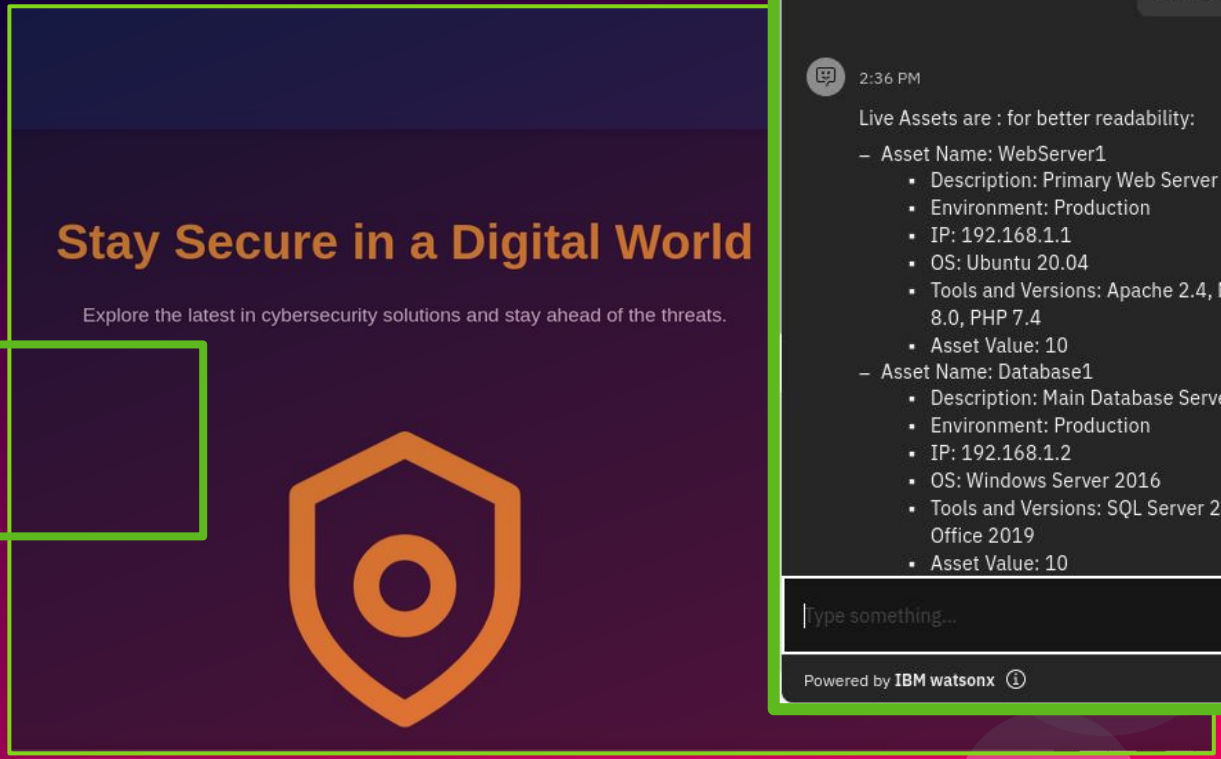
Team : NeeON

Candidate:
Balasubramaniam Sridar (Sri)
hello@sridarsri.com

Solution : SecAAI
Security Analysis Assistant

IBM Cloud

lab lab ai



Problem : **Increasing Cyber Attacks**

Targeted to address for challenges in following domains;

Domain 1. Lack of proper security operations at SOCs(Security Operations Centers) / MSSPs

Domain 2. Lack of infosec expertise in organizations / General SMLE

IBM Cloud

lab lab ai

SecAAI

Solution : Knowledge gaining and applying on the go!

SecAAI
v1

Your Virtual Security Analyst!

IBM Cloud

lab lab ai

Market Scope : For Cyber Security Solution

Category	Market Value	Sources
IT Skills Gap	- Global cybersecurity market projected to grow from $202 billion (2022) to $433 billion (2030), CAGR: ~9.4%.	- ISC² Cybersecurity Workforce Study - Grand View Research
Increasing Cyber Attacks	- Cybercrime costs expected to reach $10.5 trillion annually by 2025, indicating a strong demand for innovative solutions.	- IBM Cost of a Data Breach Report - Cybersecurity Ventures
SMEs and Information Security	- SMEs contribute to a significant market, with the SME cybersecurity market projected to reach $25 billion by 2027.	- MarketsandMarkets - Statista
The Definite Demand	- Total Addressable Market (TAM) for AI-driven cybersecurity solutions is estimated at over $50 billion globally, with significant growth potential.	- Allied Market Research - Deloitte Cyber AI Market Insights

Disclaimer: The above analysis is based on available data and projections. Actual market conditions may vary.

IBM Cloud

lab lab ai

SecAAI

Market Scope : **TAM, SAM and SecAAI Target**

Total Addressable Market (TAM) and Serviceable Addressable Market (SAM) with SecAAI Targets

Market Segment	TAM (2030) ($ Billion)	SAM (2030) ($ Billion)	SecAAI Target Market (%)	SecAAI Potential Revenue (2030) ($ Million)
AI in Cybersecurity	101.5	15	0.1	100.0
SME Cybersecurity	9	2.25	0.1	10.0
Vulnerability Management	25.1	3.8	0.1	30.0
Threat Intelligence	20	2	0.1	20.0
Total	155.6	23.05	-	160.0

Disclaimer: The above analysis is based on available data and projections. Actual market conditions may vary.

