

Chatbots to AgentOps:

From Conversational Tools to Autonomous NOC Agents

Presented by

Dadepo Aderemi | www.dedasense.com

Imagine it's 2 a.m.
and you get 30 alerts - hijack
suspected, prefix disappeared!

You open five tabs -
WHOIS, RIPEstat, PeeringDB...

Every second counts - the
longer the issue goes
unresolved (if it's real), the
greater the potential damage.



The Real Problem: No Quick Overview

The hardest part isn't
collecting data - it's making
sense of it fast.



Imagine it's 2 a.m.
and you get 30 alerts — hijack
suspected, prefix disappeared!

You open five tabs —
WHOIS, RIPEstat, PeeringDB...

But what if we have a way to
get an incidence report with
actionable items before you
even open your laptop?



<https://easy-peasy.ai/>

Can AI help?

Chatbot: the good, the bad and the ugly



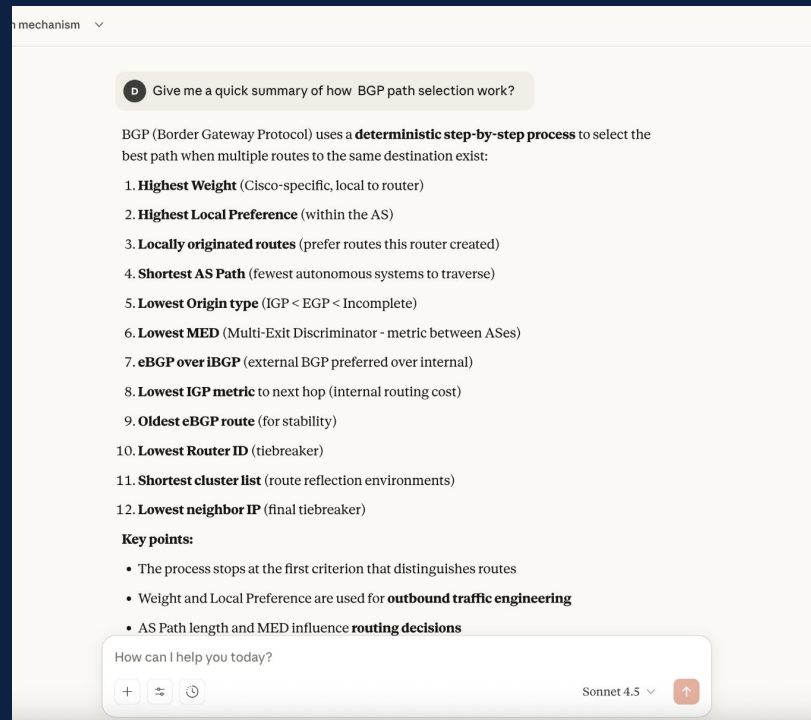
Smart. Helpful.
Sometimes confidently wrong.

Chatbots: The Good

Natural language interface
easy access to information
without complex queries

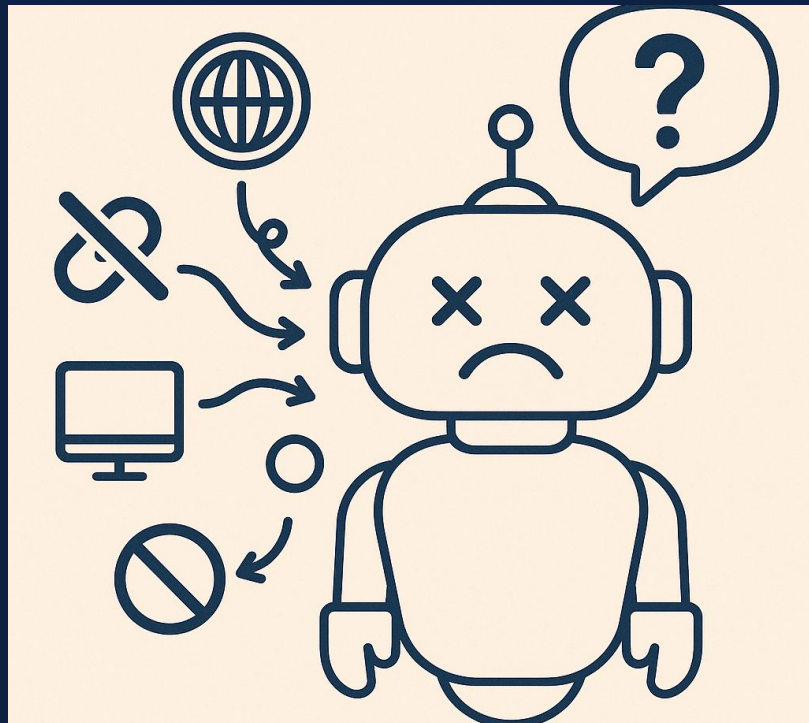
Great for knowledge recall
"What is RPKI?", "How does BGP
path selection work?"

