Following a structured routine for monitoring and maintaining your Cloudflare security setup provides a strong foundation for proactive threat detection and response. By regularly checking firewall events, reviewing traffic patterns, and responding swiftly to anomalies, you can significantly reduce the risk of security breaches.

Here are the tasks I do with the frequency.

Daily Tasks - Focus on active threat detection and fast response.

Check Firewall Events

- Navigate to Cloudflare > Security > Events.
- Filter by “Blocked”, “JS Challenge”, or “Captcha” actions.
- Look for spikes in blocked requests from single IPs or countries.
- Investigate newly blocked URLs or patterns.

Review Traffic Analytics

- Go to Cloudflare > Analytics > Traffic.
- Identify any anomalies in traffic patterns (sudden spikes or dips).
- Monitor top countries, top paths, and status codes.
- Log & Tag Suspicious Activity
- Maintain a log (spreadsheet or SIEM integration) of suspicious IPs, URLs, or patterns.
- Optionally tag/block known bad actors.

Alert Monitoring

- Ensure email or webhook alerts (via Cloudflare or integrations like Slack) are being received.
- Review any alerts triggered by WAF or rate limiting.

Weekly Tasks - Trend analysis and policy tuning.

- Review WAF Rules & Firewall Rules
- Evaluate top triggered WAF rules.
- Tune or add rules based on repeated behavior.
- Make use of Cloudflare’s Managed Rulesets and custom WAF rules.
- Analyze access patterns, user agents, referrers, and unusual paths.
- Update IP Lists / Threat Feeds
- Add known malicious IPs to blocklists.
- Remove false positives from blocklists/allowlists.
- Check Rate Limiting Logs
- Ensure legitimate traffic isn’t being throttled.
- Identify APIs or URLs being brute-forced or scraped.

Monthly Tasks - Comprehensive review and optimization.

Review all security settings:

- WAF status
- Bot Fight Mode
- SSL/TLS mode
- HSTS, HTTP/2, and gRPC support
- Firewall rules
- Page rules or transform rules
- Update & Document any changes improvement
- Cloudflare Logs / Analytics Deep Dive

- Examine Most targeted URLs, Top user agents, Referrer abuse, GEO targeting

User Access Audit

- Review Cloudflare dashboard access.
- Remove or modify any unused accounts or over-privileged users.