EQUITY MARKET REINVENTED
BUYING & SELLING SHARES SHOULD BE EASY

SECURITY WHITEPAPER

05/11/2017
v1.1

Table of Contents

1 Introduction

Over the past few years, many individuals and organizations have started to look to blockchain for services that are more democratic, transparent and efficient. At the same though, there have also been a number of high profile security vulnerabilities, hacks and scams that have negatively affected the reputation of the industry, and have the potential to adversely affect adoption rates. Chainium recognizes that blockchain companies can, and must, invest more in the people, processes and technology required to deliver secure solutions.

We realize that many "blockchain security" attacks have nothing to do with underlying blockchain technology at all. Many successful attacks have been the result of organizations failing to implement very basic security principles.

We are committed to getting the basics right. We see security as a basic fundamental requirement of our customers and a positive business differentiator, if done well. Recognizing this our founders embedded security as a core function within Chainium right from the very beginning.

This paper aims to give an overview of our security posture by looking at *our security culture, our security design and our security operations*. We are never complacent and we constantly look to evolve and develop as we learn more.

2 Our Security Culture

The primary defense in our security posture is our people. Chainium has worked hard to create an open, supportive and challenging security culture for all employees.

Our security culture was not created overnight and takes time and effort to maintain. We are constantly working on it by building security into our day-to-day processes and through positive reporting of security incidents and near misses.

Here are some of the key elements that help define our security culture.

2.1 Awareness

Chainium hosts regular internal workshops to raise awareness and drive innovation in security. One example would be our Threat Hunting Workshop, where staff (technical & non-technical) are put into mixed ability teams and given access to security monitoring data to learn how to look for suspicious activity. At other workshops, we have shared the results of company-wide security initiatives such as simulated email phishing attacks.

2.2 Business Processes

Preventing breaches also involves ensuring our business support processes are secure. For example, ensuring Human Resources inform IT quickly when staff leave or change roles, so accounts and access can be suspended. Our security team work hard with all of our business support functions to ensure security requirements are included in all of our operations.

2.3 Specialist Support

Whilst we would never outsource responsibility for our security we do recognize, as a relatively small company, we cannot have access to all of the specialist security disciplines we need in house. We use a number of third party security consultants, and managed services, to enhance the scale and depth of our internal security team. We also use external experts to provide independent review, audit and testing, as well as surge support, as defined in our security incident response plan. For these purposes, we only use third party organizations who are certified members of the CHECK and CREST schemes (schemes endorsed by the UK's National Cyber Security Centre, part of GCHQ).

2.4 Security Researchers

Chainium wants to build a close relationship with the security research community. We are committed to responding positively to researchers who make us aware of security vulnerabilities in a responsible and collaborative manner. We will publicly thank these individuals and list them as contributors to our platform. Whilst we are not currently in a position to pay bounties, we will consider this as we grow.

2.5 Continuous Learning

We are constantly learning and updating the security of our platform. We know attackers are innovative and well-resourced and, as such, we are never complacent. We actively encourage our staff to report security incidents and "near misses" so we can learn from them.

3 Our Security Design

Chainium has used the principles of “defense in depth”, to create a secure platform that meets our customers' expectations for confidentiality, integrity and availability.

The defense in depth approach ensures that multiple security controls are present at network, physical, personnel, logical and data layers so, should any one area fail, there are compensating controls to maintain security at all times.

3.1 Network

The key principle of our network is to allow only connections necessary to allow systems to operate, blocking all other ports, protocols and connections. Perimeter protection is achieved through firewalls at the network edge. Our ACLs are regularly reviewed and updated. We also use other devices such as IPS and WAF to enhance protection of certain access points.

Chainium networks are further subdivided internally and devices are placed at defined boundaries within the network. Additionally, by design, we operate full physical segregation between certain critical back end services, and other corporate services, like email and website.

As data is at risk when it travels across the Internet, we support strong encryption protocols such as TLS to secure the connections between customer devices and our platform and APIs.

