Synthetic Users Intrusion Detection & Prevention Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

1. Purpose

This policy defines how Synthetic Users detects, prevents, and responds to intrusion attempts across its network and application infrastructure.

2. Scope

This policy applies to all production and corporate systems, including cloud infrastructure, web applications, and APIs.

3. Intrusion Detection & Prevention Solutions

3.1 Network-Level Protection — Cloudflare

Synthetic Users uses **Cloudflare** as its primary network-level intrusion detection and prevention solution. Cloudflare provides:

- **Web Application Firewall (WAF):** Inspects all incoming HTTP/HTTPS traffic and blocks requests matching known attack signatures (SQL injection, XSS, RCE, etc.).

- **DDoS Protection:** Automatic detection and mitigation of volumetric and application-layer DDoS attacks.
- **Bot Management:** Identifies and blocks malicious bot traffic while allowing legitimate automated access.
- **Rate Limiting:** Enforces request rate limits to prevent abuse and brute-force attacks.
- **IP Reputation & Threat Intelligence:** Cloudflare's threat intelligence network blocks traffic from known malicious IP addresses and sources.

3.2 Infrastructure-Level Protection — AWS

- **AWS Security Groups and NACLs** act as virtual firewalls controlling inbound and outbound traffic to all compute resources.
- **Render Network Isolation** provides application-level network segmentation within the hosting platform.

3.3 Application-Level Detection

- Centralized logging captures all authentication events, API access, and data operations.
- Anomalous patterns (e.g., unusual login locations, repeated failed authentication, unexpected data access volumes) trigger alerts for security team review.

---

4. Monitoring & Alerting

Layer	Tool	Monitoring Scope
Network / Edge	Cloudflare	WAF events, DDoS mitigation, bot activity, rate limit triggers
Infrastructure	AWS Security Groups, Render	Network access violations
Application	Centralized logging (Axiom, PaperTrail)	Auth events, API access, data operations

- Security events from all layers are reviewed regularly.
- Critical alerts (active attacks, WAF blocks, DDoS events) trigger immediate notification to the security team.

---

5. Incident Response

Intrusion events are escalated per the Incident Response Plan:

1. **Detection** — Automated alerting from Cloudflare, AWS, or application logs.
2. **Containment** — Block offending IPs, revoke compromised sessions, isolate affected systems.
3. **Investigation** — Analyze logs to determine scope and impact.
4. **Remediation** — Patch vulnerabilities, update WAF rules, strengthen controls.
5. **Post-Incident Review** — Document findings and update detection rules.

---

6. Review

This policy is reviewed annually or following a significant intrusion event.