YesWeHack

Service Definition - Lot 2a Infrastructure Software as a Service (I-SaaS)

Continuous Penetration Testing

TABLE OF CONTENTS

I. INTRODUCTION

YesWeHack was founded in 2015 and provides a cloud-based Bug Bounty and Vulnerability Management Platform. Headquartered in Europe, with a team of 10 based in the UK, YesWeHack operates internationally, working with public and private sector organisations to strengthen digital resilience through collaboration and transparency.

YesWeHack helps enterprises, governments, and critical infrastructure providers to advance their security posture through our suite of vulnerability management products.

Value Proposition

Continuous Penetration Testing (CPT) provides ongoing assessment of an organisation's security posture by continuously identifying and validating vulnerabilities as systems and applications evolve. Unlike traditional point-in-time testing, CPT delivers ongoing visibility of security risks, enabling organisations to maintain assurance and reduce exposure between test cycles.

CPT addresses several common challenges faced by public and private sector organisations. It removes blind spots between annual tests, reducing the risk of undetected vulnerabilities caused by system changes or new deployments. It supports more efficient vulnerability management by integrating with existing security workflows and providing verified, prioritised findings for remediation. It also assists with compliance requirements by evidencing continuous monitoring in line with frameworks such as NCSC guidance, ISO 27001, GDPR, and NIS2.

In addition to continuous detection and validation, organisations may optionally run one-off, in-depth penetration testing campaigns. These campaigns complement the continuous service by enabling targeted, human-led assessments at defined intervals or for specific systems, offering deeper assurance where required.

Available through G-Cloud 15, Continuous Penetration Testing enables organisations to maintain up-to-date assurance, demonstrate ongoing risk management, and strengthen overall cyber resilience in accordance with government and industry standards. This approach allows security teams to focus on remediation and compliance, while ensuring vulnerabilities are identified, reported, and tracked in a structured and auditable manner.

What the Service Provides

The service combines two complementary approaches to security assessment: continuous, risk-driven testing and time-bound pentest campaigns.

1. Continuous, risk-driven assessment

Ongoing manual penetration testing is performed by YesWeHack's in-house security team under the supervision of a dedicated Customer Success Manager (CSM). These tests are supported by

YesWeHack's proprietary automated testing framework, which uses a regularly updated library of "checkpoints." Each checkpoint corresponds to a specific, exploitable vulnerability and includes a defined exploitation scenario. The checkpoint library is continuously maintained to reflect current threat intelligence, ensuring focus on vulnerabilities most likely to be targeted or exploited in real-world attacks. This approach allows testing to remain relevant to the evolving threat landscape and to prioritise the vulnerabilities that present the highest risk to the customer's environment.

2. On-demand Pen-Test Campaigns

Customers may also schedule targeted penetration testing campaigns. Each campaign is planned in advance and managed by the assigned CSM, who selects appropriate testers based on the systems in scope, required methodologies, and technical requirements. Pentesters are drawn from YesWeHack's verified community of security researchers, selected based on demonstrated expertise and reliability. All submitted findings are reviewed and validated by YesWeHack prior to delivery. Reports follow a standardised format across both internal and community testers, with clear indication of the report source.

Social Value

Make Britain a clean energy superpower

At YWH, we measure our carbon emissions annually to track progress and have already achieved a reduction in our environmental footprint (3,36tCO2e/employee in 2023; 3,04tCO2e/employee in 2024). In the UK, all our employees work remotely to minimize greenhouse gas emissions. Our offices are carefully selected for their energy efficiency and accessibility by public transport, helping reduce individual travel impact. In addition, our organization is assessed each year by Ecovadis, which reflects our ongoing commitment to continuous improvement across the four sustainability pillars (Ethical, Social, Environmental and Responsible Procurement). Although we do not yet have a defined target date for achieving net zero, we are fully committed to reducing our emissions and are implementing all necessary measures to improve year after year our carbon footprint. These initiatives demonstrate our proactive approach to responsible environmental management and our contribution to supporting the UK's net zero objectives. Although we do not yet have a defined target date for achieving net zero, we are fully committed to reducing our emissions and are implementing all necessary measures to improve year after year our carbon footprint.

