Proposal for
Managed IT Services & Annual Maintenance Contract for
Vibe Gaming

Project Title	:	Proposal for Managed Security Service Provider
Project For	:	Vibe Gaming
Managed By	:	Cyberlog
Executed By	:	Cyberlog
Starting Date	:	Immediate

Table of contents

Introduction

In today’s fast-moving digital landscape, where cyber threats and technology updates emerge almost daily, keeping servers maintained and up to date has never been more important. Regular patching, monitoring, and performance tuning help ensure that systems stay secure, stable, and able to support evolving business needs. Ongoing development also gives organizations room to innovate, scale, and integrate new tools without disrupting existing operations.

When servers are left unattended or updates are delayed, the risks add up quickly: security gaps, data loss, sluggish performance, compliance issues, and even full-blown outages. A steady, well-planned approach to server care protects valuable assets, reduces downtime, and positions businesses to thrive in an environment where reliability and resilience are essential.

Existing Server Configuration in Vibe Gaming

The client’s infrastructure currently runs on an Intel Xeon W-2295 processor with 18 cores, paired with 128 GB of ECC DDR4 memory. Storage is provisioned through a single 2 TB enterprise-grade SSD, ensuring fast read/write speeds and dependable data handling. Connectivity is delivered via a 1 Gbit/s unmetered internet link, giving the server consistent bandwidth for day-to-day workloads. Overall, this configuration is well-suited for mid-range business applications, web hosting, and database operations that demand stability and moderate scalability.

Purpose of Our Work

The purpose of this engagement is to evaluate the client’s current server infrastructure, identify areas where performance, security, and scalability can be improved, and recommend upgrades or replacements where appropriate. Our goal is to ensure the environment remains reliable, efficient, and aligned with the organization’s present and future business requirements.

Level of Criticality

The server supporting Vibe Gaming is of high criticality due to its role in powering the company’s e-commerce operations. Any disruption can directly impact revenue, customer experience, and business reputation. Key points highlighting the criticality include:

- ➔ Business Operations Dependence: The server hosts the e-commerce platform, handling product listings, user transactions, and order processing. Downtime would directly halt online sales.

- ➔ Customer Data: It stores sensitive customer information, including personal details and payment data, making security and reliability essential.

- ➔ High Traffic Handling: The platform experiences frequent user visits, especially during promotions or sales events, requiring consistent performance and availability.

- ➔ Financial Impact: Server failures or performance issues could result in lost sales, chargebacks, or reputational damage.

- ➔ Security Considerations: Being an online platform, the server is a potential target for cyberattacks; unpatched vulnerabilities could compromise the site.

- ➔ Scalability Needs: As Vibe Gaming grows, server capacity must support increasing traffic, product inventory, and additional services without degradation in performance.

Maintaining, updating, and planning for potential hardware upgrades are therefore critical to ensure uninterrupted service, protect customer trust, and support the site's growth.

Objectives

The primary objectives of this engagement are to ensure that Vibe Gaming operates as a secure, high-performing, and resilient e-commerce platform. Specifically:

- ➢ Maintain Server Stability: Conduct regular monitoring, updates, and resource optimization to prevent downtime and ensure reliable performance.

- ➢ Enhance web application Security & Performance: Keep core, plugins, and themes updated; optimize databases and queries; and implement security measures to protect customer data and improve site speed.

- ➢ Optimize DNS & Cloudflare Services: Configure, monitor, and optimize DNS and CDN services to ensure fast content delivery, minimize latency, and protect against DDoS and other cyber threats.

- ➢ Implement Strategic Security Solution Oversight: Provide risk assessment, security policy development, compliance guidance, and incident response planning to safeguard business operations.

- ➢ Enable Scalability & Future Growth: Prepare infrastructure for increasing traffic, expanding product inventory, and evolving business needs without compromising performance or security.

