Lightup
Defence Solution

SECURITY ASSESSEMENT REPORT

Presented By:
Samuel U. George

Prepared For:
United Kingdom Atlantis (UKA)

Executive Summary

In this report, we present the results of the security assessment conducted on Crownbit.org and the Atlantean Crown (ATC) App.

The objective of this assessment is to identify security risks and provide recommendations to strengthen overall security. Security breaches have been reported, highlighting critical vulnerabilities that could further expose users and the platform to cyber threats.

Strengthening security measures is essential to prevent future incidents and enhance overall platform protection.

Key Findings Summary

This assessment highlights critical security weaknesses that could expose Crownbit.org and the Atlantean Crown (ATC) App to cyber threats. Below are the key findings and risk areas identified:

1. **Weak Authentication & Access Control**
   - MFA Not Enforced: Users and administrators can access accounts without Multi-Factor Authentication (MFA), increasing the risk of account takeovers.
   - Weak Password Policies: No strict password enforcement, making brute-force attacks easier.
2. **API Security Gaps**
   - Lack of API Authentication Controls: APIs do not enforce strong authentication, exposing sensitive data and transactions.
   - Missing Rate Limiting & Monitoring: APIs are vulnerable to brute-force and denial-of-service (DoS) attacks due to the absence of request throttling.
3. **Wallet & Transaction Security Risks**
   - Over-Reliance on Hot Wallets: A large portion of funds is stored in hot wallets, increasing exposure to hacks.
   - No Multi-Signature Authorization: High-value transactions do not require multiple approvals, increasing the risk of fraudulent withdrawals.
4. **Phishing & Social Engineering Risks**
   - No Anti-Phishing Alerts: Users receive no warnings about suspicious login attempts or phishing attempts.
   - Lack of User Awareness Training: Users are not educated on phishing scams and fake investment schemes.
5. **Compliance & Regulatory Risks**
   - Weak KYC/AML Implementation: The platform lacks automated fraud detection to monitor suspicious activity.
   - Insufficient Data Protection Measures: User data storage and encryption do not fully comply with GDPR and industry standards.

By addressing these vulnerabilities, Crownbit.org and the ATC App can strengthen their security framework, reduce risks, and improve compliance.

Security Recommendations

To enhance the security of Crownbit.org and the Atlantean Crown (ATC) App, the following critical measures should be implemented:

- Strengthen Authentication & Access Control – Enforce Multi-Factor Authentication (MFA), biometric authentication, and strong password policies while restricting admin access through Role-Based Access Control (RBAC).
- Improve API Security – Implement OAuth 2.0, enforce API key rotation, and apply rate limiting to prevent unauthorized access and brute-force attacks.
- Secure Wallets & Transactions – Store the majority of funds in air-gapped cold wallets, require multi-signature authorization, and implement AI-based fraud detection for real-time monitoring.
- Enhance Phishing & Social Engineering Defenses – Introduce anti-phishing alerts, conduct security awareness training, and add a “Report Suspicious Activity” feature for users.
- Strengthen Compliance & Regulatory Security – Improve KYC/AML verification, enforce GDPR-compliant data encryption, and conduct quarterly security audits.
- Improve Threat Monitoring & Detection – Deploy Intrusion Detection & Prevention Systems (IDS/IPS), implement 24/7 SOC monitoring, and perform regular penetration testing.

Implementing these security measures will reduce cyber risks, protect user funds, and ensure compliance with industry standards

Atlantean Crown (ATC) Wallet Security Best Practices

To ensure the security of ATC wallets and user funds, the following key measures should be implemented:

✓ Secure Wallet Storage – Store long-term holdings in cold wallets or air-gapped devices. Avoid keeping large amounts in online wallets or exchanges.
✓ Private Key & Seed Phrase Protection – Keep seed phrases offline in secure locations. Never share private keys.
✓ Strong Authentication & Access Control – Enforce Multi-Factor Authentication (MFA), use biometric security, and implement strong password policies.
✓ Device & Network Security – Use dedicated, updated devices for transactions, install endpoint security solutions, and avoid public Wi-Fi.
✓ Phishing & Social Engineering Protection – Manually enter wallet URLs, verify official sources, and double-check transaction addresses to prevent scams.
✓ Secure Transactions & Backup Strategy – Use multi-signature wallets, keep transaction limits, and maintain encrypted offline backups in secure locations.
✓ Threat Monitoring & Detection – Regularly audit wallet activity, revoke unnecessary permissions, and enable real-time alerts for suspicious transactions.

By implementing these best practices, the security of ATC wallets will be significantly strengthened, ensuring protection against cyber threats and unauthorized access.

Tracing Stolen Atlantean Crown (ATC) Assets

Introduction

As part of efforts to secure Atlantean Crown (ATC) assets in Nigeria, this report outlines a structured approach to tracking and recovering stolen funds. With the increasing adoption of ATC, cybercriminals may exploit vulnerabilities to move stolen assets. A forensic approach, combined with law enforcement collaboration, is crucial for effective recovery.

1. Identifying & Tracking Stolen Funds

Step 1: Gathering Transaction Data

- Identify the compromised wallet address and affected transactions.
- Use blockchain explorers (e.g., Etherscan, Blockchair) to trace fund movements.

Step 2: Blockchain Forensic Analysis

- Track stolen ATC across multiple wallets and possible laundering attempts.
- Identify links to known fraudulent addresses or mixing services.

Step 3: Monitoring Exchanges & Off-Ramps

- Check if stolen ATC has been deposited on Nigerian or international exchanges.
- Work with exchanges to freeze related accounts and obtain KYC details of suspected users.

2. Investigative & Legal Actions in Nigeria

Step 4: Reporting & Law Enforcement Engagement

- Report the incident to the Nigerian Financial Intelligence Unit (NFIU) and the Economic and Financial Crimes Commission (EFCC).
- Provide detailed blockchain evidence to law enforcement agencies for further action.

Step 5: Engaging Local & International Cybersecurity Firms

- Utilize blockchain forensic tools such as Chainalysis or TRM Labs for advanced tracking.
- Collaborate with financial crime units to analyze laundering patterns and off-chain movements.

Conclusion

preventive security measures must be continuously improved to stay ahead of evolving threats. The platform should implement ongoing security enhancements, compliance reviews, and regular penetration testing to maintain high security standards and user trust.