CrowdStrike Store

DOMAINTOOLS

CROWDSTRIKE

Data Sheet

DOMAINTOOLS: IRIS THREAT INTELLIGENCE

Delivering predictive risk assessments with DNS threat intelligence

CHALLENGE

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 associated with attacks or data exfiltration. But because threat actors rapidly "burn" infrastructure, a reactive approach leaves an organization open to new attacks.

SOLUTION

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.

Iris from DomainTools provides predictive risk assessments and DNS intelligence within the CrowdStrike Falcon® platform to enable rapid in-context profiling of domain observables.

BUSINESS VALUE

Use Case	Solution	Benefit
Threat Intelligence	Reduce the window of vulnerability between the time a malicious domain is registered and when it is observed and reported publicly as a component of an attack.	Make instantaneous decisions based on domain context and predictive risk assessment and identify potential threats before they appear on industry blocklists.
Threat Hunting	Use DomainTools predictive risk scoring along with connected infrastructure intelligence to actively hunt for emerging threats within your network. Proactively look for evidence and accelerate detection, prioritization, and hunting activities.	Uncover high-risk domains and associated DNS infrastructure, exploring connections and identifying threat actor tactics, techniques and procedures (TTPs) to supercharge your threat hunting.
Incident Response	Provide predictive risk assessments and DNS intelligence directly to the analyst inside the CrowdStrike® Falcon platform, enabling rapid in-context profiling of domain observables.	Reduce your mean time-to-respond and increase confidence in your decisions on domain indicators.

KEY BENEFITS

Block malicious domains based on your network activity

Proactively monitor high-risk domains based on DomainTools Threat Profile scoring

Make faster decisions based on domain context and predictive risk assessment

DOMAINTOOLS: IRIS THREAT INTELLIGENCE

"Invoking DomainTools market-leading domain and DNS context, alerting and risk scoring allows CrowdStrike customers to further leverage their investment in EDR, and accelerate the discovery and triage of malicious and potentially malicious IOCs. The DomainTools Iris Threat Intelligence app for CrowdStrike natively pairs network-wide endpoint telemetry with the critical external context needed to inform and automate alerting, blocking and response orchestration."

Tim Chen
CEO, DomainTools

TECHNICAL SOLUTION

The DomainTools Iris application for the Falcon platform automates the contextualization of domain indicators using the proprietary DomainTools Risk Score and the entire DomainTools Threat Profile dataset to help Falcon users make instantaneous decisions on malicious domain indicators. Falcon users can further their investigations by launching DomainTools Iris directly from the Falcon card without disrupting their current investigation within Falcon.

DomainTools Risk Score predicts how likely a domain is to be malicious — often before it is operationalized. This can reduce the window of vulnerability between the time a malicious domain is registered and when it is observed and reported publicly as a component of an attack.

DomainTools Threat Profile provides further predictive analytics by giving security practitioners insight into which domains possess characteristics indicative of "malicious intent." These algorithms analyze the intrinsic properties of the domain and provide phishing, malware and spam scores for the investigated domains.

KEY CAPABILITIES

- Contextualize and profile domains inside the Falcon platform
- Add actionable Risk Scores and Threat Profile intelligence to domain indicators
- Extend your investigations from Falcon without losing context via direct integration with DomainTools Iris

ABOUT DOMAINTOOLS

DomainTools helps security professionals identify malicious infrastructure and allows organizations to get ahead of attacks. Its market-leading domain and DNS infrastructure intelligence allows its customers to get immediate context and visibility on threats, thereby accelerating risk assessments and incident response, and improving overall security posture. Fortune 1000 companies, global government agencies and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work.

Try the App
in the CrowdStrike Store

Learn more **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today:
https://www.crowdstrike.com/free-trial-guide/