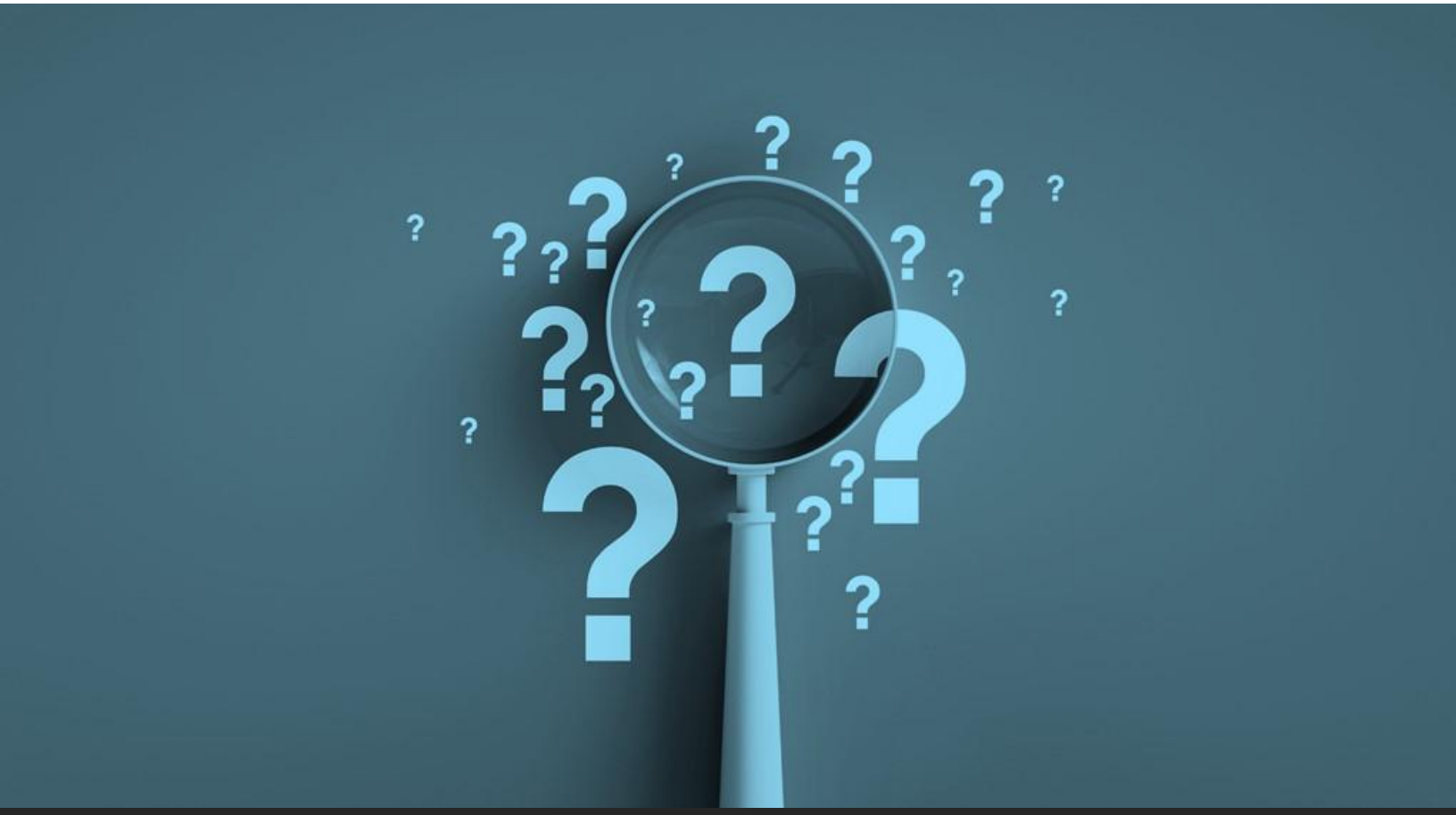
yodlee



Security FAQ

(Frequently Asked Question)

VERSION 1.0

Table of Contents

Enterprise Cybersecurity Program

Does Yodlee have an Enterprise Cybersecurity Program?

