404.COMMUNITY
<TECH_COMMUNITY_FOUND />

> We connect people, encourage knowledge sharing, and promote professional growth within Israel's technology ecosystem.

// CORE_VALUES

Practitioner-First
Real-world experience over marketing fluff.

Vendor-Neutral
Unbiased technology discussions.

Open Access
Welcoming all skill levels, from juniors to experts.

DOMAIN_FOCUS [R/W]

- Cloud
- Security
- AI
- Code

EXECUTION_FORMAT [EXE]

Meetups // Networking & Lectures

Hands-on Labs // Practical Skills

Real-world Talks // Case Studies

Live Demos // Technical Deep Dives

```
user@guest:~$ join --force https://www.meetup.com/404community/
```

ELLI SHLOMO

Security Research

Guardz.

ID_VERIFIED

CONNECT_PROTOCOL:

/in/elishlomo

SYSTEM_STATS [R/O]

EXPERIENCE

25+ Yrs

RECOGNITION

Microsoft Security MVP

KERNEL_MODULES [LOADED]

- Information Security
- DevSecOps
- Cloud Security
- Detection Engineering
- Identity Defense
- SOC Automation

COMMUNITY_ROLE:

404.Community Advocate

LOG_OUTPUT [PUBLIC]

RECENT_PUBLICATIONS:

Offensive Security

Cloud Security Research

Defending through Offensive thinking

Building an AI-Driven SOC with Sentinel MCP

> Autonomous defense is the future. Learn how to combine AI with expert oversight to triage alerts and investigate threats.

SYSTEM_DIAGNOSTICS [CRITICAL]

⚠ ERROR: Alert_Fatigue_Detected

⚠ WARN: Log_Noise_Level > MAX

> Solution_Patch: Deploying_AI_Assisted_Triage...

AGENDA_SEQUENCE [01-04]

1. Fundamentals of Sentinel MCP
2. Configuration & Data Ingestion
3. Contextual Data Exploration
4. AI-Assisted Investigation

ACCESS_GROUPS [USERS]

- Defenders
- SOC Analysts
- Researchers
- Managers

> Requirement: Interest in AI Ops

EXPECTED_OUTPUT [SUCCESS]

- ✓ Understand Sentinel MCP architecture
- ✓ Explore data in a controlled environment
- ✓ Witness AI-assisted triage in action
- ✓ Start using Vie Hunting

ℹ SCOPE_LOCK: Fundamentals++ Only. (Adv. Hunting/Forensics/Copilot = Future_Events)

// SECTION_02

AI & SOC

From Noise to Insight

Automating the Future of Defense

CONTEXT_ANALYSIS

⚠Why It Matters Now

Alert volumes and attacker automation have finally outpaced human scale. Traditional triage is no longer sustainable.

> ERROR: Human_Capacity_Exceeded
> ACTION: Initiate_Autonomous_Defense

MODULE_MANIFEST

In This Section

- The Core SOC Challenges
- Where AI Fits Today (Reality vs. Hype)
- How Human Defender Roles Evolve

root@404.community:~/analysis/soc_gaps# cat report.log

AI + SOC: CHALLENGES, GAPS, REALITY

// ANALYZING_CORE_OPERATIONAL_BOTTLENECKS

ALERT OVERLOAD

[CHALLENGE]

10,000+ daily alerts overwhelm human capacity, leading to fatigue and missed threats.

[AI_SOLUTION]

Autonomous investigation in 3-10 minutes. 90% faster processing processing speed.

24/7 VIGILANCE

[CHALLENGE]

Human fatigue and off-hours gaps create windows of vulnerability vulnerability for attackers.

[AI_SOLUTION]

Continuous, sleepless coverage. No degradation in quality during quality during night shifts.

SLOW RESPONSE

[CHALLENGE]

Manual triage and data gathering delay MTTR/MTTC, increasing dwell time.

[AI_SOLUTION]

Automates first-pass investigation & enrichment instantly upon alert alert ingestion.

SKILLS SHORTAGE

[CHALLENGE]

Limited senior analyst capacity; junior staff struggle with complex context.

[AI_SOLUTION]

Operationalizes expert playbooks and boosts junior analyst analyst capabilities.

FALSE POSITIVES

[CHALLENGE]

~67% of analyst time is wasted chasing noise and benign anomalies.

[AI_SOLUTION]

Intelligent filtering and noise reduction focuses humans on real risk. real risk.

TOOL SILOS

[CHALLENGE]

"Swivel-chair" investigations across disconnected UIs slow down correlation.

[AI_SOLUTION]

Integrates via API across SIEM, EDR, and Cloud to correlate correlate context seamlessly.

90% REDUCTION IN MTTC	**100%** TIER-1 ALERT AUTOMATION	**10X** ALERT HANDLING CAPACITY

THE AI SOC BOOM IS REAL

...But The Work Started Long Before The Buzz

REF: FORBES / TONY BRADLEY

SYS.CONTEXT [WHY_NOW]

> "Security operations is one of the few places AI has moved has moved beyond promise to production."

