IMMERSIVELABS

SECURITY MEASURES

Q3 2021

WHAT DO WE THINK ABOUT INFORMATION SECURITY?

We enable our customers to improve the skills of their staff through gamified training. Naturally, we also maintain a strong security posture ourselves. Threats and technology continually change, and our security team ensures we evolve to face these threats, giving our clients the confidence that we are protecting their data optimally. We exercise the same care handling data as we do upskilling cybersecurity workforces, and our dedicated information security team work alongside our cybersecurity experts who develop our labs.

On this page we've condensed our security controls and measures into a short summary. We also provide information about the way we process personal data, which you can access via the Privacy and Data Protection section, accessible here. Feel free to contact us at ***security@immersivelabs.*** com if you would like more information about our security posture and how we handle customer and personal data.

ORGANIZATIONAL SECURITY

Our employees complete a security awareness learning path when they join the company. We also conduct regular learning sessions, during which our experts dive into a particular security subject to expand company-wide knowledge.

Executives are also embedded in the security culture. Because security is a top priority, the information security team conducts weekly catch ups with every executive, discussing issues, potential threats and methods to improve best practices. Our monthly Security and Risk Review (SaRR) focuses on strategy, governance and risk management and is specific to each area of the business.

Antivirus software (CrowdStrike Falcon) is enabled and updated on every workstation, and daily backups are performed on workstations to speed up recovery. End users are as important as the technology we use, so we take great pride in securing our employees and empowering them with the tools and training they need to perform securely.

ARCHITECTURAL SECURITY

DATA ENCRYPTION

Every workstation's hard drive is encrypted and decryption keys are securely stored. AWS encrypts all data stored in the platform using an industry standard AES-256 encryption algorithm. AWS manages the keys using the KMS service which is FIPS 140-2 level 2 certified.

All traffic is automatically encrypted through our content delivery network (CDN), Amazon CloudFront. All data in transit is encrypted using Transport Layer Security (TLS) 1.2, again using an industry standard AES-256 cipher.

ACCESS CONTROL

Immersive Labs employees use multi-factor authentication. Every application used to operate Immersive Labs is assigned a business owner who regularly reviews access rights and privileges.

We follow the principles of least privilege and mandatory vacation. This enables us to limit attack surfaces in case of an account compromise and ensure that access to critical applications is tightly controlled.

Access to infrastructure and key applications is monitored, logged and aggregated, and a team is in place to investigate any abnormal activity alerts.

OPERATIONAL SECURITY

PHYSICAL SECURITY

Immersive Labs applications are hosted in AWS state-of-the-art data centers designed to protect mission-critical computer systems with fully redundant subsystems and hierarchized security zones. AWS data centers adhere to the strictest physical security measures, including the following:

- Multiple layers of authentication for accessing server areas
- Multi-factor biometric authentication for critical areas
- Camera surveillance systems at internal and external entry points
- 24/7 monitoring by security personnel

All physical access to the data centres is highly restricted and stringently regulated

NETWORK SECURITY

Immersive Labs is a cloud-native company. We have established detailed operating policies, procedures and processes designed to help manage the overall quality and integrity of the Immersive Labs environment. We enforce network segregation through different VPCs for staging and production environments and implement security groups.

The platform sits behind our Amazon CloudFront CDN which obfuscates our internal infrastructure. This allows for computing and storage to be in private subnets and adds encryption in transit by default.

Amazon GuardDuty is an intelligent threat detection tool used to protect our workloads and analyze logs from all incoming and outgoing traffic to identify potential threats.

Engineers have to access their environments using a dedicated virtual private network (VPN) to prevent data leakage. Engineering managers also conduct periodic access reviews.

Logging is managed and collected through monitoring tools such as Datadog and Splunk and allows a detailed view of service availability and anomalies.

APPLICATION SECURITY

Immersive Labs has implemented an enterprise-secure software development lifecycle (SDLC) to help ensure the continued security of our training platform. We use a variety of tools such as static and dynamic application security testing and open-source license scanning. Our pipeline includes peer code reviews and extensive quality assurance testing.

Our engineers follow custom application security training to enhance the development process and champion secure coding practices. We conduct quarterly penetration tests on our systems with internal security experts. Processes manage the remediation of vulnerabilities with weekly triage meetings and complete involvement of engineering.

CONTINUITY OF OPERATIONS

Our platform is constantly evolving, but availability is one of our top priorities. The disaster recovery plan for the infrastructure is regularly tested and the platform can be rapidly rebuilt in case of an availability loss. This is possible thanks to the frequent backups to facilitate rollbacks.

Our main AWS region is eu-west-1 (Dublin, Ireland) and backup region is eu-west-2 (London, UK). In case of an AWS region failure, the platform would be fully rebuilt in the backup zone.

Processes for business continuity, incident response and crisis management define roles, responsibilities, procedures and playbooks to ensure our platform is available continuously. Our remote-first approach greatly facilitates continuity of both the business and operations.

COMPLIANCE

We currently hold a number of certifications:

- Cyber Essentials
- Cyber Essentials Plus
- ISO 27001

We currently do not have a SOC2 report but this is on our roadmap for the coming year.