3.2 Physical

The vast majority of our physical infrastructure is housed in fully managed data centers with some of the world’s most stringent physical security standards. We also operate our own physical office in Lichtenstein with a modest IT infrastructure, primarily used for development and testing. However we still treat physical security in our Lichtenstein office with just as much importance.

Our offices are designed with strong physical security controls including, manned reception, multi-zonal swipe and pin access control, intruder alarms systems, CCTV and security patrols. Within the office, our infrastructure is located in a dedicated access and climate controlled communications room, with individually locked racks.

We track the location and status of all equipment within our offices from acquisition to destruction via asset tags. When a hard drive is disposed of we will make use of a certified third party who physically destroy disks for us on site and provide us with a certificate of safe disposal.

Our crypto-currency will be stored in multiple offline cold storage wallets. The private keys are secured on our behalf by Bank Frick of Liechtenstein. The keys are held in a highly secure physical vault, requiring multiple signatories to gain access.

3.3 Personnel

As discussed previously we recognize that our people our often our first line of defense. As such, we take personnel security seriously. We use an independent third party to undertake financial, credit and criminal records checks on all staff before they start with us. We also verify candidate’s previous employment and take up third party references. All staff sign a formal contract that includes a schedule on their personal responsibilities for security and privacy.

Our staff are given security training, as part of our onboarding process, and they receive ongoing mandatory security training throughout their employment. Staff are required to sign our Acceptable Use Policy which clearly explains their personal responsibilities in regards to keeping customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required.

3.4 Logical

The key principle of our logical layer security is that users should have the least rights possible to perform their legitimate functions. In practice, this means we operate a strict Role Base Access Control (RBAC) to enforce the least rights model. Any deviation to RBAC policy must be requested, authorized and audited and will usually require additional controls such as time limits and enhanced monitoring.

We use the RBAC model for both off-chain and on-chain logical processes. This approach, which includes the Smart Contracts we have built within the Ethereum blockchain, ensures that risks associated with unnecessarily elevated rights and accumulation of rights across multiple accounts are minimized.

As a further technical control, we plan to use a commercial software package to manage administrator elevations, time limit sessions and record all administrator actions on our Linux and Windows estates.

All administrative accounts, including third party services such as Slack, Facebook and LinkedIn, use multi-factor authentication. We also enforce this policy for our staff due to their enhanced personal risk. Wherever possible we utilize a dedicated app, such as Google Authenticator, rather than SMS to minimize the risks associated with cell phone cloning.

3.5 Data

Chainium ensures that no personal customer information is ever held “on-chain”. This ensures that transaction data can be processed by a public blockchain infrastructure without the need for heavy security and monitoring overheads. To complement this, Chainium has its own “off-chain” structured and unstructured databases holding other personal and sensitive personal information for our customers. This off-chain data is protected through segregation, obfuscation, encryption and other techniques. A number of data and input validation techniques are used at trust boundaries to minimize the risk of malicious attacks.

We use full disk encryption wherever possible, to protect data at rest. We implement this ourselves for our own end points. In our cloud services, we pay additional fees for full disk encryption options.

3.6 Obfuscation

It does not make sense to publish your entire security position in detail, as clearly that might help a potential attacker. With this in mind our last layer of defense is that we have some additional security measures, which we do not describe in this paper.

4 Our Security Operations

Our security team is responsible for the overall management of our security risks. The team follows a process that includes security design requirements, analysis of attack surfaces, and threat modeling. They run this process from Dev-Ops through the entire lifecycle. The team measures the effectiveness of these mitigations and reports this to the board regularly.

This section discusses some of the key security operations we undertake at Chainium.

4.1 Basic Security Hygiene

Chainium runs all the basic IT security hygiene techniques you would expect of any responsible financial services company. This includes, but is not limited to, URL blacklisting, email filtering and multiple anti-virus / malware engines on hosts and servers. Servers and core applications are built following industry standard hardening guidance. End points are built to a standard hardened image, local administrator rights are not provided and removable media drives are access limited.

