Connect Your AI to Real-Time DNS Intelligence

Giving the SOC a **Boost**

As the industry explores AI-driven security operations, DomainTools offers a new method of accessing the world's most comprehensive DNS intelligence via natural language prompts. LLM-powered workflows and assisted users can now connect directly to DomainTools APIs via MCP, enabling them to incorporate world class domain intelligence data into their AI workflows and retrieve rich domain insights for their LLM to interpret.

What is MCP?

The Model Context Protocol (MCP) is a universal, open standard for connecting AI systems with data sources, replacing fragmented integrations with a single protocol. The result is a simpler, more reliable way to give AI systems access to the data they need.

THREAT INTELLIGENCE AND HUNTING

Query DomainTools datasets and pivot on relevant indicators to map out attacker infrastructure.

INCIDENT RESPONSE

Leverage LLM capabilities to rapidly discover, prioritize, analyze, and summarize detected threats.

APPLICATION ENRICHMENT

Get more from the tools you already have by integrating DomainTools data into existing workflows.

Security, Accelerated

Eliminate Tool Fatigue

Context-switching takes time - by connecting your LLM to DomainTools datasets, you can instantly retrieve domain intelligence data without leaving your current environment. Get detailed insights, perform pivots, and build out investigations, all at machine speed.

Key Benefits

FRICTIONLESS ADOPTION:

Integrate DomainTools data directly into existing toolsets

ACCESSIBLE INVESTIGATIONS:

Execute complex investigations using natural language, narrowing the skill gap between junior and senior analysts

OPERATIONAL SCALE:

Maximize your SOC's AI automation's decision making capabilities and empower one to do the work of many.

ZERO INFRASTRUCTURE OVERHEAD:

The DomainTools MCP Server is fully hosted and managed in the cloud; no server setup, no maintenance, no operational burden on your team.

DomainTools

Three Deployment Models

Reliable, Programmatic Intelligence:

Reliable, Programmatic Intelligence: DomainTools doesn't use GenAI to generate outputs — every response is constructed from our proprietary databases. Your AI gets consistent, structured data it can reason over with confidence, not hallucinated approximations.

DIRECT ANALYST ACCESS

Connect the DomainTools MCP Server to your LLM of choice (Claude, Gemini, ChatGPT and more). Investigate suspicious domains, map attacker infrastructure, and retrieve Risk Scores through natural language—right inside your existing AI workflow.

BROKER-ORCHESTRATED MCPs

Your LLM of choice such as Claude, ChatGPT, or Gemini CLI acts as the central broker, connecting to the DomainTools MCP Server and a third party MCP such as Splunk SIEM. The AI pulls log data and threat intelligence in one workflow, without the analyst switching tools.

NATIVE ORCHESTRATION INSIDE A SECURITY PLATFORM

Embed the DomainTools MCP directly into a third party security platform that supports multi-MCP orchestration. DomainTools threat intelligence becomes a native capability within the platform's agent workflows, enriching alerts and triggering automated response actions.

About DomainTools

DomainTools is the global leader for Internet intelligence. We've mapped malicious online infrastructure for over 20 years, helping security teams to identify external risks, investigate threats, and proactively protect their organizations from sophisticated cyber attacks.

DomainTools