Break Down Barriers to Opportunity

At Yes We Hack, we value all employees, based on their skills, performance and potential. We encourage everyone with the required experience, and if needed, with a background in the cybersecurity ecosystem, to apply to Yes We Hack job opportunities, whatever their gender, academic or cultural background are.

Our job postings are written to be inclusive of all profiles, with no reference to educational qualifications—skills are what truly matter.

As of today, women at Yes We Hack represent 32.4 % of the total of our employees, worldwide.
In the UK, women at Yes We Hack represent 45.5% of the total of our UK employees.
Those figures should be compared to the rate of women :

- In the Tech Industry in Europe : 32-35 %
- In the cybersecurity in Europe : 20-25%

As of today, gender equality is only measured in France, with the local governmental Professional Equality Gender Index. Yes We Hack France has evolved from 40/100 FY2022 to 87/100 FY2024, in line with the national average index (88/100). Yes We Hack will continue its efforts regarding gender equality, aiming to improve the two indicators that are not currently achieving the maximum score: gender pay gap, particularly in the 40–49 age group, and parity among the highest-paid positions. When transposing the French Gender Equality Index methodology to the UK employees, a score of 85 out of 85 would be achieved (1 indicator is not relevant as no maternity leave occurred). With the salary transparency regulations in Europe, we plan to measure gender equality more widely in the future, provided we have a minimum employees per job category, as required by local rules.

The nationalities of our employees demonstrate our diversity : we count 14 nationalities out of 138 employees at the end of October 2025.
In UK, the proportion is even higher, as 4 nationalities are represented out of 11 employees.

Kick-Start Economic Growth

At YesWeHack, we encourage each year employees to express their skills development needs, as part of our annual reviews. Based on those needs and strategic initiatives, we implement a yearly skills development plan. As an illustration, in 2024, at Company level, our skills development plan represented 74 training actions, 55 employees who received a purchased training (rate of 47% of employees, the double vs. 2023), and overall approximately 900 hours of training. In 2025, in the UK, as the team is growing, the focus was made on Sales Management and Leadership development courses for our local leaders. 2 UK employees also received a e-learning platform license, to autonomously progress in their training objectives. All employees were also invited to join a micro-learning platform focusing on digital and ecological transition, business processes, and soft skills. Also, all new joiners benefit from an onboarding path, with coaching from their manager, and peer-mentoring from their colleagues. When possible, we also encourage mobility and career evolution within the company. Over 2024 & 2025, 18 individual evolutions can be identified, from international mobility to leadership positions appointments.

Build an NHS Fit for the Future

At YesWeHack, all employees whatever their country of work, are proposed a health insurance plan, a contribution from Yes We Hack. This is also applicable in the UK, where the employer-paid private health insurance plan coverage includes Medical, Dental and Vision benefits.
In France, each year, we conduct an assessment of occupational risks and develop an action plan to improve working conditions. This approach will soon be extended internationally as part of the implementation of a Group Health and Safety Policy. This would lead to implement at least regular awareness actions or share content on Health at work in order to contribute to our employees well-being at work.

Overview of the G-Cloud Service

YesWeHack Continuous Penetration Testing (CPT) is a cloud-based, managed service that provides continuous security testing of external digital assets, including web applications, APIs, connected devices, and other IT infrastructure. The service aligns with the Software-as-a-Service (SaaS) model, offering on-demand access, scalability, and remote availability consistent with G-Cloud framework principles.

