Whitepaper

Okta Secure Development Lifecycle

The Secure Development Lifecycle encompasses Okta's security practices and imposes requirements during product development.

Whitepaper

Okta's Secure Development Lifecycle is the process of ensuring security is prioritized from the outset.

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

Learn how Okta’s Secure Development Lifecycle fits in to both the Product Development Lifecycle and the Software Development Lifecycle.

We’re prioritizing security from the outset with the Okta Secure Development Lifecycle.

At Okta, we know that our customers rely on us to protect what matters most: their data, their users, and their reputation. This responsibility drives everything we do, shaping our approach to secure development and ensuring we deliver on our promise: Always Secure. Always On.

As the Chief Security Officer at Okta, I have the privilege of leading a team that places the security and trust of our customers at the heart of everything we do. Security isn’t just a step in our process — it’s woven into the very fabric of how we build, test, and deploy our products. Our developers, security engineers, and product teams work hand-in-hand to embed robust security practices at every stage of the software development lifecycle.

This whitepaper outlines the principles, methodologies, and technologies that power Okta’s secure development practices. It showcases our comprehensive approach to security at every stage of the development lifecycle, ensuring the integrity and resilience of our products and services.

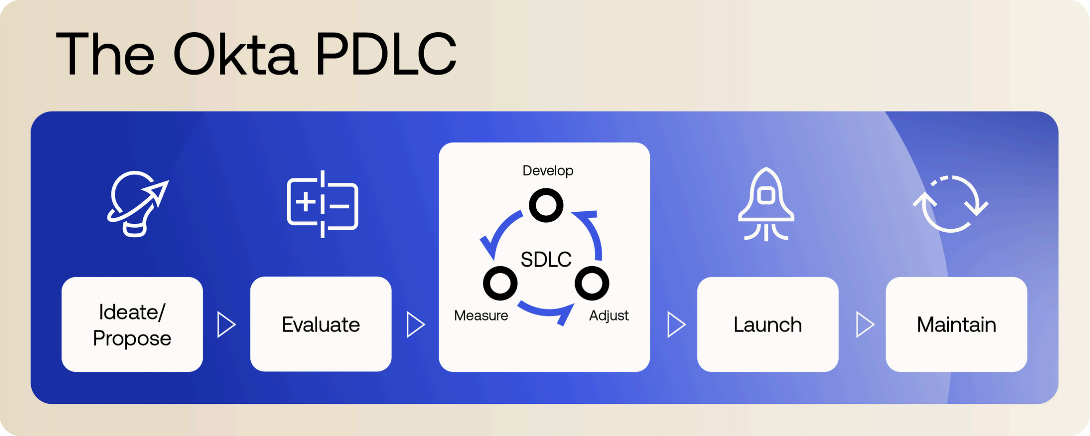
Our ongoing commitment is to deliver reliable security you can trust.

David Bradbury

Chief Security Officer, Okta

Introduction: What is the Secure Development Lifecycle?

The Secure Development Lifecycle, or SDL is a process Okta leverages which encompasses critical security practices and imposes requirements on both the Product Development Lifecycle (PDLC), and the Software Development Lifecycle (SDLC) to prioritize security from the beginning.


The Okta PDLC

Ideate/ Propose
Evaluate
Develop
SDLC
Measure
Adjust
Launch
Maintain

The Secure Development Lifecycle (SDL) consists of product security practices, prioritizing security resilience of Okta products. Each individual security practice uniquely targets differing elements of secure software and system development which operates synergistically with Okta’s product development process.

The Secure Development Lifecycle (SDL) is Okta’s standard for integrating security seamlessly into Okta software products and solutions. Okta’s engineering organizations leverage the SDL for incremental development, bug fixes, feature additions or capabilities, security updates, incremental library changes, and continuous feature delivery.

Both the Software Development Lifecycle (SDLC) and the Product Development Lifecycle (PDLC) are interdependent, each playing distinct roles as products and features are released.

Secure Development Lifecycle: The breakdown

Throughout various stages of the product and software development lifecycles, the following Okta Secure Development Lifecycle (SDL) practices cover a range of security practices aimed at improving the foundational security of our products. While each practice independently focuses on critical aspects of secure software and system development, their interdependent implementation establishes a multi-layered and comprehensive security model.

The following security practices are crucial in handling and mitigating product-development risks with a security-first focus:

Security education
Okta employees are subject to role-specific security training to keep current on industry themes, trends, and technologies.

Secure design
Okta's product teams employ a practice of planning and building with a security-centric lens from the outset of the design and ideation process.

Secure implementation
Okta's product development teams prioritize security pre-releases in order to capture, address and resolve potential vulnerabilities ahead of time.

