MCP SERVER | NO CODE | CLOUD HOSTED

SecurityTrails MCP

Map an Organization's Entire Digital History

SecurityTrails MCP connects deep domain and IP intelligence into your AI agent. Instantly map an organization's entire digital footprint by accessing historical DNS records, enumerating hidden subdomains, checking WHOIS ownership changes, and running advanced threat queries against the world's largest database of network data.

A+ Quality Score 98.33/100

osint | dns-history | subdomain-enumeration | whois | bug-bounty | threat-intelligence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/securitytrails

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

SecurityTrails MCP

10 tools available
Cloud-hosted on Vinkius

You can use this MCP to treat any target domain like a live intelligence feed. Instead of spending hours clicking through separate databases for IP history, you ask your agent to find connections between domains, IPs, and people. It pulls together historical DNS records—the kind that show where an organization was five years ago but has since abandoned. You can expand the scope of any investigation by finding other domains associated with a primary target or look up every domain hosted on a specific IP address. These capabilities let you track infrastructure migration, unmask forgotten assets, and identify potential brand squatters before they cause trouble. Connecting this MCP through Vinkius allows your agent to perform these complex OSINT tasks without needing specialized terminal commands. You simply ask the question, and it gives you the historical data required for bug bounty hunting or threat intelligence.

Core Capabilities

01 — Map Asset Footprint

Automatically discovers all active and inactive subdomains linked to a target domain.

02 — Trace Historical Records

Retrieves past DNS records (A, MX, NS, TXT) to map out how an organization's infrastructure has changed over time.

03 — Identify Shared Infrastructure

Finds all domains that share the same IP address, helping locate hidden virtual hosts or related assets.

04 — Determine Ownership Changes

Accesses current and historical WHOIS data to track domain ownership changes and identify potential malicious actors.

05 — Execute Advanced Queries

Uses a specific Domain Specific Language (DSL) to query the entire internet for niche tech stacks or vulnerable infrastructure patterns.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/securitytrails** — connect your AI agent in three steps.

01 Subscribe to this MCP and sign up at SecurityTrails to get your API key.

02 Connect your agent by providing the necessary credentials via Vinkius. Your AI client handles all authentication.

03 Ask your agent a specific question, like 'What historical records point to example.com?' The MCP executes the query and returns structured data.

The bottom line is that you get deep, actionable domain intelligence without ever leaving your primary chat interface.

Built For

This connector serves security researchers, pentesting teams, and threat intelligence analysts. If your job involves mapping an organization's attack surface or tracking down hidden digital assets, this MCP is a necessity. It solves the pain of manually cross-referencing decades of domain records across multiple tools.

Penetration Tester

Uses the MCP to quickly enumerate all subdomains and find forgotten endpoints associated with a target company.

Bug Bounty Hunter

Runs advanced queries using the DSL to locate out-of-scope assets or older, less protected infrastructure related to client targets.

Threat Intelligence Analyst

Correlates WHOIS history with DNS records and IP lookups to build timelines of Advanced Persistent Threat (APT) group activity.

What Changes When You Connect

01 Discover hidden assets: Instead of just checking the main site, use `get_subdomains` to map every associated subdomain and find overlooked attack vectors.

02 Track infrastructure changes: Use `get_dns_history` to see where a domain pointed five years ago. This reveals abandoned services or legacy systems that are still vulnerable.

03 Scope expansion: When you find one target, use `get_associated_domains` to automatically pull in every related corporate site without manual research.

04 Identify shared risks: Run `get_domains_by_ip` on a suspicious IP address. This shows every other domain that shares it, flagging potential cross-site compromises.

05 Deep intelligence gathering: Use the advanced `search_dsl` tool to query for specific tech stacks (e.g., 'all domains using Nginx and hosted in Germany').

06 Ownership tracking: The combination of `get_whois` and `get_whois_history` allows you to build a timeline of who controlled a domain over decades.

Real-World Applications

Finding old forgotten systems after a company merger

A threat analyst needs to know if the merged company retained any legacy infrastructure. They query `get_dns_history` for the original domain, and the MCP reveals A records pointing to an IP address that hasn't been active in years, flagging it as a potential data leak source.

Mapping out a competitor's entire web presence

A bug bounty hunter starts with one domain. They immediately run `get_subdomains` and then `get_associated_domains`. The agent returns hundreds of subdomains, allowing them to test the full breadth of the competitor's digital assets.

Investigating a suspicious IP for related criminal activity

A researcher gets an unknown IP. They use `get_domains_by_ip` and find four unrelated domains all pointing to it. This suggests shared hosting, allowing them to focus their investigation on the likely primary owner.

Tracing a domain back through multiple hands

A brand protection team suspects typosquatting. They use `get_whois` and then `get_whois_history` to trace ownership changes, determining when the malicious actor first registered the related domain.

Patterns to Avoid

Thinking only of current records

✗ AVOID

Running a simple WHOIS check on example.com and assuming all information is accurate because it's today's date.

✓ INSTEAD

Always pair `get_whois` with `get_whois_history`. This shows the true lineage, revealing owners and details that were private or changed years ago.

Only checking primary domains

✗ AVOID

Manually listing all subdomains for a target company because they are easy to guess.

✓ INSTEAD

Use `get_subdomains` first. This automates the enumeration process, finding inactive or obscure subdomains you would otherwise miss.

Using general search tools

✗ AVOID

Searching generic web logs for an IP address, which gives thousands of irrelevant results.

✓ INSTEAD

Run `get_domains_by_ip` to get a curated list of only the domains known to point to that specific IP. This cuts the noise instantly.