// DRIVERS_FOR_ADOPTION

High-Volume, Repetitive Data

Time-Critical Decisions

Zero Margin for Error

Centralized, Federated, Distributed, Edge

The "Old Model" broke when alert volumes exceeded human human scale.

OP.EVOLUTION [SHIFT]

PHASE 1: ASSISTANCE

Enrichment & Playbooks

Tools helped analysts investigate.

PHASE 2: AUTONOMY

Handling Volume

AI handles defined workflows autonomously.

90%

FASTER INVESTIGATIONS

HUMAN.IMPACT

WAS	NOW
Alert Chaser	**Strategist**

"If people don't have to do the boring stuff, they can go deeper." deeper."

MARKET.REALITY

Enterprises prioritize STABILITY & SCALE over novelty.

// SECTION_03

MCP
+
VIBE
+
NL2KQL

Supercharging Threat Hunting

Connecting AI, Tools, and Human Intuition

CONTEXT_ANALYSIS

⚡Why Now?

We're moving beyond chat. It's time to connect AI to real tools and data (MCP), turn (MCP), turn expert instincts into guided hunts (Vibe Hunting), and remove the KQL the KQL barrier with natural language (NL2KQL).

> GOAL: Practical patterns & workflows you can use today
> ROLE: Humans decide, AI accelerates

MODULE_MANIFEST

In This Section

MCP: "USB-C for AI" integrations to data & tools

Vibe Hunting: Conversational, hypothesis-driven loops

NL2KQL: Natural Language → KQL in Defender/Sentinel

MODEL CONTEXT PROTOCOL (MCP)

> The "USB-C for AI Applications"

WHAT_IS_IT?

An open-source standard for connecting AI assistants to external systems. Like a universal port, it enables LLMs to access Data Sources (files, DBs), Tools (search, execution), and Workflows securely.

CAPABILITIES_MANIFEST

- Personal Agents Access Google Calendar Calendar & Notion directly.
- Claude Code Generate full web apps from Figma Figma designs.
- Enterprise Chat Query multiple internal internal SQL DBs via chat.
- Physical Control Control Blender for 3D printing workflows.

SECURITY_OPS_RELEVANCE: Creates standardized connectors to SIEM, EDR, Threat Intel, and Intel, and Ticketing systems—enabling agents to perform unified investigations.

STAKEHOLDER_IMPACT

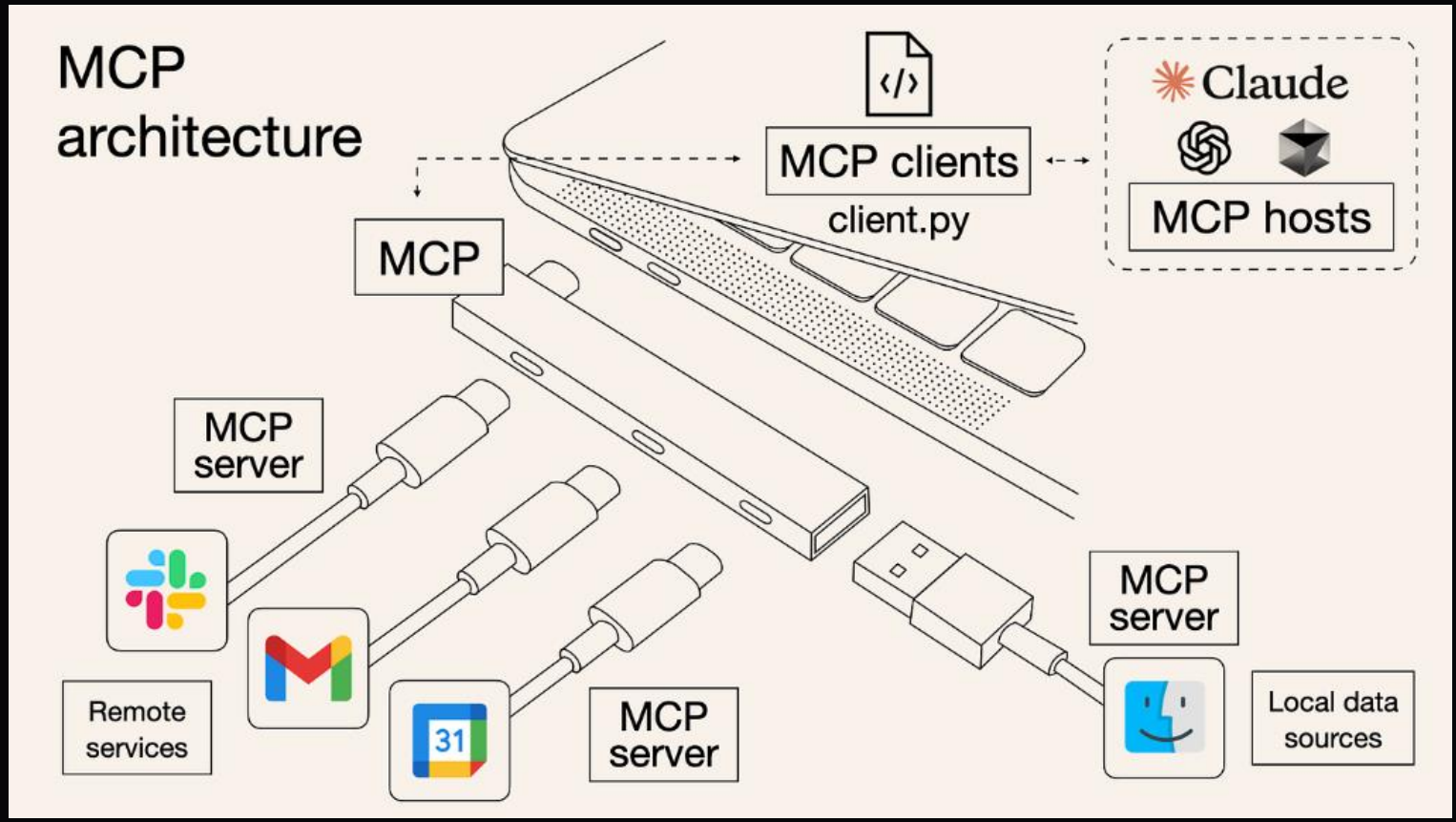
[DEVELOPERS] Drastically reduces integration complexity. Build once, connect to any MCP-compliant AI client. Faster build times.