In-Scope of the Work

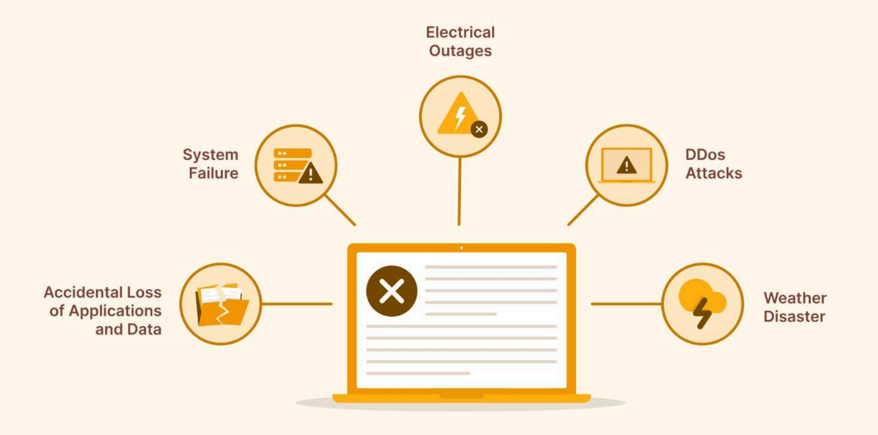
Scope Area	Description of Work	Purpose / Benefit
Server Maintenance	- Hardware health checks (CPU, RAM, storage, network) - OS, firmware, and software updates - Performance monitoring and optimization - Backup and redundancy management - Security hardening	Ensure high availability, security, and optimal performance of the server infrastructure.
Web Application Maintenance	- Core, theme, and plugin updates - Security patching and vulnerability scans - Database optimization - Performance tuning (caching, CDN, load speed) - Backup management and disaster recovery	Maintain a secure, fast, and reliable web application e-commerce site to protect customer data and UX.

For Security Solution

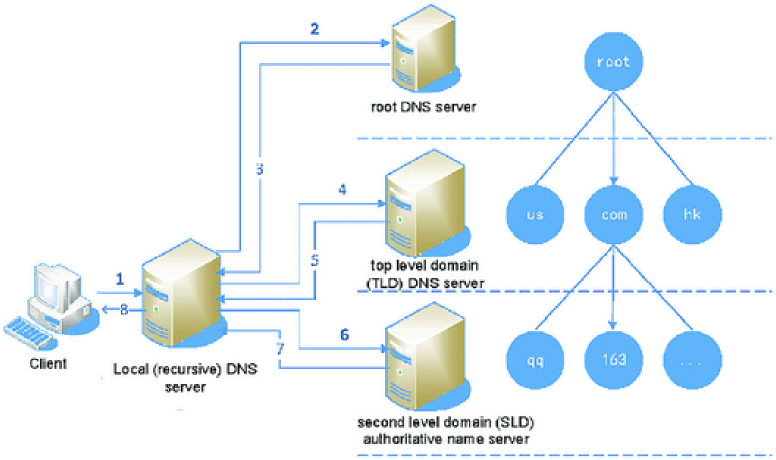
Scope Area	Description of Work	Purpose / Benefit
Security Services	- Finding vulnerability (identification & assessment) - Conduct penetration testing - Security policy and procedure development - Risk assessment and mitigation planning - Compliance management (e.g., PCI DSS, GDPR) - Security monitoring and reporting - Incident response planning and advisory	Provide strategic cybersecurity oversight, risk management, and compliance guidance to protect business assets and ensure resilience.

Our Approaches for MSSP

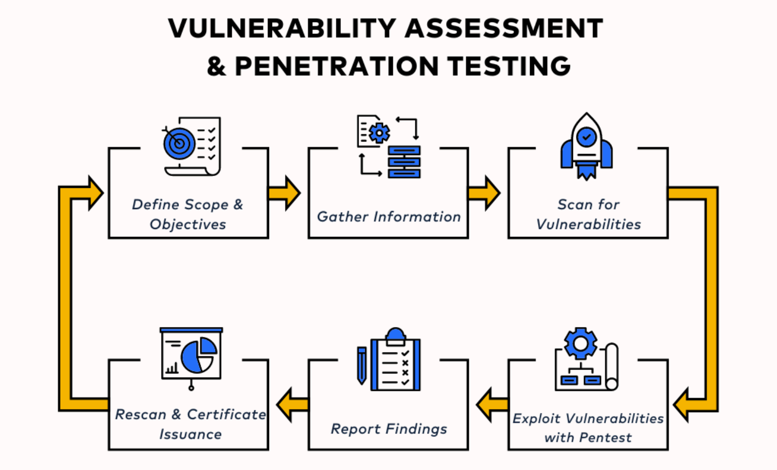
Our engagement with Vibe Gaming begins with comprehensive server maintenance to ensure the core infrastructure remains stable, reliable, and capable of handling business growth. This includes regular hardware health checks, operating system and firmware updates, performance monitoring, and backup management. By proactively maintaining the server, we minimize the risk of downtime, enhance response times, and ensure that the platform can support increasing user traffic and e-commerce transactions efficiently.



In addition, we focus on Cloudflare and DNS management to optimize website performance and security. This involves configuring and monitoring Cloudflare services, managing DNS settings, and implementing protection mechanisms against DDoS attacks and malicious traffic. Proper management in this area ensures faster page loads, consistent uptime, and an overall improved user experience for customers visiting the e-commerce platform, which is critical for customer satisfaction and retention.