The Right Fit

Use this MCP if your investigation relies on time, association, or scope depth. You need to know what *was* there, not just what's live right now. If you only care about today's publicly visible DNS records, other simple lookups will suffice. However, if you suspect historical data—like finding an old IP address from 2018 that the company hasn't decommissioned yet—this MCP is required because it accesses `get_dns_history` and `get_whois_history`. Don't use this if your goal is simply generating a list of current, active websites. This tool specializes in intelligence gathering by cross-referencing historical records with modern domain structures.

The Pain of Manual Digital Forensics

Right now, mapping an organization's infrastructure is a tedious crawl through multiple interfaces. You check the main site, then jump to a separate WHOIS page for ownership details. Then you have to run a subdomain brute-forcer, and if that fails, you try looking up historical DNS records on another service. It’s copy-pasting between three or four different tabs just to get one coherent picture.

With this MCP, your agent handles all those jumps. You tell it the target, and it orchestrates checks for current details, past ownership, associated domains, and deep subdomains—all in a single conversation thread. You get the full intelligence map without leaving your chat.

SecurityTrails MCP: Comprehensive Domain Intelligence

Before this MCP, tracking domain ownership meant relying on basic WHOIS lookups that often failed or were outdated. Tracking infrastructure changes required manual checks of historical DNS logs, which few services provided in a unified format.

Now, you can ask for the full picture: who owned it, what IPs did it use years ago, and every single domain linked to it—all instantly available through your AI agent.

SecurityTrails MCP with 10 Tools

These tools let you perform deep intelligence queries, covering everything from current domain registration to historical IP usage.

#	TOOL	DESCRIPTION
01	`get_api_usage`	Checks how much of your SecurityTrails API quota you've used for the day.
02	`get_domain_tags`	Provides classification tags that categorize the purpose and type of a specific domain.
03	`get_dns_history`	Retrieves historical DNS records for a domain, useful for seeing old IPs or tracking infrastructure moves.
04	`get_subdomains`	Discovers all subdomains for a given domain, regardless of whether they are currently active or inactive.
05	`get_whois`	Gets the current registration and ownership information (WHOIS) for any specified domain.
06	`search_dsl`	Runs highly advanced, targeted queries across the entire internet using the full SecurityTrails Domain Specific Language syntax.
07	`get_domains_by_ip`	Lists all domains that have been pointed to a single IP address, identifying shared hosting environments.
08	`get_domain_details`	Gathers complete current domain intelligence, including DNS records and core structural data for mapping.
09	`get_associated_domains`	Finds other domains that are strongly linked to a primary target domain, expanding your investigation scope.
10	`get_whois_history`	Retrieves historical WHOIS records for a domain, useful for tracking owners before privacy protection was used.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Find all subdomains for tesla.com.

I've queried SecurityTrails and found 482 subdomains for tesla.com, including: autodiscover.tesla.com, sso.tesla.com, ir.tesla.com, shop.tesla.com, and energy.tesla.com.

U Check the historical 'A' records for example.com. Were there any changes in 2021?

Looking at the DNS history for example.com, the A record currently points to 93.184.216.34. However, back in 2021, the domain pointed to 93.184.216.119 before migrating infrastructure in late 2022.

U What domains are hosted on the IP 8.8.8.8?

I performed a reverse IP lookup on 8.8.8.8 (Google Public DNS). As expected for a public resolver, there are millions of historical records pointing here, but currently, domains like dns.google and google-public-dns-a.google.com resolve directly to this IP address.

Frequently Asked Questions

01 **What is the difference between `get_subdomains` and `get_associated_domains` using SecurityTrails MCP?**

`get_subdomains` finds all variations attached to a single domain (like 'staging.example.com'). `get_associated_domains`, however, finds entirely separate domains that are strongly linked to the primary target company.

02 **Can I use SecurityTrails MCP to find out who owned a domain in 2015?**

Yes. You must use `get_whois_history` or `get_dns_history`. These tools retrieve historical records, bypassing modern privacy protections that hide old ownership data.

03 **Does SecurityTrails MCP only work for major corporate websites?**

No. It handles anything from large corporations to small personal sites, allowing you to run advanced searches using the `search_dsl` tool on any domain or IP range.

04 **How do I check if a domain is part of a larger network?**

Run `get_domains_by_ip`. This tool lists every known domain that shares an IP address, which is critical for identifying shared hosting or hidden virtual machines.

05 **Is SecurityTrails MCP better than standard DNS lookup tools?**

Yes. Standard lookups only give you the current record. This MCP provides historical depth and cross-referencing capabilities that connect ownership, IP usage, and domain names over time.

06 **Is the SecurityTrails API free to use?**

SecurityTrails offers a Free Tier API plan which allows 50 API requests per month. This is excellent for specific, targeted OSINT investigations. For automated or large-scale recon, you would need a commercial subscription.

07 **What is historical DNS good for?**

Companies often migrate infrastructure and hide behind WAFs like Cloudflare. Historical DNS reveals the original origin IP addresses used before the WAF was implemented, which might still be active and vulnerable to direct attacks. It's a critical tool in penetration testing.

08 **How can I find related domains for a target company?**

Use the `get_associated_domains` tool. It uses proprietary correlation to find other domains owned by the same entity. You can also use `get_domains_by_ip` to find what else is hosted on their IP space.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"securitytrails": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

SecurityTrails is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by SecurityTrails. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	SecurityTrails MCP
Server ID	`019d847b-e7b9-700b-938e-d6bdc7e4a90b`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/securitytrails.