At Yodlee, we take the security of our clients' data and assets very seriously. Security is important because it helps to protect against unauthorized access, theft, and misuse of sensitive information. It also helps to ensure the integrity and availability of critical business data and assets.

Yodlee has adopted a risk-based Enterprise Cybersecurity policy framework at the enterprise level. Yodlee is committed to protecting all information accessed, processed, stored, or exchanged, from unauthorized access, use, modification, disclosure, or destruction, by implementing controls defined to meet organizational objectives. Yodlee has a comprehensive Enterprise Cybersecurity management program and policy framework that leverages elements from NIST (National Institute of Standards and Technology), CSF (Cybersecurity Framework), NIST 800-53 Standards, ISO 27001, and CSA (Cloud Security Alliance).

Who is responsible for the Enterprise Cybersecurity Program at Yodlee?

The Enterprise Cybersecurity team at Yodlee is responsible for defining, implementing, and monitoring the Enterprise Cybersecurity Program. This team operates under the supervision of the executive-level Cybersecurity Governance Committee.

While the culture at Yodlee emphasizes individual responsibility for security at all levels, the Enterprise Cybersecurity team has the primary responsibility for ensuring the security of our systems and data. They work closely with all levels of the organization to promote a culture of security and to ensure that security measures are integrated into all aspects of our operations.

What is the Yodlee Enterprise Cybersecurity team?

The Yodlee Enterprise Cybersecurity team functions within the Yodlee business unit dedicated to security, privacy, risk, and compliance. The team reports to Yodlee's executive management and security leadership.

The Enterprise Cybersecurity team is organized into different functions which include.

- *Regulation and Attestations.*
- *Risk Management*
- *Client Assurance*

- *Product security*
- *Security Operations*
- *Infrastructure security*

Each group has engineers, architects, and analysts with responsibilities relating to their primary role, and who also serve as backup for each other.

Working closely with its security partners, the Enterprise Cybersecurity team drives security, privacy, risk management, and compliance throughout the organization.

Does Yodlee have a governance, compliance, and regulatory monitoring program?

Yodlee's Enterprise Governance, Risk Management and Compliance organization is responsible for staying up to date with changes in the regulatory environment. The company also has a process in place to identify new laws and regulations, new internal activities, and new contractual obligations with Enterprise Cybersecurity implications. Yodlee closely monitors regulations and potential changes, with a focus on the impact they may have on product design and technical solutions.

Does Yodlee have a Risk Management Program?

Yes, Yodlee has a comprehensive risk management program in place. This program is designed to focus resources and efforts on the assessment, monitoring, and management of our corporate and Enterprise Cybersecurity risk profiles.

The program consists of formal risk assessments at the organizational and product levels, and is incorporated into all facets of our processes, including application development, data center operations, and internal security management. Our company-wide Enterprise Risk Management Program (ERM) ensures that the necessary information is available for our Executive Management team and Board to make effective risk-based decisions.

The Yodlee ERM is standards-based and incorporates requirements from ISO, COSO, FFIEC, and the Basel Committee's Risk Management Principles for Electronic Banking. This ensures that our risk management practices align with industry standards and best practices.

Does Yodlee have documented security policies and procedures?

Yes, Yodlee has documented security policies, procedures, and NIST-based standards that define our security controls. These are an essential component of our Enterprise Cybersecurity Program. The

Enterprise Cybersecurity team is responsible for creating and updating these policies and working with other groups, such as Operations and Customer Care, to develop procedures that allow them to perform their tasks while protecting our users' data.

Our security policies are reviewed and approved by the Enterprise Cybersecurity team annually, or when material updates are made during the year. A current listing of our policy library is available upon request.

Does Yodlee have a Security and Privacy Awareness Program?