Key service capabilities include:

- Continuous Penetration Testing: Exploits engine-powered, ongoing, manual pentests, allowing ongoing identification of security vulnerabilities in line with release cycles and development schedules.
- Managed Tester Engagement: Selection, coordination, and secure access setup for qualified human pentesters, reducing the operational overhead for the client.
- Structured Vulnerability Reporting: Findings are triaged and validated before being delivered with technical details, severity ratings, reproducible proof-of-concept, and remediation guidance.
- Dashboards and Analytics: Real-time tracking of vulnerabilities, remediation progress, testing coverage, and trend analysis.
- Integration with Existing Workflows: API and connector support for platforms such as Jira and Slack, enabling seamless incorporation of findings into existing development and security processes.
- Compliance and Audit Reporting: Generation of executive summaries, detailed reports, and certificates suitable for regulatory or internal audit purposes.

Cloud characteristics of the service include multi-user access, platform-based delivery, and scalable coverage for multiple scopes or environments. The service provides benefits such as continuous visibility of security posture, structured and auditable reporting, reduced operational effort for managing pentests, and faster remediation of vulnerabilities.

YesWeHack CPT has been deployed with organisations across multiple sectors, including public sector bodies, providing demonstrable support for compliance, risk reduction, and ongoing security assurance.

Associated Services

Services included in License:

- Continuous penetration testing across in-scope assets included within the selected asset tier.

- Use of YesWeHack's proprietary Security Check engine, providing continuous, automated detection of top-exploited vulnerabilities through real-world attack "checkpoints."
- Manual validation, retesting, and assessment of all potential findings by YesWeHack's in-house pentesters.
- Continuous discovery, vulnerability triage, alerting, and verified reporting through the YesWeHack platform.
- A dedicated Customer Success Manager (CSM) responsible for oversight of continuous testing activities and for coordination of the maximum number of campaigns included within the asset tier.
- Access to the YesWeHack platform for vulnerability management, reporting, tracking, and audit history.
- All services delivered on an annual subscription basis, aligned with G-Cloud contract terms.
- On-demand compliance and audit reporting, allowing customers to generate downloadable reports at any point during continuous testing or during/after a campaign,

II. Data Protection

Information Assurance

YesWeHack holds the following accreditations and certifications:

- ISO/IEC 27001 – Information Security Management System
- ISO/IEC 27017 – Cloud Security Controls
- Cyber Essentials
- CREST accreditation for penetration testing services
- EU-based and fully GDPR compliant

YesWeHack operates a refined Information Security Management System (ISMS) covering all aspects of data handling, storage, and processing. Information is managed in accordance with strict security and privacy principles, including data minimisation, access control, and continuous monitoring.
All customer data is hosted in secure, EU-based cloud environments with encryption applied at rest and in transit. Access to systems and information is governed by role-based permissions, enforced through multi-factor authentication and regular access reviews. Comprehensive logging and monitoring are in place to detect, analyse, and respond to security events in real time.

The YesWeHack Chief Information Security Officer (CISO) oversees the implementation and continual improvement of the ISMS in coordination with the Executive Committee and the Data Protection Officer. Regular internal audits, external assessments, and staff security awareness programmes ensure compliance with ISO standards and data protection regulations.

Data Back-Up and Restoration

As Described in our Operations Security Policy and Disaster Recovery Plan (DRP), backups are copied on two different remote datacenters (Hesse region in Germany; and Ile-de-France region in France) from two different providers (OVH and Scaleway) to cope with potential wide-area or provider-wide incident. Service can be restarted from backed up configurations and data on a dedicated spare server.

Backup copies and the restoration process are checked at least twice a year.

Backup copies are created for every kind of operational or production data. Real-time backups are in place for our production database and report attachments. Daily backups are carried out using Proxmox Backup Service on all VMs including those hosting production databases, report attachments, and all other services. Every 2 hours database dumps are performed locally on the VM member of the database cluster located on the remote server. Dumps are stored on a separate partition. Partition usage monitoring is in place to periodically remove old dumps. Th VM backup retention policy is implemented on the PBS servers. The retention policy ensures availability at all times, for each VM, of: + A daily snapshot for the last 14 days + a weekly snapshot for the last 8 weeks + a monthly snapshot for the last 12 months.

