Current network visibility and breach detection technologies can provide a wealth of information about suspicious or malicious activities within an organization, and can identify the domains or IP addresses behind an attack or data exfiltration. But because threat actors rapidly “burn” infrastructure, a reactive approach leaves the organization open to new attacks. Fortunately, it is possible to take a more proactive approach by profiling adversaries and their infrastructure, and orienting detection and blocking around domains and IP addresses that may be in the process of being weaponized. With DomainTools, organizations can:

**DETERMINE**
Determine the risk of domains observed on the network, but not found in threat intelligence feeds or blacklists

**BUILD**
Build a profile based on historical data, location, associated domains, and how they build their sites

**IDENTIFY**
Identify associated domains, hosts & IPs to stop further attacks

**MONITOR**
Monitor the Internet for future infrastructure being prepared by threat actors

**ENTERPRISE SECURITY SOLUTIONS**
With nearly two decades of domain expertise, our analytics on infrastructure allow us to uniquely identify potentially malicious domains often before they are weaponized. Our customers utilize these analytics in a variety of ways:
PRODUCTS

DomainTools helps organizations turn threat data into threat intelligence by connecting indicators, including domains and IPs, and correlating them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

PHISHEYE
Discovered newly-registered domain names with the ability to identify existing and new domains that spoof legitimate brand, product, organization, or other terms, for defensive or investigative actions.

IRIS
Combines enterprise-grade domain intelligence and proactive risk scoring with industry-leading passive DNS data to guide threat investigations and uncover connected infrastructure.

DOMAIN RISK SCORE
DomainTools Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. This can close the window of vulnerability between the time a malicious domain is registered, and when it is observed and reported causing harm. The Domain Risk Score algorithms analyze a domain’s association to known-bad infrastructure, as well as intrinsic properties of the domain that closely resemble those of known phishing, malware, and spam domains.

APIS
The DomainTools APIs bring a critical subset of capabilities to third-party products and custom integrations, enabling rapid in-context profiling of domain-based threats and effective pivots that help build comprehensive lists of malicious infrastructure.

IRIS ENRICH
Designed to support high query volumes with batch processing and actionable insights-at-scale for a seamless view of data and easy transition from SIEM alert to human analysis, or SOAR platform.

IRIS INVESTIGATE
Suited for investigation and orchestration at human-scale, delivering domain name attributes on every result including risk score, DNS, Whois, SSL, and more for easy pivoting to expose meaningful insight.
**INTEGRATIONS**

Through close partnerships with leading security vendors, DomainTools embeds our market-leading infrastructure intelligence with support from domain profiles and risk scores directly into preferred SIEM, SOAR, and TIPs. These featured integrations leverage DomainTools Enterprise APIs to bring DomainTools premier data directly into the product experience.

- Expedite incident response with in-context domain profile data
- Target threat hunting on actor profiles & TTPs
- Realize security product ROI faster with turn-key solutions

Intelligence surfaced from DomainTools, including shared infrastructure and historical identities, stays in the same investigative context, which avoids rework and improves collaboration across team members.

<table>
<thead>
<tr>
<th>CHALLENGE: DETECT &amp; ALERT</th>
<th>SOLUTION: DomainTools provides domain event enrichment with predictive domain risk scoring and supporting evidence of malicious infrastructure.</th>
<th>CUSTOMER BENEFIT: Enables precisely-targeted threat intelligence and threat hunting on domain infrastructure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHALLENGE: INCREASING EFFICIENCY</td>
<td>SOLUTION: DomainTools data informs SOAR platforms with predictive domain risk scoring and supporting evidence of malicious infrastructure, so organizations can intelligently inform playbooks/workflows.</td>
<td>CUSTOMER BENEFIT: The ability to speed up incident handling, avoid context switching, and create intelligent playbooks/workflows.</td>
</tr>
<tr>
<td>CHALLENGE: MTTR</td>
<td>SOLUTION: DomainTools threat data integrated with TIPs, allows for data set correlation and the ability to automatically export into existing security and ticketing systems.</td>
<td>CUSTOMER BENEFIT: Automation decreases the amount of time needed to remediate the most serious threats.</td>
</tr>
</tbody>
</table>
FEATURED INTEGRATIONS

**SPLUNK**
Rapid enrichment of domains with Domain Risk Score, Whois, IP, active DNS, website & SSL data to surface evidence of malicious activity to execute high query volumes with increased response times.

**IBM QRADAR**
Uncover advanced threats and thoroughly investigate incidents with domain profiles and risk scores for every Internet domain name.

**SPLUNK PHANTOM**
Automate and orchestrate the IR processes with essential domain profile, web crawl, SSL and infrastructure data to create custom workflows to trigger IoC investigations, block threats, and identify potentially malicious incidents before weaponization.

**IBM RESILIENT**
Automate the IR process with essential domain profile data to create dynamic workflows for identification and remediation of potentially malicious incidents.

**CORTEX XSOAR**

**ANOMALI**
Context-based enrichment for domain names, IP addresses, hostnames, and SSL hashes to correlate with additional datasets and export into an organization’s existing security systems or ticketing systems, automating proactive threat management and mitigation.

**MALTEGO**
Expedite the investigation process with Whois, DNS, web crawl and SSL data, with dynamic properties to show risk and highlight useful pivots. An extensive set of transforms then operate on IPs, identities, SSL hashes, hostnames, and more to deliver matched domain names.

**MISP • THE HIVE AND CORTEX**

To test the power of DomainTools or get pricing information:

WWW.DOMAINTOOLS.COM • SALES@DOMAINTOOLS.COM • 206.838.9020

© Copyright DomainTools, 2020