Great at summaries



Chatbots: The Bad

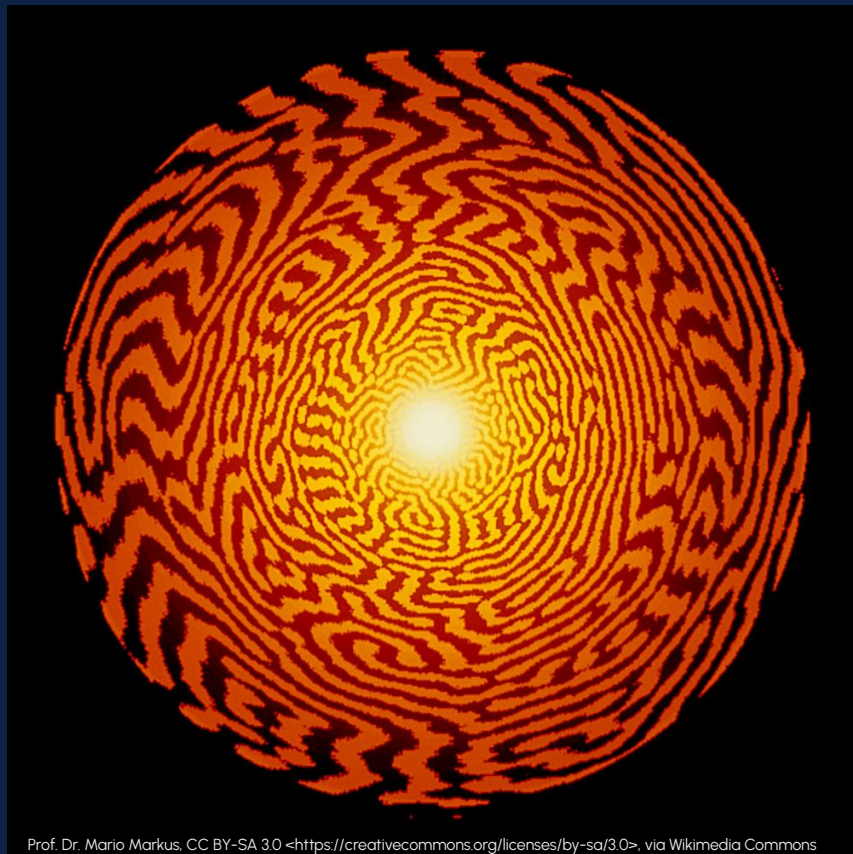
- No real-time information*
- No domain specific context
- No integration with NOC tools
- No actions, can't enrich, triage, or propose workflows
- No autonomy



Chatbots: The Ugly

Hallucinations.

Confident but wrong and
totally made up answers,
especially dangerous in
NOC/ops context



Prof. Dr. Mario Markus, CC BY-SA 3.0 <<https://creativecommons.org/licenses/by-sa/3.0/>>, via Wikimedia Commons

BREAKING | BUSINESS

Judge Fines Two Lawyers For Using Fake Cases From ChatGPT

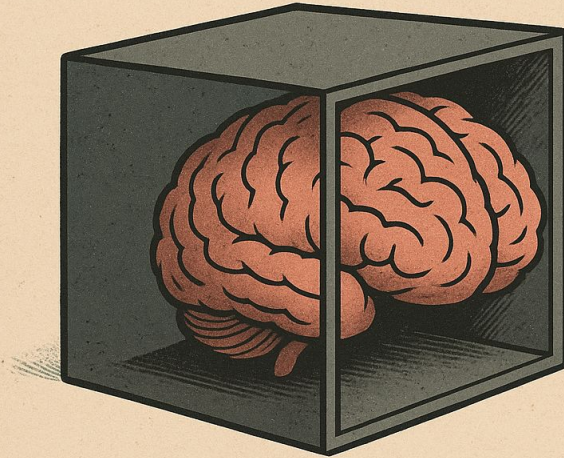
By Molly Bohannon, Former Staff. Molly Bohannon has been a Forbes news reporter since 2023.

