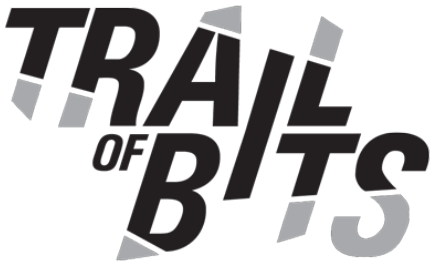


Voatz

Security Assessment

Volume II of II: Threat Modeling Findings

March 12, 2020

Prepared For:

Bradley Tusk | *Tusk Philanthropies*
btusk@tuskholdings.com

Nimit Sawhney | *Voatz*
ns@voatz.com

Aileen Kim | *Tusk Philanthropies*
akim@tuskstrategies.com

Sheila Nix | *Tusk Philanthropies*
sheila@tuskholdings.com

Prepared By:

Stefan Edwards | *Trail of Bits*
stefan.edwards@trailofbits.com

Brian Glas | *Trail of Bits*
brian.glas@trailofbits.com

Introduction

From January 28, 2020 to February 14, 2020 Trail of Bits (“the assessment team”) also undertook a threat model of the Voatz system to help Voatz (herein referred to as “the client” or “the implementation team”) understand wider design concerns within the system. The assessment included 20 identified components across five trust zones, and resulted in a total of 31 findings, ranging in severity from High to Informational.

The client identified several policy and control frameworks that were in use. Listed frameworks include NIST 800-53 (“Security and Privacy Controls for Federal Information Systems and Organizations”), ISO 27001 (“Information technology—Security Techniques - Information Security Management Systems—Requirements”), and the NIST Cybersecurity Framework (CSF). This document mainly uses NIST 800-53 controls, with the addition of two control families. Sections of this document that deviate from NIST 800-53 are marked, and controls from other policy frameworks, specifically ISO 27001:2013, are noted.

Voatz is a complex system with many connections and components. The discovery phase of the assessment identified 20 components across multiple cloud providers, trust zones, and security levels. Additionally, the system used a second cloud site that was not at parity with the primary site, so controls across the system depend on the location in question. The following components were reviewed by the assessment team:

- Core Servers
- HyperLedger Fabric
- Audit Application
- Admin Portal
- Apache WS
- MongoDB
- MySQL DB
- Centralized Logging Solution
- Cloud C
- Application Load Balancer
- WAF
- KMS
- Cloud Storage Service
- File Hosting Provider
- DBaaS
- Mobile Integrity Provider
- Email Provider

- SMS Provider
- Geo IP Provider
- Identity Verification Provider

The assessment team believes that additional components, connections, and risks lurk in the Voatz system, as it is highly convoluted, manual, and under-documented as a whole. However, we believe that this threat model accurately reflects the risks identified in the system as discussed with the implementation team. The remainder of this report is split into three sections:

1. This introduction, including Key Findings and the Report Position
2. Descriptions of components and their connections, and an analysis of them
3. Specific security findings by area

Key Findings

Voatz allows the general public to vote via mobile device in an election. In this role, Voatz allows voters who would otherwise use the absentee ballot or vote by mail systems to install a mobile app to perform these actions. However, we noted a number of weaknesses in the design of the Voatz system which we have grouped into six key areas:

1. Governance and Compliance
2. Internal Processes
3. Voting Processes
4. External Storage
5. Infrastructure and Administration
6. Mobile Application

Governance and compliance are commonly overlooked areas of many system designs. These areas generally lead to regulatory or legal risk, and are often missed when first designing an application. In the case of Voatz, standard adherence was *ad hoc*, with minimal rigor applied to the control families and requirements of these standards.

In general, we recommend overhauling standards compliance, and iterating over the chosen frameworks. If NIST 800-53 and CSF are used as a baseline, evaluate the system criteria via FIPS 200 and FIPS-199, then document and apply all controls required by your Security Categorization (SC). Use other relevant NIST 800 series documents, such as NIST 800-61, to ensure that your implementations are robust and well documented. If ISO 27001:2013 compliance is desired, ensure that you follow all controls required by Annex A, and maintain strong documentation as to the location, description, and status of all controls, even if they are not currently implemented.

Internal Processes are also easily overlooked when initially creating a system, but it's quickly evident they do not scale in a production setting. In terms of Voatz, these processes primarily impacted the Incident Response (IR) and Business Continuity and Disaster Recovery (BC/DR, covered by various NIST 800-53 control families) areas of the system.

In general, we recommend moving away from manual IR and hunt processes to more automated and robust solutions. This should include alerting out of Centralized Logging Solution when certain conditions are met; having baseline monitoring across the enterprise; and having robust tools, techniques, tactics and procedures (TTTPs) extracted from hunt processes and automated into an alert. By moving away from manual IR, hunt, and BC/DR processes, the implementation team can have a more robust view into the state of the Voatz system, and understand when failovers or incident response procedures must be enacted.

Voting Processes covers the verification of voter identity and the handling of ballots. In general, Voatz's voting processes are error prone and manual, relying on manual verification of voter identity and long-term storage of this identity on Voatz's premises. Wherever possible, we recommend moving away from manual processes (including re-digitizing ballots) in favor of processes that remove humans from the loop. Additionally, we recommend moving away from long-term storage of voter identity documents in a system accessible to Voatz administrators, in favor of a system that allows auditors to review such documents but does not allow Voatz staff to see the credentials once verified.

External Storage concerns areas of the system that access and store data in external providers. Within Voatz, these locations are myriad, and a number of external systems have wide access to voting data. While this may be acceptable to Voatz , since the voter must acknowledge that Voatz is not an anonymous voting system before casting a ballot, any application of Voatz that does require anonymity (including future applications of voting) cannot use these systems in the same way. We recommend moving away from the large number of external storage locations in favor of fewer, easily audited, Voatz-controlled locations.

Infrastructure & Administration encompasses the infrastructural components and procedures that make up the system. Here again, Voatz is generally a manual system, with bespoke instances of many standard components. For example, there are no automated processes for deploying Apache Web Server or Voatz Core Server instances; instead, the implementation team must manually deploy cloud server instances, then access these instances via secure shell (SSH) to further deploy the required subcomponents.

We recommend automated deployments, either via custom images that hold the required software components, or through some auditable instance definition language, such as Terraform. In either case, instances should be made immutable, with no required administrator access, and minimal room for operator error or attacker access.

Finally, the **Mobile Application** includes a system of cryptographic controls surrounding the generation of keys and the signing of data. However, this system was not configured with a trusted root, meaning that mobile devices effectively trust whatever key is produced via secured (e.g. TLS) channels. A technical finding was added in a similar vein in the Technical Report Volume I (TOB-VOATZ-033: Voatz API server lacks OCSP stapling). Here, we recommend adding key pinning to the cryptographic layer beneath channel security. This will ensure that the mobile application need not trust any components except the Voatz Core Server, and that the implementation team will be alerted should that key ever change.

Report Position

Voatz is a large, intricate system, with many security controls and design choices that arose from organic decisions that made sense during product development. This report attempts to catalog many of the discussions captured within the threat modeling meeting processes.

The remainder of this report analyzes components, trust zones, data flows, threat actors, controls, and findings of the Voatz threat model. This was a point-in-time assessment, and reflects the state of Voatz at the time of the assessment, rather than any current or future state.

Methodology

This document is the result of four person-weeks of effort from both the assessment and implementation teams. It is a control-focused threat model, with each discovered component reviewed against the control frameworks mentioned by the implementation team and refined in finding TOB-VOAT-TM01: Missing Security Categorization as per FIPS-199/200.

Performing a threat model and architecture review on a system as complex as Voatz is fraught with challenges. First, we held a series of meetings between the assessment and implementation teams to discover as many components as possible. Next, we attempted to uncover the processes and controls that were designed in place to document the current system state and potential future recommendations. Lastly, we discussed a number of threat scenarios, with the actors specified below in Threat Actors.

Components

The following components were in scope for the threat modeling discussions:

Component Name	Description
Core API Servers	Voatz Core Server (VCS) API hosts, which are composed of a Scala application using the Akka and Play! frameworks
HyperLedger Fabric	Open source blockchain, used to store ballots
Audit Application	Bespoke application to facilitate election audits
Admin Portal	Administrative portal for election management
Apache WS	Apache Web Servers (x4), used as front ends to components such as VCS
MongoDB	Mongo database primarily for write operations
MySQL DB	MySQL database primarily for read operations
Centralized Logging Solution	Log aggregation and reporting tool, used as a centralized logging point for the Voatz system as a whole
Cloud C	Cloud CDN, routing, and security provider
Cloud A ALB	Cloud A application load balancer
WAF	Web application firewall
KMS	Key management system
Cloud Storage Service	Cloud Storage Service storage
File Hosting Provider	Internet file hosting service
DBaaS	A real-time database as a service (DBaaS) platform hosted in a large Cloud Provider's Platform
Mobile Integrity Provider	Mobile device integrity defense software
Email Provider	Email provider used for external communications with voters and officials

SMS Provider	SMS provider used for external communications with voters and officials
Geo IP Provider	GeoIP data provider used for geo-locating IP addresses for threat-hunting and banning purposes
Identity Verification Provider	Identity verification provider used for verifying identification documents such as drivers' licenses

Trust Zones

Components are situated within trust zones: logical boundaries made up of components that have similar or related sensitivity. We identified the following trust zones:

Trust Zone Name	Description	Included Components
Internet	The wider internet zones	Cloud C ALB WAF Cloud Storage Service File Hosting Provider DBaaS Mobile Integrity Provider Email Provider SMS Provider Geo IP Provider Identity Verification Provider
Voatz Corp	Internal Voatz corporate network	Centralized Logging Solution Administrative machines
Cloud A	Cloud network	Voatz Core Servers Audit application Admin portal HyperLedger MongoDB MySQL DB KMS
Cloud B	Cloud network	Voatz Core Servers Audit application Admin portal HyperLedger MongoDB MySQL DB KMS
DMZ	Apache web servers in a “DMZ”	At least four Apache web servers

Trust Zone Connections

Trust zones become useful when data that flows between zones is understood.

Originating Zone	Destination Zone	Data Description	Connection Type	Authentication Type
Internet	DMZ	All voting data, registration, voter PII, auditing, and the like	Certificate-pinned TLS	Potentially unauthenticated during registration, authenticated thereafter
DMZ	Cloud A	All voting data, registration, voter PII, and the like	TLS	Client-side certificates for TLS, IP filtering
DMZ	Cloud B	All voting data, registration, voter PII, and the like	TLS	Client-side certificates for TLS
Voatz Corp	Cloud A	Systems administration	VPN, TLS, SSH	Keyed authentication
Voatz Corp	Cloud B	Systems administration	VPN, TLS, SSH	Keyed authentication
Cloud A	Internet	All voting data, registration, voter PII, auditing, and the like to external processors such as Identity Verification Provider	TLS	Authentication token
Cloud B	Internet	All voting data, registration, voter PII, auditing, and the like to external processors such as Identity Verification Provider	TLS	Authentication token
Cloud A	Voatz Corp	Logging telemetry data	syslog	IP filtering

Threat Actors

Similar to establishing trust zones, defining malicious actors ahead of time is useful in determining which protections, if any, are necessary to mitigate or remediate a vulnerability. We use these actors in all subsequent findings from the threat model. Additionally, we define other "users" of the system who may be impacted by or enticed to undertake an attack.

For example, in a confused deputy attack such as Cross-Site Request Forgery, a normal user is both the victim and the potential direct attacker, even though a secondary attacker entices the user to undertake the action.