[AI_APPLICATIONS] Instant access to a massive ecosystem of tools and data and data without custom integrations for each service.

[ADMIN] More capable assistants that can actually "do" things, accessing your specific data and taking authorized actions.

MCP USB-C DIAGRAM

> Visualizing the "USB-C" Connection Layer



VIBE HUNTING

> AI-Augmented Threat Hunting Workflow

VISION: HUMAN + AI LOOP

DEFINITION

Applying LLMs to the hunt loop in a conversational way. Not replacing the hunter, but removing the DSL barrier and "chair-swivel" toil.

> GOAL: Make hunting accessible & strategic.

THE_ANALOGY

TONY STARK
Decides & Judges

+

JARVIS
Accelerates & Scaffolds

THE_VIBE_LOOP

HYPOTHESIS
Prompt-based, natural language

QUERY
AI translates to DSL/KQL

RESULTS
Raw telemetry retrieval

ENRICHMENT
Fused context (TI + Assets)

DECISION
Human validation

KEY CAPABILITIES

- Prompt-based hypothesis mapped to ATT&CK
- Feedback loops with synthetic data validation
- Fused context (Docs + SIEM + Threat Intel)

GUARDRAILS

Manage hallucinations, privacy & permissions via:

Scoped Access | Validation

MINUTES

VS HOURS OF TOIL

Lateral Movement ID

NL2KQL

> From Natural Language to Executable Kusto Query Language

REF: arXiv:2404.02933

[PROBLEM]

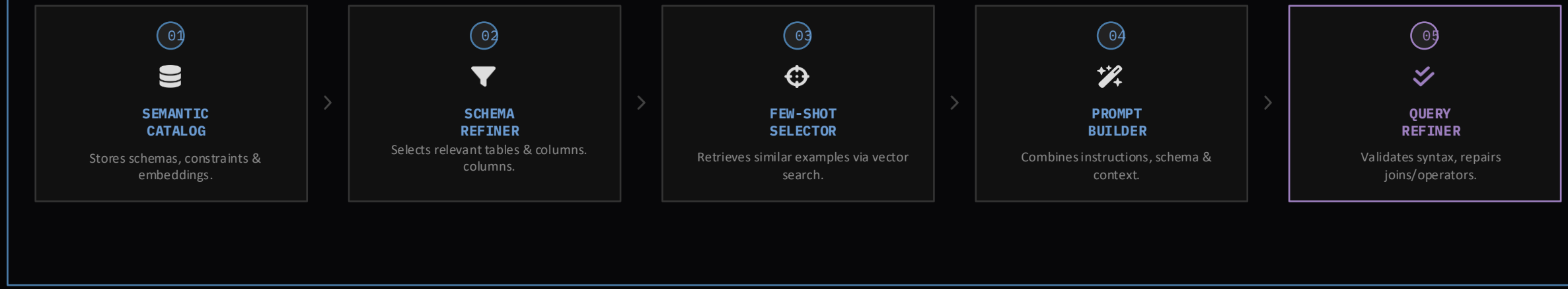
KQL is powerful but unforgiving. Syntax errors, complex schema knowledge, and logic gaps slow down critical slow down critical investigations.

[SOLUTION]

LLM-powered translation framework that converts analyst intent into syntactically perfect KQL using schema-using schema-aware context.

INPUT: "Show failed logins from 10.0.0.5"

OUTPUT: SecurityEvent | where EventID == 4625...



OPERATIONAL_IMPACT

- ✓Accelerate Time-to-Insight
- ✓Democratize Hunting (Low Code)
- ✓Reduce Syntax Errors
- ✓Future-Ready Schema Adaptability

AVAILABILITY & RESOURCES

AVAILABLE IN: Defender XDR (Advanced Hunting) & Security Copilot (Standalone).

