YesWeHack

Service Definition - Lot 2a Infrastructure

Software as a Service (I-SaaS)

Bug Bounty Program: Security Penetration Testing and Vulnerability Disclosure Platform

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 has established one of the world's largest and most diverse communities of ethical hackers. YesWeHack partners with enterprises, governments, and critical infrastructure providers to advance responsible vulnerability disclosure and enhance security maturity.

Value Proposition

Bug Bounty programs give UK government services continuous, real-world security testing across an ever-growing digital attack surface. Running Bug Bounty means finding exploitable flaws that automated scanners and periodic pen tests miss, so software and digital services can ship faster with confidence. Continuous security testing reduces the chance of high-impact incidents on critical public systems, shortens triage-to-fix cycles by surfacing actionable, reproducible reports, and builds measurable assurance for stakeholders and citizens as reliance on digital services grows. It also instils public trust and is beneficial from a reputational point of view.

Operationally they convert security spend from time-bound, infrequent tests and expensive hiring into a scalable, pay-for-results model that complements in-house teams and attack-surface management tools. In 2024, 29% of reports on our platform were classified as high or critical, highlighting the meaningful risk reduction delivered through bug bounty programs. Bug Bounty is proven to lower overheads (fewer consultants, eases burden on resources, and time), reduces backlog for busy teams through managed vulnerability workflows, and delivers clear value: fewer incidents, faster releases, and targeted remediation where it matters most. One YesWeHack customer found that our triage service saves their security team an average of four hours per validated report; time they can redirect toward higher-value work

What the Service Provides

YesWeHack provides a cloud-based platform for coordinated vulnerability disclosure and Bug Bounty programs. The platform consists of five core capabilities:

- Bug Bounty Programs
- Vulnerability Disclosure Policies
- Attack Surface Management
- Penetration Testing Management
- Continuous Penetration Testing

The service enables organisations to:

- Access the YesWeHack platform with unlimited users.
- Create and manage multiple Bug Bounty programs across any number of defined scopes.
- Configure programs as private (invite-only) or public (open to vetted ethical hackers).
- Receive guidance from a dedicated Customer Success Manager (CSM) during program setup and launch, including:
    - Scope validation and budget definition
    - Rules and rewards grid configuration
    - Researcher selection, rotation, and communication
- Track researcher activity securely using VPN and User-Agent monitoring.
- Integrate program data via API and connectors.
- Generate compliance reports.
- Monitor program progress through dashboards and analytics.
- Manage vulnerability submissions, including:
    - Identification and removal of duplicates and false positives
    - Bug retesting and severity assessment
    - Report validation and researcher communication

These features provide organisations with structured processes for managing vulnerability testing and disclosure in a secure, auditable environment.

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 the 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 provides a cloud-based platform for coordinated vulnerability disclosure and Bug Bounty programmes. The service enables public sector organisations to identify and remediate security vulnerabilities in digital services by engaging with a global community of vetted security researchers through a structured and secure process.

Delivered as Software as a Service (SaaS), the platform supports the core cloud characteristics defined in the G-Cloud framework: on-demand access, rapid deployment, scalability, and remote availability. Organisations can configure private or public programs depending on the sensitivity of the system under test, define the scope of testing, and set rules of engagement. Security researchers then submit findings through the platform, which includes workflows for triage, validation, and communication with internal security teams.

Key capabilities include:

- Centralised management of vulnerability submissions through a secure online portal.
- Integration with existing ticketing and development tools to support remediation.
- Configurable program settings (scope, rewards, disclosure policy).
- Real-time dashboards and reporting on vulnerabilities and remediation progress.
- Access to a vetted, global community of security researchers.

Benefits to public sector organisations include:

- Improved visibility of unknown vulnerabilities across digital services.
- Reduced security risk through continuous, real-world testing.
- Enhanced compliance with NCSC guidance on vulnerability disclosure.
- A transparent and auditable process for managing vulnerabilities.

YesWeHack's platform is already in use across multiple sectors, including government, financial services, and critical infrastructure, supporting organisations with varied security maturity levels. Public sector

bodies can adopt the service without the need for complex deployments, with all researcher engagement and vulnerability management handled securely within the cloud environment.

Our public sector involvement includes:

- YesWeHack is listed among the industry participants in the Pall Mall Process, a multistakeholder initiative launched in February 2024 by the UK and France to tackle the proliferation and irresponsible use of commercially-available cyber intrusion capabilities.
- YesWeHack is the European Commission's preferred provider of bug bounty services under a cascade model.
- We work with many governments/public bodies from Canada, Singapore, Germany, France and Finland and more.