Published Jun 22, 2023, 04:59pm EDT

source: <https://www.forbes.com/sites/mollybohannon/2023/06/22/judge-fines-two-lawyers-for-using-fake-cases-from-chatgpt/>

Really bad things can happen.

**BRAIN IN
A BOX**



HALLUCINATES

**DISCONNECTED
FROM EXTERNAL
WORLD**



**CANNOT TAKE
ANY ACTION**

Tool-Aware Chatbots

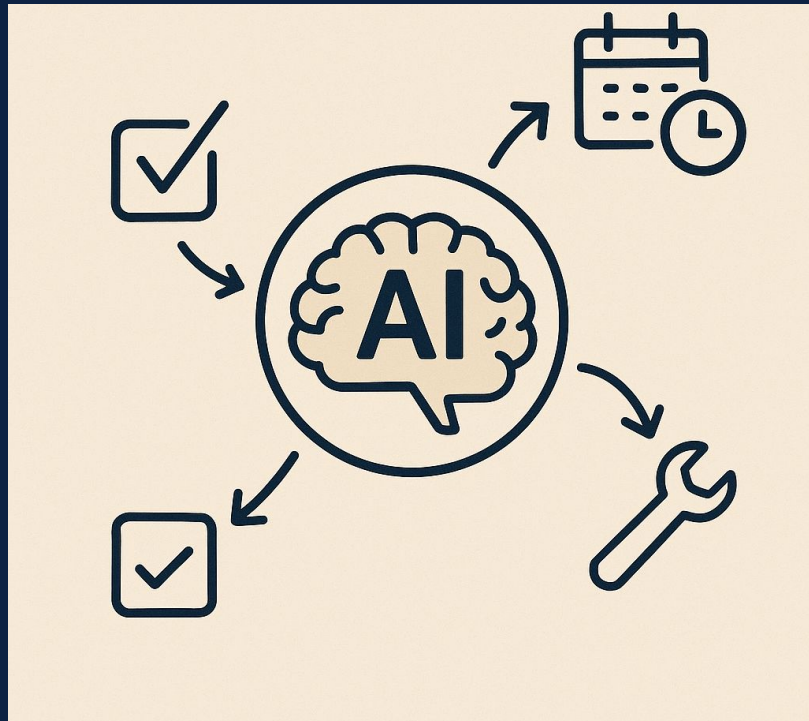


Connecting LLMs to external
systems

Tool-Aware Chatbots

The big idea: Give the AI access to **function calls** it can use to **take real actions**, **fetch fresh data**, and **execute tasks** beyond text generation.

Model Context Protocol: A standardized way to enrich chatbots with tools.

