all security and compliance criteria were signed and released to production, safeguarding the company's software ecosystem.

Outcome:

This integration provided the financial services company with unmatched confidence in their software's security and compliance. By automating key elements of the SDLC and embedding security into their workflows, they reduced the risk of supply chain attacks, ensured regulatory compliance, and accelerated their release cycles.

The Case for Mandatory Policy Enforcement in SDLC

Embedding security into the SDLC using policy as code is essential for organizations to deliver secure products consistently. Traditional security approaches that rely on reactive measures or manual enforcement are insufficient in today's high-stakes environment. By mandating compliance with secure SDLC frameworks through automated policies, organizations can:

- **Achieve Greater Scalability**: Automation reduces the reliance on specialized security teams, making secure development accessible at scale.
- **Reduce Costs**: Addressing vulnerabilities early in the lifecycle is exponentially cheaper than post-deployment fixes or damage control.
- **Enhance Customer Trust**: Delivering secure products by design strengthens customer confidence and reinforces brand integrity.

Conclusion

The journey toward Secure by Design software development is complex but essential. With Scribe Security's advanced policy-as-code capabilities, organizations can confidently enforce secure SDLC frameworks, prevent vulnerabilities from progressing through the development lifecycle, and accelerate time-to-market without compromising security.

By adopting these technologies and practices, organizations can create a new standard for software security—one where Secure by Design is not an aspiration but a reality embedded into every release. The time to act is now, and the tools to succeed are here.