The IT department head is responsible for testing backup copies. Tests are performed every six months by mounting database and virtual machine backups on dedicated virtual machine and running several integrity checks. Among them, a full restoration including virtual machine back-ups is done at least once a year. The other annual back-up restoration test can be carried out using a containerized version of the platform that allows inspecting only the backed-up databases.

Results are reviewed by the head of IT Departments.

Business continuity statement/plan

Business Continuity

YesWeHack's Business Continuity Plan (BCP) applies to all business areas, supporting processes, and information systems covered by the company's Information Security Management System (ISMS). Its scope includes both operational and technical continuity, ensuring the continued delivery of the YesWeHack SaaS platform and associated business functions in the event of a disruptive incident.

A Business Impact Assessment (BIA) identifies key business areas, critical functions, and supporting assets, with each asset assigned an availability and integrity level from 1 (very low) to 4 (high). This mapping allows YesWeHack to prioritise recovery efforts and determine the potential operational, legal, and financial impacts of disruption.

The critical functions supporting service continuity include:

- Operation and availability of the YesWeHack SaaS platform
- Security and integrity of customer and internal data
- Core IT infrastructure and supporting systems
- Communication and coordination between geographically distributed teams

Dependencies between these functions are reflected in the Disaster Recovery Plan (DRP), which defines recovery procedures, responsibilities, and escalation paths. Continuity of information security underpins the entire plan, with integrity and confidentiality of data maintained through enforced controls such as cryptography, access management, and regular backups.

Acceptable downtime and recovery objectives are as follows:

- Recovery Time Objective (RTO): 48 hours for level 4 and 3 assets (critical systems)
- Recovery Point Objective (RPO): 2 hours for platform data; 24 hours for other systems
- Maximum Tolerable Downtime (MTD): up to 5 working days for level 2 and 1 assets (limited functionality or productivity loss)

To maintain operations during disruption, YesWeHack relies on both technical and organisational measures, including:

- Remote-work capability for all employees
- Geographical distribution of critical human resources
- Duplication of technical components for high availability
- Automated infrastructure recovery through Infrastructure as Code (IaC) and CI/CD deployment
- Distributed backups across multiple hosting providers and locations
- Defined crisis management responsibilities, periodic testing, and recovery exercises

These measures ensure continuity of operations and rapid restoration of services in the event of an incident.

Privacy by Design

YesWeHack adheres to the principles of Privacy by Design and in full compliance with the EU General Data Protection Regulation (GDPR). Privacy and data protection are embedded throughout the lifecycle of all systems and services from initial design through development, deployment, and continuous improvement.

A Compliance Policy, annexed to the company's Information Security Management System (ISMS), defines the controls and procedures in place to ensure GDPR compliance. These include data protection risk assessments, Data Protection Impact Assessments (DPIAs), and security reviews to identify and mitigate privacy risks at an early stage.

YesWeHack has appointed an external Data Protection Officer (DPO) who works closely with the Legal Department to ensure that privacy and the protection of personally identifiable information (PII) are systematically addressed in all data processing activities.

Personal data is processed only for legitimate and defined purposes, applying the principles of data minimisation, purpose limitation, and storage limitation. Access is governed by least-privilege controls, supported by authentication, monitoring, and logging measures.

All data is hosted and processed within secure, EU-based environments, ensuring compliance with GDPR and maintaining the highest standards of privacy and information security.

