DomainTools

DomainTools Integrations in Popular SOC Tools

DomainTools Internet Intelligence provides best in class DNS and related data to enable analysts, incident responders, and threat hunters to evaluate and address threats quickly and confidently. Our integrations place this intelligence exactly where the team needs it - in the most popular SOC tools.

The right data, when and where you need it.

In order to reduce pivoting among different tools, DomainTools has built ready-made applications for some of the most popular SOC platforms, including SIEM, TIP, SOAR, and E/XDR.

TIP: For early warning and proactive defense, ingesting DomainTools feeds into a TIP and filtering the feeds down to what is most relevant to the analyst enables the creation of detection or blocking rules for high-risk domains and serves as a starting point for investigations.

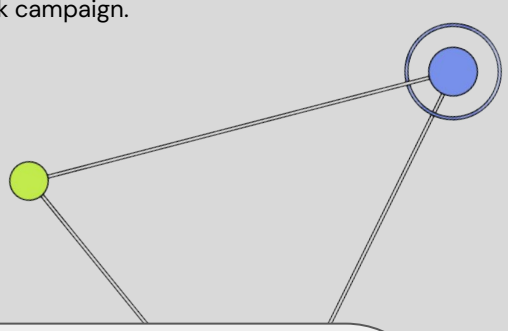
SIEM: DomainTools SIEM integrations provide enrichment of alerts and events that contain domain names and in some cases, such as the Threat Hunting Dashboard in the DomainTools Splunk App, show all instances of newly-created and/or high-risk domains seen in the customer's environment.

SOAR: With ready-made playbooks in several popular orchestration platforms, the SOC team can automate enrichment and investigative tasks, saving valuable time and giving teams a head start on defensive or forensic measures.

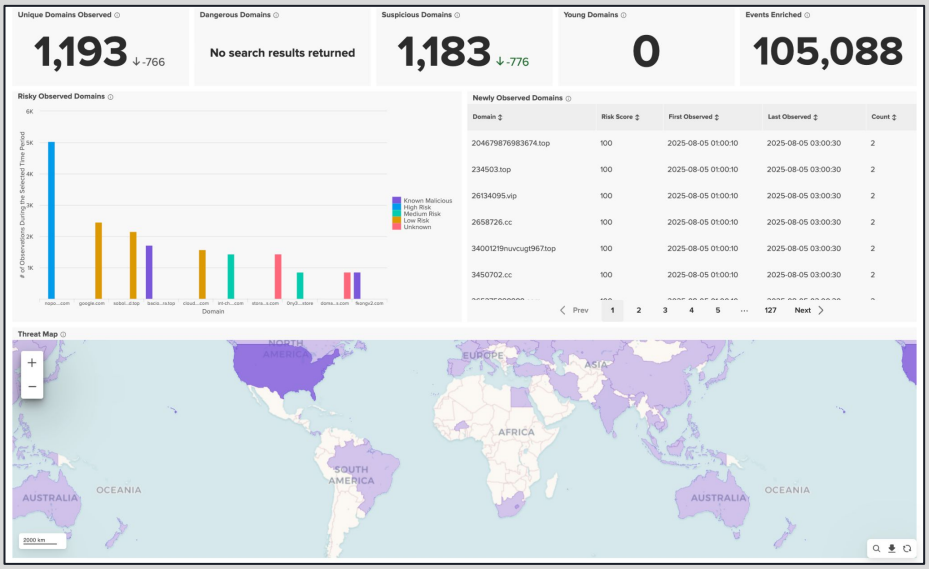
E/XDR: Endpoint-based alerts can be enriched with domain risk data, placing the analysis of potential risk close to the means of enforcement.

LLMs: DomainTools data can power defensive or forensic inquiries into adversary infrastructure data, combining this with other data sources to build a comprehensive overview of an attack campaign.

The API and data feed endpoints that power our ready-made integrations are easy to use for custom configurations. RESTful APIs, flexible output formats (JSON, text, .csv, etc), and simple access methods such as https calls make it straightforward to ingest feeds or enrich events in custom or third-party tools.



PLATFORM	ALERT/EVENT ENRICHMENT	DOMAIN PROFILES AND RISK SCORES	PIVOTING ON INFRASTRUCTURE	WHOIS/RDAP DATA
SIEM	✓	✓		✓
TIP		✓	✓	✓
SOAR	✓	✓	✓	✓
E/XDR	✓	✓	✓	✓



Key Benefits

Getting Ahead of Emerging Threats
DomainTools tracks the evolution of the Internet in real time and provides predictive risk scoring and up-to-the-minute infrastructure data, which helps teams identify, anticipate, and act against quickly-evolving threat campaigns.

Optimizing Security Resources
Placing DomainTools intelligence in commonly-used tools boosts the value those tools deliver. Teams work more efficiently with less context-switching.

Reducing Cyber Risk
Better understanding of adversary campaigns means the organization can align defenses with greater precision, reducing the risk of a breach.

Use Case Snapshot: SIEM Alert Enrichment Leads to Successful Hunt and Response

An alert containing a domain name is automatically enriched with the DomainTools Risk Score and the domain's age.

In the SIEM, the analyst reviews the domain profile and determines that the alert represents a valid threat based on criteria such as a spoofed domain name or unconventional hosting.

Knowing that the most high-risk domains are part of a larger campaign, the analyst performs pivots using DomainTools Iris Investigate to find related infrastructure.

The analyst hands off this larger set of indicators to peers in incident response, threat hunting, detection engineering, industry trust groups, etc.

These other teams generate detections and/or blocking rules against the extended threat infrastructure, or share the findings with industry peers or law enforcement.

Using such workflows, DomainTools customers gain insight and contextual decision-making data critical to defense against a larger adversary campaign based on what was observed in a single SIEM alert.

About DomainTools

DomainTools is the global leader for internet intelligence. We've mapped malicious online infrastructure for over 25 years, helping security teams to identify external risks, investigate threats, and proactively protect their organizations from sophisticated cyberattacks.