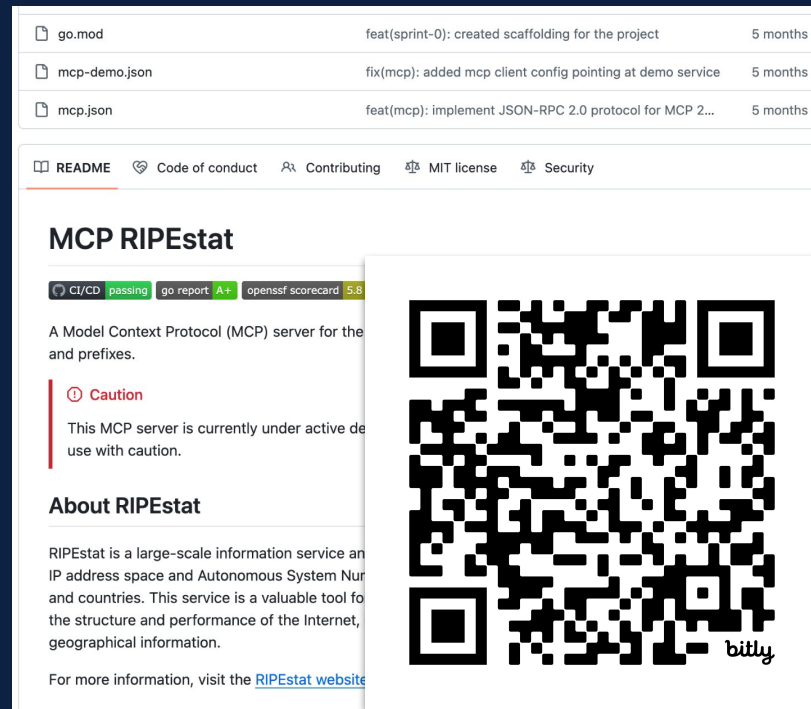


MCP-ripestat

(MCP) server for the RIPEstat Data API, providing network information for IP addresses and prefixes.

Query **up-to-date** RIPEstat data in natural language.

<https://github.com/taihen/mcp-ripestat>
By AJ Wolski (@taihen)



MCP-ripestat: Currently 22 tools

getNetworkInfo Get network information for an IP address or prefix. ...View Input Schema ☒ Enable	getASOverview Get an overview of an Autonomous System (AS). ...View Input Schema ☒ Enable
getAnnouncedPrefixes Get a list of prefixes announced by an Autonomous System (AS). ...View Input Schema ☒ Enable	getRelatedPrefixes Get related prefixes that are connected or associated with the given prefix. ...View Input Schema ☒ Enable
getRoutingStatus Get the routing status for an IP prefix. ...View Input Schema ☒ Enable	getRoutingHistory Get routing history information for an IP address, prefix, or ASN. ...View Input Schema ☒ Enable
getWhois Get whois information for an IP address, prefix, or ASN. ...View Input Schema ☒ Enable	getAbuseContactFinder Get abuse contact information for an IP address or prefix. ...View Input Schema ☒ Enable
getRPKIVValidation Get RPKI validation status for a resource (ASN) and prefix combination. ...View Input Schema ☒ Enable	getASNNeighbours Get ASN neighbours for an Autonomous System. Left neighbours are downstream providers, right neighbours are upstream pro... ...View Input Schema ☒ Enable
getLookingGlass Get looking glass information for an IP prefix, showing BGP routing data from RIPE NCC's Route Reflection Collectors (RR... ...View Input Schema	getCountryASNs Get Autonomous System Numbers (ASNs) for a given country code. ...View Input Schema ☒ Enable

whois-MCP

(MCP) server that provides LLMs with network information lookup tools through WHOIS and RIR Database queries..

Query **up-to-date** RIR data in natural language.

<https://github.com/dadepo/whois-mcp>

[README](#) [MIT license](#)

whois-mcp

A Model Context Protocol (MCP) server that provides LLMs with network information lookup tools through WHOIS and RIPE Database queries.

Features

Available Tools

- `whois_query` - Query WHOIS s
- `expand_as_set` - Recursively ex
- `validate_route_object` - Chec
- `contact_card` - Fetch abuse, a

Regional Internet Registry (RIR)