Secure deployment
Throughout Okta's technology lifecycle, we emphasize security's importance through deployment, maintenance and retirement.

Security education

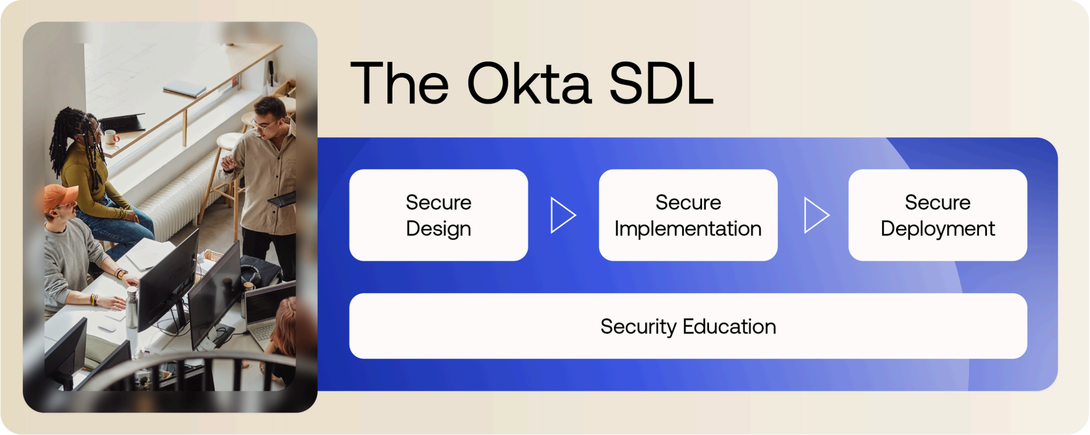
Security training

At the heart of Okta's commitment to making its products more secure is dedication to training our engineering community in secure coding techniques. New hires receive security training within their first quarter of employment, and must complete training and certification annually throughout their tenure. Additionally, the Security Education program offers targeted training for personnel involved in the development of Okta products. Security training is tailored and targeted for specific roles.

Security standards and guidelines

A security education program is incomplete without specific guidance for the development community on how to develop secure software. Security standards and guidelines offer Okta developers specific guidance on secure coding best practices.

All of Okta's products and software artifacts follow general design principle standards for secure software development. Secure coding guidelines are crucial to ensure that applications and products are developed with security in mind from the outset. Okta's principles offer specific guidance on how to make use of frameworks to ensure that resulting applications are resilient to threat actor attacks, minimizing security vulnerabilities.



The Okta SDL

Secure design

This stage defines the requirements that apply to the Product Development Lifecycle (PDLC) and encompasses all required security practices that take place during the creation and design of software systems. These security practices are performed during the design phase of a software system, enabling identification of security concerns earlier. This allows for strategic system design changes ahead of developing code.

During the ideation and design phases of any software system, teams engage with product and security teams on security considerations documentation, threat modeling, and design reviews.

Security considerations

Engineering teams document their product specifications in a standard format including security considerations and requirements. Security considerations may include compliance requirements, Denial-of-Service (DoS) risks, processing of Personally Identifiable Information (PII), integrations with third-party applications, or other.

Threat modeling

Threat models are a great tool for exploring potential security concerns early in the design of a new feature, allowing Okta to adhere to security best practices. Identifying and documenting these considerations early in the development lifecycle offers guidance to the following phases of development.

Secure design review and sign-off

A comprehensive review ensures that security business objectives are aligned with the design of a given product or solution. The design review involves a thorough evaluation of a product or solution's technical details, including evaluating the design of the user interface (UI), networking connections, architecture components, data storage, dependencies and other. This process enables system designers to collect feedback on implemented controls and security features necessary to protect the integrity of the application and customer data. This review yields a complete report, outlining our test cases and processes and any potential findings.

Secure implementation

As development begins, engineering teams must capture high-level requirements and translate them into stories, breaking down the work into manageable phases, allowing developers to write code that meets both functional and non-functional requirements. Development teams follow coding standards and guidelines, leveraging programming tools (or compilers) to test functionality as code is developed.

Application Security Testing (AST)

Okta’s teams leverage industry-leading best practices such as Static Application Security Testing (SAST), Software Composition Analysis (SCA) and Dynamic Application Security Testing (DAST) to analyze an application's source code, bytecode, or binaries.

Our application security testing methods are in place to mitigate technology risk by identifying any potential security vulnerabilities, including bugs, third-party dependencies, known defects or others. These methods are performed on all code modifications.

Application Penetration Testing

The purpose of a penetration test, or pentest, is to verify the presence of sufficient security controls, assess the security impact of existing vulnerabilities, and identify additional security issues not yet identified by other security practices. It is a type of simulated cyberattack on an application, service, or solution. During a pentest, we often simulate real threats by real adversaries against our products. Penetration tests on our solutions are performed both internally and by third-parties.

