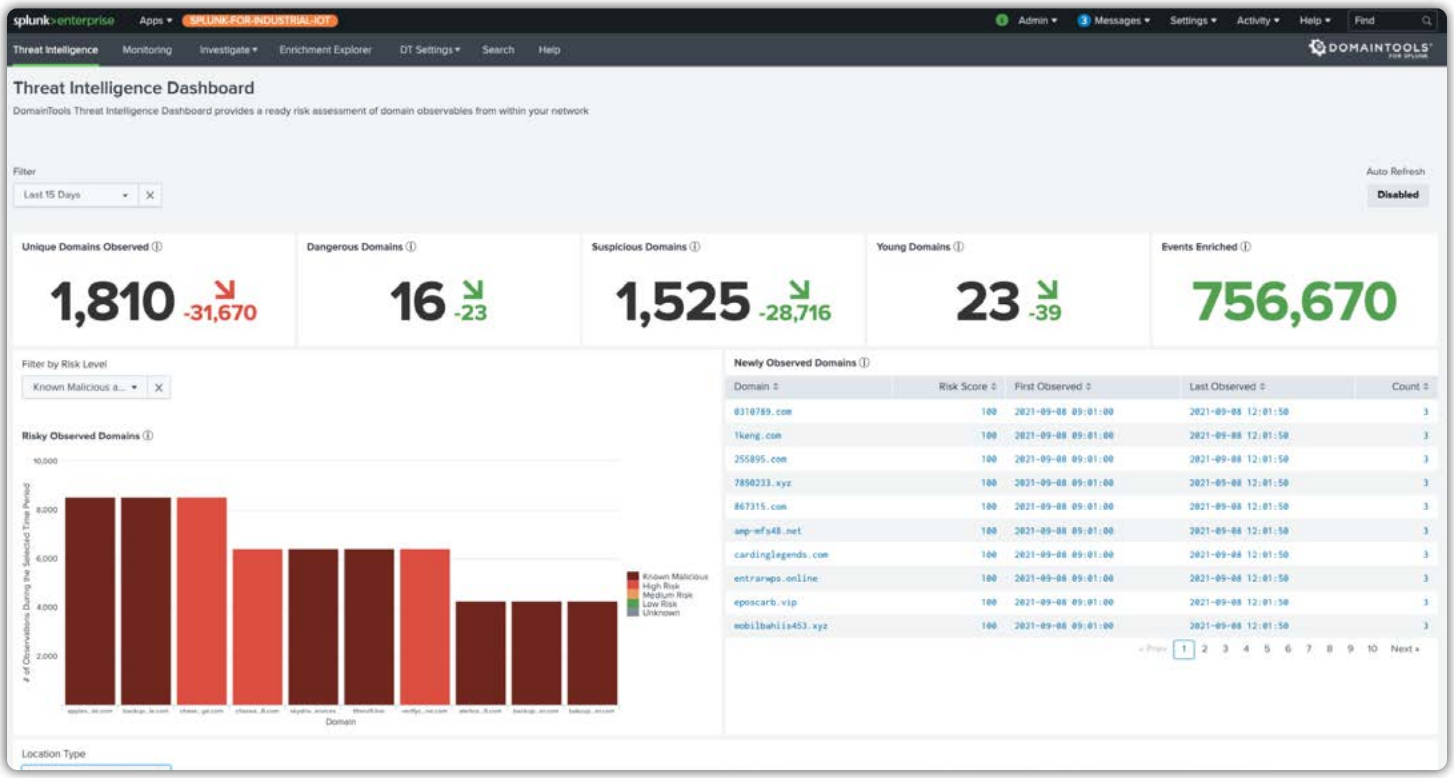
DOMAINTOOLS®

DomainTools App for Splunk

Gain fast insights and situational awareness around risky infrastructure

DomainTools enables Security Operations Centers (SOCs) and security analysts to take domain observables from their network and connect them with other active domains on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

With the influx in events per second rising, organizations need the ability to execute high-volume queries with improved response times. The DomainTools App for Splunk delivers, with enrichment at scale and drill-down details to add context. Leveraging the DomainTools Iris and Farsight DNSDB datasets, users have immediate access to dozens of attributes attached to every domain event in Splunk, efficiently delivering event enrichment at scale.



Domain Monitoring

SOCs and Security Analysts can leverage the DomainTools Iris Detect product in Splunk to discover and watch newly registered domains associated with any terms their organization currently monitors (such as a brand or company name), and to monitor domains and append domains to your allowlist (list of trusted domains) from the Domain Investigation workflow.

Proactive Risk Scoring

DomainTools Risk Score gives teams with emerging threat hunting skills an instant advantage inhelping to identify and optionally alert on Splunk events with suspicious domains they would have otherwise missed. Individual component scores give experienced hunters the tools they need to refine their alerts and precisely target their resources. DomainTools Risk Score, including Proximity and Threat Profile classifiers, is available in both key-value stores and Splunk indexes.

Proven Capability for Enterprise Organizations

DomainTools' proven solution for Splunk includes a cloud-certified Splunk Application that deploys on Splunk search heads in both standalone and clustered configurations, with and without Splunk Enterprise Security. Event sources can be customized to match the unique requirements of each environment.

"We're losing millions to fraudulent purchases via spoofed and compromised emails. DomainTools is now helping our investigators manually assess large volumes of malicious email domains. DomainTools will help us shore up our defenses from domain and DNS intel via API at machine scale in Splunk". -Head of Global Fraud Investigations, Fortune 50 Company

DomainTools Capabilities in Splunk

Reduce MTTD

- ✓ Bulk enrichment of domains with meaningful context
- ✓ At-a-glance alerting and reporting of malicious network traffic
- ✓ Domain monitoring using DomainTools Iris Detect

Reduce MTTR

- ✓ Discover newly registered domains and further enable monitoring
- ✓ Create a Splunk ES notable event in case a high-risk domain is observed
- ✓ Investigate connected infrastructure using Iris and Farsight Passive DNS

DOMAINTOOLS®

Test the power of the world's Largest DNS Forensics Database Today.

WWW.DOMAINTOOLS.COM