This MCP server supports all five Re

Tool	RIPE NCC
WHOIS Query	✓
AS-SET Expansion	✓
Route Validation	✓
Contact Card	✓



bitly

whois-MCP: Currently 14 tools

ripe_whois_query Perform raw WHOIS queries against the RIPE NCC database to get complete object information in RPSL format. This tool isView Input Schema ☒ Enable	ripe_expand_as_set Efficiently expand AS-SET objects from the RIPE NCC database into concrete ASNs with configurable depth. This tool is sp... ...View Input Schema ☒ Enable
ripe_validate_route_object PREFERRED TOOL for validating route object registration in the RIPE NCC database. This tool is specifically for the RIPE... ...View Input Schema ☒ Enable	ripe_contact_card PREFERRED TOOL for retrieving contact information (abuse, NOC, admin, tech) for IP addresses, ASNs, or organizations fro... ...View Input Schema ☒ Enable
arin_whois_query Perform raw WHOIS queries against the ARIN database to get complete object information in RPSL format. This tool is spec... ...View Input Schema ☒ Enable	arin_validate_route_object PREFERRED TOOL for validating route object registration in the ARIN database. This tool is specifically for the ARIN RIR... ...View Input Schema ☒ Enable
arin_expand_as_set Efficiently expand AS-SET objects from the ARIN IRR database into concrete ASNs with configurable depth. This tool is sp... ...View Input Schema ☒ Enable	arin_contact_card PREFERRED TOOL for retrieving contact information (abuse, NOC, admin, tech) for IP addresses, ASNs, or organizations fro... ...View Input Schema ☒ Enable
apnic_whois_query Perform raw WHOIS queries against the APNIC database to get complete object information in RPSL format. This tool is spe... ...View Input Schema ☒ Enable	apnic_contact_card PREFERRED TOOL for retrieving contact information (abuse, NOC, admin, tech) for IP addresses, ASNs, or organizations fro... ...View Input Schema ☒ Enable
afrinic_whois_query Perform raw WHOIS queries against the AfriNIC database to get complete object information in RPSL format. This tool is s... ...View Input Schema	afrinic_contact_card PREFERRED TOOL for retrieving contact information (abuse, NOC, admin, tech) for IP addresses, ASNs, or organizations fro... ...View Input Schema



Thought for 5 seconds >

AS-HETZNER is an AS-SET (autonomous system set) maintained by Hetzner. To find the current ASNs included in AS-HETZNER, you can query Internet Routing Registry (IRR) databases.

Here are a few ways to check:

Using whois:

 bash

```
whois -h whois.radb.net AS-HETZNER
```

Using IRR Explorer tools:

- RIPE Database: <https://apps.db.ripe.net/db-web-ui/>
- RADB: <http://www.radb.net/>
- IRR Explorer: <https://irrexplorer.nlnog.net/>

Known Hetzner ASNs typically include:

- AS24940 (Hetzner Online GmbH - main ASN)

AI Thought for 4 seconds >

I'll look up the ASNs contained in the AS-HETZNER AS-SET for you.

whois-mcp · ripe_expand_as_set

Success Re-run

AI Thought for 1 seconds >

AS-HETZNER contains **209 ASNs**:

AS1342, AS2876, AS9197, AS11528, AS12630, AS13251, AS15372, AS15540, AS15866, AS16097, AS16302, AS20795, AS21413, AS24940, AS24978, AS26383, AS29192, AS30774, AS31184, AS31259, AS31723, AS35065, AS35170, AS35205, AS35624, AS35830, AS39441, AS39857, AS41242, AS41369, AS41466, AS41745, AS42335, AS42699, AS43329, AS43444, AS43581, AS43847, AS43937, AS44477, AS44559, AS45012, AS45031, AS47105, AS47279, AS47462, AS47518, AS48154, AS48585, AS48755, AS49189, AS49283, AS49418, AS50050, AS50053, AS50064, AS50113, AS51176, AS51311, AS51401, AS51571, AS51726, AS51765, AS51895, AS52125, AS56418, AS56594, AS56971, AS57037, AS57043, AS57739, AS58243, AS59651, AS59921, AS60156, AS60412, AS60414, AS60522, AS60574, AS61074, AS61352, AS62365, AS136258, AS197540, AS197558, AS197753, AS198167, AS198225, AS199326, AS199644, AS199854, AS200096, AS200186, AS200249, AS200297, AS200303, AS200508, AS200599, AS200651, AS200740, AS201059, AS201206, AS201600, AS201729, AS201744, AS201764, AS201832, AS202208, AS202269, AS202426, AS202437, AS202509, AS202753, AS202784, AS203034, AS203195, AS203224, AS203296, AS203391, AS203437, AS203602, AS203724, AS203817, AS203969, AS204187, AS204591, AS204877, AS204924, AS205071, AS205090, AS205435, AS205582, AS205691, AS205741, AS205876, AS206141, AS206196, AS206240, AS206303, AS206715, AS206818, AS206855, AS206878, AS206888, AS206988, AS207077, AS207088, AS207010, AS207568, AS207718, AS207788



Thought for 4 seconds >

I don't have access to real-time BGP routing data or network monitoring information to assess the stability of the 5.30.0.0/15 IP range over the last 90 days.

