MODEL
TECHNOLOGY SOLUTIONS

Security Checklist

Daily

01	Review: dashboards - reports - logs - alerts - threat detections - risk detections - incidents - SOC escalation tickets - admin submission details - email campaigns - automatic remediation activity	☐
02	Triage, classify, investigate, and resolve or escalate detected incidents	☐
03	Implement updates based on reviews and investigations: Release false positives from quarantine - Update tenant allow/block list - Configure tuning rules	☐

Weekly

01	Review: Threat Analytics threats & reports - Email Detection reports - Campaign Views - Top Targeted Users - Governance Logs - Emerging Threats - Tracked changes - Secure score reports and recommendations	☐
02	Perform proactive hunting for threats	☐
03	Review security platform infrastructure health: App connectors - Log connectors - Agent health - Service health - Etc.	☐
04	SOC/Security team collaboration, sync, and planning	☐
05	Implement policy, report, detection rule, workbooks, other configuration updates based on review and team collaboration	☐

Monthly

01	Review: Security policy vs. baseline - Detection overrides - Priority accounts - Policy assessments - Activity logs - File quarantines	☐
02	Review tuned alerts and update tuning as needed	☐
03	Update policies, campaigns, based on review and changes to threat landscape	☐
04	Generate security status reports	☐
05	Cybersecurity strategic planning & guidance	☐

Ad Hoc / As Needed

01	Implement updates, changes, exclusions, etc. as requested	☐
02	Incident response process testing	☐
03	Generate executive reports	☐
04	Additional Incident Response & Initiative Implementation	☐
05	Perform SCUBA assessment	☐

Reach Out With Your Questions

www.model-technology.com
(314) 254-4138
linkedin.com/company/model-technology-solutions
steve.bowman@model-technology.com