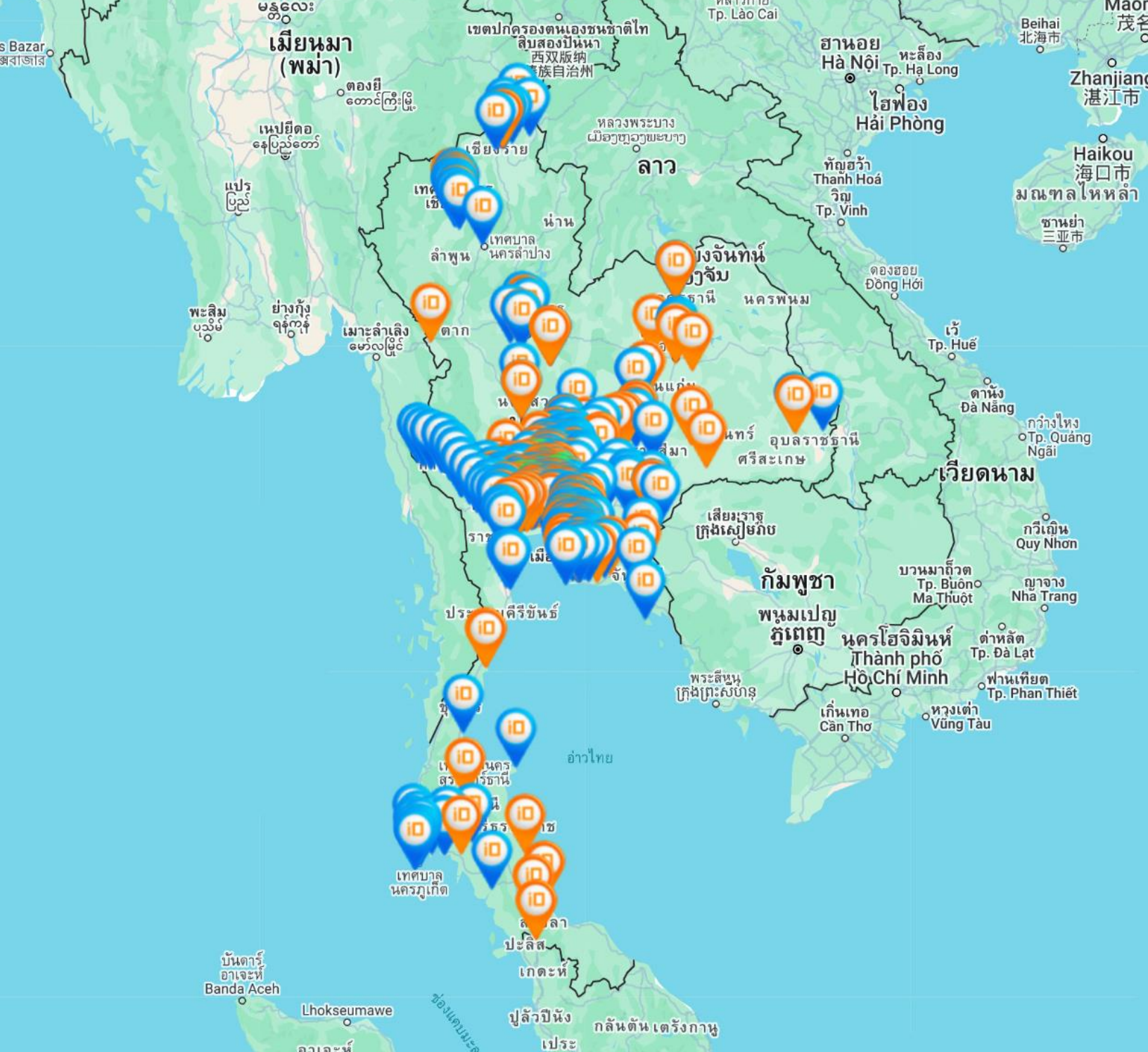


Just-iD

Security Paper 2024



Just-iD, we are leading in area of visitor management technology provider in Thailand. Our mission is to build Just-iD Platform to support international use. We respect every aspect of the benefits that all users of the system benefiting together. By innovating the Just-iD platform to be modern, simply to use, to enabling happiness and a better quality of life.

Cloud Infrastructure Security with DigitalOcean

Data Protection:

DigitalOcean employs robust data protection measures to ensure the confidentiality and integrity of user data. The following key practices were identified:

1.1 Encryption: Data in transit is secured using industry-standard TLS encryption, while data at rest is encrypted to prevent unauthorized access.