To check the routing stability of this prefix, you could use:

BGP monitoring services:

- Hurricane Electric BGP Toolkit (bgp.he.net)
- RouteViews (routeviews.org)
- RIPE RIS (ris.ripe.net)
- BGPmon or similar services

What to look for:

- Route announcements/withdrawals
- AS path changes
- Prefix hijacks or leaks
- Outage incidents

Network monitoring tools:

- RIPE Atlas measurements
- Pingdom or similar uptime monitors



AI

Thought for 5 seconds >

I'll check the routing stability of the 5.30.0.0/15 prefix by examining its routing consistency data.

🔗 MCP RIPEstat · getPrefixRoutingConsistency

✓ Success Re-run ↕

> 5.30.0.0/15

AI

Thought for 2 seconds >

Let me check the routing history for this prefix over the past 90 days to assess its stability.

🔗 MCP RIPEstat · getRoutingHistory

✓ Success Re-run ↕

> 5.30.0.0/15, 2024-08-29T00:00:00Z, 2025-11-28T00:00:00Z

AI

Thought for 20 seconds >

Based on the routing history data for 5.30.0.0/15 over the past 90 days, the prefix shows **moderate stability with some concerning recent instability**.

Here's the analysis:

Overall 90-day stability:

- For most of the period (September through mid-November 2025), the prefix maintained relatively stable visibility with 340-345 BGP peers seeing the route
- Minor fluctuations were observed but stayed within a reasonable range (337-345 peers)

Recent instability concerns:

- **November 22-23:** Visibility dropped to 333 peers





Lacks Autonomy

**CONNECTED
TO EXTERNAL
WORLD**



CAN DO THINGS



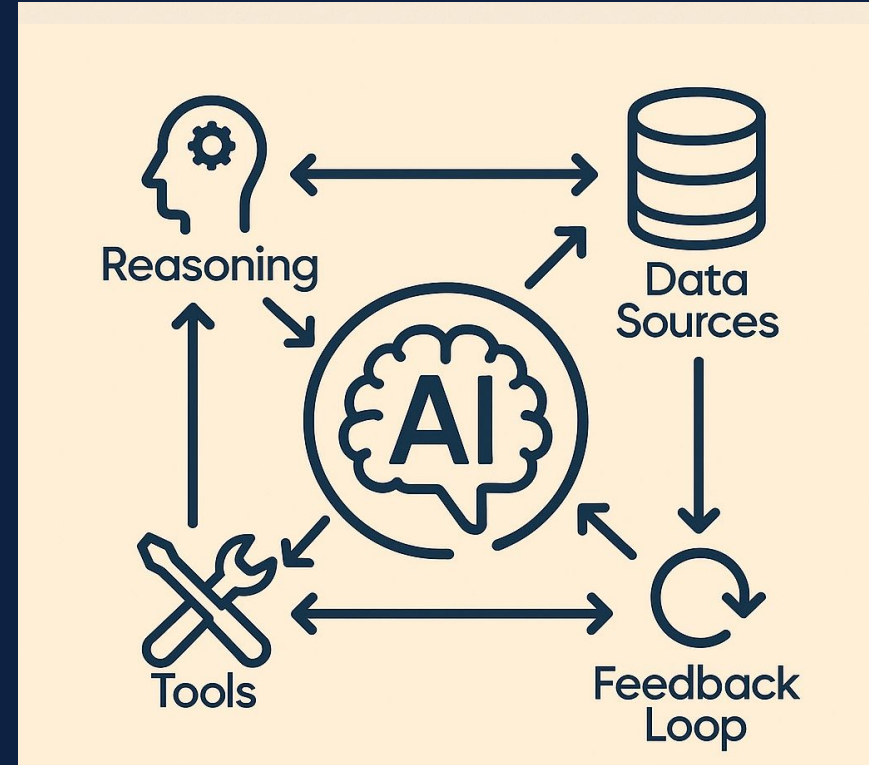
AgentOps: Beyond Chatbots



Giving LLM autonomy

What are Agents

Agents are AI systems that combine reasoning, data sources, tools and a feedback loop to achieve a defined goal autonomously without human coordination.



Introducing AgentNOC

AgentNOC: An Agent for Network Ops

Prototype of an agent built specifically for network operation coordination.

