AgentSOC on Azure – Solution Document

1. Solution Overview

AgentSOC is an Azure-native, GenAI-powered system designed to detect, analyze, and respond to security threats autonomously. Built on a multi-agent architecture, it enables organizations to protect cloud environments like **AWS** and **Azure** from real-time threats such as **privilege escalation**, **unauthorized access**, and **misconfigurations** — even during off-hours. AgentSOC acts as a 24x7 intelligent SOC assistant that automates triage, response, containment, and analyst support, while ensuring observability, security, and human oversight.

2. Problem Statement

Modern cloud environments face growing challenges in threat detection and incident response, including:

- Delayed response to high-risk actions (e.g., privilege escalation)
- Analyst fatigue from constant alert triage
- Lack of proactive policy enforcement during off-hours
- Manual investigations consuming valuable security team bandwidth
- Difficulty in maintaining an audit trail for auto-responses and overrides

AgentSOC addresses these gaps by introducing real-time automation across the SOC workflow, with full transparency and human override capabilities.

3. Solution Detail

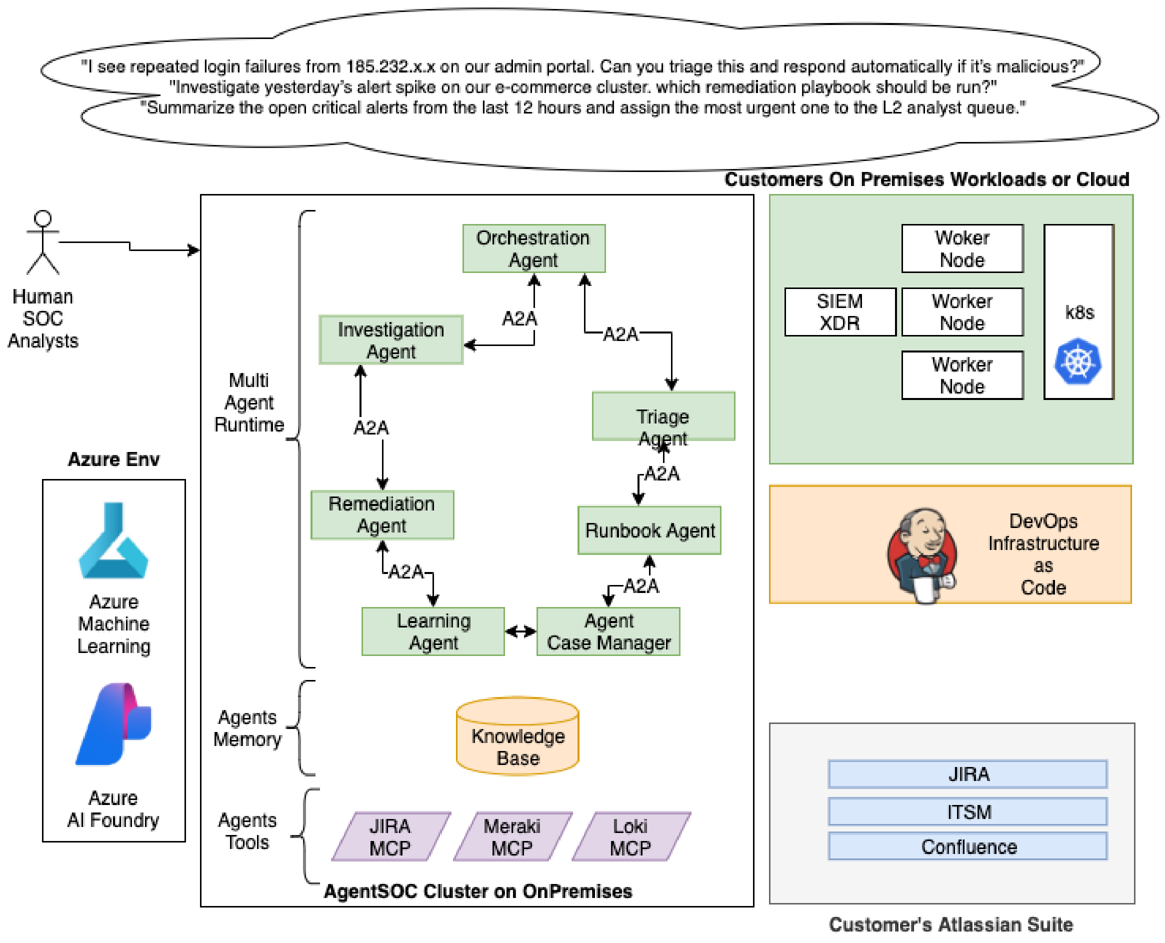
AgentSOC is composed of multiple modular agents, each responsible for a distinct SOC function. These agents are coordinated by a central decision-making entity (Main SOC

Agent). The solution leverages Azure-native services to run, orchestrate, and monitor the full incident response lifecycle.

Key agents include:

- **Triage Agent** – Parses events, enriches context using HR and security metadata.
- **Investigation Agent** – Performs root cause and impact analysis.
- **Containment Agent** – Blocks or revokes access in real-time based on policy outcomes.
- **Runbook Agent** – Selects appropriate response actions using past patterns.
- **Case Management Agent** – Logs incidents, enables analyst reviews, and manages overrides.
- **Learning Agent** – Records outcomes and tunes decision models based on analyst feedback.

