AGILEBLUE

THE AI POWERED SECOPS PLATFORM

Configuration & Success Blueprint

The definitive guide to a fully deployed and successful AgileBlue environment

REQUIRED	RECOMMENDED	SUPPORTED
Must be completed for full platform functionality.	*Gold standard; strongly advised for all customers.*	*Available and beneficial where applicable.*

SECTION 1

Client Scope & Environment

The full client environment must be documented before monitoring begins. Every asset category below should be confirmed, scoped, or explicitly excluded.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Endpoints		
Workstations & Servers	All physical and virtual endpoints are inventoried and enrolled in AgileBlue with the Cerulean agent deployed.	REQUIRED
Operating Systems	Windows, Linux, and Mac endpoints are documented by OS type and version, and are actively monitored by AgileBlue. Legacy systems are flagged and reviewed.	REQUIRED
OT / ICS Systems	OT/ICS systems are identified, documented, and their network segmentation from corporate IT is confirmed and reflected in AgileBlue monitoring scope.	RECOMMENDED
Network		
Network Segmentation	Network zones are documented and the segmentation architecture is confirmed, ensuring AgileBlue monitoring reflects accurate network topology.	RECOMMENDED
Remote Access / VPN	VPN solution is identified, conditional access policies are documented, and VPN authentication logs are ingested by AgileBlue.	RECOMMENDED
Cloud & Identity		
Cloud Platforms	Cloud environments in use (Azure, AWS, GCP) are confirmed and integrated with AgileBlue. Hybrid connectivity is documented.	RECOMMENDED
Identity Platform	IAM solution (EntraID, Okta, or Active Directory) is confirmed, integrated with AgileBlue, and user provisioning processes are documented.	REQUIRED
Containers / Serverless	Containerized or cloud-native environments are identified and, where applicable, scoped into AgileBlue monitoring.	SUPPORTED
Applications & Security Tooling		
SIEM / Log Aggregation	Existing SIEM or log aggregation tools are documented to ensure AgileBlue ingestion does not duplicate or conflict with existing pipelines.	SUPPORTED
Vulnerability Scanning	Vulnerability scanning tool is confirmed and integrated where applicable. Patch management cadence is documented and reflected in risk scoring.	RECOMMENDED
SaaS Applications	Third-party SaaS applications with sensitive data access are identified and, where integrations exist, logs are forwarded to AgileBlue.	RECOMMENDED
Compliance & Third Parties		

Regulatory Frameworks	Applicable compliance frameworks (HIPAA, PCI-DSS, CMMC, SOC 2, etc.) are confirmed and documented within the AgileBlue platform.	REQUIRED
Third-Party Vendors	External vendors with environment access are identified and their access scope is documented and monitored within AgileBlue.	RECOMMENDED
Managed Service Provider	MSP role, access level, and responsibilities are clearly defined and reflected in AgileBlue platform permissions and escalation paths.	RECOMMENDED
Backup & Recovery	Backup platform is confirmed, offline or air-gapped backup status is documented, and backup processes are excluded from false-positive triggering rules in AgileBlue.	RECOMMENDED