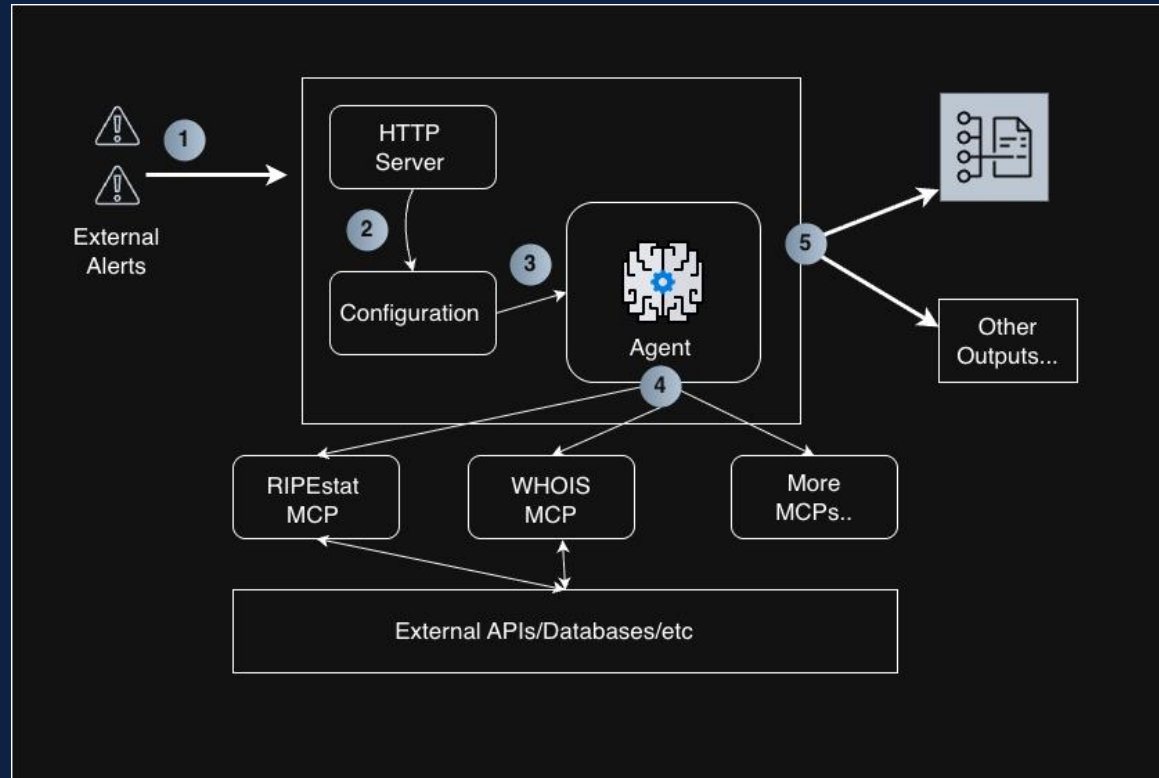
Plugs into existing monitoring tools (e.g. BGPalerter)

Human-in-the-loop design, read-only by default

Built in Rust, and open-source

Work in progress

AgentNOC: Overview



Scenario: BGP Hijack Suspected

An ASN announces a prefix it is not authorized to announce.

Scenario: BGP Hijack Suspected

 prefixes.yml

```
1 217.164.0.0/15:
2  | description: No description provided (No ROA available)
3  | asn:
4  |   - 5384
5  | ignoreMorespecifics: false
6  | ignore: false
7  | group: noc
8 192.0.2.0/24:
9  | description: Expected prefix for AS 3333 (for misconfiguration testing)
10 | asn:
11 |   - 3333
12 | ignoreMorespecifics: false
13 | ignore: false
14 | group: noc
15 options:
16 | monitorASns:
17 |   '3333':
18 |     group: noc
19 |   '5384':
20 |     group: noc
21
22 | %I to chat, %K to generate
```

Scenario: BGP Hijack Suspected

AgentNOC

Connected

Alerts3

192.0.2.0/24
45 agoHijack

192.0.2.0/24
6h agoHijack

192.0.2.0/24
6h agoHijack

192.0.2.0/24

23/11/2025, 15:14:03

Delete

MEDIUM SEVERITY

AS9999 (AT TOKYO Corporation, Japan) announcing 192.0.2.0/24, conflicting with expected origin AS3333 (RIPE NCC). This prefix is IANA-reserved documentation space (TEST-NET-1, RFC 5737) and should never appear in live routing tables. 30-minute incident with 2 peers observing. Likely misconfiguration or testing error by AT TOKYO.