4. Technical Architecture



"I see repeated login failures from 185.232.x.x on our admin portal. Can you triage this and respond automatically if it's malicious?"
"Investigate yesterday's alert spike on our e-commerce cluster. which remediation playbook should be run?"
"Summarize the open critical alerts from the last 12 hours and assign the most urgent one to the L2 analyst queue."

The architecture includes the following layers:

- **User Interaction Layer**: SOC dashboard or SIEM/ITSM integration for ticket and review workflows
- **Orchestration Layer**: Main SOC Agent coordinating specialized agents via Azure Kubernetes Service (AKS)
- **Agent Execution Layer**: Containerized agents handling detection, triage, investigation, and response
- **Memory & Decision Layer**: Cosmos DB, Redis, Azure AI Search for enrichment and recall
- **Observability & Compliance Layer**: Azure Monitor, Prompt Flow, and Responsible AI services for tracking and fairness

5. Key Components

- **Main SOC Agent**: Oversees decision-making and agent coordination
- **Remote Agents**:
  - Triage Agent
  - Investigation Agent
  - Containment Agent
  - Runbook Agent
  - Case Management Agent
  - Learning Agent
- **Context Memory**: Stores user profiles, policies, and prior decisions
- **Security Event Ingestion**: From AWS CloudTrail, Azure Activity Logs, and EventBridge

6. Integration Points

- **AWS**: CloudTrail, IAM, EventBridge, GuardDuty
- **Azure**: Activity Logs, Defender for Cloud, Azure AD
- **SIEM Platforms**: Sentinel, Splunk, QRadar
- **ITSM Tools**: ServiceNow, Jira for case creation and analyst workflows
- **HRIS Systems**: For employee metadata (tenure, designation)

7. Use Cases

- Privilege escalation detection and containment
- Off-hours autonomous response
- Access governance for interns, contractors, and third parties
- Analyst co-pilot for security case reviews
- Policy enforcement with human-in-the-loop overrides

8. Customer Pain Points Addressed

- Missed or delayed response to critical threats
- Lack of contextual awareness in access reviews
- Analyst fatigue due to repetitive triage tasks
- Risky access granted without sufficient oversight
- Inability to capture learnings from incident outcomes

9. Industry-Specific Applications

- **Finance**: Blocking unauthorized access to production accounts
- **Healthcare**: Enforcing minimum tenure policies for access to PII
- **Retail**: Protecting cloud supply chain systems from rogue elevation
- **Technology**: Securing multi-cloud CI/CD environments during escalated builds

10. Sample Customer Journey

Scenario: An intern requests admin access on AWS at midnight.

1. Request is approved by an admin in IAM.
2. AgentSOC receives the access grant event.
3. Triage Agent evaluates the request against HR data.
4. Main SOC Agent scores the risk and decides it's unsafe.
5. Containment Agent revokes the access in seconds.
6. A dashboard entry is created for analyst review.
7. The next morning, the SOC analyst overrides the block, justifying the need.
8. Learning Agent records this as a false positive to improve future scoring.

11. Technical Requirements

- Azure subscription with AKS, Cosmos DB, Redis, Azure OpenAI

- Access to AWS or Azure audit logs (e.g., CloudTrail, Defender for Cloud)
- SIEM or ITSM integration for ticket workflows
- EventBridge or Azure Event Grid configured for real-time event routing

12. Security Architecture

- Authentication via Azure AD and cloud-native RBAC
- Private networking using VNets and Private Link
- Data protection with encryption at rest/in-transit
- Observability via Azure Monitor and Application Insights
- Responsible AI compliance for decision-making transparency

13. Performance Considerations

- Sub-minute response time for containment
- Asynchronous investigation and enrichment pipelines
- Memory-first design to avoid redundant triage
- Scalable across thousands of alerts per hour using AKS

14. Tools and Azure Services Used

- Azure Kubernetes Service (AKS)
- Azure OpenAI + Prompt Flow
- Cosmos DB, Azure Redis, Azure AI Search
- Azure Monitor, Application Insights
- Azure AD, Private Link, Defender for Cloud

15. Users of AgentSOC

- SOC Analysts
- Cloud Security Engineers
- IT Administrators
- Compliance and Governance Officers
- CISOs / Risk Officers (for dashboard visibility)

16. Dependencies

- CloudTrail and IAM access from AWS accounts
- Agent prompt logic pre-defined for access events
- SIEM and ITSM integration APIs available
- Reliable HR system integration for context enrichment

17. Key Benefits and Differentiators

- Real-time automated containment with full traceability
- Context-aware decisioning using HR + access metadata
- Human-in-the-loop workflows with audit trails
- Continuous learning from analyst feedback
- Modular agent system with Azure-native scalability

18. Value Proposition

AgentSOC empowers enterprises to modernize their SOC operations through automation, intelligent decision-making, and secure agent-based orchestration. It enables organizations to minimize risk, respond faster, and enforce access policies — even when human analysts are offline.

19. Conclusion

AgentSOC is a transformative solution that redefines incident response for the cloud era. By blending AI-driven automation, human oversight, and deep integration with Azure and AWS ecosystems, it delivers faster, smarter, and safer security outcomes.