III. Using the Service

Ordering and Invoicing

- Orders can be placed via the Digital Marketplace using a purchase order or through direct engagement with YesWeHack by emailing gcloud@yeswehack.com. Calls can also be made directly to Sales Director, Sam Lowe, on 07342132662.
- Once an order is confirmed, the client account is set up and the relevant programs are activated.
- Billing is subscription-based and issued annually
- To meet G Cloud requirements, invoices will show the cost excluding VAT and including VAT. They are sent electronically to the nominated billing contact.
- Payment can be made by BACS or other standard methods agreed in the contract.
- When a customer requests an upgrade or modification to an existing license, the current license is cancelled and replaced with a new license using the same start date as the original license. The cancellation invoice is adjusted with a named discount in the format: “Discount for Cancel/Rewrite – Cancelled Invoice Number – Cancelled License Start Date–End Date.”
    - The new license maintains the exact same start date day as the cancelled license to ensure full-month coverage. For example, if the original license start date was 25th November 2022, the new license start date is set to 25th January 2023.
    - Line items in the Cancel/Rewrite quote are structured to reflect this adjustment, ensuring accurate billing and continuity of service.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

- On-Boarding:
  When a new organisation begins using the YesWeHack Continuous Penetration Testing (CPT) service, an initial kick-off meeting is held with key stakeholders. This session establishes the objectives of the engagement, confirms the scope of testing, defines roles and responsibilities, and outlines operational and reporting procedures. A dedicated Customer Success Manager (CSM) is assigned as the primary point of contact, supported by a technical specialist where required. The CSM provides guidance on best-practice configuration, vulnerability management workflows, and integration with existing security or development tools.
- Onboarding materials include platform documentation, process overviews, and reporting templates. Training is delivered remotely.

- Off-Boarding:
  If an organisation chooses to discontinue use of the platform, a termination notice is agreed in line with contractual terms. The CSM works with the client to plan the transition, including setting a timeframe for closure of open reports and researcher engagement. Clients can export all relevant vulnerability data and reports in common formats prior to account deactivation. Access to the service is then removed in a controlled manner.

- Service Migration:
  In circumstances where migration is required to the YesWeHack platform from other vulnerability management systems or disclosure processes, the customer is supported by the CSM and technical team. This includes mapping existing workflows, importing historical vulnerability data (where feasible), and advising on policy alignment.

- Scope of Service:
  The service covers access to the YesWeHack SaaS platform, onboarding support, vulnerability submission management, reporting, triage services, and standard customer success engagement.

Training

YesWeHack provides training to support public sector organisations in the effective use of the platform and the management of Bug Bounty programs.

Training is included as part of the standard onboarding process and typically covers:

- Navigating the platform and managing vulnerability submissions.
- Account set up
- Campaign planning and rules of engagement.
- Reporting and metrics available through the dashboard.

Training is delivered remotely.

Implementation Plan

A detailed implementation plan can be provided to each buyer on request. The plan is tailored to the organisation's context and outlines the key steps required to establish and operate a Continuous Penetration Testing (CPT) service through the YesWeHack platform.

Assessment and Preparation
Review of the organisation's security objectives, including testing priorities and reporting requirements. Identification of assets to be covered within the continuous testing scope. Clarification of testing parameters such as environment type (e.g. production, staging), testing methodology (black-box, grey-box), and applicable standards (OWASP, NIST, ISO 27001). Consideration is also given to internal resourcing, vulnerability management processes, and integration needs.

Service Configuration
Definition of the continuous testing scope and initial configuration of the YesWeHack platform. Allocation of a Customer Success Manager (CSM) to oversee service delivery, supported by technical specialists as needed. The CSM coordinates tester assignment, access setup, and testing logistics, and ensures alignment with organisational requirements and change management processes.

Operation and Continuous Delivery
Once configured, ongoing manual testing is conducted by YesWeHack's internal penetration testing team, supported by proprietary automation that prioritises testing against the most exploited

vulnerabilities in the current threat landscape. Findings are validated, documented, and shared through the platform in real time, including remediation guidance. Clients can assign, track, and manage vulnerabilities through the platform interface or integrate findings with their own workflows. Regular service reviews are conducted with the CSM to assess progress, update scope, and ensure continuous improvement.

This structured approach ensures that continuous penetration testing is implemented in a consistent, transparent, and measurable way, supporting ongoing assurance and compliance with relevant security standards and frameworks.