⚠ Note: Review generated queries before execution.

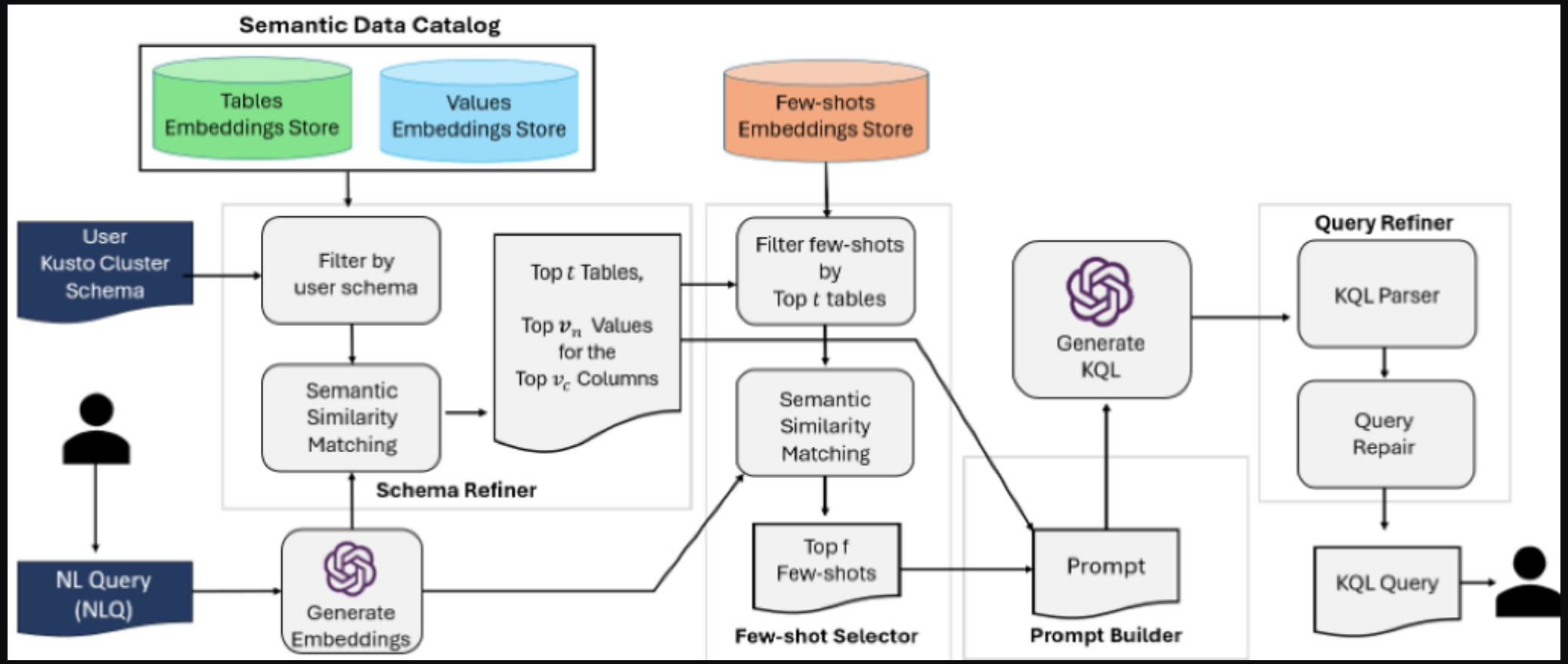
github.com/microsoft/NL2KQL

NL2KQL ARCHITECTURE

> Natural Language to KQL Translation Flow

FMT: PNG

RES: HIGH



// QUERYING_KNOWLEDGE_BASE...

WHAT IS MICROSOFT SENTINEL'S SUPPORT FOR MCP?

Bridging AI Agents & Enterprise Security Data

DEFINITION

Native Integration

Microsoft Sentinel now introduces native support for MCP, enabling a unified, hosted interface for AI-driven security operations.

> STATUS: Unified_Server_Interface_Active
> TARGET: Natural_Language_Security_Ops

SECTION_MANIFEST

What We Will Cover

- Unified Hosted Interface (No Infra Needed)
- Scenario-Focused Security Tools
- Accelerated Agent Development

MICROSOFT SENTINEL + MCP

> Unified, Hosted AI Security Operations

SYSTEM_OVERVIEW

Sentinel introduces MCP support via hosted, unified MCP server interfaces secured with Microsoft Entra. It enables scenario-focused, natural-language tools over the Data Lake & Defender, accelerating effective security agent development and context-rich data integration.

MCP_ARCHITECTURE_COMPONENTS

MCP HOST

The AI application (e.g., Visual Studio Code) that coordinates and manages clients. manages clients.

MCP CLIENT

Maintains secure connection to the server; handles context exchange for the host. host.

MCP SERVER

Provides context and tools (Sentinel Data/Defender) to clients via unified interface. interface.

IDENTITY_PROVIDER: **MICROSOFT ENTRA ID**

ENABLED_SCENARIOS

DATA_EXPLORATION

Interactively explore long-term security data using using natural language queries without needing needing KQL expertise.

