carbonhalo

Security Alignment with NIST Framework and ASD Essential 8

Introduction

We are committed to providing a secure and reliable application by implementing robust security measures that align with industry-recognised frameworks. This document outlines how our security practices correspond with the **National Institute of Standards and Technology (NIST) Cybersecurity Framework** and the **Australian Signals Directorate (ASD) Essential Eight** strategies to mitigate cybersecurity incidents.

Alignment with NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a comprehensive guideline consisting of five core functions: **Identify, Protect, Detect, Respond,** and **Recover**. Below is an evaluation of our solution against these functions.

1. Identify

Asset Management

- AWS Resource Explorer: We utilise the AWS Resource Explorer dashboard to maintain a comprehensive inventory of all operational services and assets used in our solution. This provides visibility into all deployed services and their configurations, aiding effective asset management.
- Access Control Policies: We implement strict role-based access control (RBAC) and maintain IP allowlists for sensitive areas, ensuring that only authorised personnel have access to critical systems and resources.

Understanding of Dependencies

- Cloudflare Services: While our Cloudflare resources are managed separately, we recognise their critical role in our overall security posture and ensure they are configured to meet our security needs.

Network Configuration

- MongoDB (Private Network Isolation): Our MongoDB database is hosted on a private network, accessible only via private endpoints or via trusted IP addresses. This setup reduces exposure to potential threats by isolating the database from public internet access.
- Cloud Object Store (Amazon Simple Storage Service): Our Cloud Object Store is accessible over the public internet but is restricted to authenticated access only. All interactions with the Cloud Object Store require proper authentication credentials, ensuring that only authorised services and users can access the stored data.

2. Protect

Access Control, Data Security, and Maintenance

- **HTTPS Enforcement**: All communications are encrypted using HTTPS, ensuring data in transit is secure between clients and our services.
- **Encryption at Rest**: Data stored in MongoDB and Cloud Object Store is encrypted, protecting sensitive information from unauthorised access.

- **Cloudflare Security Features**:
    - **DDoS Protection**: We utilise Cloudflare's built-in DDoS mitigation to safeguard against Distributed Denial of Service attacks.
    - **Bot Mitigation with Turnstile**: Cloudflare Turnstile helps differentiate legitimate users from bots without disrupting user experience.
    - **Web Application Firewall (WAF)**: Additional firewall rules block known attack vectors, such as SQL injection and cross-site scripting (XSS) attacks.
    - **Autoscaling with AWS Elastic Container Service**: Our backend infrastructure can scale dynamically, ensuring availability and preventing resource exhaustion.

3. Detect

Anomalies and Events, Continuous Monitoring

- **Logging and Monitoring**:
    - **Cloudflare Logs**: Detailed logs of all traffic enable us to detect suspicious activity and provide an audit trail for security analysis.
    - **Backend Logging and Monitoring**: We use AWS Cloudwatch logging and monitoring services for our backend systems. This allows us to monitor access patterns and system performance within Amazon Web Services to identify anomalies.

4. Respond

Response Planning, Mitigation

- **Incident Response Plan**: We have established procedures to address detected cybersecurity events promptly, ensuring a coordinated response to security incidents.
- **Cloudflare Automated Mitigation**:
    - **Automatic Bot Attack Mitigation**: Cloudflare utilises advanced machine learning algorithms to automatically detect and mitigate bot attacks. This includes blocking malicious bots and mitigating automated threats without manual intervention.
    - **Automatic DDoS Mitigation**: Cloudflare's network automatically absorbs and mitigates DDoS attacks at both the network and application layers, ensuring uninterrupted service availability.
    - **Real-Time Threat Intelligence**: Cloudflare continuously updates its security measures based on global threat intelligence. This enables automatic responses to emerging threats, enhancing our ability to respond swiftly to new attack vectors.
- **Cloudflare Rate Limiting**: By configuring rate limiting, we can automatically mitigate the impact of excessive requests or brute-force attempts in real time, preventing potential abuse or overload of our backend services.

5. Recover

Recovery Planning, Improvements

- **Regular Backups**: MongoDB databases are backed up daily, with encrypted backups ensuring data can be restored securely.

