



## 24/7 Website Monitoring Audit Checklist

### 20-Point Continuous Threat Visibility Audit

- Is uptime monitoring active?
- Is homepage integrity checked?
- Are SSL expiration alerts configured?
- Are failed login attempts monitored?
- Are suspicious successful logins flagged?
- Is file integrity monitoring enabled?
- Are malware alerts active?
- Are WAF/firewall notifications reviewed?
- Are suspicious traffic bursts monitored?
- Are bot reconnaissance patterns inspected?
- Is domain reputation watched?
- Are ecommerce failed payments reviewed?
- Are suspicious orders monitored?
- Are customer account anomalies flagged?
- Do alerts reach active humans?
- Is emergency escalation documented?
- Are weekly reviews scheduled?
- Are monthly deeper reviews scheduled?
- Is alert noise tuned?
- Would a 2 AM incident be noticed quickly?

Scoring:

17–20 = Strong continuous visibility maturity

12–16 = Moderate monitoring readiness

0–11 = High delayed-discovery risk