ENTITY_ENRICHMENT

Analyze and enrich entities (URLs, users, IPs) across across all fragmented security data sources with a with a single click.

AGENT_BUILDING

Build Security Copilot agents by describing describing intent in natural language, automating playbooks efficiently.

TRIAGE_&_HUNTING

Prioritize incidents and hunt for threats using integrated AI tools that reduce risk exposure and and dwell time.

Sentinel MCP — Client Integrations

> COMPATIBLE MCP HOSTS

Visual Studio Code
IDE-based Agent Context

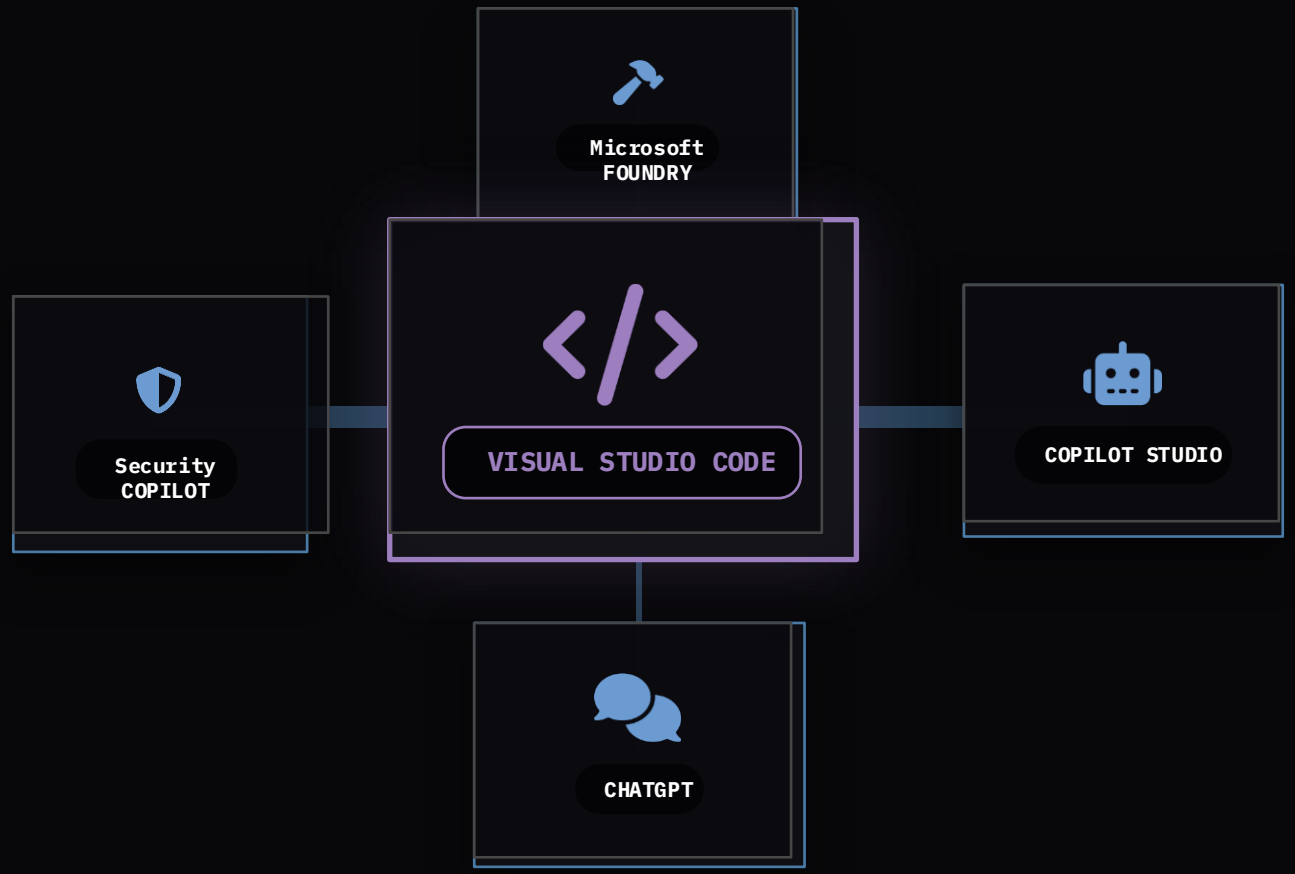
Security Copilot
Native SOC AI Assistant

Microsoft Foundry
Custom AI App Building

Copilot Studio
Low-code Agent Creation

ChatGPT
OpenAI Model Integration

Connect any MCP-compliant client



// SECTION_04

MCP, VS CODE & SENTINEL

Hands-on Implementation Guide

From Setup to Triage Execution

SCOPE_DEFINITION

Operational Readiness

Bridge the gap between theory and practice. We will configure the VS Code Code environment, connect to Sentinel, and execute real-world security tasks using tasks using the MCP framework.