Actor	Description
Malicious Internal User	A user, such as an administrator or developer, who uses their privileged position or stolen credentials maliciously against the system.
Internal Attacker	An attacker who transits one or more trust boundaries, i.e., an attacker with container access.
External Attacker	An attacker who is external to the system and is unauthenticated.
Administrator	An actual administrator of the system, tasked with operating and maintaining the cluster as a whole.
Developer	An application developer who deploys an application to a cluster, either directly or via another user (such as an administrator).
End User	An external user of an application hosted by a cluster.

Threat Actor Paths

Defining attackers' paths through the various zones is useful when analyzing potential controls, remediations, and mitigations within the current architecture:

Actor	Originating Zone	Destination Zone	Description
Malicious Internal User	Voatz Corp	Cloud A, Cloud B	An administrator, or an attacker with stolen valid administration credentials , could access a wide range of infrastructure hosted within Cloud A or Cloud B to impact the confidentiality, integrity, and availability (CIA) of voters' data. Furthermore, this traffic would look perfectly normal since the access pattern is within the bounds of normal Voatz Administration access.
	DMZ	Cloud A, Cloud B	An administrator, or an attacker with stolen valid administration credentials, could access a wide-range of infrastructure hosted within Cloud A or Cloud B to impact the confidentiality, integrity, and availability (CIA) of voters' data. This traffic would look abnormal to normal access patterns since administrators do not normally access machines from outside the Voatz Corporate network. However, there is minimal anomaly detection that would notice this situation and alert incident responders. Additionally, if an attacker were to use normal access channels, netflow information would be insufficient to capture this anomaly.
	Voatz Corp, Cloud A, Cloud B	Internet	An administrator, or an attacker with stolen valid administration credentials, could access all downstream, internet-accessible applications, such as Identity Verification Provider, SMS Provider, or the like, and masquerade

			as the Voatz application. Additionally, due to missing key-pinning, a sufficiently advanced attacker could generate a voting encryption key that would be controlled by the attacker and unavailable to the Voatz Core Server. This would be accepted by the Voatz mobile application.
Internal Attacker	DMZ	Cloud A, Cloud B	An internal attacker could access a wide range of infrastructure hosted within Cloud A or Cloud B to impact the confidentiality, integrity, and availability (CIA) of voters' data. This traffic would look abnormal to normal access patterns since administrators do not normally access machines from outside the Voatz Corporate network. However, there is minimal anomaly detection that would notice this situation and alert incident responders. Additionally, if an attacker were to use normal access channels, netflow information would be insufficient to capture this anomaly.
	Cloud A, Cloud B	Internet	An internal attacker could access all downstream, internet-accessible applications, such as Identity Verification Provider, SMS Provider, or the like, and masquerade as the Voatz application.
External Attacker	Internet	DMZ, Cloud A, Cloud B	An external aAttacker could transit external trust boundaries and gain deeper access to the Voatz system. An additional attack could deny access to Voatz infrastructure, either via volumetric denial of service or items such as credential stuffing.

Security Control Analysis

The Committee on National Security Systems (CNSSI) 4009 defines "security controls" as the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Controls are grouped by a type or *family*, which collects controls along logical groupings such as authentication or cryptography. Our assessment focused on the following control families primarily from NIST 800-53r4, supplemented with a few additional categories:

Code	Control Family	Description
AC	Access Control	Authorization, session management, separation of duties, and related controls
AU	Audit and Accountability	Logging, non-repudiation, monitoring, analysis, reporting, and related controls
AT	Awareness and Training	Policy, procedures, and related capabilities
CA	Security Assessment and Authorization	Assessments, penetration testing, authorization to deploy, and related controls
CM	Configuration Management	Inventory, secure baselines, configuration management, change control, and related controls
CP	Contingency Planning	Disaster recovery, continuity, backups, testing, and related controls
CY	Cryptography	The cryptographic controls implemented at rest, in transit, and in process
DS	Denial of Service	The controls to defend against different types of denial-of-service attacks impacting availability
IA	Identification and Authentication	User and system identification and authentication controls
IR	Incident Response	Policy, process, handling, reporting, and related controls
MA	Maintenance	Preventative and predictive maintenance, and related controls

MP	Media Protection	Identification, storage, sanitization, and removal
PS	Personnel Security	HR Processes, screening, and related controls
PE	Physical and Environmental Protection	Controls to protect work sites and related assets
PL	Planning	Security architecture, policy, procedures, management, and related controls
PM	Program Management	Managing elements of security program controls
RA	Risk Assessment	Security categorization and overall risk assessment of the organization
SC	System and Communications Protection	Network level controls to protect data
SI	System and Information Integrity	Software integrity, malicious code protection, monitoring, information handling, and related controls
SA	System and Services Acquisition	Development lifecycle, documentation, supply chain, and related controls

Our review assessed the controls along the following criteria:

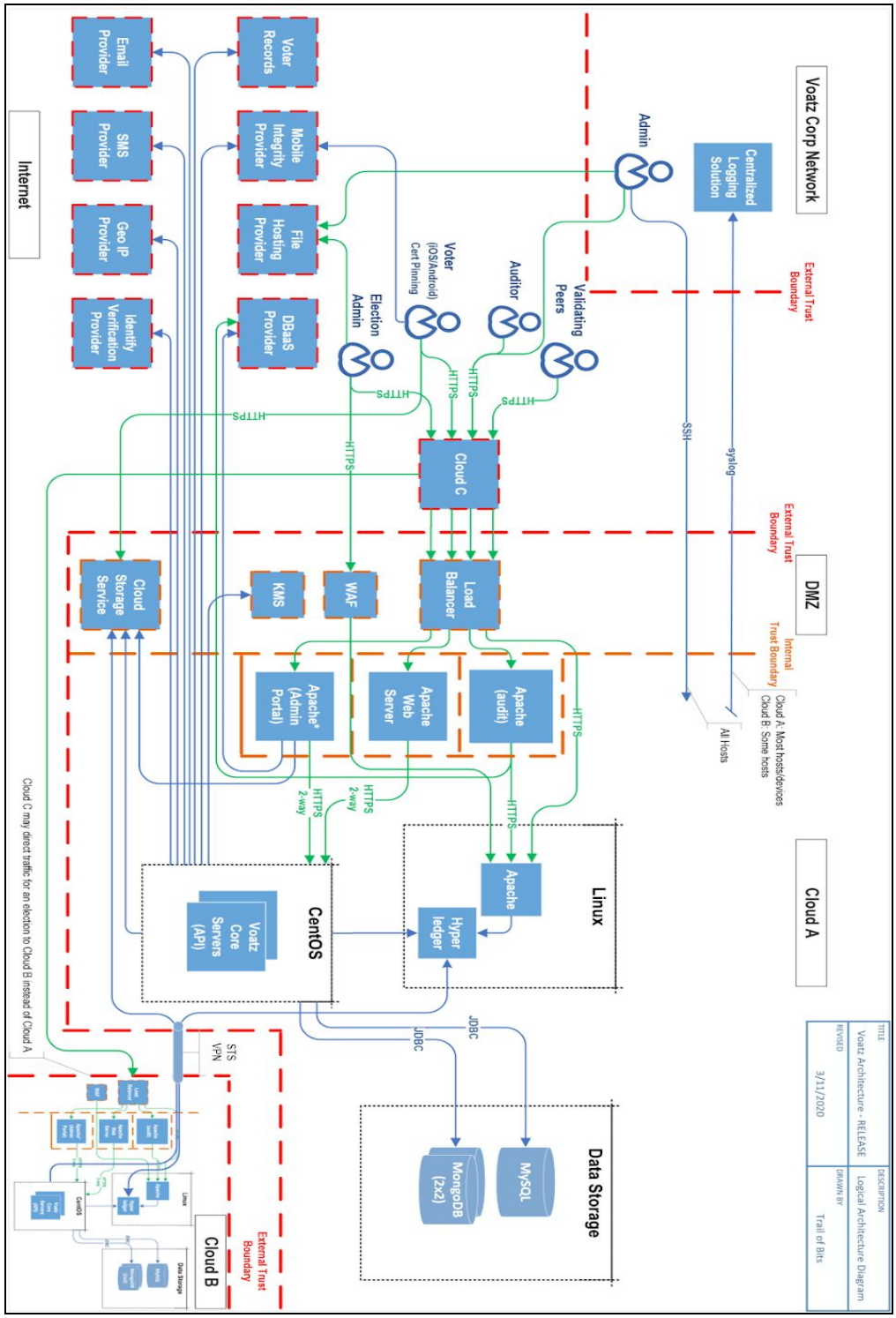
Strength	Description
Strong	Controls were well implemented, centrally located, not bypassable, and robustly designed
Good	Controls were well implemented, but may be weakened by vulnerabilities or are diffuse in location
Acceptable	Controls were implemented to the baseline industry standards and guidelines, but could be strengthened
Weak	Controls were either partly unimplemented, applied, or contained flCloud A in their design or location
Missing	An entire family of control was missing from a component
Not Applicable	This control family is not needed for protecting the component

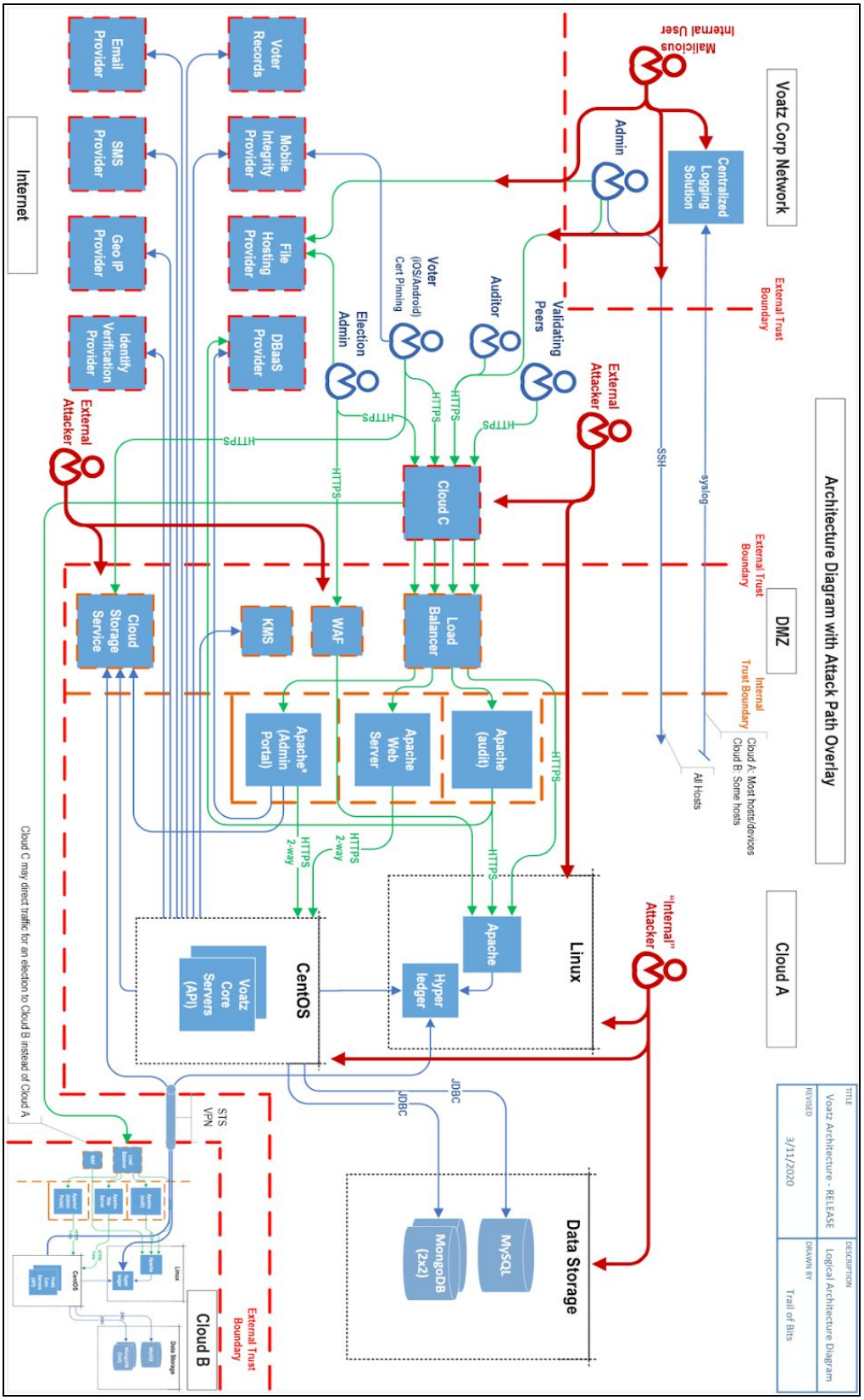
Resulting in the following control analysis table:

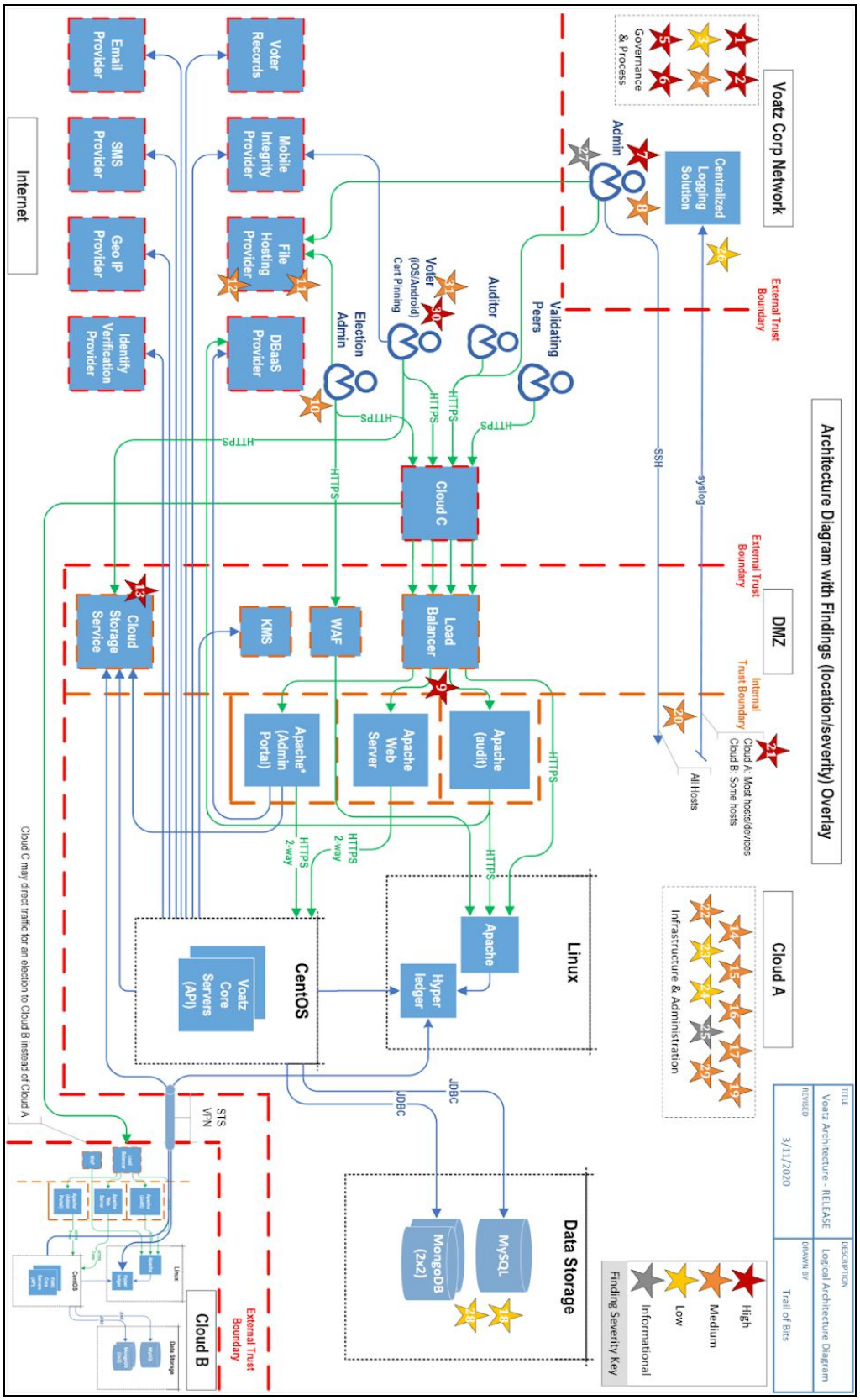
Control Family	Strength	Description
Access Control (AC)	**Good**	The systems generally used strong access control mechanisms in central locations with overlapping enforcement. However, the mobile application access control was marred by areas that appeared to allow cross-user access control violations.
Audit and Accountability (AU)	**Missing**	The audit logging capabilities are lacking the ability to track commands issued by administrators, or provide a detailed audit trail within a cloud infrastructure, and there are gaps in the auditability of ballot- and receipt-handling.
Awareness and Training (AT)	**Missing**	The implementation team had minimal training or documentation to support awareness around security, specifically for role-based awareness training.
Security Assessment and Authorization (CA)	**Missing**	The implementation team did have minimal documentation surrounding an assessment process. However, these did not include continuous monitoring, documented procedures, documented connections, and so on.
Configuration Management (CM)	**Missing**	The system was manually configured via run books, but did not have baseline configurations, security impact analyses, or other required CM controls.
Contingency Planning (CP)	**Missing**	The implementation team had minimal plans for disaster recovery and business continuity, but these were nascent and manually focused.
Cryptography (CY)	**Acceptable**	The system used modern, vetted, and FIPS/NIST-approved cryptographic modes. However, weaknesses were noted in the key pinning process, such that a mobile client cannot validate that the key provided was actually the one expected.
Denial of Service (DS)	**Acceptable**	The system used robust denial-of-service controls in the form of external providers such as Cloud C and Cloud A. However, the application itself had what appeared to be potential locations where denial-of-service attacks could occur.
Identification and Authentication (IA)	**Good**	The system included robust controls for identification and authentication.

Incident Response (IR)	**Missing**	The implementation team did not have the minimal set of incident response controls implemented. Specifically, the team had minimal insight into normal operations of the system, and any IR actions were bespoke and artisanal.
Maintenance (MA)	**Missing**	The implementation team did not have maintenance plans or even downtime for the system. For example, it was noted during the assessment that keys were aspirationally rotated, with no actionable plan for maintenance or downtime.
Media Protection (MP)	**Not Applicable**	Not applicable for this scenario
Personnel Security (PS)	**Not Applicable**	Not applicable for this scenario.
Physical and Environmental Protection (PE)	**Not Applicable**	Not assessed for this scenario.
Planning (PL)	**Missing**	The system did not include plans for component interconnections, design intent, and the like.
Program Management (PM)	**Not Applicable**	Not assessed for this scenario.
Risk Assessment (RA)	**Missing**	The implementation team did not have a codified risk assessment process.
System and Communications Protection (SC)	**Acceptable**	The implementation team used strong, centrally managed TLS with certificate pinning in order to secure communications. However, the system used one wild-card certificate for all systems within the Voatz infrastructure, meaning that an attacker with access to one certificate could have complete access to all non-forwardly secret TLS communications.
System and Information Integrity (SI)	**Weak**	The system had minimal and diffuse controls surrounding the integrity of information stored therein. Notably, procedures, alerting, monitoring, and non-persistence were missing.
System and Services Acquisition (SA)	**Acceptable**	The implementation team acquired systems and services from reputable third parties, mainly Cloud C, Cloud A, and Cloud B.

Dataflow Diagrams




Architecture Diagram with Attack Path Overlay
Internet
Voatz Corp Network
DMZ
Cloud A
Cloud B
Malicious Internal User
Admin
Centralized Logging Solution
Auditor
Validating Peers
Voter (iOS/Android) Cert Pinning
Election Admin
External Attacker
External Attacker
"Internal" Attacker
External Trust Boundary
External Trust Boundary
Internal Trust Boundary
Cloud A: Most hosts/devices
Cloud B: Some hosts
All Hosts
SSH
syslog
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS
HTTPS 2-way
HTTPS 2-way
JDBC
JDBC
Email Provider
SMS Provider
Geo IP Provider
Identify Verification Provider
Voter Records
Mobile Integrity Provider
File Hosting Provider
DBaaS Provider
Cloud C
Cloud Storage Service
KMS
WAF
Load Balancer
Apache* (Admin Portal)
Apache Web Server
Apache (audit)
Apache
Hyper ledger
Voatz Core Servers (API)
CentOS
Linux
Data Storage
MongoDB (2x2)
MySQL
Cloud C may direct traffic for an election to Cloud B instead of Cloud A
STS
VPN
TITLE
Voatz Architecture - RELEASE
REVISED
3/11/2020
DESCRIPTION
Logical Architecture Diagram
DRAWN BY
Trail of Bits


Architecture Diagram with Findings (location/severity) Overlay
Voatz Corp Network
Governance & Process
Admin
Centralized Logging Solution
External Trust Boundary
Voter (iOS/Android) Cert Pinning
Auditor
Validating Peers
Election Admin
DMZ
Internal Trust Boundary
Cloud A: Most hosts/devices
Cloud B: Some hosts
All Hosts
Cloud A
Infrastructure & Administration
Internet
Email Provider
SMS Provider
Geo IP Provider
Identity Verification Provider
Voter Records
Mobile Integrity Provider
File Hosting Provider
DBaaS Provider
Cloud C
Cloud Storage Service
KMS
WAF
Load Balancer
Apache (audit)
Apache Web Server
Apache* (Admin Portal)
HTTPS
HTTPS 2-way
SSH
syslog
Linux
Apache
Hyper ledger
CentOS
Voatz Core Servers (API)
JDBC
Data Storage
MySQL
MongoDB (2x2)
Cloud C may direct traffic for an election to Cloud B instead of Cloud A
STS
VPN
Cloud B
External Trust Boundary
TITLE
Voatz Architecture - RELEASE
REVISED
3/11/2020
DESCRIPTION
Logical Architecture Diagram
DRAWN BY
Trail of Bits
High
Medium
Low
Informational
Finding Severity Key

Findings Summary

Our discussion with the development team identified **31** issues, ranging in severity from High to Informational. Further investigation should be made to review other potential missing or weak security controls. Notably, the IR, RA, AU, and CM control families must be further reviewed, especially as they manifest in governance & compliance and internal processes.

All findings were rated by two metrics:

- Severity, meaning “how bad” the finding was in an uncategorized fashion.
- Difficulty, meaning “how hard” is the finding to remediate by the organization.

Once the implementation team has accepted these findings, they should appropriately recategorize the findings with their chosen risk assessment and management framework, as per finding TOB-VOATZ-TM06: Risk management is lacking.