Yes, Yodlee does have a comprehensive security and privacy awareness program. It is embedded in all aspects of employee communications and includes mandatory security and privacy awareness training and testing, ongoing awareness training programs, monthly simulated phishing tests and feedback from monitoring systems. The Enterprise Cybersecurity team is responsible for developing, implementing, and maintaining this program, ensuring that our employees are aware of the importance of security and privacy in everything we do.

Does Yodlee have an Incident Response Program that includes patch and vulnerability management?

Yodlee has a comprehensive incident response program that includes patch and vulnerability management. Our Security Incident Response Program is designed to align with industry standards and applicable requirements, such as GDPR, CCPA/CPRA, ACDR APA, GLBA, NYDFS and PCI DSS, and aligns with best industry practices such as NIST and CERT (Community Emergency Response Team). The following measures are in place:

- *Yodlee has an incident reporting process with an email ID where security incidents can be reported for systematic tracking and management. The company monitors mailing lists from vendors and industry partners such as FS-ISAC and Recorded Future that provide notification of new vulnerabilities.*
- *When a reported vulnerability has been identified and confirmed, the security office conducts a formal review of the applicable patches provided by the vendors. According to Yodlee's policy, vulnerabilities must be patched or otherwise remediated (i.e., compensating controls) as soon as possible.*
- *Yodlee subscribes to various sources to keep current on Enterprise Cybersecurity issues, including threat intelligence from industry sources and clients.*
- *Incident response plans are tested at least annually.*

- *Critical patches are always evaluated when released by vendors and applied out-of-cycle if deemed necessary.*
- *For the platform, Yodlee follows a quarterly release schedule for major enhancements. The standard application software patch release schedule is weekly if changes are required.*
- *Centralized patch management and antimalware systems ensure that the servers have the latest approved security fixes, patches, and anti-malware definitions with real-time protection. It also ensures that operating systems have the latest approved hot fixes and patches.*
- *Network and infrastructure changes/patches are applied quarterly as part of a maintenance release.*

Does Yodlee have an Application Security Program?

Yes, Yodlee has an Application Security Program. The program is run by the Yodlee Product Security team. The goal of the program is to apply security input, testing, and certification at all phases of the software development lifecycle.

The Application Security team is independent from the development staff and has full veto power at every step of the process. The program is human-driven and supported by leading application security products and tools in the industry. The team ensures that security and privacy are built into Yodlee products and the core Yodlee platform from the specification stage and tested at multiple points up to and including release. Code cannot be released to production until the Application Security team signs off.

The Yodlee application security program includes the following components:

- *Driving enhancements to products to incorporate evolving security features.*
- *Reviewing all functional enhancements from a compliance perspective*
- *Publishing secure coding standards*
- *Creating developer security training*
- *Performing manual and automated code reviews*
- *Conducting manual and automated vulnerability testing*
- *Monitoring and continual protection by tracking*
- *Developing tools and monitoring profiles for security tools to automate security processes.*
- *Providing CVE/NVD listings for new vulnerabilities and threats*
- *Managing third-party assessments performed by external vendors or clients.*

Overall, the application security program is designed to ensure that their products meet the highest standards of security and privacy. The program includes rigorous testing, training, and monitoring to protect against potential risks and threats throughout the software development lifecycle.

Does Yodlee carry cybersecurity insurance?

Yodlee maintains extensive cybersecurity insurance coverage as part of the company's enterprise insurance policy binder, which is reviewed by executive leadership on a quarterly basis to ensure transparency and adequacy in coverage requirements.

Personnel Security

What is Yodlee's employee vetting process?

Yodlee has a strict employee, contractor and subcontractor vetting process conducted before employment. This includes a comprehensive background investigation that verifies education and professional qualifications, employment history, criminal record, address, and drug screening. This process applies to all candidates, regardless of their role in the organization. This applies to contractors and key subcontractor's employees.

Does Yodlee have confidentiality agreements for employees?