Service Management

The YesWeHack platform is delivered as a Software as a Service offering, managed under formal service management processes designed to ensure availability, stability, and security in line with recognised best practice.

YesWeHack's Information Security Management System (ISMS), certified to ISO 27001 and ISO 27017, defines the operational and security controls applied throughout the service lifecycle. These controls incorporate key elements of IT Service Management (ITSM) principles, including change management, incident management, capacity management, vulnerability management, and business continuity.

Service operations are supported by defined policies for change control, system monitoring, incident detection, backup and recovery, and patch management. Changes to production systems are reviewed, approved, and deployed using Infrastructure as Code (IaC) and automated CI/CD processes to minimise disruption and ensure traceability.

YesWeHack does not operate regular planned maintenance or outage windows. Any scheduled maintenance expected to exceed 30 minutes is communicated to clients at least 24 hours in advance via email and the public status page.

New platform releases are deployed two to three times per month, following rigorous testing in development and pre-production environments. Most releases occur without service interruption. A monthly changelog is published online, summarising all customer-impacting changes and new features.

While YesWeHack does not currently hold formal ITIL certification, its service management approach aligns with ITIL and ISO 20000 best practices, ensuring continuous improvement, operational transparency, and high service quality.

Service Constraints

The YesWeHack platform is delivered as a SaaS service with high availability and operational continuity. Platform availability is supported by a 99.7% SLA, with redundant virtual machines, distributed backups, and automated recovery mechanisms. Performance is continuously monitored to ensure responsiveness under expected load.

There are no regular maintenance windows; any scheduled maintenance exceeding 30 minutes is communicated to clients at least 24 hours in advance via email and the public status page. New platform releases occur 2–3 times per month after testing in development and pre-production environments, with minimal impact on service availability. A monthly changelog summarises all customer-impacting changes. Deprecated features are managed through formal notification and change procedures.

Customisation is limited to documented configuration options and APIs. High-risk changes, including security-related updates, follow formal change management and review procedures. All production data is hosted in EU-based, GDPR-compliant datacenters, and critical infrastructure depends on OVHcloud and Scaleway IaaS services, including DDoS mitigation and network resilience.

Service Levels

The YesWeHack platform is operational and accessible to customers 24 hours a day, 7 days a week, at least 99.7% of the time during a calendar year. Platform availability relies on OVHcloud private cloud solution in France which provides an SLA of 99.9% of availability.

Customer support team members are located in France, Singapore and Canada.

The team is thus available from Monday to Friday, 01.00 am (GMT) to 5.00 pm (GMT)

Although every customer has a dedicated Customer Success Manager (CSM), which should be the preferred contact, any member of the team would be capable to address an urgent request if sent to csm@yeswehack.com

YesWeHack does not have any regular planned maintenance or outage window. We must provide at least 24 hours' notice to the Client for scheduled maintenance of more than 30 minutes. Notification will be sent by email.

Outage and Maintenance Management

YesWeHack minimises the risk of service disruption through formal incident and outage management processes. Our Incident Management Procedure defines lead incident managers (CISO, CTO, Head of IT, Head of Singapore office), with one designated per incident depending on type and impact. A backup is appointed for incidents lasting more than 8 hours.

A core incident management team is established for each incident, including leads for IT infrastructure, development, customer success, legal, and external communications. Each lead coordinates a dedicated team, ensuring information is filtered and tasks are efficiently allocated. For major incidents or crises, a pyramidal structure is adopted, enabling teams to work without interruption while maintaining clear communication. Dedicated communication channels prevent information overload during high-volume incidents.

Service performance is continuously monitored via Zabbix, Graphana, and BetterStack dashboards, covering uptime, system metrics, and capacity utilization. Capacity reviews are carried out every six

months, with a 10% margin maintained to handle unexpected demand. Critical systems and data are protected with redundant virtual machines, distributed backups, real-time database replication, and DDoS mitigation to reduce downtime.