SECTION 2

Integrations & Log Sources

Every data source below represents a visibility layer. Missing integrations create blind spots. All applicable sources must be confirmed active and ingesting data into the AgileBlue platform.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Endpoint Log Sources		
Cerulean Agent	Cerulean agent is deployed on all in-scope workstations and servers and is actively forwarding endpoint telemetry to AgileBlue — including process execution, network connections, file activity, and registry changes.	REQUIRED
Third-Party EDR Integration	API integration is active for the existing EDR platform. Alerts and detections are confirmed ingesting into AgileBlue.	RECOMMENDED
Network Log Sources		
Firewall Logs	Firewall traffic logs are actively forwarded to AgileBlue. Vendor, model, and log verbosity level are confirmed.	REQUIRED
VPN / Remote Access Logs	VPN authentication and session logs are forwarded to and ingested by AgileBlue. Known VPN exit IPs are documented for geo-detection baselining.	RECOMMENDED
IDS / IPS Logs	IDS/IPS logs are ingested by AgileBlue where the tool is present.	SUPPORTED
Identity & Directory Log Sources		
Active Directory / EntraID	AD/EntraID authentication events, account changes, group policy events, and admin activity are ingested by AgileBlue.	REQUIRED
Okta / SSO Platform	Okta SSO login events, MFA activity, and application access logs are ingested by AgileBlue where applicable.	RECOMMENDED
Cloud Platform Log Sources		
AWS CloudTrail	AWS CloudTrail logs are forwarded to AgileBlue where AWS is in use. API activity, access events, and configuration changes are confirmed ingesting.	RECOMMENDED
Azure Monitor / Sentinel	Azure Monitor activity logs are forwarded to and ingested by AgileBlue where Azure is in use.	RECOMMENDED
GCP Logging	GCP audit logs are forwarded to and ingested by AgileBlue where GCP is in use.	SUPPORTED
Email & DNS Log Sources		

Email Security Platform	Email security platform logs (Defender for O365, Proofpoint, or Mimecast) are forwarded to and confirmed ingesting into AgileBlue.	RECOMMENDED
DNS Security Platform	DNS query and threat logs from Cisco Umbrella or equivalent are forwarded to and ingested by AgileBlue.	SUPPORTED

SECTION 3

Agent Deployment

The Cerulean agent is AgileBlue's proprietary endpoint agent. Deployment model determines the depth of visibility and containment capability available to the SOC.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Deployment Model		
Cerulean Agent Only	Cerulean is the sole EDR on all endpoints. Full behavioral detection, telemetry collection, and device containment are active within AgileBlue.	RECOMMENDED
External EDR + Cerulean	Cerulean is deployed alongside the existing EDR. Cerulean forwards telemetry to AgileBlue while the third-party EDR handles active protection. Both are ingesting into AgileBlue.	RECOMMENDED
No Cerulean Agent	Where Cerulean cannot be deployed, third-party EDR API integration is active and ingesting into AgileBlue. Visibility limitations are documented and the business justification is on file.	SUPPORTED
Deployment Completeness		
Multi-EDR Review	Any endpoint running more than one EDR solution has been reviewed, conflicts resolved, and the configuration documented in AgileBlue.	RECOMMENDED
OIC / Undeployed Systems	Any system not yet enrolled in AgileBlue is tracked with an assigned owner, documented justification, and a confirmed target deployment date.	REQUIRED

SECTION 4

Response Actions

AgileBlue offers four response models. Every customer must have a response model configured. Escalation Only and Disabled configurations leave the SOC unable to act on confirmed threats.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Response Model Selection		
Manual Response	Manual Response is configured in AgileBlue. The SOC performs containment actions on confirmed threats following analyst review before any action is taken.	RECOMMENDED
Hybrid Response	Hybrid Response is configured in AgileBlue. Critical servers are set to Manual or Escalation Only. Workstations are enrolled in automated response policy.	RECOMMENDED
Automated Response (Sapphire AI)	Sapphire AI automated response is configured in AgileBlue for applicable workstations. Automated containment triggers on high-confidence confirmed threats.	RECOMMENDED
Playbook Configuration		
Per-Customer Playbooks	Per-customer response playbooks are defined and documented in AgileBlue. Playbooks are reviewed and updated quarterly.	REQUIRED

Automated Response Scope	Systems enrolled in AgileBlue automated response policy are documented. Critical infrastructure is explicitly excluded from automated containment.	RECOMMENDED
Playbook Quarterly Review	AgileBlue playbooks are reviewed quarterly and updated whenever significant environment changes occur.	RECOMMENDED