> CHECK: Client_Compatibility... OK
> INITIATE: Tool_Collection_Import

EXECUTION_PLAN

XS

Implementation Steps

- Configuring VS Code as an MCP Client
- Exploring Sentinel's Tool Collections
- Applying Tools to Data Exploration & Triage

VS CODE + SENTINEL MCP SETUP

> Configuration Sequence: 5 Steps to Operational Status

STEP_01

Initialize Server

Open Command Palette with Ctrl+Shift+P. Select: MCP: Add Server Type: HTTP / SSE

STEP_02

Configure Connection

Enter the Sentinel Tool Collection URL provided in the the documentation. Assign ID: Sentinel_MCP

STEP_03

Define Scope

Choose availability scope: Current Workspace All Workspaces Workspaces (Global)

STEP_04

Authenticate

When prompted, allow authentication via Microsoft Entra Entra ID. *Requires 'Security Reader' role minimum.

STEP_05 // VERIFICATION

Verify Integration

Confirm the toolset is loaded in the Chat interface.

View > Chat > Agent Mode

```
> [INFO] Configure Tools icon visible under MCP Server
> [SUCCESS] Sentinel Collection Loaded
```

SYSTEM_NOTE: Ensure Visual Studio Code is updated to the latest version. This setup supports both official Microsoft Sentinel collections and custom tool definitions.

SENTINEL MCP TOOL COLLECTIONS

> Ready-to-use security toolsets for your AI agents

DATA_EXPLORATION

Explore security data lake naturally without complex complex KQL.

- Search tables semantic catalog
- Query data lake directly
- Entity analyzer (Users/URLs)

`https://sentinel.microsoft.com/mcp/data-exploration`

AGENT_CREATION

Build robust Security Copilot agents for complex tasks. tasks.

- Complex workflow automation
- Multi-step reasoning
- Guided agent building

`https://sentinel.microsoft.com/mcp/security-copilot-agent-creation`

TRIAGE_&_HUNTING

Rapid incident prioritization and threat hunting.

- Incident & Alert management
- Threat hunting operations
- Evidence collection

`https://sentinel.microsoft.com/mcp/triage`

CUSTOM_TOOL_SUPPORT: Enable agents to reason over your saved KQL queries and advanced hunting logic for tailored workflows.

DOCS: learn.microsoft.com/.../sentinel-mcp-tools-overview

DATA EXPLORATION COLLECTION

> CORE_TOOL_DEFINITION

API ENDPOINT

https://sentinel.microsoft.com/mcp/data-exploration

search_tables

Semantic search on table catalog to identify schema definitions.

query_lake

Execute KQL queries against Sentinel Data Lake to retrieve retrieve raw results.

list_sentinel_workspaces

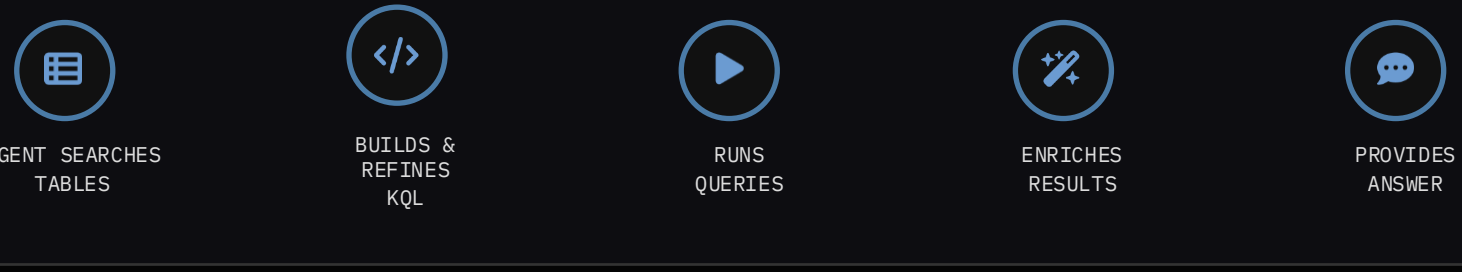
Enumerate all accessible workspace names and IDs. IDs.

Entity analyzer (Preview)

Deep analysis of entities without manual query construction.

- analyze_user_entity
- analyze_url_entity

EXECUTION_PIPELINE



>_SAMPLE_INPUT_PATTERNS

```
> "Top 3 risky users and why"
    # Invokes analyze_user_entity + query_lake
> "Signin failures last 24h"
    # Generates KQL: SigninLogs | where ResultType != 0 ...
> "Devices with abnormal outbound connections"
    # Correlates DeviceNetworkEvents via search_tables
```

TRIAGE & HUNTING COLLECTION

> INCIDENT_RESPONSE_OPS

API ENDPOINT
https://sentinel.microsoft.com/mcp/triage

INCIDENT MANAGEMENT

- ListIncidents
- GetIncidentById
- ListAlerts / GetAlertByID

ADVANCED HUNTING

- FetchAdvancedHuntingTables
- RunAdvancedHuntingQuery

DEFENDER ASSETS

- GetDefenderFileInfo / Stats
- GetDefenderIpAlerts / Stats
- GetDefenderMachine*
- ListDefenderIndicators

>_SAMPLE_INTERACTION_LOG

> "List last 5 incidents and pick most urgent"

→Calls ListIncidents(top=5) → Analyzes Severity/Status

> "Provide alerts for Incident-1234 and analyze evidence"

→Calls GetIncidentById(1234, includeAlerts=true) → Reasons over evidence

> "Hunt which users interacted with MaliciousEntity.exe"

→Builds KQL via FetchSchema → RunAdvancedHuntingQuery(DeviceFileEvents | where FileName...)