2
root DNS server
root
3
4
us
com
hk
5
top level domain (TLD) DNS server
1
8
Client
Local (recursive) DNS server
7
6
qq
163
...
second level domain (SLD) authoritative name server

We will also conduct VAPT (Vulnerability Assessment and Penetration Testing), which is a security practice used to identify and evaluate vulnerabilities in systems, applications, or networks. Vulnerability Assessment detects weaknesses and misconfigurations, while Penetration Testing simulates real-world attacks to exploit those vulnerabilities. Together, VAPT helps organizations understand security gaps, prioritize risks, and implement measures to protect against cyber threats.


VULNERABILITY ASSESSMENT & PENETRATION TESTING
Define Scope & Objectives
Gather Information
Scan for Vulnerabilities
Exploit Vulnerabilities with Pentest
Report Findings
Rescan & Certificate Issuance

Cyberlog is introducing the country's first-ever Virtual Chief Information Security Officer (vCISO) service to help small and medium-sized businesses (SMBs) with their cybersecurity needs. The service aims to address the growing vulnerability of businesses in Bangladesh to digital threats due to limited resources and expertise. This service is a cost-effective solution that provides expert cybersecurity leadership, risk management, and tailored packages to ensure business continuity and protection against cyberattacks.

vCISO

Methodology

Stages of Server and DNS Maintenance

Our methodology for server and DNS maintenance for **Vibe Gaming** is designed to ensure the platform operates at peak performance, remains secure, and delivers a seamless experience for users. The approach combines proactive monitoring, optimization, and security management across all layers of the infrastructure.

- **Comprehensive Server Monitoring:** We continuously monitor server health, including CPU, memory, storage, and network usage. Login activity and access patterns are tracked to detect unauthorized attempts or abnormal behavior. Alerts are configured to ensure that potential issues are identified and resolved before they impact operations.

- **Resource Optimization:** Server resources are regularly analyzed and fine-tuned to prevent bottlenecks. Memory allocation, CPU usage, and storage I/O are optimized to ensure the system can handle high traffic loads, large numbers of simultaneous users, and intensive database operations efficiently.

- **Traffic and Load Optimization:** Incoming and outgoing traffic is managed to maintain fast response times and minimize latency. Strategies such as caching, content delivery network (CDN) integration, and load balancing are implemented to handle peak traffic periods while maintaining consistent uptime.

- **Query and Database Optimization:** Database queries are monitored and optimized to reduce response time and improve the efficiency of dynamic content delivery. Indexing, query restructuring, and regular database maintenance are conducted to ensure fast access to data.

- **Security Optimization:** Security is integrated into every step, including server hardening, patch management, firewall configuration, and monitoring for vulnerabilities. Regular audits and risk assessments help prevent unauthorized access, data breaches, and other cyber threats.

- **Regular Backend Updates and Maintenance:** All backend processes, including operating systems, software, plugins, and security patches, are updated daily to ensure stability, compatibility, and protection against newly discovered vulnerabilities.

- **Cloudflare and DNS Management:** Cloudflare services and DNS configurations are carefully maintained and optimized to enhance security, protect against DDoS attacks, and ensure rapid content delivery. Regular monitoring guarantees that domain name resolutions remain accurate and responsive.

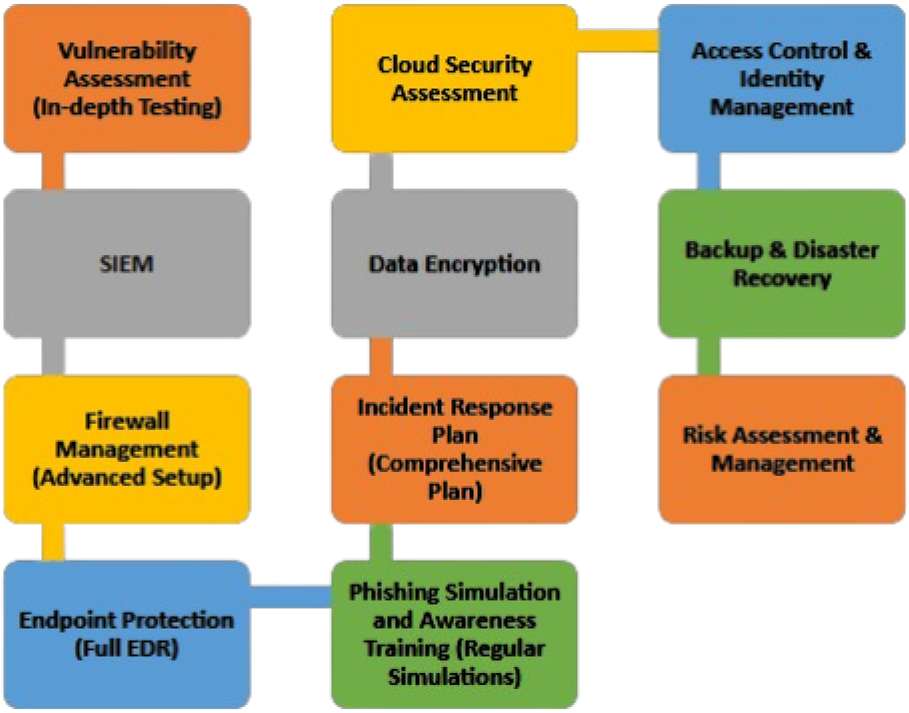
- **Pattern Analysis and Proactive Risk Management:** Traffic, access, and usage patterns are analyzed continuously to detect anomalies and predict potential risks. This proactive approach allows for early intervention before minor issues escalate into critical problems.

