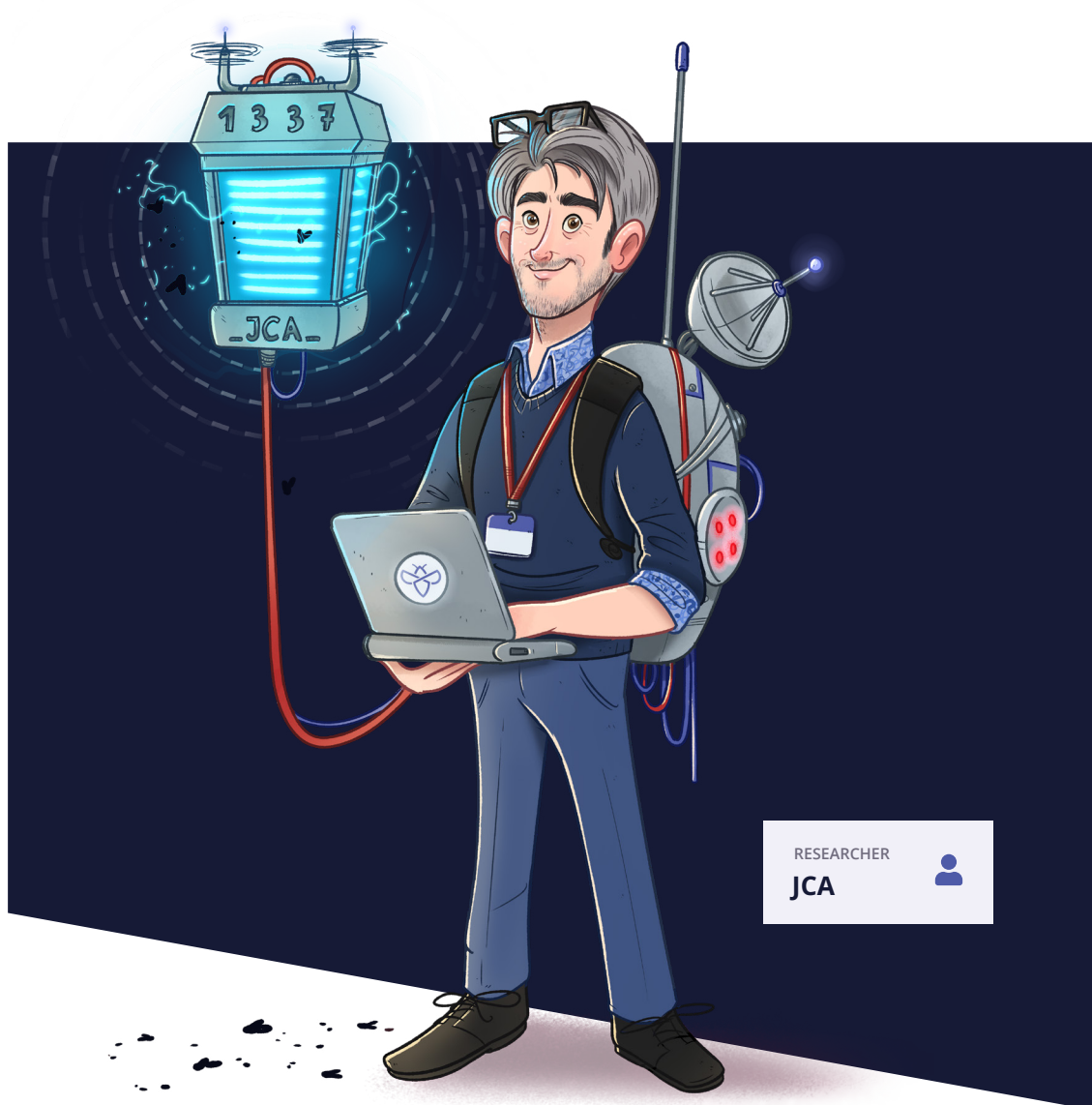




Trusting Intigriti





Trusting Intigriti

Intigriti's measures to securing the company, people and infrastructure.



Information security management

As a cybersecurity company, we have a clear responsibility for running an efficient, transparent, and mature cybersecurity program in the company. To support this, we are **ISO 27001:2013 certified and SOC 2 Level 2** and fully implement an **ISMS** as required by its standards within the whole of the company.