All Yodlee personnel, including contractors, sign non-disclosure and confidentiality agreements as part of their on-boarding process. These agreements ensure that our personnel are aware of Yodlee's obligations for security, privacy, and compliance. Yodlee personnel reaffirm their compliance with our acceptable use policy and confidentiality agreement annually. Additionally, Yodlee has formal procedures in place for employee separation and role changes, which involve coordination between HR, Enterprise Cybersecurity, Internal Audit, and IT. The procedures establish protocols for scheduled and immediate terminations. The Enterprise Cybersecurity team, in conjunction with the Internal Audit team, conducts quarterly entitlement audits to ensure that accounts of terminated personnel are either disabled or deleted.

Physical Security

How are Yodlee sites secured?

Yodlee employs various security measures to safeguard our offices and data centers. At our offices, access is granted through electronic badges and all physical access logs are retained for more than

90 days. Visitors are also required to sign in at reception and receive a visitor badge, and they are escorted while on site. Offshore facilities that support platform operations are located in secured work bays with standard controls.

Our data centers have additional security measures, including biometric access, key cards, and security staff on duty 24/7. Access is strictly limited to pre-authorized Yodlee personnel who possess a data center card key.

Vendor Risk Management

Does Yodlee have a Third-party risk management program?

Yes, Yodlee has a comprehensive Vendor Risk Management Program that ensures new vendors and service providers are selected and assessed using a formal risk-based formula. The program considers contractual agreements, criticality of the service, and the sensitivity of the data they are handling.

The assessment involves due diligence, third-party attestations, and security questionnaires evaluating the financial status, Enterprise Cybersecurity maturity, and privacy of the vendors and service providers. Existing vendors and service providers are regularly reviewed, with ongoing management oversight for our most critical service providers.

Yodlee's vendor risk evaluations are aligned with financial industry standards and supervisory guidelines, and we utilize the Shared Assessment Vendor Risk Management Maturity Model. Reports on key vendors, such as data center collocation providers and support outsourcing, are available for client review.

Business Continuity Program and Disaster Recovery

Does Yodlee have a Business Continuity Program (BCP) in place?

Yes, Yodlee has a formal Business Continuity Program in place that covers all functions and sites. In addition, we have designated teams and procedures in place to manage and respond to disruptions, with a focus on maintaining the availability and integrity of our systems and data.

Does Yodlee test their BCP and DR?

Yodlee regularly tests its Business Continuity Program (BCP) and Disaster Recovery (DR) plans to ensure they are designed and operating effectively. These tests are conducted annually and involve various scenarios and situations to validate the effectiveness of our plans. The results of these tests are reviewed, and any necessary improvements are made to enhance our preparedness and response capabilities.

Does Yodlee consider pandemic planning as part of their BCP?

The Yodlee BCP includes a specific section on pandemic planning. The plan includes measures to protect the health and safety of our employees, maintain critical operations, and communicate effectively with clients and stakeholders during a pandemic.

Change Control

Does Yodlee have a formal documented change control process?

Yodlee has a formal and documented Change Management process based on ITIL methodology. This process includes requesting, testing, approving, and promoting changes to our production and stage environments. The Enterprise Cybersecurity team is responsible for reviewing and approving critical changes to infrastructure or applications. This rigorous process ensures that changes are properly authorized, tested, and implemented, thereby reducing the risk of negative impact on our systems and services.

Enterprise Cybersecurity Operation

Does Yodlee monitor its infrastructure and application security?

Yodlee has a comprehensive security monitoring program that includes a Security Operations Center (SOC). The SOC is staffed 24/7 and has run book procedures and SLAs for handling alerts. Yodlee's layered monitoring infrastructure incorporates data from various sources such as point security solutions, monitoring tools, discovery scans, and SIEMs to produce a real-time view of the entire security architecture. This view is presented in Yodlee's custom security dashboard, which provides risk data visualization to all internal stakeholders with granular visibility at the asset, alert, or user level. The SOC also reviews security advisories from vendors and third-party sources of threat information, assesses them for the Yodlee environment, and recommends suitable action as applicable.

