DOMAINTOOLS

# DomainTools for Recorded Future

Enabling Rapid Alert Triage and Response

## DomainTools Iris Investigate API in the Recorded Future Domain Intel Card

Domain names factor into almost every variant of cyberattacks, and yet analysts must frequently consult multiple disparate resources to build a complete risk assessment. The DomainTools Iris Investigate API delivers a comprehensive domain profile in the Recorded Future Domain Intel Card, enabling rapid alert triage and response. With immediate, in-context access to the unparalleled DomainTools Iris dataset, analysts will gain domain data in a carefully designed, expandable manner allowing information groups be easily navigated.

## Domain Risk Assessment

Risk factors including domain age and registration status appear at the very top of Iris results to enable rapid threat assessments, including the Domain Risk Score. Domain 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. Data shown on the intel card includes the classifiers and evidence behind the score to better inform analyst actions.


**Additional sections appear on-demand below the risk factors, offering details including:**

- Domain registration details
- IP location and ASN for web host, name server and mail server
- SSL certificate details, including common name and certificate hash
- Website tracking codes & response profile

## DomainTools Iris

Analysts can also continue their domain name research directly in the DomainTools Iris platform with a link that preserves their context and starts an Iris Investigation with the domain they were researching in Recorded Future.

 | sales@domaintools.com | (206) 838-9020 | www.domaintools.com