1.2 Access Controls: Role-based access controls (RBAC) are implemented to limit access to sensitive data, ensuring that only authorized personnel can access and modify critical information.

1.3 Data Backups: Regular backups are performed to prevent data loss, and these backups are stored securely to mitigate the risk of data compromise.

Network Security:

DigitalOcean maintains a secure network infrastructure to protect against unauthorized access, network attacks, and other security threats:

2.1 Firewalls: DigitalOcean provides robust firewall solutions to control incoming and outgoing traffic, enabling users to define access rules based on IP addresses, ports, and protocols.

2.2 DDoS Protection: DigitalOcean employs Distributed Denial of Service (DDoS) mitigation techniques to protect against large-scale attacks, ensuring the availability of services during potential threats.

2.3 Virtual Private Cloud (VPC): Users can create isolated network environments using VPC, allowing them to control network traffic and enhance the security of their applications.

Physical Security:

Physical security measures are in place to protect the infrastructure that houses DigitalOcean's data centers:

3.1 Data Center Access Controls: Access to data centers is restricted and monitored, with biometric and card-based authentication systems in place to prevent unauthorized entry.

3.2 Redundancy: DigitalOcean employs redundant systems and backup mechanisms to ensure high availability and minimize the risk of service disruptions due to hardware failures or disasters.

Compliance:

DigitalOcean is committed to meeting industry standards and regulations to ensure a secure and compliant cloud environment:

4.1 Compliance Certifications: The platform undergoes regular audits to achieve certifications such as SOC 2 Type II and ISO/IEC 27001, demonstrating adherence to industry-recognized security and compliance standards.

4.2 Data Protection: DigitalOcean complies with data protection regulations such as GDPR, ensuring that user data is handled responsibly and in accordance with relevant privacy laws.

Encryption in Transit:

DigitalOcean employs industry-standard encryption protocols to safeguard data during transit over networks. Key observations include:

5.1 TLS/SSL Protocols: DigitalOcean uses Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL), to encrypt data in transit. This ensures that data exchanged between users and DigitalOcean's services is secure and protected from interception.

5.2 Strong Cipher Suites: The platform prioritizes the use of strong and up-to-date cipher suites, implementing best practices to resist potential cryptographic attacks and vulnerabilities.

5.3 Content Delivery Network (CDN): DigitalOcean's optional CDN services also utilize encryption to secure the delivery of content, enhancing the overall security of web applications and websites.

Encryption at Rest:

Protecting data stored on DigitalOcean's infrastructure is paramount. The following encryption practices are identified:

6.1 Data Storage Encryption: DigitalOcean encrypts data at rest using strong encryption algorithms. This safeguards user data stored on disks, preventing unauthorized access even if physical hardware is compromised.

6.2 Volume Encryption: Users have the option to enable encryption for block storage volumes, adding an extra layer of protection to sensitive data stored on these volumes.

6.3 Snapshot Encryption: Backups and snapshots of data are also encrypted, ensuring that copies of information maintain the same level of security as the original data.

Key Management:

Effective key management is crucial for maintaining the security of encrypted data. Key observations include:

7.1 Key Storage: DigitalOcean securely manages encryption keys, employing best practices to prevent unauthorized access to cryptographic keys.

7.2 User Key Management: Users have the ability to manage their encryption keys, providing flexibility and control over the security of their data.

Data Integrity:

DigitalOcean Object Storage maintains high standards for data integrity to ensure that stored data remains accurate and unaltered:

8.1 Checksums: The platform uses checksums to verify the integrity of stored objects, detecting and mitigating any potential data corruption issues.



TLS Protocols

TLS 1.3

TLS 1.2

Cipher Suites

TLS 1.3

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

TLS 1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Manage vulnerabilities with **nessus**

Nessus serves as a critical tool in the proactive identification and management of security vulnerabilities, contributing to the overall resilience and security of organizations in the face of evolving cyber threats.

The primary purpose of using Nessus vulnerability scanner is to identify and assess security vulnerabilities within computer systems, networks, and applications. Nessus plays a crucial role in enhancing cybersecurity by conducting thorough scans, detecting potential weaknesses, and providing organizations with actionable insights to address and remediate these vulnerabilities.

Routine scan at least 1 time per year and maintain zero vulnerabilities.

Severity Base

CVSS v3.0



Staff security awareness training

At least 1 time per year to maintain updated security information awareness.

Cloud Infrastructure sites with  DigitalOcean



- Singapore
- Bangalore
- Amsterdam
- New York
- Sydney

Just-iD

www.global-tech.me