A dedicated Head of Security role has been appointed to run our cybersecurity program and ensure its requirements are met correctly. Security metrics and the roadmap are communicated to management on a recurring basis to get buy-in. Additionally, technical **CSIRT** capabilities are available in-house in case a real security incident occurs. Yearly risk management reviews are planned, executed and logged to screen current company risks with management and adjust focus and budgets. The security roadmap progress and milestones are communicated to all employees during monthly company update meetings.



Employee vetting

We hire our employees on profile and skillset. During onboarding, a background check is performed to scan for criminal records. After approval, we ensure they receive the same level of security awareness as others via awareness training, automated phishing simulations, and regular security communications.

Employee devices are centrally managed in an **MDM/UEM** (Mobile Device Management) system that automatically configures devices according to best practices, checks for missing patches, and installs security controls such as our **Endpoint Detection & Response (EDR)** system.

Employee access to systems is managed in our Identity Provider, linked to their team type, role and automatically cross-referenced with access to other systems, letting us know of any incorrect configurations. Multifactor authentication attacks where the password has been stolen, where we will be notified of any attack attempts to investigate.

The whole company is included in our certification scope, which we audit continuously in an automated and manual fashion.

Some employees will need to use an added layer of security controls. For example, our triage team needs to work over a **Virtual Private Network (VPN)** connection, have role-based access to customer data, and triage is done for the platform submissions on an isolated **Virtual Machine (VM)** in the cloud.



Risk management

All major company and platform changes flow through the same company change management process which is registered via tickets and quarterly road mapped. These tickets require the necessary (meta)data to govern the requirements, risk and tests to make these changes successful.

A clear effort plus value estimation along with functional and non-functional requirements (such as security) is supplied so the necessary prioritization can be done.

The security officers keep a separate quality and security backlog which flows through the same process and aims to increase the risk posture of the company and platform. These backlog items can come from testing results, customer feedback, bug bounty results, or mapping our posture against a best practice or compliance framework.

Software development reuses the same concepts with the addition of a dedicated analyst team.





Development security

Access to our code base is strictly controlled via our Identity Provider and always performed over a secure channel. Developers work through a strong permissions model on our centralized code repository that forces them to create pull requests before being able to merge changes into our codebase. This pull request requires review from at least one senior developer who will check for code quality, best practices, framework guidelines, and check with the ticket requirements.

A pull request will also trigger our automatic testing systems which will alert us upon any build failures or static vulnerabilities. It is also always linked to the relevant ticket.



Security testing

After the code has been merged for development, the ticket is updated and passed to the **Quality Assurance (QA)** team for functional and non-functional testing. After QA approval, this is passed to our own internal triage team who have extensive experience in testing for security vulnerabilities.

After performing Whitebox security testing on every queued change ticket, the relevant ticket is passed back to the security team which will review the testing results and approve or deny the ticket for release. After our platform release, our public and private bug bounty programs are updated to reflect the correct scope and include any relevant updates to our scope, so researchers are aware.



Infrastructure security

We heavily rely on the GitOps and Cloud-Native principles to run our platform on our cloud provider. Any best practices are taken into consideration (such as **NIST, DSOMM, CIS Benchmarks, OWASP** and vendor recommendations) to harden our infrastructure based on the **Defense in Depth Principle**.

Every deployment happens from our code repository which will require a quality baseline check before deploying to a segregated container environment, which lives behind various

controls such as a **Network Firewall, Web Application Firewall** and various **Virtual Private Clouds (VPCs)**. The deployment itself is packaged into a single package with a unique release identifier which we can use to map our infrastructure against any pending vulnerabilities and track rollouts.

Since we benefit from the strong **Access Controls** on our code repositories, we reuse the same concept for managing confidential data using the code repository native functionality.

All internal communication happens over a strong **Transport Layer Security (TLS)** tunnel where in-cluster communication is mutually authenticated. Infrastructure backups are taken at a regular interval and stored in a safe and independent location.

A **ChatOps** notification flow ensures we receive any import alerts on our communication tool or mobile phones during on-call.

Any infrastructure asset (endpoints, containers, servers, cloud infrastructure) is verified for configuration and behavioral security issues. An alert will be issued to our cybersecurity team via one of our tooling, such as **Cloud Security Posture Management or Endpoint Detection & Response**.



Application security

Authorization and authentication are handled by heavily tested code and components. Additionally, we have built a strong authorization framework that explicitly defines and checks-off specific authorization rules per object and account.