⚠OPERATIONAL_CONSTRAINTS

SYSTEM RESTRICTIONS

Home Tenant Only
No cross-tenant / delegated access

Workspace Scoping
Single workspace context

No Data Lake Query
Use Data Exploration collection instead

BILLING MODELS

Data Lake Tools

PAY-PER-QUERY

MCP server interface offered at no extra cost.

Billed per KQL data retrieval execution

Entity Analyzer

HYBRID MODEL

AI compute reasoning is FREE.

Billed only for underlying KQL queries

Triage Tools

INCLUDED

No additional cost for tools using existing API access.

Requires valid product onboarding/license

SYSTEM QUOTAS & LIMITS

STREAMING TIMEOUT	QUERY WINDOW
120 sec	800 chars
ENTITY ANALYZER	**DEFENDER HUNTING**
100 runs/hr	STD quotas

REGIONAL AVAILABILITY

US US	GB UK	EU EU	CA CA
AU AU	JP JP	IN IN	NO NO
CH CH	SEA		

SUPPORTED LANGUAGE

English Prompts Only

SYSTEM OPTIMIZATION

Prompt Specificity

Avoid generic queries. Always specify the target context to context to reduce latency and errors.

```
Use 'list_sentinel_workspaces'
```

```
Prompt: "Use workspaceId: X..."
```

Client Compatibility

MCP protocol updates frequently. Ensure your client (VS Code) is Code) is running the latest version.

```
Check: Update Release Notes
```

Tool Selection

For complex logic, avoid overlapping tools. Guide the agent to use agent to use specific toolsets for specific tasks (e.g., Data Exploration Exploration vs Triage).

COMMON ISSUES & FIXES

SYMPTOM	RESOLUTION PATH
Tools Not Called	Reduce overlapping tools in active collection Pick a more capable reasoning model (GPT-4o) Start a new chat session to clear context Verify product onboarding (Defender/Sentinel)
HTTP 404 (VS Code)	Remove MCP Server config → Restart VS Code → Add Server Verify account has access to the Data Lake workspace
Wrong Tenant Auth	Add header to MCP config: x-mcp-client-tenant-id Ensure authentication uses Home Tenant account

VS Code Debug View

Export Chat logs as JSON to analyze prompt routing.

Browser HAR Capture

Use DevTools to capture network traffic for custom tool API errors.