#	Title	Type	Severity
1	Missing security category (SC) as per FIPS-199/200	Governance & Compliance	High
2	Missing data classification	Governance & Compliance	High
3	Policies do not follow NIST 800-61/800-34	Governance & Compliance	Low
4	Missing and incomplete documentation	Governance & Compliance	Medium
5	Incident response is not automated and is under-documented	Internal Processes	High
6	Risk management is lacking	Internal Processes	High
7	Voter identity verification is manual with minimal training support	Voting Processes	High

8	Internal team has full access to voter PII	Voting Processes	Medium
9	Voters or admins could be blacklisted in denial-of-service attacks	Voting Processes	High
10	Receipt- and ballot-handling processes increase risk of mishandling	Voting Processes	Medium
11	Voting receipts and ballots are in shared File Hosting Provider folders	External Storage	Medium
12	Manual process to purge voter data from shared File Hosting Provider folders	External Storage	Medium
13	Single Cloud Storage Service storage is used for multiple elections and jurisdictions	External Storage	High
14	Cloud deployments are not aligned in maturity or capability	Infrastructure & Administration	Medium
15	Infrastructure and application deployments are manual	Infrastructure & Administration	Medium
16	Missing host verification process	Infrastructure & Administration	Medium
17	Lack of defined process to remove or refresh infrastructure	Infrastructure & Administration	Medium
18	Self-hosted MySQL & MongoDB instances	Infrastructure & Administration	Low
19	Mutable infrastructure with minimal security monitoring	Infrastructure & Administration	Medium
20	Virtual Private Cloud (VPC) peering is too permissive	Infrastructure & Administration	Medium
21	Administrator commands are not logged	Infrastructure & Administration	High

22	Window for log retention is too short due to costs	Infrastructure & Administration	Medium
23	Administrator login activity recorded in Cloud Logging Service, without alerting	Infrastructure & Administration	Low
24	Missing alerts for actions related to Cloud Block Storage volume administration	Infrastructure & Administration	Low
25	Missing Cloud A Audit for email use across service accounts	Infrastructure & Administration	Informational
26	Centralized Logging Solution is sent via syslog, potentially exposing information	Infrastructure & Administration	Low
27	Two-person rule/no-lone zone is not implemented	Infrastructure & Administration	Informational
28	Missing key rotation policy for MySQL/MongoDB	Infrastructure & Administration	Low
29	Infrastructure hosted outside the US	Infrastructure & Administration	Medium
30	Lacking a pool of pre-generated keys or multiple certs pinned	Mobile Application	High
31	Use of a custom crypto layer below TLS without pinning	Mobile Application	Medium

Governance & Compliance

TM1. Missing Security Category (SC) as per FIPS-199/200

Severity: High
Type: CM
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM01

Description
The Voatz team noted that they used NIST 800-53 and the NIST Cybersecurity Framework (CSF) as the basis of security controls for Voatz systems. However, the Voatz team had not picked a Security Category (SC) as noted in NIST 800-53, page IV. This directive states that organizations must first select Security Category via FIPS-199 and then derive a system impact level from FIPS-200. They may then use this value to determine the baseline set of controls from NIST 800-53. While CSF provides baseline controls, the most effective use of NIST 800-53 requires the selection of an SC.

Justification
The severity is High for the following reasons:

- NIST 800-53 defines an excellent set of controls for many security applications.
- Understanding when, where, and which controls to apply requires having an understanding of the risk profile of the system.
- Controls may be missing, or needlessly added, without the correct understanding of a SC.

The difficulty is Low for the following reasons:

- Ready-made guidance is available to developers.
- Selection criteria is simple and easily made.

Recommendation
We calculated a SC of Moderate for the Voatz application, due to the following guidance in FIPS-199:

The *potential impact* is **MODERATE** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

References

- List of relevant NIST 800-53 security controls for a Moderate evaluation
- NIST 800-53 Rev 4 (see page VI)
- FIPS-200: Minimum Security Requirements for Federal Information and Information Systems
- FIPS-199: Standards for Security Categorization of Federal Information and Information Systems

TM2. Missing Data Classification

Severity: High
Type: CM-4,CM-8, RA-2
Component(s): All

Difficulty: High
Finding ID: TOB-VOATZ-TM02

Description
The implementation team mentioned that ISO27001 and NIST 800-53 were control frameworks in use during the development of Voatz. However, neither an ISO27001 nor a NIST 800-53/800-60 style data classification system were available during the assessment.

Understanding data classification and where that data is accessible is important under either control family. For ISO27001, this is required by the ISO 27001:2013 A.8.2 series of controls; within NIST 800-53, controls such as CM-4, CM-8, and RA-2 apply.

This allows developers, implementers, and responders to know how to handle information processed by individual components within the system, and to know what controls, if any, are required for the normal operation of a specific component.

Justification
The severity is High for the following reasons:

- Implementers currently have decreased visibility into sensitive data flows within the system.
- Data classification and system catalogs are required by both control frameworks identified by the implementation team.

The difficulty is High for the following reasons:

- Implementers must review the entire system to understand the types of data accessible at each system boundary.
- Implementers must further review the accessible data to ensure that the system should have access to the data and that this data is applicable to the component's function.

Recommendation
Audit all data processed within the system, and apply a data classification label to that data. Then, catalog all components within the system, and apply the correct security controls based upon the most-sensitive data that the component processes. This will ensure that data is never "downgraded" by being passed in aggregate with data of lower risk to the system.

References

- NIST 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories
- ISO27001 Annex A.8.2: Data Classification

- NIST 800-53 CM-4: Security Impact Analysis
- NIST 800-53 CM-8: Information System Component Inventory
- NIST 800-53 RA-2: Security Categorization

TM3. Policies do not follow NIST 800-61/800-34

Severity: Low
Type: CP-9, IR-4
Component(s): All

Difficulty: High
Finding ID: TOB-VOATZ-TM03

Description
The Voatz system included a partial disaster recovery process, however, it was not based on NIST 800-61 ("Computer Security Incident Handling Guide") or 800-34 ("Contingency Planning Guide for Federal Information Systems"). Following these standards will ensure that all Incident Response (IR), Disaster Recovery, and Business Continuity (DR/BC) functions within Voatz follow the same, well tested plan.

Justification
The severity is Low for the following reasons:

- Missing IR and DR/BC plans do not impact the normal operation of the system.
- However, in the event of an attack or disaster, they may hinder the resumption of normal operation.

The difficulty is High for the following reasons:

- The system does not include a full data classification guide, as noted in TOB-VOAT-TM02: Missing Data Classification.
- The implementation team must know which data, and where, can be safely handled, and by which staff members, in order to effectively implement IR and DR/BC plans

Recommendation
Implement robust incident response, disaster recovery and business continuity plans are well documented and exercised. This should include the generation of policy documents that robustly cover the areas noted in their respective NIST 800 series documents, should be automated wherever possible, and rigorously tested against production-like environments. This will ensure that the selected solution works with realistic data, and can be tested prior to an actual incident requiring response.

References

- NIST 800-61: Computer Security Incident Handling Guide
- NIST 800-34: Contingency Planning Guide for Federal Information Systems

TM4. Missing and Incomplete Documentation

Severity: Medium
Type: SA-5, SI-1, IR, RA
Component(s): All

Difficulty: High
Finding ID: TOB-VOATZ-TM04

Description
The implementation team noted that documentation was missing or incomplete throughout the system. For example, NIST 800-60-style system catalog with data access, even if nascent, would have helped both teams in understanding the design and location of security controls and the data they acted upon. Additionally, the "Voatz Information Security Risk Management (DRAFT)" document was a single page, with no identified actionable policies, identified accountable parties, or testable outcomes for a security policy stance.

Justification
The severity is Medium for the following reasons:

- Missing or incomplete documentation does not in and of itself impact the normal operation of the system.
- However, missing documentation may hinder the correct implementation, remediation, or related activities such as incident response by the implementation team.

The difficulty is High for the following reasons:

- The implementation team must perform an inventory of all assets and data throughout the system.
- The team must also have previously completed TOB-VOAT-TM02: Missing and Incomplete Data Classification.

Recommendation
Audit the system, and document all design choices, security controls, and, more broadly, developer intent. This will allow the implementation team to understand the current system more broadly, and allow the team to understand what controls are in place in which location throughout the system.

Furthermore, name specific individuals as information security officers (ISOs) within their respective portion of the organization. Follow a system such as Incident Command System (ICS), that ensures a unified command and terminology, as well as accountability and objective-based management. In this way, all members of the Voatz implementation team will have a single ontology, command structure, and objective set to follow in the case of an incident, cyber security-related or not.

References

- NIST 800-53: SA-5: Information System Documentation

- NIST 800-53: SI-1: System and Information Integrity Policy and Procedures
- Incident Command System (ICS)

Internal Processes

TM5. Incident Response is not automated and is under-documented

Severity: High
Type: IR,RA
Component(s): All

Difficulty: High
Finding ID: TOB-VOATZ-TM05

Description
The implementation team noted that Incident Response and Threat Hunting processes were neither automated nor directly documented. Most IR or Hunt activities involved systems administrators sifting through logs manually via tools such as `grep`. Manual tooling increases the chances that an incident will be missed, both in terms of how long an incident occurs and what is the actual impact of the incident.

Justification
The severity is High for the following reasons:

- Missing or incomplete documentation does not in and of itself impact the normal operation of the system.
- However, missing documentation may hinder the correct implementation, remediation, or related activities such as incident response by the implementation team.
- Additionally, not alerting on incidents in an automated fashion increases the chance that incidents may be missed, or that more serious incidents will be missed by disaggregate data.

The difficulty is High for the following reasons:

- The implementation team must perform an inventory of all assets and data throughout the system.
- The team must also have previously completed TOB-VOAT-TM02: Missing and Incomplete Data Classification.

Recommendation
Implement a robust incident response process that is both well documented and largely automated. This will require having a known-good host baseline, as per TOB-VOAT-TM16: Missing Host Verification Process, as well as a defined data classification, as per TOB-VOAT-TM02: Missing Data Classification. Furthermore, leave manual processes that rely upon tools such as `grep` or a list of regexes to search in Centralized Logging Solution for threat hunting and other exploratory exercises.

References

- NIST 800-53:IR Family
- NIST 800-61: Computer Security Incident Handling Guide

- Intelligence Drive Incident Response (physical book)
- The Blueteam Handbook (physical book)

TM6. Risk Management is lacking

Severity: High
Type: IR, RA
Component(s): All

Difficulty: High
Finding ID: TOB-VOATZ-TM06

Description
The implementation team noted that their risk management setup did not include robust threat intelligence, threat hunting, automated actor extraction. All three are needed for wholistic detection of threats:

- Robust threat intelligence provides an updated feed of actors from multiple sources, and includes their Tools, Techniques, Tactics, and Procedures (TTTPs).
- Threat hunting provides a mechanism to determine new actors and attacks within your system.
- Automated extraction combines the outputs from the above two processes, and combines them into a simple solution that front-line analysts can use for detecting and responding to threats in a simple way.