4.2 Patching

Operating System and application updates, hotfixes, and patches are applied following a rigorous change management process. Security patches are prioritized and we implement within the time frame specified by the issuer.

4.3 DDOS

Chainium deliberately uses different cloud service providers for different elements of our corporate estate. We have commercial agreements in place for DDOS protection for our critical Internet facing services. For some critical services, we may use multiple DDOS protection solutions.

4.4 Vulnerability Scanning

Chainium runs a vulnerability management process that actively scans for security threats using commercially available tools, manual threat hunting and independent penetration tests. The security team is responsible for tracking and following up on all vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner.

4.5 Security Monitoring

Our in-house security team will be supported by a 24/7 protective monitoring and prevention service as we scale. This service aggregates disparate log data from servers, end point security software and network devices and parses them into a single Security Incident & Event Management (SIEM) tool. Correlation rules, based on our threat modeling use cases, are run across the data to look for suspicious behavior. The outputs are monitored for us 24/7 in near real time.

The security monitoring service will provide us with security incident alerting within defined SLAs, notification within 10 minutes for priority 1 events, as well as service availability SLAs for our key security appliances.

4.6 Advanced Behavioral Analytics

In addition to the SIEM monitoring, we also plan further investment in cutting-edge automated behavioral analytic tools that use unstructured machine learning to baseline, and then identify abnormal and suspicious user behavior. This tool set will complement, rather than replace, our traditional security monitoring tools.

4.7 Intelligence Sharing

We subscribe to a number of open source and commercial threat intelligence feeds which we actively integrate with our monitoring tools to ensure we are always running the latest signatures. The security team also takes part in intelligence sharing forums to help protect the wider community. We never share customer information in these forums.

4.8 Data Loss Prevention

Although malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. To mitigate this risk, we will run DLP software that identifies, monitors, and protects sensitive data. For example, DLP proactively identifies sensitive information in an email message, such as social security or credit card numbers.

4.9 Incident management

We recognize that, despite all our efforts, eventually we will have a security incident. With this in mind, we have developed a rigorous incident management process that should minimize the impact of incidents when they occur. Testing of incident response plans is performed at least annually. To help ensure the swift resolution of security incidents, our security team is on call 24/7. If an incident involves customer data, we are committed to informing the customer as soon as possible.

4.10 Third-party suppliers

Chainium relies on a number of trusted third parties to allow us to provide our services. We recognize that this presents a significant attack surface and, as such, we manage our suppliers extremely carefully. Prior to using any third-party suppliers, we will conduct an assessment of the security and privacy practices of third-party suppliers, to ensure they provide a level of security and privacy that is at least as good as our own. We carefully pre-agree the level of logical and data access required and ensure appropriate technical controls are in place to enforce this. We also ensure that suppliers, have appropriate security, confidentiality, and privacy contract terms, and we regularly audit to ensure these are satisfied.

4.11 Audit

Chainium is committed to undertaking the following independent audits;

- ISO/IEC 27001(2013) by UKAS accredited auditor
- Regular Penetration Tests by CHECK approved company

We will track and monitor any audit findings and ensure they are prioritized and given owners.

5 Summary

Chainium will not succeed unless we have our customers' trust that we have done everything possible to ensure the confidentiality, integrity and availability of their data.

Our founders recognized, right from the start, how important security would be to Chainium. We have worked hard to learn lessons from other high profile blockchain security incidents. We recognize that security, particularly in the blockchain industry, is a constantly developing field as attackers change and evolve their tradecraft. We also realize that a significant proportion of attacks can be mitigated by simply getting the basics right.

We have invested already, in the people and processes required to create a mature security posture, and plan significant further investment particularly in technology. We are not complacent and realize that a serious attack is inevitable at some point, and we have planned accordingly.

We are committed to meeting our customers' high security expectations as *Chainium*.