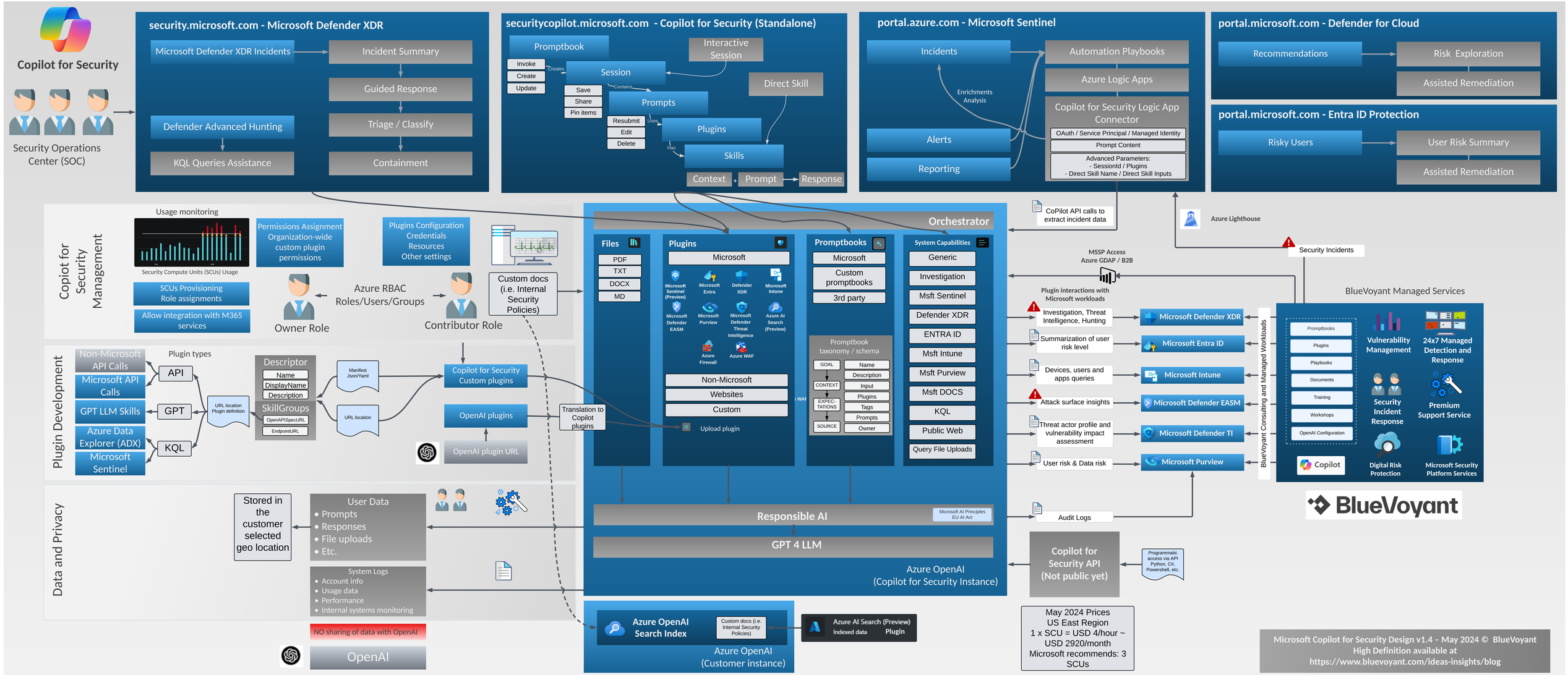
Copilot for Security
Security Operations Center (SOC)
security.microsoft.com - Microsoft Defender XDR
Microsoft Defender XDR Incidents
Incident Summary
Guided Response
Defender Advanced Hunting
Triage / Classify
KQL Queries Assistance
Containment
securitycopilot.microsoft.com - Copilot for Security (Standalone)
Promptbook
Invoke
Create
Update
Creates
Interactive Session
Session
Save
Share
Pin items
Contains
Direct Skill
Prompts
Resubmit
Edit
Delete
Uses
Plugins
Has
Skills
Context
+
Prompt
Response
portal.azure.com - Microsoft Sentinel
Incidents
Automation Playbooks
Azure Logic Apps
Enrichments Analysis
Copilot for Security Logic App Connector
OAuth / Service Principal / Managed Identity
Prompt Content
Advanced Parameters:
- SessionId / Plugins
- Direct Skill Name / Direct Skill Inputs
Alerts
Reporting
portal.microsoft.com - Defender for Cloud
Recommendations
Risk Exploration
Assisted Remediation
portal.microsoft.com - Entra ID Protection
Risky Users
User Risk Summary
Assisted Remediation
Copilot for Security Management
Usage monitoring
Security Compute Units (SCUs) Usage
SCUs Provisioning
Role assignments
Allow integration with M365 services
Permissions Assignment
Organization-wide custom plugin permissions
Plugins Configuration
Credentials
Resources
Other settings
Azure RBAC
Roles/Users/Groups
Owner Role
Contributor Role
Custom docs (i.e. Internal Security Policies)
Plugin Development
Plugin types
Non-Microsoft API Calls
Microsoft API Calls
GPT LLM Skills
Azure Data Explorer (ADX)
Microsoft Sentinel
API
GPT
KQL
URL location
Plugin definition
Descriptor
Name
DisplayName
Description
SkillGroups
OpenAPISpecURL
EndpointURL
Manifest Json/Yaml
URL location
Copilot for Security Custom plugins
OpenAI plugins
OpenAI plugin URL
Translation to Copilot plugins
Data and Privacy
Stored in the customer selected geo location
User Data
• Prompts
• Responses
• File uploads
• Etc.
System Logs
• Account info
• Usage data
• Performance
• Internal systems monitoring
NO sharing of data with OpenAI