INITIAL CONFIGURATION

> VS Code Environment Setup: Adding the MCP Server

STEP_01

Open Command Palette

Access the global command menu in Visual Studio Code. Shortcut: Ctrl + Shift + P

STEP_02

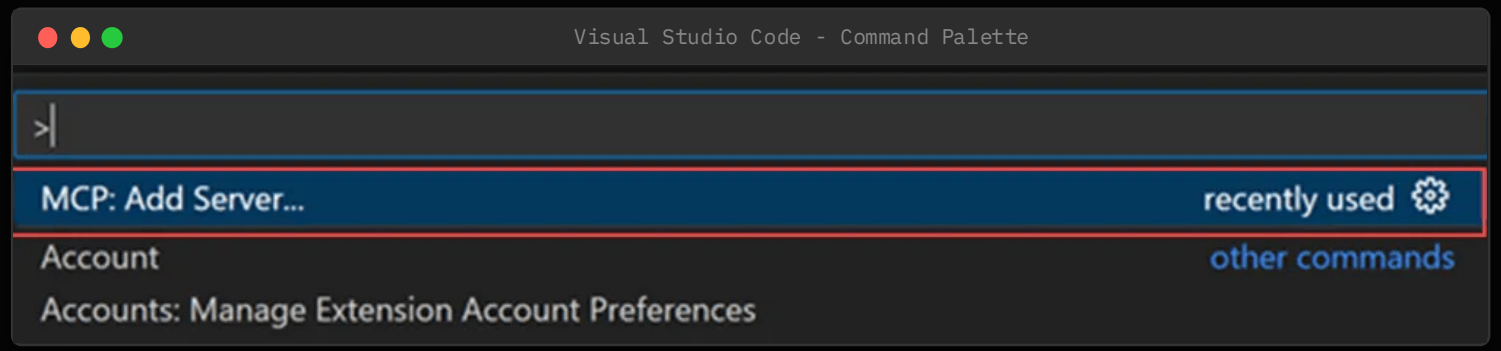
Execute Command

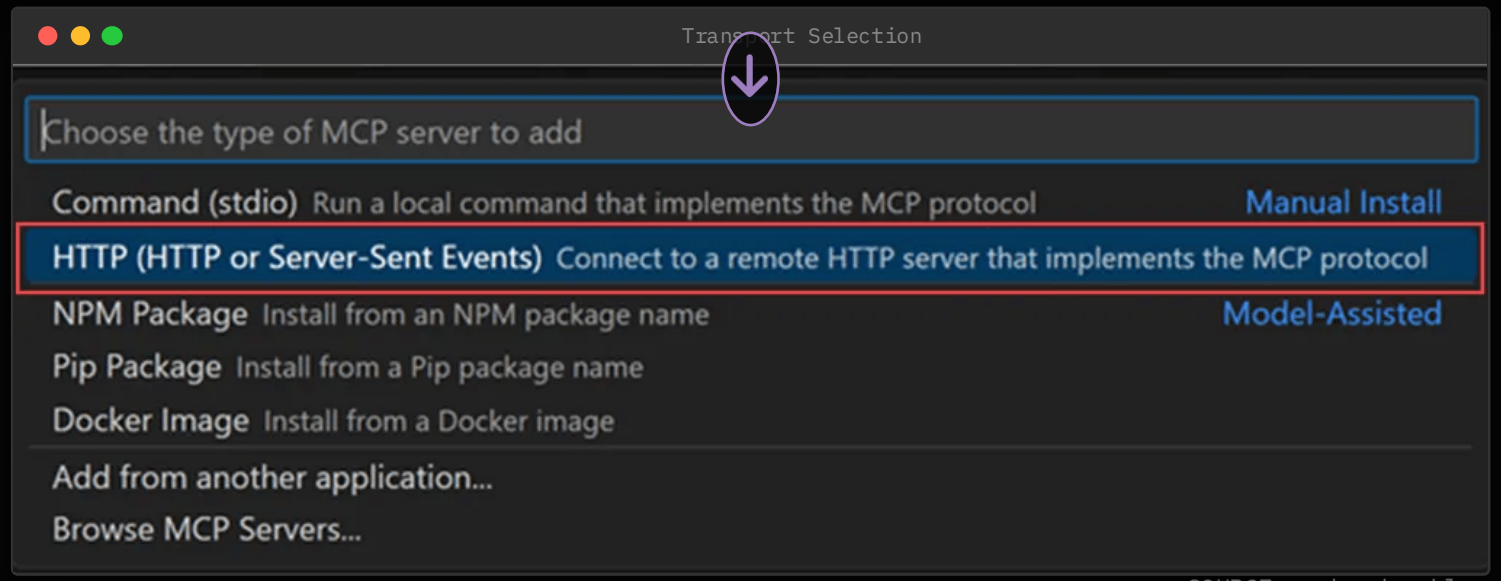
Type and select the server addition command. Input: MCP: Add Server Server

STEP_03

Select Transport

Choose the communication protocol for the MCP connection. Select: Select: HTTP (HTTP or Server-Sent Events)





> SOURCE: cyberdom.blog

IDP TRUST ANCHOR

Entra ID acts as the trust anchor and choke point. Every action action the MCP agent takes is decided here.

```
> Auth_Decision = Entra_ID
> Scope_Control = Entra_ID
> Audit_Trail = Entra_ID
```

NON-HUMAN PRINCIPALS

1. App Registration Uses application permissions. permissions. High privilege, broad scope.

2. System-Assigned MI Tied directly to compute resource lifecycle. Safer.

3. User-Assigned MI Portable identity reused reused across workloads. Risk of lateral movement.

*OAuth tokens represent the **Agent**, not a human user*

SCOPE CHALLENGES

Permissions are not session-scoped or intent-aware. aware.

`Log Analytics Reader` `Sentinel Contributor` `Directory.Read.All`

Once granted, every token inherits the full authority regardless of the specific workflow context.

CA LIMITATIONS

CA evaluates only at token issuance.

- Built for human sign-ins, not machines.
- Workload identities often exempted.
- No construct for "Hunt but don't Operationalize".

CRITICAL RISK: TOKEN LIFETIME

MCP agents cache tokens aggressively to reduce latency. Entra latency. Entra ID permits this without strict rotation enforcement for workloads.

STOLEN TOKEN IMPACT

A stolen access token provides a clean, low-noise foothold that foothold that mimics legitimate automation perfectly.

MODEL SELECTION — AGENT MODE

> Configuring AI Backend for VS Code Agent

FMT: PNG | RES: HIGH | CTX: GPT-5.1

FILENAME: model_selection.png

ZOOM: 100%

root@event:~/session# shutdown -h now

STATUS: COMPLETED // EXIT_CODE: 0

THANK YOU

PRESENTATION_COMPLETED_SUCCESSFULLY

Q&A SESSION

The floor is now open for questions, technical discussions, and implementation scenarios.

```
guest@404:~$ ask_question
> Listening for input...
```

404.COMMUNITY

Connect people, share knowledge, grow together. together. Join our next event!

meetup.com/404community

404.community

SPEAKER

Elli Shlomo

Security Research
Microsoft MVP

linkedin.com/in/elishlomo

STAY CURIOUS // STAY SECURE // KEEP LEARNING