Additionally, extraction should focus on items that are easier to extract:

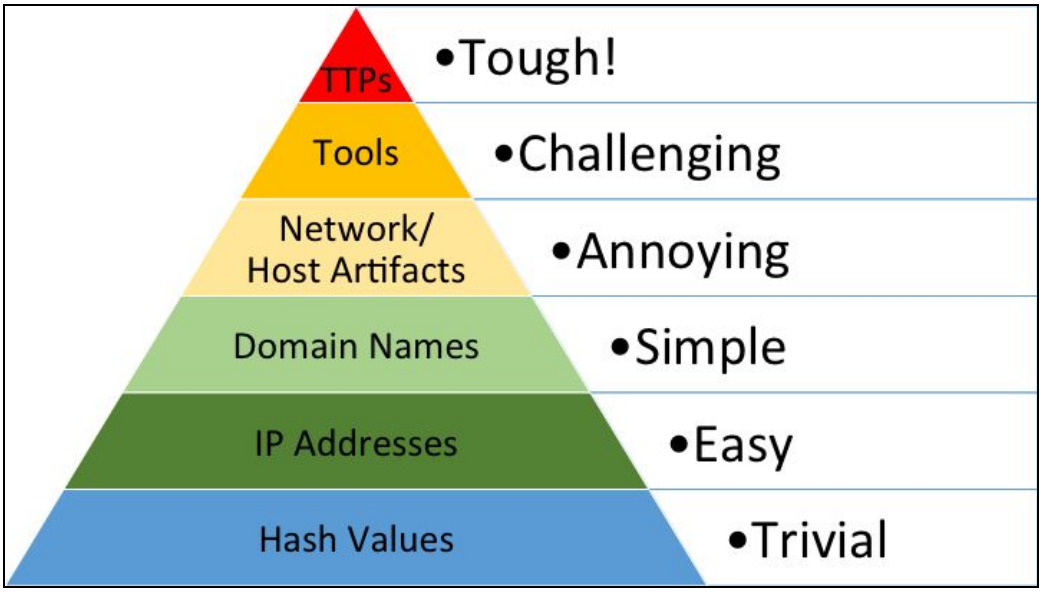


Figure 6.1: The Sqrrl/David J. Bianco Pyramid of Pain

More broadly, the Risk Management processes at Voatz as a whole should be flushed out. At the time of the assessment the "Voatz Information Security Risk Management (DRAFT)" document was missing major portions of cyber security policy:

- Risk Identification: while the Voatz policy document defined their desire to seek vulnerabilities and risks from all sources possible, it defined no processes for accepting, triaging, contextualizing risk, or even identifying risk within the organization.
- Risk Assessment: no formal process was identified as to the risk assessment process, nor was any risk rating system mentioned within the provided documentation.
- Risk Reporting: the document notes "several internal tracking mechanisms," but neither reports what they are nor specifies how a team member may interact with or add to the report.
- Risk Controls Implementation: the document states that Voatz "need[s] to beef up" their Risk Controls across the organization.
- Continuous Risk Monitoring: the document mentions that there are several automated tracking mechanisms in place, which is good, but neither lists them nor defines to what level they are automated.

Justification
The severity is High for the following reasons:
- Missing or incomplete documentation or automation does not in and of itself impact the normal operation of the system.
- However, missing documentation or automation may hinder the correct implementation, remediation, or related activities such as incident response by the implementation team.
- Not having defined processes in place to accept, triage, remediate, and test threats across the Voatz system means that the implementation team cannot effectively prioritize which fixes should be applied where at which time.

The difficulty is High for the following reasons:
- The implementation team must perform an inventory of all assets and data throughout the system.
- The team must also have previously completed TOB-VOAT-TM02: Missing and Incomplete Data Classification.

Recommendation
Automate your processes for extracting data from threat hunts, threat intelligence feeds, and normal SOC analysis into automated alerts. These should take the form of alerts to responsible parties within the Voatz organization, who must also be defined.
More broadly, document all Risk Assessment and Risk Management Goals. We make the following recommendations based on the provided policy documentation:

- Risk Identification: identify Voatz staff that are responsible for triaging results from external third parties and internal assessments alike. This should take the form of identifying the asset that is impacted, the data that may or may not be exposed, and the team responsible for the component. This requires that at least TOB-VOAT-TM02

and TOB-VOAT-TM16 have been completed. Furthermore, implement your own internal Risk Identification process, using something like NIST 800-115.
- Risk Assessment: Adopt a unified Risk Assessment process; since the implementation team is already using the NIST 800 series for other controls and the CSF for maturity modeling, an obvious answer would be NIST 800-30, NIST 800-37, and NIST 800-39.
- Risk Reporting: adopt a unified "Risk Registry," where ISOs and their respective component development teams may see risks assigned to their components.
- Risk Controls Implementation: Beef up the controls across the organization. This should include following at least the NIST 800-53 controls required for a Medium SC.
- Continuous Risk Monitoring: define what continuous monitoring looks like within the organization, and ensure that all ISOs are able to receive it.

References

- The Cyber Hunting Maturity Model
- Effective Threat Intelligence (physical book)
- Election Infrastructure Intelligence Sharing and Analysis Center (EI-ISAC)
- NIST National Vulnerability Database (NVD)
- MISP, an open source threat sharing project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
- NIST 800-30: Guide for Conducting Risk Assessments
- NIST 800-37: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST 800-39: Managing Information Security Risk: Organization, Mission, and Information System View

Voting Processes

TM7. Voter identity verification is manual with minimal training support

Severity: High
Type: AT, IA-8
Component(s): Cloud Storage Service

Difficulty: Medium
Finding ID: TOB-VOATZ-TM07

Description
The current process for voter verification is a manual process of a team of two people at Voatz. There is an identity verification provider in the process, but the voter is not able to vote until manual confirmation of their identity. The voter uploads a picture of a government issued photo id and a selfie through the mobile app to the Cloud Storage Service bucket. A notice is sent to the verification team and they must manually pull up provided documentation and using basic guidance provided by a state or other identification issuing body the team must make a decision to verify the voter or not.

Justification
The severity is High for the following reasons:

- The manual process is not scalable or really auditable
- It is unlikely that the team would be able to identify targeted fraud attempts without formal identification verification training

The difficulty is Medium for the following reasons:

- Should state sponsored actors (or of similar means) decide to attack this process it will be a serious challenge to maintain the integrity of the identify verification
- It will take some time to determine a long term solution that is trustworthy (as much as it can be) and scalable

Recommendation
Short term recommendation would be to employ a small team specially trained in identity verification with an auditable process. Longer term would be to institute automated tooling to aid in an initial round of identity verification, supplemented with the specially training team to handle anomalies.

TM8. Internal team has full access to voter PII

Severity: Medium
Type: AC-21, SI
Component(s): All

Difficulty: Medium
Finding ID: TOB-VOATZ-TM08

Description
Manual voter verification process requires access to verify identity. The small team that conducts the manual voter validation has full access to the federal or state issued identification images that are uploaded by the voters, as they must attempt to match to the selfie and any known, identifiable markings. There is a manual process to remove the data provided by voters for verification within 24 hours of verification.

Justification
The severity is Medium for the following reasons:

- There is no audit trail nor detective control to prevent or detect harvesting the voter PII to sell or abuse
- Breach of trust in the process may result in serious damage to the reputation of the organization

The difficulty is Medium for the following reasons:

- There are not many viable alternatives at this time to satisfy the voter verification requirements
- Need to establish a formal, auditable process to handle and verify voter PII

Recommendation
Short term recommendation would be to employ a small team specially trained in identity verification with an auditable process. Longer term would be to institute automated tooling to aid in an initial round of identity verification, supplemented with the specially training team to handle anomalies.

TM9. Voters or admins could be blacklisted in denial-of-service attacks

Severity: High
Type: DS, SC-5
Component(s): Admin Portal, Apache WS, ALB, WAF

Difficulty: Medium
Finding ID: TOB-VOATZ-TM09

Description
The controls put in place to help defend against brute forcing voter accounts, could be turned against the system to blacklist voters and admins in a denial of service attack. Credential stuffing and brute force attacks would generate the traffic that would result in account locks for voters and IP Blacklisting for admins. This finding assumes that there is a Malicious Internal User or Internal Attacker with sufficient position to affect this attack.

Justification
The severity is High for the following reasons:

- If a denial of service attack against the voters attempting to utilize the Voatz application was successful it would be immensely damaging to the trust in Voatz
- Denying election admins access to their management portal could cast doubt on the integrity of the election results.

The difficulty is Medium for the following reasons:

- To be effective, it would need to be a targeted attack with knowledge of eligible voters with email address and/or mobile phone number
- Implementing authentication controls with the proper balance between defense against brute force without sizably increasing the risk of a denial of service attack can be difficult

Recommendation
Account lockouts should be implemented as small delays, it should provide enough protection against brute forcing without creating an abusable denial of service condition. IP Blacklisting should not be blindly implemented, if malicious traffic is detected from a known and whitelisted IP address a response team should be notified to triage and take appropriate actions.

References

- OWASP Authentication Cheatsheet

TM10. Post-election handling processes increase risk of mishandling

Severity: Medium
Type: SI
Component(s): Admin Portal, File Hosting Provider

Difficulty: Medium
Finding ID: TOB-VOATZ-TM10

Description
The post-election verification process Voatz is to have an election admin export the voting receipt PDFs and ballot PDFs, print them out, run them through a tabulation machine, rescan them all, and upload them to a shared File Hosting Provider folder. Then a Voatz admin will retrieve the uploaded files from File Hosting Provider and move them to the file system on the Audit Application Apache server to be accessed by citizen auditors.

The process of printing and rescanning the ballots and receipts leaves opening for unintentional and intentional errors to be introduced in the vote counting process. A verification check to compare the re-scanned and uploaded ballots and receipts against what was originally captured is not currently implemented. Specifically, this process lacks any cryptographic guarantees that the integrity of votes are maintained as they transit the system.

Justification
The severity is Medium for the following reasons:

- Breach of trust in the process may result in serious damage to the reputation of the organization
- Errors or malicious activity at this part of the voting process may impact the results of the election and may be hard to detect

The difficulty is Medium for the following reasons:

- The need to develop a verification process to test the re-scanned ballots and receipts against the originals to verify matching, and a process to handle failed verification.
- It is our understanding that much of this part of the process in the election may be dictated to Voatz by the election administrators, making changes to the process is likely difficult as it may be outside of the control of Voatz

Recommendation
Review the vote count and validation process and attempt to eliminate areas that introduce weaknesses that may jeopardize the integrity of the vote counting process.

External or Third-Party Storage

TM11. Post-election information shared via File Hosting Provider folders

Severity: Medium
Type: AC-21, SI
Component(s): File Hosting Provider

Difficulty: Medium
Finding ID: TOB-VOATZ-TM11

Description
Rescanned voting receipts and ballots are stored in File Hosting Provider folders to transmit them back to Voatz from election administrators in a jurisdiction. The ownership of the File Hosting Provider folder may vary between elections, and is typically under Voatz control, but may also be managed by someone in the jurisdiction. Maintaining an auditable chain of custody through this transfer mechanism is very difficult and leaves the process vulnerable to tampering.

Justification
The severity is Medium for the following reasons:

- Breach of trust in the process may result in serious damage to the reputation of the organization
- Altering the results of an election could cause reputational and regulatory impact to both Voatz and the jurisdiction.

The difficulty is Medium for the following reasons:

- An attacker would need access to the folder through a misconfiguration or another vulnerability.
- An internal attacker with access to the folder would need the capability to replace the genuine receipts and ballots with forged versions.

Recommendation
Leverage a file transfer solution that can include a verifiable audit trail and file hashes to help ensure that it can be verified that the files containing the ballots and receipts moved to the audit server are the same ones that were placed there by an election administrator.

TM12. Manual process to purge post-election data from shared File Hosting Provider folders

Severity: Medium
Type: AC, SI
Component(s): File Hosting Provider

Difficulty: Medium
Finding ID: TOB-VOATZ-TM12

Description
It is a manual process to purge voter receipts and ballots from File Hosting Provider folders. This could result in election data sitting in a File Hosting Provider folder owned by Voatz or someone representing a jurisdiction for an undetermined amount of time.

Justification
The severity is Medium for the following reasons:

- Breach of trust in the process may result in serious damage to the reputation of the organization

The difficulty is Medium for the following reasons:

- Election administrators or Voatz administrators would need to forget to remove the voter receipts and ballots once they are no longer needed
- An attacker would need to gain access to the folder to extract the voter data

Recommendation
If File Hosting Provider must be used, set auto-deletion time frames in File Hosting Provider to automatically expire and delete voter related data from the folder after it is determined to no longer be needed. Recommend replacing File Hosting Provider with a file transfer solution that can include a verifiable audit trail and file hashes to help ensure that it can be verified that the files containing the ballots and receipts moved to the audit server are the same ones that were placed there by an election administrator.

