AGILEBLUE

THE AI-NATIVE SECOPS PLATFORM

Cybersecurity Readiness Review

CLIENT	ACCOUNT EXECUTIVE	IMPLEMENTATION MANAGER
CUSTOMER SUCCESS MANAGER	**TOTAL DATA SOURCES**	**LAST UPDATED**

SECTION 1

System Inventory

A complete picture of your environment enables targeted, effective protection.

TOPIC AREA	QUESTION	YES / NO	NOTES / DETAILS
Endpoints			
Endpoints	Do you use workstations and servers?	☐ Yes ☐ No	
	Do you have virtual machines?	☐ Yes ☐ No	
	Do you have Windows / Linux / Mac systems?		
	Do you have any legacy systems?	☐ Yes ☐ No	
	Do you have any OT/ICS or industrial control systems?	☐ Yes ☐ No	
Mobile / BYOD			
Mobile / BYOD	Do you use mobile devices (phones/tablets)?	☐ Yes ☐ No	
	Is there a Mobile Device Management (MDM) solution in place?	☐ Yes ☐ No	
	Do you have a BYOD policy for personal devices?	☐ Yes ☐ No	
Network			
Network	How many firewalls do you have (Host, NGFW, WAF, etc.)?		
	Are your firewalls centrally managed?	☐ Yes ☐ No	
	Is your network segmented (guest, remote offices, external)?	☐ Yes ☐ No	
	Are there any other network devices in your environment?	☐ Yes ☐ No	
	Do you have any network monitoring or IDS/IPS tools in place?	☐ Yes ☐ No	
Remote Access / VPN			
Remote Access	Do you use a VPN solution (e.g., Cisco AnyConnect, Zscaler, Citrix)?	☐ Yes ☐ No	
	Do you have any conditional access policies in place for your VPN?	☐ Yes ☐ No	
Cloud & Hosting			
Cloud	Are you running public cloud, SaaS, hybrid, or multi-cloud?		
	Are you using Azure, AWS, or GCP?	☐ Yes ☐ No	
	What M365 license tier? (Basic / Premium / E3 / E5)		
	Is Conditional Access enforced in M365 / EntraID?	☐ Yes ☐ No	
	Do you have any serverless functions, containers, or Kubernetes environments?	☐ Yes ☐ No	
Identity & Access Management (IAM)			
IAM	Are you using EntraID, Okta, or Active Directory?	☐ Yes ☐ No	
	Do you enforce MFA across all systems and endpoints?	☐ Yes ☐ No	
Applications			

SaaS Applications	Do you use third-party SaaS apps with sensitive data access (e.g., Salesforce, ServiceNow)?	☐ Yes	☐ No	
Email Security				
Email Security	Do you use an email filtering tool (e.g., Defender for O365, Proofpoint, Mimecast)?	☐ Yes	☐ No	
DNS / Web Filtering				
DNS / Web Filter	Do you use a DNS security or web filtering tool (e.g., Cisco Umbrella)?	☐ Yes	☐ No	
Security Tools				
Security Tools	Do you use an EDR tool (e.g., Microsoft Defender, CrowdStrike)?	☐ Yes	☐ No	
	Do you use a SIEM tool (e.g., Sentinel, Splunk)?	☐ Yes	☐ No	
	Do you use Antivirus (AV) tools?	☐ Yes	☐ No	
Vuln Mgmt	Do you use a vulnerability scanning tool (e.g., Tenable, Qualys)?	☐ Yes	☐ No	
	How often do you apply software and security updates?			
Third Parties, Backup & GRC				
Third Parties	Do you have external vendors with access to your environment?	☐ Yes	☐ No	
	Do you use a Managed Service Provider (MSP)?	☐ Yes	☐ No	
Backup	Do you use a backup and recovery platform (e.g., Veeam)?	☐ Yes	☐ No	
	Are backups stored offline or air-gapped?	☐ Yes	☐ No	
GRC	Do you adhere to regulatory requirements / frameworks (HIPAA, PCI-DSS, CMMC, etc.)?	☐ Yes	☐ No	

SECTION 2

Client Baseline & Behavior

Captures per-client context to reduce alert noise and enable geo-tailored detection rules.

TOPIC AREA	QUESTION	YES / NO		NOTES / DETAILS
Account Conventions	What naming convention do you use for user accounts (e.g., first.last)?			
	Who typically creates new user accounts (IT / HR / manager self-service)?			
	Approximately how many new accounts are created per month?			
Business Hours	What are your standard business hours and primary time zone?			
	Do any teams operate outside standard hours (shift workers, on-call)?	☐ Yes	☐ No	
Geography	Do you have any offices or locations outside of your headquarters?	☐ Yes	☐ No	
	In which states/cities are your employees primarily located?			
	Do employees regularly travel, and to which regions?	☐ Yes	☐ No	
	Do you have employees or contractors working from outside the US?	☐ Yes	☐ No	
	Do all remote workers connect through the same VPN?	☐ Yes	☐ No	
AD / Directory	Do you have scheduled AD sync jobs or automated account provisioning?	☐ Yes	☐ No	
Third-Party Access	Do you have any contractors or third-party vendors with access to your environment?	☐ Yes	☐ No	

High-Risk Users	Are there any known high-risk or high-privilege accounts we should be aware of?	☐ Yes ☐ No	
	Are service accounts or automated processes creating/modifying accounts?	☐ Yes ☐ No	

SECTION 3

Alert Playbook

Defines your escalation process so AgileBlue acts on threats the right way, every time.

TOPIC AREA	QUESTION	YES / NO	NOTES / DETAILS
Escalation Contacts	Primary Contact 1 — Name / Email / Phone		
	Primary Contact 2 — Name / Email / Phone		
	Primary Contact 3 — Name / Email / Phone		
Emergency Contacts	Emergency Contact 1 — Name / Phone (Priority 1)		
	Emergency Contact 2 — Name / Phone (Priority 2)		
	Emergency Contact 3 — Name / Phone (Priority 3)		
Business Hours	What are your business hours?		
	Do you expect users to be working outside of business hours?	☐ Yes ☐ No	
	Who has authority to approve suppression of recurring benign alerts?		
	Preferred communication format for cases (email / ticketing / phone)?		
Prior Incidents	Have you experienced a breach in the last three years?	☐ Yes ☐ No	
	Was there a specific event that led you to AgileBlue?		
Whitelisting	Do you have employees or contractors working from locations outside the US that we should account for?	☐ Yes ☐ No	
Prior Suppression	Were there alert types suppressed in your previous security tool? (if applicable)		
After-Hours Response	For a confirmed incident after hours, should we call immediately or wait until business hours?		
IR Relationships	Do you have an existing IR retainer or third-party IR firm on contract?	☐ Yes ☐ No	

SECTION 4

Other

Additional context that helps AgileBlue plan ahead and keep your monitoring accurate.

TOPIC AREA	QUESTION	YES / NO	NOTES / DETAILS
Future Changes	Any planned system changes or new tools in 2026–2027?		
Exclusions	Are there tools or systems to explicitly exclude from monitoring?		
	Are there log sources requiring special configuration or approval to forward?	☐ Yes ☐ No	