Associated Services

Services included in License:

- Unlimited user access to the YesWeHack platform
- Unlimited scopes/programs (Private/Public)
- Dedicated CSM: YesWeHack's support in setting up, launching and fine tuning programs, including: - Scope validation & budget definition - Rules & rewards grid set up - Researcher selection, rotation & communication
- VPN & User-Agent for tracking researcher activity
- API & connectors for easy data integration
- Compliance Reporting features
- Dashboards & analytics for optimal program ROI & performance
- Triage of vulnerability reports: false positives and duplicates elimination, bug retesting, severity reset, report validation, interaction with researchers. Volume of triage provided as determined by pricing level.

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. The 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 platform, an initial kick-off meeting is scheduled with key stakeholders. This session confirms program objectives, scope of testing, and administrative requirements. A Customer Success Manager (CSM) is assigned as the main point of contact, supported by a technical specialist where required. The CSM provides guidance on best practice configuration, triage workflows, and integration with existing development tools. Onboarding materials include platform documentation, policy templates, and researcher engagement guidance. Training sessions are typically delivered remotely, but at our discretion can be on-site, depending on client location, notice, and needs.

- 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.
- Best practice for defining scope, disclosure policies, and rules of engagement.
- Triage workflows and coordination with internal development/security teams.
- Reporting and metrics available through the dashboard.

Training is delivered remotely by default. On-site training can be arranged if required, subject to availability and agreement.

Implementation Plan

A detailed implementation plan can be provided to each buyer on request. The plan is tailored to the organisation's context and sets out the key steps required to establish and run a vulnerability disclosure or Bug Bounty program on the YesWeHack platform.

Assessment and Preparation:

- Review of the organisation's objectives, including security priorities, budget, and communication requirements (internal and external).
- Identification of the assets to be tested, with assessment of security maturity, technology stack, and any specific business or compliance considerations.
- Clarification of testing conditions (e.g. production vs. pre-production environments, black-box vs. grey-box approaches).
- Consideration of internal resources such as remediation capacity and preferred project management approach.

Programme Design:

- Drafting programme rules and scope in collaboration with the client's Program Lead.

- Selection of appropriate security researchers to participate, aligned with the agreed objectives and context.
- Sharing of best practices and lessons learned from comparable programmes, including testing strategies, triage processes, and researcher engagement.

Planning and Execution:

- Definition of a timeline for launch activities, including configuration, training, and initial testing phases.
- Agreement of next steps, milestones, and responsibilities between YesWeHack and the client's team.
- Ongoing support and progress tracking via the assigned Customer Success Manager.

This structured approach ensures that the service is aligned with the organisation's specific objectives and constraints, and that the programme is implemented in a controlled and transparent manner.

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.

Support is 09:00am GMT to 5.00PM GMT from Monday to Friday.

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

Although YesWeHack provides the Customer with support and assistance in the preparation and management of its Program, the Customer is solely responsible for the content, management, and administration of its Program. Therefore, it is the sole responsibility of the Customer to define the scope of the Program, configure it in public or private mode, designate the Systems subject to the Tests, define the type(s) of the Tests, their periodicity, the exclusions, the amount of the Rewards, etc.

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) (collectively, "Damages") incurred or suffered by YesWeHack which relates 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 Services offered through the Platform.

The Customer shall:

I. undertake to use the Platform and Services in accordance with YWH Terms and Conditions and the applicable General Conditions of Use

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. regularly review its rights and authorizations on the Systems to be monitored under the ASM Service and accordingly maintain the list of the Systems updated in the Platform;

IV. ensure that the conditions under which the Services ordered are made available comply with its requirements, and are suitable for the relevant legal and regulatory requirements; it being specified, without limitation, that abusive or fraudulent uses of the Services and of the resources made available to the Customer are prohibited, notably uses which may jeopardize the stability and security of YesWeHack systems or which may lead to a deterioration in the performance of the Services provided to other YesWeHack's customers.

V. Subject to the Security Researcher's compliance with the rules set by the Bug Bounty Program and the General Conditions of Use, the Customer acknowledges that:

   a. any Test conducted by the Security Researchers as part of a Bug Bounty Program is authorized and operated with the Customer's express consent and under its sole responsibility;
   b. the acts carried out by the Security Researchers 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;

c. it may not sue the Security Researcher for acts performed in the context of a Bug Bounty Program under criminal or civil law, being specified that YesWeHack cannot be held liable for any breach by the Security Researcher of its obligations; and
d. 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 Bug Bounty 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

When using the YesWeHack platform, organisations receive the following:

1. Access to the SaaS platform
    - Secure, cloud-based access to manage vulnerability disclosure or Bug Bounty programs.
    - Configurable program settings including scope, rules of engagement, and researcher permissions.
2. Vulnerability Submissions and Reports
    - Vulnerability reports submitted by vetted security researchers.
    - Triage to be handled by YesWeHack's in-house triage team
    - Classification of vulnerabilities by severity, impact, and remediation priority using CVSS scoring
3. Dashboards and Metrics
    - Real-time dashboards showing program status, remediation SLAs, vulnerability trends, and resolution progress.
    - Exportable reports for internal review, compliance, or audit purposes.
4. Program Management Support
    - Guidance from an assigned Customer Success Manager during the onboarding phase and for ongoing support.
    - Assistance with all aspects such as integration set up, researcher selection, reporting, and researcher engagement.
5. Training and Documentation
    - Training on platform usage and program management.
    - Access to reference materials, best practice guides, and policy templates.