TM13. Cloud Storage Service storage is used for multiple elections and jurisdictions

Severity: High
Type: AC-3, SC-4
Component(s): Cloud Storage Service

Difficulty: Low
Finding ID: TOB-VOATZ-TM13

Description
During the interviews it was disclosed that there is only a single bucket that is used for elections. While possible to use a unique Cloud Storage Service bucket per election and/or jurisdiction; historically the current Cloud Storage Service bucket has been reused for a number of elections. The pattern greatly increases the risk of disclosure of voting related information to other jurisdictions and others that shouldn't be authorized to view.

Justification
The severity is High for the following reasons:

- Breach of trust in the process may result in serious damage to the reputation of the organization
- A breach of the singular Cloud Storage Service bucket could divulge critical information about multiple elections

The difficulty is Low for the following reasons:

- Cloud A allows for 100 buckets to be created per account and supports raising the limit to 1000 buckets by request
- Cloud A provides audit logging and monitoring for buckets to help identify and alert on usage with in a bucket

Recommendation
Create a unique, permissioned bucket per election, jurisdiction, or other logical point of separation. Implement an auditable process with a data retention policy to help ensure they are cleaned up when no longer needed. This will minimize the risk of a single bucket divulging all the election related information in a single attack or misconfiguration.

References

- REDACTED

Infrastructure & Administration

TM14. Cloud deployments are not aligned in maturity or capability

Severity: Medium
Type: MA, CM, AU-12
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM14

Description
Cloud deployments are not aligned in maturity or capability between Cloud A and Cloud B. Specifically, components within logging, load balancing, and web application firewall (WAF) are missing from the Cloud B environment which exist within Cloud A. Attacks that occur within the Cloud B environment may not be noticed due to missing logging or may succeed where they would be denied should they occur within the Cloud A environment.

Justification
The severity is Medium for the following reasons:

- The application is load balanced across the cloud environments.
- Attacks that occur in one environment may not be traceable globally.
- In general, this disparity does not create an attack vector, but rather increases the likelihood that an attack would go unnoticed.

The difficulty is Low for the following reasons:

- Analogs for the impacted components exist within the Cloud B environment.

Recommendation
Ensure that all hosting providers, cloud or otherwise, are at parity with reporting and security tooling. This will ensure that all data is stored in the same centralized locations, and that incident responders and analysts within the implementation team have only one location to analyze for data.

TM15. Infrastructure and Application deployments are manual

Severity: Medium
Type: CM
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM15

Description
The implementation team mentioned that all deployments are manual, across both infrastructure and application deployments. The implementation team has runbooks that are used to deploy systems; for example, when an Apache instance is needed for the DMZ, a stock CentOS image is taken from the image repository, and then an administrator runs a series of commands that configure the machine. This is ripe for abuse by Malicious Internal Administrators, and limits the implementation team's ability to quickly stand up infrastructure in response to an event. This is especially problematic in light of TOB-VOAT-TM16: Missing Host Verification Process.

Justification
The severity is Medium for the following reasons:

- Manual processes are difficult to run and error prone.
- A Malicious Administrator, or an attacker who had included a key or other surreptitious access onto the running machine could have free reign over a machine.
- The team has no process for verifying that an installation is correct.

The difficulty is Low for the following reasons:

- Multiple robust solutions exist for infrastructure automation.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Automate as much of the deployment process as possible. This should include the instantiation of nodes, the installation of keys, the configuration of host policies, and so on. This will help make deployments repeatable, and reduce the likelihood that an attacker may gain access to a system.

Furthermore, move towards immutable deployments, that do not allow administrators to login. This will ensure that deployments do not outlast their timeframe, and can be easily updated by simply deploying new infrastructure as needed.

TM16. Missing host verification process

Severity: Medium
Type: CM-2, CM-3
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM16

Description
The implementation team mentioned that they have no secure baseline for systems, that is specific to Voatz usage, similar to the Secure Host Baseline. A secure baseline helps improve operations across the organization, as developers know which systems they are allowed to use, and automated processes need not be tailored for each deployment. Furthermore, secure baselines mean that the system is easier to update, as the changes must be tracked in a change control system, and all elements of the implementation team have visibility into the proposed changes.

Justification
The severity is Medium for the following reasons:

- Manual processes are difficult to run and error prone.
- A Malicious Administrator, or an attacker who had included a key or other surreptitious access onto the running machine could have free reign over a machine.
- The team has no process for verifying that an installation is correct.

The difficulty is Low for the following reasons:

- Multiple robust solutions exist for infrastructure automation.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Design a secure host baseline for the Voatz system, and use this for all deployments. Furthermore, build off this baseline for all deployment types within the Voatz system. This will ensure that changes to the core baseline improve all other systems, and that Malicious Internal Users have minimal space to tamper with deployments.

References

- NIST 800-53: CM-2: Baseline Configuration
- NIST 800-53: CM-3: Configuration Change Control

TM17. Lack of defined process to remove or refresh infrastructure

Severity: Medium
Type: SA-3
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM17

Description
The implementation team discussed the current life cycle for infrastructure, both owned by Voatz and external to the platform itself, and noted that most removal and refresh processes are aspirational in nature. This means that sensitive data, such as ballots, may not be removed from internal or external assets ever, which could expose voters' data.

Justification
The severity is Medium for the following reasons:

- Manual processes are difficult to run and error prone.
- A Malicious Administrator, or an attacker who had access to the host could maintain that access indefinitely

The difficulty is Low for the following reasons:

- Multiple robust solutions exist for infrastructure automation.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Design a strict process for removing or refreshing infrastructure whenever possible. This should include as much automation as possible. In the case of voter data, particular care should be taken to ensure that all data is removed from all assets across the system, which is difficult given how manual the process is and how diffuse the data storage within the current system is.

References

- NIST 800-53:SA-3: System Development Life Cycle

TM18. Self-hosted MySQL & MongoDB Instances

Severity: Low
Type: CM-3, SA-3, SC-12
Component(s): MySQL, MongoDB

Difficulty: Low
Finding ID: TOB-VOATZ-TM18

Description
Voatz mentioned during the assessment that MongoDB and MySQL were not using cloud-hosted versions, but rather manually provisioned machines. This discussion further noted that while the systems do support key rotation, there were no processes in place to actually rotate keys, and that this rotation was aspirational in nature.

Justification
The severity is Low for the following reasons:

- General best practices, such as encryption at rest, have been implemented.
- Manual processes are difficult to run and error prone.
- While best practices have been largely implemented, items such as key rotation remain aspirational.

The difficulty is Low for the following reasons:

- Both cloud environments include managed options.
- Cloud-managed options implement items such as key rotation and compliance.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Migrate to a cloud-managed option for MySQL and MongoDB to take advantage of several configuration and security features to reduce the risk to the voter data stored

References

- REDACTED

TM19. Mutable infrastructure with minimal security monitoring

Severity: Medium
Type: CA-7, IR-5
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM19

Description
The implementation team noted that the current configuration does not include either network- or host-based intrusion detection systems (NIDS, HIDS). Continuous monitoring is appropriate for any system, as it allows defenders to have accurate and timely information about anomalous network traffic or host executions. However, with mutable infrastructure, it is extremely important to have continuous monitoring and alerting, to help defenders in knowing an attack may be underway before it has successfully breached a host.

Justification
The severity is Medium for the following reasons:

- Manual processes are difficult to run and error prone.
- A Malicious Administrator, or an attacker who had included a key or other surreptitious access onto the running machine could have free reign over a machine.
- The team has minimal insight into correct infrastructure operation.

The difficulty is Low for the following reasons:

- Multiple robust solutions exist for infrastructure automation.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Add a NIDS, such as Suricata or Snort, to the network to monitor the network for malicious or anomalous activity. This may be in line, with a NIDS running on each host, or may utilize VPC Flow Logs to examine data out of band. There are also on-server web application firewalls, such as mod_security, which provide in-band WAF/IDPS functionality at the web server layer. Additionally, utilize a HIDS, such as Tripwire or OSSEC, to monitor hosts for anomalous behavior in the executables they run.

Furthermore, as noted in TOB-VOAT-TM16: Missing Host Verification Process and TOB-VOAT-TM15: Infrastructure and Application Deployments are manual, the system would also be improved by moving towards an immutable infrastructure, with minimal moving parts. In this way, HIDS and NIDS are there to monitor machines, but otherwise machines are not reused, and monitoring is in place to support audit functionality, rather than protect machine integrity as a whole.

References

- NIST 800-53: CA-7: Continuous Monitoring

- NIST 800-53: IR-5: Incident Monitoring
- NIST 800-53: AU-2: Audit Events
- REDACTED
- ModSecurity

TM20. Virtual Private Cloud (VPC) Peering is too permissive

Severity: Medium
Type: CA-3, CA-6, CM-5, AC-3, AC-4
Component(s): Voatz Corporate Network, Cloud A

Difficulty: Low
Finding ID: TOB-VOATZ-TM20

Description
When discussing the interconnection between the Voatz corporate network and the cloud-hosted networks, the implementation team noted that the VPC peering allows the entire Voatz Corporate Network access to the Cloud A environment. While the servers themselves do have iptables, security group, and VPC restrictions, this does increase the risk that a Malicious Internal User may use their access to attempt access to sensitive cloud-hosted services and infrastructure.

Justification
The severity is Medium for the following reasons:

- Attackers need only access the Voatz Corporate Network in order to attempt to access sensitive infrastructure.
- VPC peering is backed by per-server iptables and other restrictions, lowering severity.
- However, iptables and other security mechanisms are manual, and could be missed for an individual host.

The difficulty is Low for the following reasons:

- The implementation team need only to further segment the Voatz Corporate Network into privileged and unprivileged zones.
- Administrators may only access the VPC segment from the privileged zone within the Voatz Corporate Network.
- Additional monitoring and access restrictions can be placed on the privileged zone to further protect and audit actions taken from that network.

Recommendation
Further segment the Voatz Corporate Network into privileged and unprivileged zones, and only allow access to production environments from the privileged zone. Furthermore, add additional scrutiny to machines within this zone, upto and including restricted internet access and physical access restrictions. This will ensure that only authorized users have access to machines that could potentially access production environments, and that additional restrictions are placed on these machines to minimize the chance of compromise or malicious access.

References

- NIST 800-53: CA-3: System Interconnections
- NIST 800-53: CA-6: Security Authorizations
- NIST 800-53: CM-5: Access Restrictions for Change

- NIST 800-53: AC-3: Access Enforcement

TM21. Administrator commands are not logged

Severity: High
Type: AU, CM
Component(s): All

Difficulty: Medium
Finding ID: TOB-VOATZ-TM21

Description
The implementation team noted that system administrator's commands are not currently logged or monitored related to the Voatz application infrastructure. This may allow for malicious behavior that would not be detected or alerted. Furthermore, due to the manual nature of the configuration management within the Voatz system, an attack by a Malicious Internal Attacker could go unnoticed for some time.

Justification
The severity is High for the following reasons:

- The configuration management is manual, meaning that regular administrator access is not anomalous.
- Administrators do not need further authorization other than VPC access and credentials (username and key material) to access production instances.
- A Malicious Internal Attacker could alter configurations or install malicious software on the servers and there would be no detective controls like audit logging to help alert or determine what happened.

The difficulty is Medium for the following reasons:

- The implementation team must add command introspection to all host-login actions.
- Additional storage and processing would be needed to handle the additional log volume that would result from implementing these controls.

Recommendation
Log all administration commands to a central repository, and audit those commands for both content and metadata. For example, if an administrator normally accesses a system during the work day, it would be anomalous for them to access a system in the middle of the night. Furthermore, consider moving towards a "No-Lone Zone" style of authorization, as noted in TOB-VOAT-TM27: Two Person Rule/No-Lone Zone not implemented. Lastly, move away from infrastructure that even requires an administrator to login, as this increases the likelihood that administrators even need to login to machines. If machines were immutable, they may be introspected via the filesystem and items such as `auditd`, rather than by direct administrator access.