All changes to production systems follow formal change management procedures, including risk assessment, approval, and controlled deployment through Infrastructure-as-Code (IaC) and CI/CD pipelines, reducing the risk of technical failures. Historical logs allow measurement of downtime, and on-call rotations ensure rapid response to ad-hoc operational needs.

Financial Recompense Model for not Meeting Service Levels

No service credits. YWH services are non critical to our customers' business (no impact on continuity nor turnover).

IV. Provision of the service

Customer Responsibilities

As set out in YesWeHack's standard Continuous Penetration Testing Contract Terms (the "CPT Terms"), the Customer shall cooperate in good faith and provide YesWeHack with a written detailed list of the technical and organizational information required to define the scope of the Service, including the designation of the Systems to be tested using the ASM feature and/or the Pentest Programs, the type(s) of Tests, any exclusions, and other relevant parameters, requirements and/or instructions.

The Customer warrants that it owns all IPRs necessary to enable it to perform its obligations under these CPT Terms. The Customer agrees to indemnify, defend, and hold harmless YesWeHack from and against any and all third-party claims and causes of action, as well as related losses, liabilities, judgments, awards, settlements, damages, expenses, and costs (including reasonable attorney's fees and related court costs and expenses) incurred or suffered by YesWeHack relating to or arising out of the violation or infringement of third-party intellectual property rights caused by the Customer's content, data, materials, or other contributions submitted, uploaded, or otherwise provided in connection with the Service offered through the Platform.

Moreover, the Customer shall:

I. undertake to use the Platform and Service in accordance with these CPT Terms;

II. be solely responsible for its Users, including the management of User accounts and the means of authentication (such as identifiers, passwords, etc.) associated therewith;

III. designate a primary point of contact for operational coordination, and establish a clear escalation path for use in the event of emergencies, incidents, or critical issues related to the performance of the Service;

IV. promptly notify YesWeHack of any circumstances that may affect the performance of the Service, including, without limitation, any changes to the Customer's rights or authorizations over the Systems to be tested. The Customer shall regularly review and ensure the validity of such rights and authorizations throughout the term of the CPT Terms;

V. assign to YesWeHack, in the context of Vulnerability reproduction, identifiers dedicated to the reproducibility of Vulnerability Reports if the creation of an account is impossible or the use of personal information is mandatory (e.g., national identity card, passport, driver's license, social security number, etc.). Failing this, YesWeHack shall only be required to perform a theoretical assessment of the Vulnerability Reports;

VI. ensure that the use of the Service complies with its internal, legal and any regulatory requirements.

Subject to the Crowdsourced Pentester's compliance with the rules set by the Pentest Program and the Pentesters Terms, the Customer acknowledges that:

I. any Test conducted by the Pentesters as part of a Pentest Program is authorized and operated with the Customer's express consent and under its sole responsibility;
II. the acts carried out by the Pentesters are free of fraudulent character, and cannot, in such cases, be qualified as a breach of an automated data processing system under the law nor classified as acts of infringement under the law;
III. it may not sue the Pentester for acts performed in the context of a Pentest Program under criminal or civil law, being specified that YWH cannot be held liable for any breach by the Pentester of its obligations; and
IV. it expressly waives, in advance, the civil interest that may result from the prosecution by the public prosecutor's office or any other prosecuting authority of an offense committed within the framework of a Pentest Program.

Technical Requirements and Client-Side Requirements

YesWeHack is a SaaS platform. It requires minimal client-side infrastructure. End users need only a stable internet connection and access to a modern web browser (Chrome, Firefox, Edge, Safari, etc).

Outcomes/Deliverables

YesWeHack Continuous Penetration Testing (CPT) provides organisations with actionable intelligence to maintain and improve their security posture. Each identified vulnerability is documented in a detailed report, including technical description, potential impact, exploitability assessment, and recommended remediation steps.

Reports are delivered in a consistent format and can be filtered, assigned, and tracked through the YesWeHack platform. Findings from ongoing manual testing and optional targeted campaigns are validated by our internal security team to ensure accuracy and relevance.