How does Yodlee manage infrastructure security?

Yodlee has dedicated Infrastructure Security and Product Security teams that monitor approved workloads and platforms, both in the cloud and on-premises. The Product Security group utilizes a suite of application security tools and an enhanced CI/CD pipeline to ensure the security of new products and applications. Yodlee's enhanced risk management covers the entire product lifecycle, including system design, data privacy, security, and retirement. In addition, Yodlee follows industry-standard practices for infrastructure deployment and configuration.

Does Yodlee report breaches and incidents to stakeholders?

Yodlee has a formal Incident Response Program in place that includes reporting security incidents to relevant stakeholders. The program defines the standards and guidelines for reporting incidents and has documented procedures for handling, communication, and reporting to clients, regulators, and law enforcement.

Yodlee's incident reporting process complies with applicable regulations and standards such as PCI DSS, and industry best practices like NIST and CERT. Reportable issues are handled based on specific contractual parameters and applicable data breach notification requirements at the federal, state, territorial, or provincial level.

Does Yodlee have data leakage prevention mechanisms?

Yodlee has implemented data leakage prevention mechanisms such as a DLP (Data Loss Prevention) tool between production and corporate environments to prevent the transfer of sensitive data from production. In addition to this, Yodlee's Enterprise Cybersecurity team regularly conducts scans on both corporate production and corporate environment using commercial DLP tools to detect any potential data breaches.

How does the Yodlee Platform handle user data privacy?

The Yodlee Platform upholds a strong privacy program that complies with applicable global privacy regulations, standards, and best practices. We comply with applicable privacy requirements in all regions where we operate, including U.S. federal and state regulations, and have received third-party certifications such as US-EU and -Data Privacy Framework and APEC Cross-border Privacy Rules. For Asia, Africa, Australia, and New Zealand, we comply with relevant banking rules, privacy regulations, and consumer protection requirements. We continuously monitor new privacy regulations

and programs to ensure that we meet privacy obligations while adhering to the spirit and letter of the law.

When service as a service provider to a specific client, Yodlee agrees as part of its contractual obligations to follow the client's privacy notice.

Does the Yodlee Platform adhere to any other global data protection laws?

The Yodlee Platform operates in various regions including the U.S., Canada, Europe, APAC, and South Africa. We adhere to prudential, consumer protection, and privacy regulations in all these regions applicable to our offerings. Yodlee monitors developments in new regions and engages with regulators to ensure compliance with any data protection requirements. Yodlee also has a dedicated data governance team to ensure compliance with applicable data regulations.

Independent Audits and Assessments'

Does Yodlee perform a SOC 2 assessment of the Yodlee Platform?

Yodlee engages in a SOC 2 Type 2 assessment of the Yodlee Platform annually. The most recent assessment report is available to clients and prospects under NDA (Non-Disclosure Agreement). The examination is conducted by an independent audit firm. The Trust Services Criteria in scope of the examination include security, availability, processing integrity, confidentiality, and privacy.

Is the Yodlee Platform PCI certified?

Yes. The Yodlee Platform is PCI-DSS 4.0.1 certified as a Level One Service Provider.

Are Yodlee Platform assessments available for review?

Assessments of the Yodlee Platform are available for review by direct clients and prospects under NDA. For indirect clients, the Yodlee Platform's channel partners (direct clients) conduct due diligence on Yodlee' s services and operations to ensure they meet the high standards expected by their clients.

Does Yodlee perform audits of its Platform and controls?

Yodlee has a robust audit program that includes entitlement audits, technical audits, and process audits, covering every critical control. The audits are conducted on a risk-based schedule and follow defined procedures. The Yodlee Platform Audit team performs the audits, and the program is regularly reviewed and vetted by independent auditors.

Infrastructure Security

What is Yodlee's Platform Infrastructure Security Program?