References

- Chapter 7: System Auditing (RHEL)

TM22. Window for log retention is too short due to costs

Severity: Medium
Type: AU, CA-7
Component(s): Cloud A Components

Difficulty: Low
Finding ID: TOB-VOATZ-TM22

Description
During discovery conversations surrounding Cloud A infrastructure, the implementation team noted that Cloud A logs may be lossy due to costs. The current configuration off-loads Cloud A logs on Friday, which are then checked on Monday. However, if a large number of events happen prior to this offload, or if large influx happens during this offloading, these logs may be lost, as audit capacity is limited due to cost.

Justification
The severity is Medium for the following reasons:

- Cloud A logs are an important source of security information, as they include administrator actions and other information from Cloud A services themselves.
- Missing visibility into logs may mean that security events are missed by defenders.
- However, the severity is lowered by the fact that attackers may only cover tracks by generating a large number of events.

The difficulty is Medium for the following reasons:

- Increasing log retention increases potential costs.
- Increasing ingestion frequency may require additional tuning and configuration for Centralized Logging Solution.

Recommendation
Increase both the log retention period for Cloud Logging Service as well as the frequency with which logs are offloaded into Centralized Logging Solution. This will decrease the likelihood that an attacker can hide their tracks by generating large volumes of logs, and will also provide more real-time views into the cloud environment to defenders. Pair this with TOB-VOAT-TM23: Administrator Login activity recorded in Cloud Logging Service, without alerting and TOB-VOAT-TM24: Missing Alerts for actions related to Cloud Block Storage volume administration.

TM23. Administrator login activity recorded in Cloud Logging Service, without alerting

Severity: Low
Type: AU, IR, SI-5
Component(s): Cloud A Components

Difficulty: Low
Finding ID: TOB-VOATZ-TM23

Description
The implementation team noted that while Cloud Logging Service captures administrator logins, it does not alert defenders when a login occurs. Instead, they must wait for this information to be ingested into Centralized Logging Solution a week later, and then must manually check for administrator logins. If an attack were to occur, defenders may not know for a week or more.

Justification
The severity is Low for the following reasons:

- Cloud A credentials use multi-factor authentication.
- A Malicious Internal User has more fruitful targets than Cloud A alone.
- Missing alerts do not impact the normal operation of the system, but rather may allow an attack to continue unnoticed.

The difficulty is Low for the following reasons:

- Cloud Logging Service, combined with Cloud Monitoring Service and other technologies, support alerting on administrator login.
- Minimal setup is required to support both alerting from Cloud Logging Service and Cloud Monitoring Service as well as after effects from Centralized Logging Solution.

Recommendation
Alert administrators whenever a sensitive role is used for login. For the most part, this should be so minor as to be barely noticeable to administrators. However, in the event of an actual attack, this could be an invaluable alert for defenders to respond to.

References

- REDACTED

TM24. Missing Alerts for actions related to Cloud Block Storage volume administration

Severity: Low
Type: AU, IR, SI-5
Component(s): Cloud A Components

Difficulty: Low
Finding ID: TOB-VOATZ-TM24

Description
While discussing Cloud A policies, the implementation team noted that no Cloud Block Storage volume alerts were enabled. Cloud Block Storage volumes generate multiple events, many of which are extremely useful in detecting an attack. For example, unmounting and reattaching a volume may belie that an attack is underway, and an attacker is attempting to access sensitive information within another system.

Justification
The severity is Low for the following reasons:

- Cloud A credentials use multi-factor authentication.
- A Malicious Internal User has more fruitful targets than Cloud A alone.
- Missing alerts do not impact the normal operation of the system, but rather may allow an attack to continue unnoticed.

The difficulty is Low for the following reasons:

- Cloud Logging Service, combined with Cloud Monitoring Service and other technologies, support alerting on administrator login.
- Minimal setup is required to support both alerting from Cloud Logging Service and Cloud Monitoring Service as well as after effects from Centralized Logging Solution.

Recommendation
Enable alerts from Cloud Monitoring Service and Cloud Logging Service for all Cloud Block Storage events. This should allow defenders to tell when, where, and how a volume is being modified, and respond accordingly.

References

- REDACTED

TM25. Missing Cloud Audit for email use across service accounts

Severity: Informational
Type: AU, AC-5
Component(s): Cloud A Components, Internet

Difficulty: Low
Finding ID: TOB-VOATZ-TM25

Description
The implementation team noted that most accounts should use separate emails; however, this was an honor system, and was not enforced by either procedural audit or technical means. An attacker with access to an account that had used the same email address across infrastructure could have access to a wide array of services.

Justification
This item is of Informational severity and, as such, represents an observation about a potential weakness within the system, rather than an actual vulnerability.

Recommendation
Audit all employees' accounts, and ensure that they use separate emails for each account, per internal policy. This will help enforce separation of duties, and ensure that attackers must compromise multiple accounts in order to attack Voatz's infrastructure.

TM26. Centralized Logging Solution is sent via syslog, potentially exposing information

Severity: Low
Type: SC-8, SC-13, SC-17
Component(s): All

Difficulty: Medium
Finding ID: TOB-VOATZ-TM26

Description
The implementation team noted that all hosts transmit logs back to Centralized Logging Solution via syslog. Syslog, by default, does not encrypt traffic, meaning attackers with sufficient position could potentially see anything included within system logs.

Justification
The severity is Low for the following reasons:

- Sensitive user data is not transmitted via logs to Centralized Logging Solution.
- The logs are not sent over the open internet, but rather via VPN and VPC peering back to Centralized Logging Solution.
- An attacker with this level of access could already view much of the same information from other sources.

The difficulty is Medium for the following reasons:

- Implementers must configure TLS certificates for all Centralized Logging Solution hosts.
- Any items using UDP for rsyslog, must use an interstitial host.

Recommendation
Implement TLS throughout the logging system. This could include encrypting rsyslog traffic with TLS, or implementing a different forwarder and securing Centralized Logging Solution itself using TLS. In either case, logs forwarded to Centralized Logging Solution should not be sent over open channels, even if these channels are only “open” to attackers with sufficient position.

References

- Encrypting Syslog Traffic with TLS
- Securing Centralized Logging Solution::Configuring TLS

TM27. Two-Person Rule/No-Lone Zone is not implemented

Severity: Informational
Type: AU, AC, IA
Component(s): Cloud A Components

Difficulty: Low
Finding ID: TOB-VOATZ-TM27

Description
During the discovery phase of this assessment, the assessment team inquired if production servers included what is called the “two-person rule,” also known as “the no-lone zone.” While not required by NIST 800-53 with an SC of Moderate, this is often a useful security enhancement to help add additional controls and insight into access control and authentication.

Justification
This finding is of Informational severity and, as such, represents an observation about a potential weakness within the system, rather than an actual vulnerability.

Recommendation
Consider adding a “two-person rule” to all production servers as an additional enhancement to those mentioned in previous findings. This will ensure that even if an attacker were able to utilize administrator’s credentials, they would have to compromise another administrator’s account to approve their login.

Furthermore, consider switching from SSH keys to certificates. This opens up a wealth of other management techniques, such as short term certificates, and allows administrators to provide more fine-grained, policy-based controls around authentication.

References
- Two-man rule
- Argonne National Labs PAM module for 2-person rule
- Symantec’s Keymaster, a short-term certificate system for SSH
- A package for handling SSH certificates
- Uber’s ussh, which handles SSH certificates at the PAM level
- Netflix’s BLESS, which is an SSH certificate authority

TM28. Missing Key Rotation policy for MySQL/MongoDB

Severity: Low
Type: SC-12, SC-13
Component(s): MongoDB, MySQL

Difficulty: Low
Finding ID: TOB-VOATZ-TM28

Description
When discussing the security surrounding the MySQL and MongoDB components, the implementation team noted that while they did support key rotation, this was not currently implemented within the system

Justification
The severity is Low for the following reasons:

- Manual processes are difficult to run and error prone.
- Key rotation is an important security control in the event of a breach.
- In and of itself, key rotation does not impact the normal day to day of server operation, but rather hinders defenders in the event of a breach.

The difficulty is Low for the following reasons:

- Both cloud environments include managed options.
- Cloud-managed options implement items such as key rotation and compliance.
- These solutions are easily audited, both for security and correctness concerns.
- Additionally, they are a force multiplier for other areas, such as incident response.

Recommendation
Switch to a cloud-hosted version of both MySQL and MongoDB. This will provide all cryptographic security required, as well as important audit and compliance controls.

TM29. Infrastructure hosted outside the US

Severity: Medium
Type: SC-1, AC-20
Component(s): All

Difficulty: Low
Finding ID: TOB-VOATZ-TM29

Description
There are no procedural protections to prevent Voatz infrastructure from being hosted outside of the United States. Currently, Voatz has three servers physically located in Canada provided by OVH, a French hosting company. Voatz indicated that these servers were test infrastructure. It is unclear whether any of these servers have been used in prior or ongoing elections.

Justification
The severity is Medium for the following reasons:

- Voatz has claimed that Canada is still considered an acceptable jurisdiction in which to host servers.
- There is no evidence that Voatz has provisioned infrastructure in countries other than the US and Canada.
- Many hosting providers run datacenters in less friendly countries. A simple provisioning error changing “CA” to “CN” could result in infrastructure being provisioned in China.

The difficulty is Low for the following reasons:

- Election servers hosted in an adversarial country with unilateral control over its Internet infrastructure could trivially and selectively deny service to Voatz.
- Voatz infrastructure hosted in the jurisdiction of an adversarial country could be subpoenaed or confiscated.

Recommendation
Update the Voatz provisioning procedures to only allow infrastructure to be hosted in the US. Use infrastructure-as-code tools to minimize the chances of manual provisioning errors. Use a hosting provider that is compliant with the US Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) and the Federal Risk and Authorization Management Program (FedRAMP).

References

- DoD Cloud Computing SRG
- Federal Risk and Authorization Management Program (FedRAMP)
- REDACTED

Mobile Application

TM30. Lacking a pool of pre-generated keys or multiple certs pinned

Severity: High
Type: SC-12, SC-13
Component(s): DMZ

Difficulty: Low
Finding ID: TOB-VOATZ-TM30

Description
The implementation team noted that all servers use the same, wild-card TLS certificate for all public facing applications. An attacker with access to any server with key material could create their own instance of Voatz infrastructure with known-good certificates. Furthermore, in the event of a certificate expiry or revocation, the mobile application would be unable to communicate with any backend services.

Justification
The severity is High for the following reasons:

- If a certificate expires or is compromised and needs to be rotated, the mobile application will cease to work until it is updated.
- Attacks that expose certificates could masquerade as backend services.
- Masquerades could allow an attacker to have access to sensitive voter and ballot data.

The difficulty is Low for the following reasons:

- Multiple, cloud-hosted solutions exist to support automatic certificate generation.
- Pinning a group of certificates is no more complex than pinning a single one.
- Additionally, they are a force multiplier for other areas, such as incident response and compliance.

Recommendation
Utilize cloud-native TLS certificate authorities, such as Cloud C or Cloud A Certificate Manager. Either will allow you to generate per-instance certificates that can be added to the mobile bundle, without requiring shared certificates anywhere in the infrastructure.

TM31. Use of a custom crypto layer below TLS without pinning

Severity: Medium
Type: SC-12
Component(s): Voatz Core Server, Mobile Clients

Difficulty: High
Finding ID: TOB-VOATZ-TM31

Description
The implementation team noted the existence of a cryptographic layer below TLS. This layer is to ensure that voter's ballots and election data are not tampered with, even if an attacker were able to compromise the channel-level security of TLS. However, this additional layer of cryptography did not include key pinning, meaning that the mobile client had no way to authenticate if the key presented by the server was the expected one or not. An attacker with sufficient position, such as a Malicious Internal User or an Internal Attacker with DMZ access could present a new key to the mobile application, and man-in-the-middle any connections going forward.