IBM Cloud

lab lab ai

SecAAI

Revenue Stream

Revenue Streams	Target Audience	Benefits
Subscription-Based Licensing	SMEs, Enterprises, MSSPs	Predictable recurring revenue, customer loyalty
Pay-As-You-Go Model	Cost-sensitive SMEs or startups	Attract cost-sensitive customers, scalable based on demand
AI-Powered Managed Security Services	SMEs and startups lacking in-house teams	Higher-value contracts, opportunity for upselling
Custom Integrations and API Access	Enterprises with complex IT infrastructures	Generates additional revenue from customization, fosters partnerships
Training and Consulting Services	SMEs, Enterprises, Educational Institutions	Expands market reach, positions SecAAI as a thought leader
Partner Ecosystem Revenue	Large enterprises, cloud providers, cybersecurity vendors	Access to broader customer base via partnerships

IBM Cloud

lab lab ai

SecAAI

Competitors and SecAAI

Competitor	Strengths	Weaknesses	Opportunity for SecAAI
Microsoft Security Copilot	Integrates with Microsoft tools	AI-powered insights.	Expensive, tied to Microsoft ecosystem, Platform-agnostic conversational AI.
Splunk AI Assistant	Strong SIEM integration	data analytics.	Focuses on logs, lacks conversational depth, Interactive conversational interface.
ChatGPT Plugins	Accessible and customizable generative AI.	Needs customization	lacks security context, Purpose-built for cybersecurity.
Palo Alto Networks	AI-driven threat detection and response.	Not conversational	complex and costly. Simplify with conversational AI.

IBM Cloud

lab lab ai

SecAAI

Strengths and Weaknesses

Strengths	Weaknesses
Conversational AI	Limited brand recognition
Easy to use	Generative AI risks.
Affordable	Complexity in configuration
Scalable	Not matured
Platform independent	

Unique Selling Proposition (USP)

Feature	Description
Conversational Intelligence	Simplifies complex analysis with natural language.
Platform Agnosticism	Works across diverse ecosystems.
Proactive Insights	AI-driven threat detection and recommendations.
Accessibility for SMEs	Affordable for SMEs and startups.
Knowledge Base Integration	Grows and retrieves from historical data.
Ease of Use	Minimal training User-friendly.

IBM Cloud

lab lab ai

SecAAI

Next Steps/Backlog – Domain 2 - General SMLE

Category	Task	Description	Year
Complete Vulnerability Management	Asset Inventory Management	Build a centralized system to track and manage discovered assets. CRUD.	2025
Complete Vulnerability Management	Automated Asset Discovery	Discover IT assets across the organization automatically.	2025
Complete Vulnerability Management	Querying Reputed Threat Intels	Integrate threat intelligence providers for risk prioritization.	2025
Complete Vulnerability Management	Automated Log Analysis	Incorporate automated log analysis for detecting anomalies.	2025
Complete Vulnerability Management	Integrate Active Scanning Tools	Add integration with active vulnerability scanning tools.	2025
Complete Vulnerability Management	Automated Scripting for Enumerations	Automate enumeration processes with scripting capabilities.	2025
SOAR/SIEM Plugin	Extend integration with SOAR/SIEM platforms	Streamline workflows by integrating with SOAR/SIEM platforms.	2026
Multi Tenant Support	Add multi-tenancy support for MSSPs	Support multiple clients using a single SecAAI instance.	2026

IBM Cloud

lab lab ai

SecAAI

Next Steps/Backlog – Domain 1 - SOC & MSSP

Category	Task	Description	Year
Threat Hunting	Develop AI-powered threat-hunting capabilities	Proactively identify and mitigate risks within networks.	2026
Threat Hunting	Introduce anomaly detection mechanisms	Detect unknown threats using machine learning models.	2026
Threat Hunting	Create interactive dashboards for threat visualization	Visualize threat-hunting data using interactive dashboards.	2026
Incident Response Lifecycle	Build a full-fledged incident response framework	Framework includes detection, categorization, and resolution.	2027
Incident Response Lifecycle	Incorporate workflows for automated evidence collection	Preserve evidence with automated workflows.	2027
Incident Response Lifecycle	Enable post-incident reporting and lessons learned analysis	Generate insights from post-incident reporting and analysis.	2027/28
Incident Response Lifecycle	Automated incident triaging and root cause analysis	Triage incidents and analyze root causes with automation.	2027/28
Knowledge Base(KB) Population and Retrieval	Automate knowledge base population and categorization	Automate collection of incident details and solutions.	2028
KB Population and Retrieval	Enable quick and accurate knowledge retrieval	Retrieve relevant knowledge quickly during incidents.	2028
KB Population and Retrieval	Use AI to recommend actionable steps based on stored knowledge	Recommend actionable steps using AI-driven insights.	2029
Compliance/Regulations	Develop compliance automation for industry standards	Automate compliance reporting for GDPR, HIPAA, and PCI DSS.	2029
UEBA	Introduce tools for user behavior analysis	Detect insider threats through user behavior analysis.	2029

IBM Cloud

lab lab ai

SecAAI

Demo：**Let run and see!**

IBM Cloud

lab lab ai

SecAAI