The Yodlee Platform Infrastructure Security Program follows industry best practices and guidelines to ensure the security of our networks. We use a zoning approach to separate our production, staging, development, corporate, and specialty networks from each other, with access control devices in place between each environment. Within each environment, we further segment networks to apply granular security and audit controls appropriate to each function. Other key controls in our Infrastructure Security Program include:

- *Centralized Bastion Hosts*
- *Multi-factor Authentication*
- *Resilient and Redundant Infrastructure*
- *Data Encryption*
- *Vulnerability Management*
- *Centralized Security Incident and Event Management (SIEM)*
- *Secure Virtual Desktop Infrastructure Limiting Data Movement*
- *Layered Security Zones*
- *Enterprise Antivirus Management*
- *Intrusion Detection/Prevention System (IDS/IPS) Monitoring*
- *Distributed Denial of Service (DDoS) Monitoring*

Does the Yodlee Platform employ public cloud-based solutions for its aggregation services to clients?

The Yodlee Platform is currently in the process of moving to AWS, however, most core services of the Yodlee Platform are delivered from our colocation data centers. We use Amazon Web Services (AWS) for scalable processing and delivery of some data services. For these use cases, we employ private VPCs (Virtual Private Cloud) and conduct comprehensive risk assessments to identify and deploy the necessary controls for each type of service.

Does the Yodlee Platform have a patching and vulnerability management program?

Yes, the Yodlee Platform has a comprehensive patching and vulnerability management program in place and a team that actively monitors new vulnerabilities through various sources, including vendor mailing lists, open-source communities, and industry partners. Once a vulnerability is identified and

confirmed, Yodlee's Platform Enterprise Cybersecurity team conducts a formal review of applicable patches and ensures that critical vulnerabilities and high-priority issues are remediated within 30 days.

Data Governance and Security

What data is collected by the Yodlee Platform?

While the Yodlee Platform connects to a variety of financial institutions and related data sources, the information we may collect to power our services broadly falls into four categories:

- ***Identity**: name, address, tax identifier, email, and phone*
- ***Account:** institution or issuer, access credentials, type (e.g., savings, credit card), identifier/number, balance, APR*
- ***Transaction:** type (debit, credit), date, amount, description, method (e.g., credit card, direct deposit) and, in case of spend, merchant information*
- ***Commercial:** data such as terms, derived content or data provided under a fee agreement*

Does each client have a dedicated environment?

The Yodlee Platform is a shared product platform, but client data is logically separated and stored in a segregated environment. Each client has a Master Key, and every end-user is assigned a member ID, and every account has an account ID, ensuring that client data is kept separate and secure. Additionally, segregation of client data is implemented at multiple levels to prevent cross-account access.

How does the Yodlee Platform manage access to client-facing systems?

The Yodlee Platform follows the principle of least privilege for all entitlement systems and implements role-based access control in its production and staging environments. The company enforces this access control using a technical privilege management system that ensures Yodlee personnel only have the entitlements they need for their role. All access is 100% keystroke and session logged, allowing the Enterprise Cybersecurity team to have full audit coverage of all activities. Security logs are integrated with The Yodlee Platform's SIEM (Security Incident and Event Management) solution and are retained for 52 weeks (approximately 12 months). These logs feed Yodlee's Platform monitoring tools, enabling the company to detect and prevent unauthorized access attempts from its personnel.

Does the Yodlee Platform encrypt data at rest?

The Yodlee Platform employs strong encryption measures to protect sensitive PII user and sensitive account data stored in our database. We use AES 256 (Advanced Encryption Standard) to encrypt the data and keep it in ciphertext form until it is necessary to decrypt for use. For keys management, the Yodlee Platform uses a FIPS 140-2 (Federal Information Processing Standards) compliant network-attached hardware security module (HSM). Access to the HSM is restricted to authorized personnel only, and Yodlee employees do not have access to the hardware-based keys. Application access to the HSM is through internal API (Application Programming Interface) calls from authorized IP addresses and requires certificate-based authentication using the HSM appliance's built-in CA (Certificate Authority). Additionally, administrator activities on the HSM require two-person controls to prevent unauthorized action.