Justification
The severity is Medium for the following reasons:

- An attacker with sufficient position could intercept the communications channel below TLS.
- Attackers with this level of access would have full view of voter data.
- The system generally uses certificate pinning and secondary security controls sufficiently, lowering severity.

The difficulty is High for the following reasons:

- The implementation team must design a full key lifecycle setup for this channel.
- Keys must be rotatable, revocable, and authenticated.
- Known-good keys must be included with all client applications, so as to enforce which Voatz Core Server is in use as a backend.

Recommendation
Extend the lifecycle of public key infrastructure to this key as well. This should include the full creation, authentication, usage, and deletion of the key. Pin this key in all mobile clients, or use a "trust on first use" (TOFU) model, but always ensure that clients are able to verify that the key presented is the key expected (save for the initial key exchange in TOFU). This will ensure that clients are never presented the opportunity to have an incorrect or forged key.

Appendix A: NIST 800-53 Moderate Controls

Showing 159 controls:

No.	Control	Priority	Moderate
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1
AC-2	ACCOUNT MANAGEMENT	P1	AC-2 (1) (2) (3) (4)
AC-3	ACCESS ENFORCEMENT	P1	AC-3
AC-4	INFORMATION FLOW ENFORCEMENT	P1	AC-4
AC-5	SEPARATION OF DUTIES	P1	AC-5
AC-6	LEAST PRIVILEGE	P1	AC-6 (1) (2) (5) (9) (10)
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8
AC-11	SESSION LOCK	P3	AC-11 (1)
AC-12	SESSION TERMINATION	P2	AC-12
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P3	AC-14
AC-17	REMOTE ACCESS	P1	AC-17 (1) (2) (3) (4)
AC-18	WIRELESS ACCESS	P1	AC-18 (1)
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	P1	AC-19 (5)
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	P1	AC-20 (1) (2)
AC-21	INFORMATION SHARING	P2	AC-21
AC-22	PUBLICLY ACCESSIBLE CONTENT	P3	AC-22
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	P1	AT-1

AT-2	SECURITY AWARENESS TRAINING	P1	AT-2 (2)
AT-3	ROLE-BASED SECURITY TRAINING	P1	AT-3
AT-4	SECURITY TRAINING RECORDS	P3	AT-4
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	P1	AU-1
AU-2	AUDIT EVENTS	P1	AU-2 (3)
AU-3	CONTENT OF AUDIT RECORDS	P1	AU-3 (1)
AU-4	AUDIT STORAGE CAPACITY	P1	AU-4
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	P1	AU-5
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	P1	AU-6 (1) (3)
AU-7	AUDIT REDUCTION AND REPORT GENERATION	P2	AU-7 (1)
AU-8	TIME STAMPS	P1	AU-8 (1)
AU-9	PROTECTION OF AUDIT INFORMATION	P1	AU-9 (4)
AU-11	AUDIT RECORD RETENTION	P3	AU-11
AU-12	AUDIT GENERATION	P1	AU-12
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	P1	CA-1
CA-2	SECURITY ASSESSMENTS	P2	CA-2 (1)
CA-3	SYSTEM INTERCONNECTIONS	P1	CA-3 (5)
CA-5	PLAN OF ACTION AND MILESTONES	P3	CA-5
CA-6	SECURITY AUTHORIZATION	P2	CA-6
CA-7	CONTINUOUS MONITORING	P2	CA-7 (1)
CA-9	INTERNAL SYSTEM CONNECTIONS	P2	CA-9
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	P1	CM-1
CM-2	BASELINE CONFIGURATION	P1	CM-2 (1) (3) (7)
CM-3	CONFIGURATION CHANGE CONTROL	P1	CM-3 (2)

CM-4	SECURITY IMPACT ANALYSIS	P2	CM-4
CM-5	ACCESS RESTRICTIONS FOR CHANGE	P1	CM-5
CM-6	CONFIGURATION SETTINGS	P1	CM-6
CM-7	LEAST FUNCTIONALITY	P1	CM-7 (1) (2) (4)
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	P1	CM-8 (1) (3) (5)
CM-9	CONFIGURATION MANAGEMENT PLAN	P1	CM-9
CM-10	SOFTWARE USAGE RESTRICTIONS	P2	CM-10
CM-11	USER-INSTALLED SOFTWARE	P1	CM-11
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	P1	CP-1
CP-2	CONTINGENCY PLAN	P1	CP-2 (1) (3) (8)
CP-3	CONTINGENCY TRAINING	P2	CP-3
CP-4	CONTINGENCY PLAN TESTING	P2	CP-4 (1)
CP-6	ALTERNATE STORAGE SITE	P1	CP-6 (1) (3)
CP-7	ALTERNATE PROCESSING SITE	P1	CP-7 (1) (2) (3)
CP-8	TELECOMMUNICATIONS SERVICES	P1	CP-8 (1) (2)
CP-9	INFORMATION SYSTEM BACKUP	P1	CP-9 (1)
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	P1	CP-10 (2)
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	P1	IA-1
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	P1	IA-2 (1) (2) (3) (8) (11) (12)
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	P1	IA-3
IA-4	IDENTIFIER MANAGEMENT	P1	IA-4
IA-5	AUTHENTICATOR MANAGEMENT	P1	IA-5 (1) (2) (3) (11)

IA-6	AUTHENTICATOR FEEDBACK	P2	IA-6
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	P1	IA-7
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	P1	IA-8 (1) (2) (3) (4)
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	P1	IR-1
IR-2	INCIDENT RESPONSE TRAINING	P2	IR-2
IR-3	INCIDENT RESPONSE TESTING	P2	IR-3 (2)
IR-4	INCIDENT HANDLING	P1	IR-4 (1)
IR-5	INCIDENT MONITORING	P1	IR-5
IR-6	INCIDENT REPORTING	P1	IR-6 (1)
IR-7	INCIDENT RESPONSE ASSISTANCE	P2	IR-7 (1)
IR-8	INCIDENT RESPONSE PLAN	P1	IR-8
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	P1	MA-1
MA-2	CONTROLLED MAINTENANCE	P2	MA-2
MA-3	MAINTENANCE TOOLS	P3	MA-3 (1) (2)
MA-4	NONLOCAL MAINTENANCE	P2	MA-4 (2)
MA-5	MAINTENANCE PERSONNEL	P2	MA-5
MA-6	TIMELY MAINTENANCE	P2	MA-6
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	P1	MP-1
MP-2	MEDIA ACCESS	P1	MP-2
MP-3	MEDIA MARKING	P2	MP-3
MP-4	MEDIA STORAGE	P1	MP-4
MP-5	MEDIA TRANSPORT	P1	MP-5 (4)
MP-6	MEDIA SANITIZATION	P1	MP-6
MP-7	MEDIA USE	P1	MP-7 (1)

PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	P1	PE-1
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	P1	PE-2
PE-3	PHYSICAL ACCESS CONTROL	P1	PE-3
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	P1	PE-4
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	P2	PE-5
PE-6	MONITORING PHYSICAL ACCESS	P1	PE-6 (1)
PE-8	VISITOR ACCESS RECORDS	P3	PE-8
PE-9	POWER EQUIPMENT AND CABLING	P1	PE-9
PE-10	EMERGENCY SHUTOFF	P1	PE-10
PE-11	EMERGENCY POWER	P1	PE-11
PE-12	EMERGENCY LIGHTING	P1	PE-12
PE-13	FIRE PROTECTION	P1	PE-13 (3)
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	P1	PE-14
PE-15	WATER DAMAGE PROTECTION	P1	PE-15
PE-16	DELIVERY AND REMOVAL	P2	PE-16
PE-17	ALTERNATE WORK SITE	P2	PE-17
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	P1	PL-1
PL-2	SYSTEM SECURITY PLAN	P1	PL-2 (3)
PL-4	RULES OF BEHAVIOR	P2	PL-4 (1)
PL-8	INFORMATION SECURITY ARCHITECTURE	P1	PL-8
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	P1	PS-1
PS-2	POSITION RISK DESIGNATION	P1	PS-2
PS-3	PERSONNEL SCREENING	P1	PS-3
PS-4	PERSONNEL TERMINATION	P1	PS-4

PS-5	PERSONNEL TRANSFER	P2	PS-5
PS-6	ACCESS AGREEMENTS	P3	PS-6
PS-7	THIRD-PARTY PERSONNEL SECURITY	P1	PS-7
PS-8	PERSONNEL SANCTIONS	P3	PS-8
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	P1	RA-1
RA-2	SECURITY CATEGORIZATION	P1	RA-2
RA-3	RISK ASSESSMENT	P1	RA-3
RA-5	VULNERABILITY SCANNING	P1	RA-5 (1) (2) (5)
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	P1	SA-1
SA-2	ALLOCATION OF RESOURCES	P1	SA-2
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	P1	SA-3
SA-4	ACQUISITION PROCESS	P1	SA-4 (1) (2) (9) (10)
SA-5	INFORMATION SYSTEM DOCUMENTATION	P2	SA-5
SA-8	SECURITY ENGINEERING PRINCIPLES	P1	SA-8
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	P1	SA-9 (2)
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	P1	SA-10
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	P1	SA-11
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	P1	SC-1
SC-2	APPLICATION PARTITIONING	P1	SC-2
SC-4	INFORMATION IN SHARED RESOURCES	P1	SC-4
SC-5	DENIAL OF SERVICE PROTECTION	P1	SC-5
SC-7	BOUNDARY PROTECTION	P1	SC-7 (3) (4) (5) (7)

SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	P1	SC-8 (1)
SC-10	NETWORK DISCONNECT	P2	SC-10
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	P1	SC-12
SC-13	CRYPTOGRAPHIC PROTECTION	P1	SC-13
SC-15	COLLABORATIVE COMPUTING DEVICES	P1	SC-15
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	P1	SC-17
SC-18	MOBILE CODE	P2	SC-18
SC-19	VOICE OVER INTERNET PROTOCOL	P1	SC-19
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	P1	SC-20
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	P1	SC-21
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	P1	SC-22
SC-23	SESSION AUTHENTICITY	P1	SC-23
SC-28	PROTECTION OF INFORMATION AT REST	P1	SC-28
SC-39	PROCESS ISOLATION	P1	SC-39
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	P1	SI-1
SI-2	FLAW REMEDIATION	P1	SI-2 (2)
SI-3	MALICIOUS CODE PROTECTION	P1	SI-3 (1) (2)
SI-4	INFORMATION SYSTEM MONITORING	P1	SI-4 (2) (4) (5)
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	P1	SI-5
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	P1	SI-7 (1) (7)
SI-8	SPAM PROTECTION	P2	SI-8 (1) (2)
SI-10	INFORMATION INPUT VALIDATION	P1	SI-10

SI-11	ERROR HANDLING	P2	SI-11
SI-12	INFORMATION HANDLING AND RETENTION	P2	SI-12
SI-16	MEMORY PROTECTION	P1	SI-16

Appendix B: Timeline of Meetings

Trail of Bits conducted eight threat modeling meetings via video conference with Voatz to help gain an understanding of the processes and architecture that are integral to the Voatz application. Most meetings were 60-90 minutes in duration and multiple members of Voatz and Trail of Bits were in attendance. These meetings were recorded for review, if needed.

2020-01-28: Meeting #1

- REDACTED

2020-01-29: Meeting #2

- REDACTED

2020-02-03: Meeting #3

- REDACTED

2020-02-05: Meeting #4

- REDACTED

2020-02-10: Meeting #5

- REDACTED

2020-02-11: Meeting #6

- REDACTED

2020-02-12: Meeting #7

- REDACTED

2020-02-14: Meeting #8

- REDACTED4