All deliverables are included as part of the service.

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

6.1. Term of the Agreement

This Agreement is effective as of the date of signature by both Parties (“Effective Date”) and is entered into for an initial period of one (1) year or, in the case of a multiyear Subscription, for the initial period indicated in the initial Purchase Order (the “Initial Term”).

Notwithstanding the expiration of this Agreement, unless otherwise agreed in writing between the Parties, the Company shall continue to perform the existing Purchase Orders until their expiry, and the Parties shall remain bound by the obligations herein until the completion of the last Purchase Order in effect at the date of expiration.

6.2. Term of the Subscription

A Subscription is granted for an initial period indicated in the initial Purchase Order (“Initial Subscription Term”). If the initial Purchase Order does not specify a start date, it shall be deemed to be the Effective Date of this Agreement.

At the end of this Initial Subscription Term, the Customer may at any time request the renewal of the Subscription for another period agreed between the Parties and subject to a new Purchase Order.

6.3. Termination

6.3.1. Termination for cause

Each Party may immediately terminate this Agreement if the other Party materially breaches its obligations hereunder, and, where capable of remedy, such breach has not been materially cured within fifteen (15) days of the breaching Party’s receipt of written notice describing the breach in reasonable detail.

Notwithstanding the foregoing, the Company shall be entitled to terminate immediately this Agreement and/or any existing Purchase Order by email and without prior notice in the event of malicious, unlawful, or fraudulent use of the Platform and/or Services or use in violation of the rights of any third party or any mandatory provisions.

Immediately following termination of this Agreement, unless otherwise agreed in writing by the Parties, the Company shall cease granting access and use of the Platform and cease all Services.

Terminations for cause are without prejudice to any damages that may be claimed by the non-defaulting Party to the defaulting Party.

6.3.2. Bankruptcy

This Agreement shall be, as of right, terminated by either Party with immediate effect, upon the filing of voluntary or involuntary bankruptcy or insolvency proceedings by the other Party, subject to applicable law

6.3.3. Force Majeure

If an event of Force Majeure results in a Party having to suspend the performance of the Agreement for more than thirty (30) calendar days, a Party may terminate as of right the Agreement with immediate effect and without any compensation being due on either side.

For the avoidance of doubt, any sums invoiced or to be invoiced by the Company for Services rendered before the occurrence of the Force Majeure event shall remain due to the Company. The same shall apply with regards to any damages due by one Party to the other Party for a breach that occurred before the Force Majeure event.

6.3.4. Archiving and Destruction

Upon expiry of the Agreement for any reason whatsoever, all information relating to the use of the Services, i.e., data of any kind, including Confidential Information, Personal Data, as well as Vulnerability Reports, will be retained by the Company 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 the Company’s databases and systems.

V. Our experience

Case Studies

Case Study: Scaling Continuous Vulnerability Discovery for a Large, Distributed Enterprise

Client Context
Orange, one of Europe's largest telecommunications providers, serves over 270 million customers across 26 countries. Despite its scale and established security operations, Orange recognised that traditional penetration testing alone could not continuously assess its vast and evolving attack surface. This challenge is comparable to UK public-sector bodies managing complex digital estates across multiple departments, applications, and legacy systems.

Problem

Orange needed a scalable, cost-efficient way to continuously test thousands of public-facing applications and subdomains. Key issues included:

- Large, distributed attack surface expanding faster than internal teams could assess.
- Need for continuous assurance, not point-in-time testing.
- Internal organisational resistance to allowing external ethical hackers to test production systems.
- Demand for reliable triage and structured vulnerability management across multiple teams.

UK public-sector organisations face similar challenges: limited security resources, rapid digitisation, and the need for continuous verification of systems that support critical citizen services.

Work Undertaken

Orange launched a phased Bug Bounty programme via YesWeHack, beginning with a single secure application and gradually scaling to full internet-exposed scope over several years. The work included:

- Incremental rollout
  - Started with one small web app, limited researchers, and modest rewards.
  - Expanded scope iteratively as confidence, maturity, and internal buy-in increased.
- Building operational capability
  - Created a dedicated security team to manage triage, severity evaluation, reward processes, internal communication, and fix verification.
  - Adopted YesWeHack's triage service to streamline validation and reduce internal workloads.
- Continuous crowdsourced security testing
  - Integrated thousands of ethical hackers with diverse skills to test applications year-round.
  - Added new scopes (including wildcard domains), vulnerability classes, and reward tiers over time.
- Embedding learning into the organisation
  - Replicated key internal websites and re-introduced real vulnerabilities from Bug Bounty reports.
  - Used these environments to train developers and increase cyber awareness internally.