Security Reviews

In addition to previously described security reviews, Okta’s products are subject to routine cloud security and product security reviews. Reviews are performed to get a better understanding of an application’s cloud, network, and infrastructure security posture, and to raise the overall security posture for Okta’s products. A secure code review is a manual review of source code conducted by the Product Security team with the aim of identifying code-level security issues that may enable an attacker to compromise an application, service, or solution.

Software Bil of Materials (SBOM)

A Software Bill of Materials, or SBOM, is a detailed, formal record containing the list of all components, libraries, modules, and dependencies that make up a software application, product, or service. Given the rise of open-source software and third-party components, SBOMs are becoming increasingly important for Okta customers. Our customers depend on an accurate inventory of all third-party and open-source dependencies used in software delivered to them to ensure that software vulnerabilities are accounted for and mitigated to ensure licensing of software components is in line with any compliance requirements.

Secure deployment

The software development process does not end when the software is deployed to production or installed; it continues through maintenance and retirement of the software. During the lifetime of the software operating in production, product security and engineering teams work to continually assess the security of the software and to publish routine security updates until retirement.

Deep Reviews

As the industry evolves, security techniques and requirements change. As such, new techniques and requirements are integrated into Product Security’s procedures. To ensure that products maintain a high-security stance and meet the same security requirements as the rest of Okta’s product portfolio, products are routinely reviewed through the Deep Reviews process.

Deep Reviews are holistic security reviews targeting product areas and features that may not have received recent security or engineering attention. Our products in production run for long periods of time without interruption and, in some cases, without additional feature developments. Routine reviews are performed through the Deep Reviews process to ensure that products maintain a high security bar and meet the same security requirements as Okta’s product portfolio.

Secure deployment

Bug bounty program

Okta’s Bug Bounty Program bolsters the security of Okta products by taking a proactive approach to cybersecurity, inviting ethical hackers and security researchers worldwide to test and report potential security flaws collaboratively. Unlike malicious hackers, these skilled individuals aim to enhance Okta’s security posture. To incentivize collaboration between the community and product security, our program offers monetary rewards for the successful discovery and reporting of vulnerabilities or bugs. This improves our overall security posture while also encouraging responsible disclosure of security issues in Okta products. All in-scope engagements can be found on Bugcrowd.

Routine penetration testing

Okta’s internal and external networks and customer-facing products undergo annual penetration testing, conducted by third-party vendors to verify the presence of sufficient security controls, assess the security impact of existing vulnerabilities, and identify additional security issues not identified by security controls. Our routine testing is performed in order to uphold best practices and maintain Okta’s compliance certifications.

Note: Vendor-produced penetration test reports may be shared by Okta with customers under contract, prospects under NDA, and auditors.

Product Security Incident Response Team (PSIRT)

The Product Security Incident Response Team (PSIRT) focuses on identifying, assessing, and managing risks associated with Okta products. This team focuses on critical and high-severity security events stemming from product vulnerabilities that could affect Okta customers. Okta’s PSIRT is activated when any of the following conditions are met: immediate impact to a customer, a security issue allowing unauthorized access to internal resources, sensitive data such as credentials, tokens are exposed, or in the event a customer is required to take immediate action. In addition to our vulnerability disclosure processes, this team is also responsible for Okta’s Bug Bounty Program.

Secure deployment

Vulnerability Management (VM)

The Vulnerability Management (VM) program is in place to collect and drive remediation of vulnerabilities. Vulnerabilities can be reported from various sources, including security researchers, bug bounty programs, employees, partners, or customers. Each source and vulnerability type may need specific actions or different engagement paths.

The Vulnerability Management (VM) team monitors intake channels for the identification of new security vulnerabilities including internal review, customer service, security-focused press, security-related academic research, and technical alerts from established organizations.

Cyber Defense

The Cyber Defense Team is composed of Okta security professionals responsible for detection and response of cyber threats that impact Okta or our customers via the Okta platform. The team monitors Okta’s ability to operate securely and is responsible for protecting Okta resources and customer orgs against cyber threats by investigating potential security incidents and monitoring of the organization's network. To achieve this mission, Okta has built an intelligence-driven capability that identifies the adversaries and threat actors most likely to cause an adverse impact and prioritizes Okta’s defensive capabilities based on the threats most likely to be realized.

Conclusion

The comprehensive Secure Development Lifecycle (SDL) methods detailed within this whitepaper play a crucial role in handling and mitigating risks associated with security concerns in product development that could otherwise impact Okta's products. Okta’s standard for secure software development, as described, includes leading security practices, methodologies and technologies in order to establish our standing as, “The World’s Identity Company”.