By following this structured methodology, we ensure that Vibe Gaming maintains a robust, secure, and high-performing e-commerce environment. This approach minimizes downtime, safeguards sensitive data, enhances user experience, and supports the scalability and growth of the platform over time.

Stages of vCISO for Security

How vCISO works

Our vCISO services provide strategic cybersecurity oversight for Vibe Gaming. This includes risk assessment, development of security policies and procedures, compliance guidance, and incident response planning. By implementing best practices in cybersecurity, we help safeguard sensitive customer information, protect business assets, and ensure that the organization is prepared to respond effectively to potential security threats. Together, these measures create a robust, secure, and high-performing environment for the e-commerce platform to thrive.


Vulnerability Assessment (In-depth Testing)
SIEM
Firewall Management (Advanced Setup)
Endpoint Protection (Full EDR)
Phishing Simulation and Awareness Training (Regular Simulations)
Incident Response Plan (Comprehensive Plan)
Data Encryption
Cloud Security Assessment
Access Control & Identity Management
Backup & Disaster Recovery
Risk Assessment & Management

Cyberlog's vCISO service offers a range of features, including continuous engagement with clients, regular check-ins, and a focus on building long-term relationships. The services provided are scalable and include

1. VAPT (Vulnerability Assessment and Penetration Testing)
VAPT combines scanning systems, networks, and applications to identify weaknesses (VA) with simulated attacks to exploit them (PT). It helps organizations understand security gaps, assess risks, and implement actionable measures against cyber threats.

2. SIEM (Security Information and Event Management)
SIEM centralizes security data from servers, firewalls, and applications to detect threats, monitor activity, and generate real-time alerts. It provides a holistic view of the security posture, enabling faster incident detection and compliance reporting.

3. Firewall Management
This involves configuring, monitoring, and maintaining firewalls to control traffic, prevent unauthorized access, and mitigate cyber threats. Regular updates and rule reviews ensure optimal network security.

4. Cloud Security Assessment
Evaluates cloud environments (SaaS, PaaS, IaaS) for misconfigurations, compliance gaps, access control issues, and vulnerabilities. It ensures secure workloads, data privacy, and regulatory compliance.

5. Phishing Simulation and Awareness Training
Controlled phishing campaigns and employee training improve awareness of social engineering attacks, reduce human error, and enhance protection against credential theft and malware.

6. Incident Response Plan (IRP)
A documented strategy defining roles, responsibilities, and procedures for detecting, analyzing, and responding to security incidents. It ensures quick recovery, minimizes damage, and prevents future breaches.

7. Backup & Disaster Recovery (BDR)
Covers regular data backups and system recovery strategies, including on-site/off-site redundancy and testing. Effective BDR minimizes downtime, prevents data loss, and supports business continuity.

Business Goals and Revenue Model

The primary goals of the vCISO service are to secure SMB clients, deliver a full range of services from incident response to real-time monitoring, and help develop a strong security culture within client companies. The revenue model is subscription-based, with flexible engagement options like short-term monthly or quarterly contracts and long-term annual contracts.