SECTION 5

Tuning & Exceptions

Alert tuning is the difference between a SOC that adds value and one that generates noise. All customers require active tuning from onboarding and on an ongoing basis.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Rule Exceptions		
Initial Tuning Complete	Rule exceptions are configured in AgileBlue during onboarding. All known-benign alerts are suppressed with documented business justification.	REQUIRED
Suppression Log Maintained	All suppressions in AgileBlue are documented with a business justification, an assigned owner, and a scheduled review date.	RECOMMENDED
Endpoint Exceptions (Cerulean Active EDR Only)		
Business-Critical App Exceptions	Business-critical applications that interact with endpoint controls have exceptions configured in AgileBlue to prevent false blocking.	RECOMMENDED
Backup Agent Exceptions	Backup agent processes are excluded from ransomware behavioral detection rules in AgileBlue to prevent false positives.	RECOMMENDED
RMM / Remote Management Tools	Approved remote management tools (RMM agents, remote access software) are excluded from AgileBlue endpoint blocking rules.	RECOMMENDED
Allow & Block Lists (Cerulean Active EDR Only)		
Allow List Configured	An allow list of approved applications and processes is configured in AgileBlue and reviewed whenever new applications are deployed.	RECOMMENDED
Block List Configured	A block list of known-malicious and unauthorized applications is active in AgileBlue and reviewed monthly.	RECOMMENDED

SECTION 6

M365 Security

Microsoft 365 is the primary attack vector across all industries. Full M365 visibility requires both integrations active and the Assessment module running quarterly.

ITEM	CONFIGURATION REQUIREMENT	STATUS
M365 Integrations		
Office 365 Integration Active	The Office 365 integration is connected and confirmed ingesting into AgileBlue — covering Unified Audit Log, Exchange, SharePoint, Teams, and identity telemetry.	REQUIRED
M365 Defender Integration Active	The M365 Defender integration is connected and confirmed ingesting into AgileBlue — covering Defender alerts, phishing detections, and XDR incident correlation.	REQUIRED

Both Integrations Confirmed Healthy	Both O365 and M365 Defender integrations are confirmed healthy and ingesting in AgileBlue. Neither integration alone provides full M365 visibility.	REQUIRED
M365 Assessment Module		
Initial Assessment Run	The AgileBlue M365 Assessment module is run at onboarding. Findings are reviewed with the customer within 5 business days and a remediation plan is produced.	RECOMMENDED
Quarterly Assessment Cadence	The AgileBlue M365 Assessment is scheduled to run quarterly. The recurring cadence is confirmed and agreed with the customer.	RECOMMENDED
Critical Findings Remediated	Critical and High severity findings from the AgileBlue M365 Assessment are remediated within 30 days of the assessment date.	RECOMMENDED
Remediation Plan Documented	A remediation plan is produced following each AgileBlue M365 Assessment, with assigned owners and target completion dates for each finding.	RECOMMENDED
M365 Configuration Baseline		
MFA Enforcement	MFA is enforced across all users and admin accounts. This is confirmed and tracked through the AgileBlue M365 Assessment module.	REQUIRED
Conditional Access Policies	Conditional Access policies are configured and enforced in M365. Coverage is reviewed and validated through the AgileBlue M365 Assessment.	RECOMMENDED
Legacy Authentication Disabled	Legacy authentication protocols are disabled in M365, preventing MFA bypass. This is validated through the AgileBlue M365 Assessment.	RECOMMENDED
Mailbox Forwarding Rules Monitored	External mailbox forwarding rules are flagged as a high-priority indicator of account compromise and monitored within AgileBlue.	RECOMMENDED
Admin Role Assignments Reviewed	Admin role assignments and privilege scope are reviewed, minimized, and validated through the AgileBlue M365 Assessment.	RECOMMENDED

SECTION 7

Communication Expectations

Both AgileBlue and the client have defined responsibilities. Clear communication expectations prevent delays during incidents and ensure the relationship functions effectively.