- **Disaster Recovery Procedures**: We have plans in place to restore services quickly in the event of an incident with an RTO of 8 hours and RPO of 24 hours.
- **Continuous Improvement**: Post-incident analyses are conducted to improve our security posture continually.

Alignment with ASD Essential Eight

The ASD Essential Eight outlines eight strategies to mitigate cybersecurity incidents. Here is how our solution aligns with each strategy.

1. Application Control

- **Access Restrictions**: We enforce strict access controls to prevent unauthorised applications from executing. Our applications run using a minimal Linux build on containers in AWS Elastic Container Service with access via Cloudflare.
- **Cloudflare Workers**: All incoming requests are proxied and controlled, reducing the risk of malicious code reaching the backend.

2. Patch Applications

- **Managed Services for Continuous Updates**: We have deliberately used managed services for both the application execution environment (AWS Elastic Container Service) and the database (MongoDB). These services provide a continuously managed and updated environment, ensuring that the underlying platforms are always up to date with the latest security patches.
- **Application Updates**: We are running a bespoke application developed by our partner ISW, which is regularly updated during application release cycles to ensure that the latest patches and security improvements are included in every build.
- **Dependency Management**: All application dependencies are regularly reviewed and updated to incorporate security patches and improvements from third-party vendors and open-source projects.

3. Configure Microsoft Office Macro Settings

- **Not Applicable:** Our application does not utilise Microsoft Office macros.

4. User Application Hardening

- **Cloudflare Web Application Firewall (WAF)**: Our application leverages Cloudflare's WAF to filter and block malicious traffic, protecting against common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). The WAF provides real-time protection by analysing and filtering requests before they reach the backend.
- **Cloudflare Content Security Policy (CSP)**: Implemented to prevent cross-site scripting (XSS) attacks, the CSP enforces a strict policy on which resources can be executed on the application, adding an additional layer of security for users by mitigating the risk of malicious content being injected.
- **Cloudflare for Edge Security**: Cloudflare is used to handle application logic and security at the edge, reducing latency while enforcing application hardening policies. This includes enforcing strict HTTPS, adding security headers (like Content-Security-

Policy, Strict-Transport-Security, etc.), and validating request integrity before they reach the backend.

- **Bot Mitigation with Turnstile**: To prevent abuse from automated scripts and bots, we utilise Cloudflare's Turnstile for bot mitigation. This feature intelligently identifies and blocks bot traffic while ensuring a smooth experience for legitimate users, thereby reducing the risk of brute-force attacks and credential stuffing.
- **Blocking Deprecated or Insecure Features**: Our application does not use deprecated or insecure web technologies like Flash, which are often targeted by attackers. We ensure our web infrastructure adheres to modern security standards, including disabling unnecessary features that could introduce vulnerabilities.
- **Rate Limiting**: Cloudflare's rate limiting features are applied to ensure that excessive requests from any single IP address are blocked, preventing brute-force attacks or abusive traffic that could overwhelm the system.

5. Restrict Administrative Privileges

- **Least Privilege Principle**: Access rights are granted based on role requirements, limiting administrative privileges to essential personnel.
- **Regular Access Reviews**: Periodic audits ensure that privileges remain appropriate over time.

6. Patch Operating Systems

- **Managed Infrastructure**: We utilise managed services for both our application execution environment (AWS Elastic Container Service) and database (MongoDB). These managed services are continuously maintained and updated by the service provider, ensuring that the underlying operating systems and infrastructure are always patched with the latest security updates.
- **Automated Updates**: As a part of these managed services, AWS automatically handles patching and updates to the underlying infrastructure, including the operating systems. This guarantees timely application of critical security patches without requiring manual intervention from our team.
- **Application Updates**: While the operating systems are managed, we also ensure that our ISW-developed application is regularly updated during application releases. This process includes incorporating the latest security patches and improvements into the application code.

7. Multi-Factor Authentication (MFA)

- **MFA for Sensitive Operations**: Access to the AWS resources is protected with MFA.

8. Daily Backups

- **Regular Data Backups**:
  - **Daily Backups**: MongoDB data is backed up daily, ensuring data can be restored in case of loss. We retain a month's worth of daily backups.
  - **Backup Compliance**: A compliance policy ensures that backup retention and frequency can only be modified by an authorised representative
  - **Encrypted Backups**: Backups are encrypted to prevent unauthorised access.