In addition, the service provides a dashboard with key performance indicators (KPIs) that allow teams to monitor trends in vulnerability discovery, remediation progress, and risk exposure over time.

Organisations can also generate compliance and audit reports aligned with standards such as ISO 27001, NIS2, GDPR, and other regulatory frameworks. These reports provide documented evidence of continuous testing, risk management, and ongoing improvement, supporting both internal governance and external assurance requirements.

Development life cycle of the solution

Development Lifecycle

We follow an Agile-inspired iterative process to deliver features efficiently while maintaining quality. The stages include:

- Identify needs: Functional requirements are presented to the development team for clarity
- Plan & Design: Technical specifications are written and validated by leads
- Build: Work items (Stories, Tasks, Sub-tasks) are created in Jira, and development is done on feature branches following Git Flow
- Test & Review: Code is reviewed via merge requests, tested locally, and validated in QA environments
- Deploy: Releases are prepared, documented, and deployed to pre-production and production environments
- Maintain: Hotfixes and release fixes are managed through dedicated branches to ensure stability

This approach ensures traceability, collaboration, and continuous improvement across all stages.

After-sales Account Management

YesWeHack provides structured account management to support ongoing use of the platform and ensure programs operate effectively.

- Primary Contact: Each organisation is assigned a Customer Success Manager (CSM) who acts as the main point of contact for all service-related queries.
- Relationship Management: The CSM facilitates communication between the organisation and internal teams (technical, security, and operations) to address any operational, technical, or program-related issues.
- Commercial Account Management: A dedicated Account Manager is available to address contractual, billing, and commercial aspects of the engagement, ensuring clear communication regarding invoicing, renewals, and service agreements.
- Program Review: Regular check-ins are scheduled to review program performance, platform usage, and emerging requirements. Recommendations for adjustments or improvements are provided where appropriate.
- Issue Escalation: Any incidents, service requests, or technical issues are tracked and resolved through CSM, with escalation paths clearly defined.
- Continued Support: Ongoing guidance and documentation are available throughout the service term, including updates on platform features, best practices, and relevant compliance information.

This approach ensures that organisations have a consistent point of contact and structured support throughout the service term.

Termination Process

Term. The CPT Terms are effective as of the date of mutual acceptance of a PO or as otherwise specified therein. They are entered into for an initial period indicated in the initial PO.

Termination for cause. YesWeHack may immediately revoke access to the Platform and use of the Service, upon:

(i) the Customer's or any of its User's material breach of its obligations hereunder which has not been remedied within fifteen (15) days of the Customer's receipt of written notice describing the breach in reasonable detail,

(ii) malicious, unlawful, or fraudulent use of the Platform and/or Service or use in violation of the rights of any third party or any mandatory provisions

(iii) the filing of voluntary or involuntary bankruptcy or insolvency proceedings by the Customer, subject to applicable law. Terminations for cause are without prejudice to any damages that may be claimed by YesWeHack to the Customer.

Archiving and Destruction. Upon expiry or termination of the Service for any reason whatsoever, all information relating to the use of the Service, i.e., data of any kind, including Confidential Information, Personal Data, as well as Vulnerability Reports, will be retained by YesWeHack for the sole purpose of complying with its applicable legal obligations in accordance with statutory periods. At the expiry of such statutory periods, they will be completely removed, at the Customer's request, from YesWeHack's databases and systems.

V. Our experience

Clients

- Government Technology Agency, Singapore
- Ministry of Defence, Singapore
- Cyber Security Agency, Singapore
- Finnish Tax Administration
- Swiss Post (including e-voting solution)
- European Commission
- French Digital Agency
- Quebec Ministry of Cybersecurity and Digital Affairs
- WaterPlus
- IG Group
- Admiral Pioneer

Contact Details

Sam Lowe – Sales Director – 44 07342132662 – gcloud@yeswehack.com