Does the Yodlee Platform encrypt data in transit?

The Yodlee Platform follows strict data security policies to ensure that all sensitive data is transmitted securely. This is achieved by using Transport Layer Security (TLS) to encrypt all communication channels, both external and most internal connections within the data flow. By utilizing TLS, we ensure that data is protected against interception and tampering during transit.

How long does the Yodlee Platform retain user data?

The Yodlee Platform retains client data until it is deleted by the client through API or written request, or until the client is decommissioned. However, certain types of data may need to be retained for a period as required by law.

Does the Yodlee Platform use user data for non-production testing and development?

No, the Yodlee Platform does not use user data for testing purposes in non-production environments. Instead, the Yodlee Platform uses synthetic data generated by in-house tools for non-production test data. As per the Yodlee Platform security policy, user data should only be stored in the production environment. To prevent user data from moving outside the secure production environment, Yodlee has implemented layered preventive and detective controls across the Yodlee Platform.

Application Security

Does the Yodlee Platform have a formal, documented and implemented SDLC Process?

The Yodlee Platform's software development lifecycle (SDLC) process involves standard procedures such as requirement analysis, functional and architectural design, development, testing, deployment, branching of code, patches vs. new development, etc. As part of the feasibility study and design stage, impact analysis is carried out. GitHub, a web-based version-control, and collaboration platform for software developers, is used for source code management. Releases are managed using internal automation tools. The Quality Assurance team performs testing of new enhancements and regression testing to ensure that existing features are not impacted by the deployment of new enhancements before deploying to production. The platform is updated with the latest versions four times per year through the Yodlee Platform's release cycles. The Yodlee Platform's SDLC process incorporates secure development practices, including:

- *Threat modeling based on Open Web Application Security Project (OWASP)*
- *A secure coding and awareness guide for developers based on OWASP.*
- *Static and dynamic scans prior to each release*
- *Enterprise Cybersecurity integrated into the software development process.*
- *Documentation of software procedures for development, testing, deployment, branching of code, patches vs. new development, etc.*

The Yodlee Platform follows a quarterly release schedule for major enhancements on the platform, while the standard application software patch release schedule is weekly, if changes are required. Depending on the severity, a fix may be rolled out into a weekly patch or future enhancement release cycle.

Are penetration tests and code scans performed on the Yodlee Platform?

Yes, The Yodlee network undergoes an annual penetration test by a third party based on OWASP Top 10 guidelines.

Yodlee conducts penetration tests and code scans on the Yodlee Platform as part of its Application Security Program. The program includes static and dynamic code scanning, manual reviews, and multiple rounds of penetration testing to test and certify the Yodlee Platform. These tests help identify and address any security vulnerabilities that may exist within the Yodlee Platform.

In addition to internal testing efforts, third-party security firms perform annual application penetration tests on all internet-facing applications. This independent testing provides an additional layer of security testing to ensure that Yodlee's products are secure and free from potential risks and threats.

Overall, Yodlee's comprehensive security testing efforts, including penetration testing and code scans, help ensure that their products are secure and meet the highest standards of security and privacy.

Does Yodlee monitor for web application attacks?

Yes, Yodlee monitors the Yodlee Platform for web application attacks using an industry-standard web application security system. The system is designed to monitor all inbound application traffic, including API calls that originate from servers or systems. The monitoring is aimed at detecting repeated attack patterns such as XSS and SQL injection.

If the Yodlee Platform's security system detects an attack pattern, the originating IP is immediately blacklisted from all communication protocols. This action helps prevent the attacker from launching additional attacks and protects the Yodlee Platform's systems and clients from potential harm.

Overall, monitoring of the Yodlee Platform for web application attacks is an essential component of their comprehensive security program. The monitoring ensures that products are protected against common web application attacks and that customers can trust the Yodlee Platform's systems to safeguard their sensitive information.