OpenAI
Orchestrator
Files
PDF
TXT
DOCX
MD
Plugins
Microsoft
Microsoft Sentinel (Preview)
Microsoft Entra
Defender XDR
Microsoft Intune
Microsoft Defender EASM
Microsoft Purview
Microsoft Defender Threat Intelligence
Azure AI Search (Preview)
Azure Firewall
Azure WAF
Non-Microsoft
Websites
Custom
Upload plugin
Promptbooks
Microsoft
Custom promptbooks
3rd party
Promptbook taxonomy / schema
GOAL
CONTEXT
EXPECTATIONS
SOURCE
Name
Description
Input
Plugins
Tags
Prompts
Owner
System Capabilities
Generic
Investigation
Msft Sentinel
Defender XDR
ENTRA ID
Msft Intune
Msft Purview
Msft DOCS
KQL
Public Web
Query File Uploads
Responsible AI
Microsoft AI Principles
EU AI Act
GPT 4 LLM
Azure OpenAI
(Copilot for Security Instance)
Azure OpenAI Search Index
Custom docs (i.e. Internal Security Policies)
Azure OpenAI
(Customer instance)
Azure AI Search (Preview)
Indexed data
Plugin
CoPilot API calls to extract incident data
Azure Lighthouse
Security Incidents
MSSP Access
Azure GDAP / B2B
Plugin interactions with Microsoft workloads
Investigation, Threat Intelligence, Hunting
Summarization of user risk level
Devices, users and apps queries
Attack surface insights
Threat actor profile and vulnerability impact assessment
User risk & Data risk
Microsoft Defender XDR
Microsoft Entra ID
Microsoft Intune
Microsoft Defender EASM
Microsoft Defender TI
Microsoft Purview
Audit Logs
Copilot for Security API
(Not public yet)
Programmatic access via API
Python, C#, Powershell, etc.
May 2024 Prices
US East Region
1 x SCU = USD 4/hour ~ USD 2920/month
Microsoft recommends: 3 SCUs
BlueVoyant Managed Services
BlueVoyant Consulting and Managed Workloads
Promptbooks
Plugins
Playbooks
Documents
Training
Workshops
OpenAI Configuration
Copilot
Vulnerability Management
24x7 Managed Detection and Response
Security Incident Response
Premium Support Service
Digital Risk Protection
Microsoft Security Platform Services
BlueVoyant
Microsoft Copilot for Security Design v1.4 – May 2024 © BlueVoyant
High Definition available at
https://www.bluevoyant.com/ideas-insights/blog