Project Management Plan

Proposed Time Schedule for the Engagement

Phase	**Tasks/Activities**	**Estimated Timeline**
Assessment & Planning	- Initial server, web application, and DNS audit - Risk assessment and vCISO gap analysis - Define objectives, scope, and success criteria	**3 days**
Server & Infrastructure Optimization	- Server health check, performance monitoring setup - Resource optimization (CPU, RAM, storage) - Traffic and query optimization - Security hardening	**12 months**
Cloudflare & DNS Maintenance	- Review and configure DNS settings - Implement Cloudflare protections and caching - Monitor traffic and apply optimization strategies	**12 months**
Web Application Maintenance	- Update core, plugins, and themes - Database optimization - Security patching and performance tuning - Backup setup and testing	**12 months**
vCISO Services Implementation	- Develop security policies and procedures - Compliance review (PCI DSS, GDPR, etc.) - Implement monitoring and incident response plans	**12 months**
Testing & Validation	- Test server performance and stability - Verify DNS propagation and website accessibility - Security testing and vulnerability assessment - Confirm backup and recovery functionality	**12 months**
Handover & Continuous Monitoring	- Deliver documentation and reports - Set up an ongoing monitoring interface - Provide recommendations for regular updates and future upgrades	**12 months/ Bi-weekly report delivery**

Deliverables

Server Maintenance Deliverables

- Server health and performance reports
- Resource optimization logs and configurations
- Security hardening documentation
- Backup and disaster recovery setup reports
- Monitoring dashboards for CPU, memory, storage, and login activity

Web Application Maintenance Deliverables

- Updated web application core, themes, and plugins
- Database optimization and performance tuning reports
- Security patching logs and vulnerability scan results
- Backup verification and restoration report

Cloudflare & DNS Deliverables

- DNS configuration and optimization report
- Cloudflare setup and performance monitoring report
- Traffic optimization and DDoS protection documentation
- Regular monitoring and anomaly detection logs

vCISO Services Deliverables

- Security policy and procedure documentation
- Risk assessment and mitigation plan
- Compliance audit report (e.g., PCI DSS, GDPR)
- Incident response plan and reporting framework
- Recommendations for future security improvements

Project Management & Reporting Deliverables

- Initial assessment and project plan
- Project timeline and milestone tracking
- Bii-weekly progress reports
- Final project report summarizing all activities, improvements, and recommendations

List of Tools to be Used for Server and DNS Maintenance

Server monitoring and optimization

- □ Libre/zabbix
- □ Htop for server monitoring and resource optimization.

Cloudflare and DNS Management.

- □ Cloudflare CDN
- □ Dashboard
- □ DDoS Protection and custom policy management.

Backup and Disaster Recovery

- □ Application and Database backup policy management to a different server (cloud/storage)

List of Tools to be Used for vCISO

- □ Wazuh - Security Information and Event Management (SIEM)
- □ OpenVAS / Nexpose / Nmap – Vulnerability scanning and assessment
- □ Metasploit / Burp Suite (Community)—Security testing and penetration verification
- □ Wazuh – Log management and threat detection
- □ CIS-CAT / Compliance Checking Tools – Regulatory compliance and audit preparation

Financial Proposal

SN	Particular	Qty	Rate	Amount
Server and DNS Maintenance				
1.	One-time server maintenance	1	0	0
2.	Regular server maintenance (per month)	1	0	0
3.	One-time web application maintenance	1	0	0
4.	Regular web application maintenance (per month)	1	0	0
vCISO Service				
5.	VAPT	1	0	0
6.	SIEM	1	0	0
VAT (15%)				0
TAX/AIT (10%)				0
Total =				0

(Note: Cloudflare Pro subscription (~20 USD/month) will be borne by the client.)

Total (including VAT & TAX/AIT) =	**0**
Taka in Words:	

Payment Terms & Conditions

a) Price: The quoted price is in Bangladeshi Taka (BDT), including VAT (15%) and TAX/AIT (10%).
b) Mode of Payment: 100% of the payment will be paid at the end of each month (within 7 working days after the invoice submission).
c) Offer Validity: The validity of this offer will be 30 days from the date of the issuance of the proposal.
d) Delivery: The delivery of work will be done according to the methodologies and deliverables mentioned in this proposal.

Conclusion

Through a structured approach encompassing server maintenance, web application optimization, DNS and Cloudflare management, and vCISO services, this project ensures that Vibe Gaming maintains a robust, secure, and high-performing e-commerce environment. By proactively monitoring performance, optimizing resources, and implementing comprehensive security measures, the platform is positioned to deliver a seamless user experience, protect sensitive customer data, and support future growth. This engagement not only addresses current operational needs but also establishes a foundation for continuous improvement and resilience against evolving technological and cybersecurity challenges.

Confidentiality

All information shared during this engagement will be treated as strictly confidential and handled in accordance with a mutually signed **Non-Disclosure Agreement (NDA)**.

Hridoy

Hridoy Mustofa
Founder and CEO
Email: hridoy@cyberlog.com.bd
Phone: +880 1864-291014
Website: https://cyberlog.com.bd