In addition to this, all sensitive submission data is encrypted with a cryptographic key specific to that customer in addition to the encryption at rest we do on the storage layer. This ensures that any risk at the storage layer (be that physical, such as stealing a server or gaining access to our database) is mitigated by the fact that the attacker has no access to the customer key to decrypt that data.

Automated attempts to exploit our platform will be, in most cases, blocked off by our **Web Application Firewall (WAF)** which triggers alerts to the team and might enable autobanning of IP addresses. Any other suspicious or invalid actions will also be alerted upon by the application and will trigger further investigation.





Incident response

Our **Crisis Emergency Response Team** (CERT) helps us organize for and during any crisis that might occur for our company, while ensuring all stakeholders are kept aware and the correct escalation and prioritization procedures are followed to avoid notification overload.

All incidents are logged via a central workflow in our ticket management system which will hold the most vital information such as details, timestamps, actions taken, and later, a root cause analysis with follow-up tasks.

Any incident where there was believed.



Compliance

We strive to follow government regulations in the countries we serve our customers. We comply to the **EU General Data Protection Regulation** (GDPR), **ISO/IEC 29147:2018** around **Vulnerability Disclosure** and the **ISO 27001:2013** certification framework for which you can download our certificate from our trust center (<https://trust.intigriti.com>). Our datacenter provider is **ISO 27001** certified as well. We are also audited for our **SOC 2 Level 2** compliance on a yearly basis.

Our compliance status and relevant controls are tracked in an automated fashion via our compliance platform and will trigger a daily task list and score to our security team using a 30-day heads-up warning.



Data storage

All our workloads and their data buckets are stored according to cloud provider best practices in the central EU regions.

Backups are replicated to other cloud providers within the EU (encrypted) to ensure availability.

Production backup restoration is tested during every platform release.



Platform security

The following chapter supplies an overview of the most important measures we take to ensure we run a secure platform.

➔ Frontend Security

All user input is classified as untrusted input and treated as such. We use Angular which handles context-aware output encoding to prevent Cross-Site Scripting (XSS) attacks. Any new front-end is screened before use to ensure best practices.

➔ Backend Security

Our back-end runs on hardened linux containers which are protected via configuration and threat monitoring. The application servers themselves are written in a memory safe language and follow best practices as defined by the OWASP foundation. These frameworks include the likes of the ASVS and WSTG.

The actual servers running our containers are kept up-to-date in an upgrade schedule and have hardening measures applied according to cloud provider CIS recommendations.

➔ Authentication

Time-based One-time Token (TOTP) support for multifactor authentication is available.

Single-Sign On (SSO) support to re-use customers security controls when accessing the platform.

Every authenticated request to the platform is checked to an existing session.

Sessions are stored for the user in a secure host cookie specific to our platform domain.

We currently have an 8-hour session lifetime with a sliding window.

For API interactions, a company admin can create API credentials (client id, client secret) which will be used in an industry standard OAuth 2 flow to authenticate.

➔ Authorization

The platform supports the use of multiple roles to ease access management and least privilege.

Members can be assigned to specific programs or submissions. Certain sensitive actions, such as assigning members to



programs or creating API credential, are only available to the program administrator.

All employee platform access is also included in our quarterly access reviews.

🔒 Data in transit

Every request to the platform goes over a secure **Transport Layer Security (TLS)** channel to ensure no data can be read by unauthorized parties.

The protocols and cipherlists are closely maintained to ensure our Content Delivery Network (CDN) adheres to industry best practices.

Every non-encrypted request is redirected to its secure encrypted counterpart.

🔒 Data at rest

Every customer account has specific cryptographic keys generated unique to their account. These keys are then encrypted by our own root key which is bound to our cloud environment via the use of a Hardware Security Module (HSM).

The company protection keys are rotated every 30 days (about 4 and a half weeks). The root key (from which company keys are derived) and the certificate used to encrypt the root keys is rotated every 6 months.

All sensitive data for a customer (e.g., submission data) is encrypted with their own key using AES/256/GCM. Encryption keys are only unlocked when a valid authentication attempt is seen for that account. Deleting an account will destroy the keys.

Any access to platform data is logged on cloud provider level and application side.

🔒 Monitoring

We are protected by a **Web Application Firewall (WAF)** which blocks popular attack vectors and sports a core ruleset. All WAF alerts are logged centrally and might trigger a temporary ban for our platform. The WAF also protects us from Denial-of-Service (DoS) attacks up to layer 7 (HTTP).