ITEM	CONFIGURATION REQUIREMENT	STATUS
AgileBlue Responsibilities		
Case Delivery	AgileBlue delivers all confirmed cases through the SecOps Platform with analyst notes, evidence, severity rating, and recommended actions.	REQUIRED
Escalation Notification	AgileBlue notifies designated client contacts via the agreed channel whenever a case requires client action or decision.	REQUIRED
After-Hours Escalation	AgileBlue calls designated emergency contacts in documented priority order for confirmed incidents that occur outside business hours.	REQUIRED
Tuning Recommendations	The AgileBlue SOC proactively surfaces tuning recommendations to reduce alert noise and continuously improve detection quality.	RECOMMENDED
Quarterly Business Review	AgileBlue delivers a Quarterly Business Review covering platform health, alert trends, gap analysis, and configuration recommendations.	RECOMMENDED
Client Responsibilities		

Primary Contacts Designated	The client designates a minimum of 1 primary contact (3 recommended) for day-to-day case communication. Contacts are kept current in the AgileBlue platform.	REQUIRED
Emergency Contacts Designated	The client designates 3 emergency contacts in priority order for after-hours escalation. Phone numbers are confirmed and documented in AgileBlue.	REQUIRED
Suppression Authority Designated	The client designates a named individual with authority to approve alert suppressions in AgileBlue. Name and role are documented.	REQUIRED
Environment Change Notification	The client notifies AgileBlue in advance of significant environment changes — new tools, acquisitions, or restructuring — so monitoring scope can be updated.	RECOMMENDED
Maintenance Window Notification	The client notifies AgileBlue of all scheduled maintenance windows, patch cycles, and disaster recovery tests to prevent false escalations.	RECOMMENDED
Pen Test Pre-Notification	The client notifies AgileBlue before any penetration test or red team exercise. Failure to do so may result in the activity being escalated as a real incident.	REQUIRED
Communication Channels		
Ticketing Integration	The client ticketing system (ServiceNow, Jira, etc.) is integrated with AgileBlue where applicable, enabling case creation and tracking within existing workflows.	SUPPORTED

SECTION 8

Escalation Playbooks

Escalation playbooks define exactly how AgileBlue and the client respond to confirmed threats. Every item below must be defined per customer and reviewed quarterly.

ITEM	CONFIGURATION REQUIREMENT	STATUS
Incident Response Workflow		
Case Creation Process	The AgileBlue SOC creates a case on confirmed malicious activity. Every case includes analyst notes, supporting evidence, severity rating, and a recommended action for the client.	REQUIRED
Client Notification Process	The client is notified via the agreed channel. Notification includes a case summary, severity level, and the specific action AgileBlue recommends the client take.	REQUIRED
Containment Actions Defined	For Manual, Hybrid, and Automated response models, containment actions (device isolation, account disablement) are defined per playbook and executed by the AgileBlue SOC.	REQUIRED
Remediation Handoff Process	Following containment by AgileBlue, remediation is handed to the client. The client is responsible for root cause analysis, system recovery, and follow-up reporting.	REQUIRED
Escalation Thresholds		
After-Hours Call Protocol	The after-hours call protocol is defined and documented in AgileBlue: for a confirmed incident outside business hours, the SOC either calls immediately or holds until business hours per the client's instruction.	REQUIRED
Critical Asset Escalation	Critical assets (servers, executive devices, finance systems) are defined in the AgileBlue playbook with elevated escalation priority configured.	RECOMMENDED
Business Hours Documented	Client business hours and time zone are confirmed and documented in AgileBlue. The after-hours window is explicitly defined.	REQUIRED

Noise Management		
Baseline Exceptions Documented	Known legitimate activity patterns are documented in AgileBlue — including offshore employees, after-hours workers, service accounts, and automated processes — to prevent false escalations.	REQUIRED
Scheduled Jobs / Maintenance	Regular maintenance windows, patch cycles, backup jobs, and automated scripts are documented in AgileBlue and excluded from alert triggering to prevent false positives.	REQUIRED
Whitelisted Locations / IPs	Known legitimate geographic locations and IP ranges are documented in AgileBlue for geo-detection baselining.	RECOMMENDED
Previous Suppressions Carried Over	Alert suppressions from any previous security tools are reviewed, documented, and carried over into AgileBlue where the business justification applies.	RECOMMENDED