AFFECTED PREFIX	OBSERVED ASN	EXPECTED ASN	DURATION
192.0.2.0/24 (IANA reserved TEST-NET-1 documentation	AS9999 (AT TOKYO Corporation, Japan)	AS3333 (RIPE NCC - Reseaux IP Europeens Network	30 minutes (2025-01-15 10:00:00Z to 10:30:00Z)

Scenario: BGP Hijack Suspected

All alerts

192.0.2.0/24
6h ago
Hijack

192.0.2.0/24
6h ago
Hijack

⚡ Immediate Actions

1

Contact AT TOKYO NOC immediately at admin-c/tech-c JP00010132 via JPNIC WHOIS gateway (whois.nic.ad.jp)
- prefix is IANA documentation space and must not be routed

2

Verify your route filters are blocking 192.0.2.0/24 (RFC 5737 martian) - this should have been rejected at ingress by peers

3

Review AS9999 announcements for other bogon/documentation prefixes (198.51.100.0/24, 203.0.113.0/24) indicating systemic filter failure

Scenario: BGP Hijack Suspected

Alerts3

192.0.2.0/24Hijack4h ago

192.0.2.0/24Hijack6h ago

192.0.2.0/24Hijack6h ago

indicating systemic filter failure

⚠ Risk Assessment

Medium severity - while prefix conflict exists, 192.0.2.0/24 is IANA-reserved documentation space that should never be routed globally. Low peer visibility (2 peers) suggests limited propagation. Root cause is likely AT TOKYO misconfiguration or testing leak rather than malicious hijack. No production traffic impact as this prefix has no legitimate Internet assignment.

Note: Successfully enriched: AS3333 confirmed as RIPE NCC with extensive peering documentation. AS9999 confirmed as AT TOKYO Corporation (Japan, APNIC region). WHOIS lookup for 192.0.2.0/24 returned IANA-BLK (documentation prefix). No historical routing data found for prefix (expected - bogon space). Alert indicates configuration error rather than hijack attempt.

Show Raw Response

Scenario: BGP Hijack Suspected

192.0.2.0/24
6h ago

Hijack

192.0.2.0/24
6h ago

Hijack

Chat with Agent

You19:25:37

Get me the email address I need to get in touch with TOKYO NOC

Assistant19:25:45

Based on the APNIC contact information for AS9999 (AT TOKYO Corporation), you should contact:

Email: hostmaster@nic.ad.jp

Phone: +81-3-5297-2311 or +81-3-5297-2312

This is the Japan Network Information Center (JPNIC) contact that handles administrative and technical matters for AT TOKYO Corporation. When you reach out, reference:

- Prefix: 192.0.2.0/24 (IANA reserved documentation space)

What Comes Next?



Building out AgentNOC

Bringing It All Together — What Comes Next

We've seen how we can move from chatbots that simply answer questions to agents that actually help operators work

Once agents are wired into the NOC and have access to operational data, a more capable class of automation becomes possible—focused, operational, and measurable.

What Agents Can Unlock for NOCs

- Autonomous Incident Enrichment
- Playbook Execution
- Reasoning on Your Data
- Human-in-the-Loop Automation
- Automatic Ticket Drafting
- Upstream/Peer Behavior Analysis
- Event Correlation Across Systems
- Documentation Extraction
- ...and much more

Where We Go From Here?

Everything presented, AgentNOC, MCP servers, is open source, evolving, and built in the open.

Network operations is one of the few domains where AI can have immediate, practical impact. But only if these systems are designed with the operator community.

How You Can Get Involved

Inviting:

Network engineers, backbone operators, IXPs, anyone who deals with operational reality of running a network

To Contribute:

Real-world scenarios, sample alert feeds, incident war stories, daily pain points, workflow and UI feedback

How You Can Get Involved



<https://bit.ly/agentnoc>



<https://bit.ly/4rg7G1V>



Thank you