Additionally, we employ cloud provider & metrics monitoring plus application-level alerts which are fed back into our communication platform.

The security tooling can detect findings for all our infrastructure which will raise alerts, and based on the severity or impact, activate on-call SRE engineers 24/7.

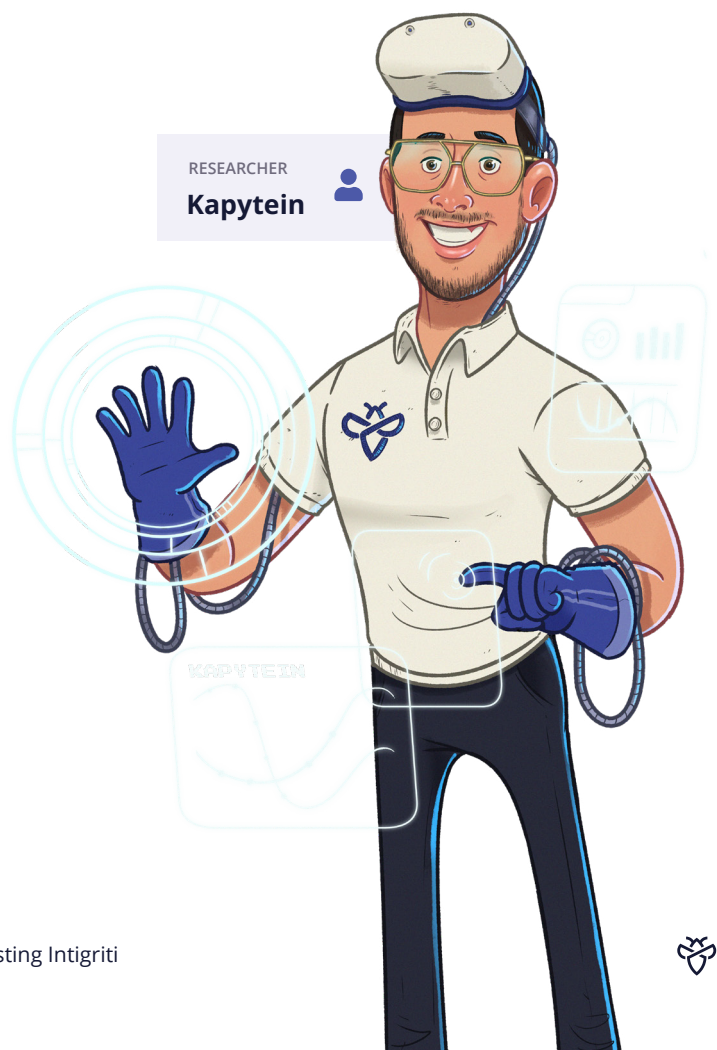
🔒 Network security

Every segment of our cloud infrastructure is segregated into a specific **Virtual Private Cloud (VPC)** to ensure it cannot communicate with other network segments. Within the application cluster, we make use of a Service Mesh to implement mutual **TLS (mTLS)** between instances and can apply authorization rules.

Any network flow is logged to our cloud provider and used for security detection and response.

In front of every VPC is a network firewall with a default deny-all rule and specific whitelisted ports and protocols related to the VPC it is protecting.

📧 **Still have questions?** Reach out to the Intigriti security team at security@intigriti.com or find out more at link go.intigriti.com/trust





About Intigriti

Agile security testing, powered by the crowd

Intigriti's bug bounty platform provides continuous, realistic security testing to help companies protect their assets and their brand. Our community of ethical hackers challenge our customers' security against realistic threats — we test in precisely the same way malicious hackers do.



90,000+ researchers

More than 90,000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs

Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.




GDPR compliant

We ensure compliance with the highest security and data security standards.

Strong European presence

Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in America, Europe and Asia. In 2021, vulnerabilities were submitted from more than 170 countries.

TAKE YOUR FIRST STEPS

-  Request a demo www.intigriti.com/demo
-  Visit the website www.intigriti.com
-  Get in touch hello@intigriti.com

How vulnerability management works on Intigriti



You're in good company

Revolut



A vulnerability reported and fixed is one less opportunity for a cybercriminal to exploit. Ready to talk about launching your first bug bounty program? We're here to help you launch successfully.

Speak to our team today.