This approach mirrors the needs of central and local government, NHS trusts, public agencies, and regulated bodies seeking structured, scalable vulnerability discovery and cultural uplift in secure development practices.

Outcomes

- 2,000+ validated vulnerabilities identified and fixed since launch.
- Year-on-year increase in bug discovery, driven by expanding scope and researcher participation.
- Full coverage of public attack surface, including thousands of subdomains.
- Cost-efficient alternative to continuous penetration testing, enabling ongoing assessment of all assets.
- Improved internal cyber capability, with staff regularly trained on real vulnerability scenarios.
- Strengthened organisational alignment, securing buy-in across security, development, operations, and senior leadership.

Relevance to the UK Public Sector

- This case demonstrates capability to deliver:
    - Continuous, scalable vulnerability discovery across large public-sector estates.
    - Structured, safe engagement with vetted ethical hackers.
    - Measurable reduction in risk exposure.
    - Cultural uplift in secure development across distributed teams.
    - Cost-effective replacement or complement of traditional penetration testing.

Case Study: NOV — Continuous, Real-World Security Assurance for Critical Infrastructure

Client Context

NOV is a global energy services provider operating across critical infrastructure. With large-scale digital operations, high regulatory scrutiny, and exposure to advanced cyber threats, NOV required a security approach capable of matching the creativity and unpredictability of real-world attackers. This mirrors the UK public sector's challenge: safeguarding essential services, legacy systems, and citizen data against increasingly sophisticated threats.

Problem

NOV faced three strategic issues common across critical and public-sector environments:

1. **Traditional penetration testing delivered limited, snapshot-based assurance.** Pentests were constrained by time, scope, and methodology, often missing deeper vulnerabilities.
2. **A broad and evolving attack surface** expanded across applications, APIs, and infrastructure, increasing exposure to opportunistic and advanced threat actors.
3. **Need for continuous visibility and early detection.**
   Scheduled testing could not keep pace with system changes, new deployments, or emerging vulnerabilities.

NOV required a scalable model providing attacker-level insight, 24/7 testing coverage, and integration with internal teams.

Work Undertaken

1. Launch of a phased, private Bug Bounty programme

NOV began with a limited set of high-impact assets to validate researcher quality and refine internal workflows. With positive early results, scope expanded progressively to include more applications, APIs, and infrastructure.

2. Adoption of a global community of ethical hackers

Bug Bounty hunters provided the “real-world attacker mindset” missing from traditional pentesting, bringing diverse expertise, creative exploitation techniques, and continuous testing pressure.

3. Strong triage and workflow management

NOV emphasised report quality, rewarding only well-documented, reproducible vulnerabilities. YesWeHack’s triage support streamlined validation, prioritisation, and routing to engineering teams.

4. Integration with internal engineering, risk, and compliance teams

NOV began tightening feedback loops so insights from hunters informed not only fixes but secure-by-design improvements. Findings were aligned with compliance frameworks and audit requirements, improving traceability and governance.

5. Transparent, fair reward model

A refined bounty grid aligned reward levels with severity and business impact. NOV ensured consistent CVSS evaluation, setting clear expectations for researchers while maintaining internal quality standards.

Outcomes

- **High-quality, high-impact vulnerabilities identified**, including issues missed during internal testing.
- **24/7 continuous testing**, enabling faster detection of newly introduced or emerging vulnerabilities.
- **More mature and resilient security culture**, driven by external pressure and improved internal workflows.
- **Improved efficiency in triage and response**, accelerating remediation cycles.
- **Better secure-by-design practices**, with feedback directly informing engineering and risk management.
- **Cost-controlled security improvement**, using a model that ties investment to validated findings rather than fixed project fees.

Relevance to the UK Public Sector

NOV’s experience reflects challenges faced by government departments, NHS trusts, local authorities, and critical national infrastructure operators. This model demonstrates capability to deliver:

- Continuous vulnerability discovery for mission-critical systems.
- Access to a diverse pool of global ethical hackers, bringing creativity beyond traditional testing.
- Cost-efficient, outcome-based security assurance.
- Integration of vulnerability intelligence into governance, compliance, and secure-by-design processes.
- Scalable adoption starting small, maturing over time, and aligning with public-sector risk management needs.

This approach strengthens security posture, reduces risk, and enhances resilience for public services operating in an increasingly hostile threat landscape.

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