BLACK KITE

DATA SHEET

Black Kite ThreatTrace™

Detect IOCs and anomalies using internet traffic flows for deeper third-party risk intelligence and stronger cyber ratings

NetFlow and DNS telemetry have long been valuable data sources in the SecOps world to detect suspicious activity and support cyber investigations. But that level of visibility hasn't historically been accessible or operationalized for third-party risk teams assessing vendor exposure.

Black Kite is the first TPCRM platform to apply internet traffic signals of compromise to third-party use cases, delivering deeper insight into vendor risk. By analyzing 1T+ internet traffic flows, ThreatTrace™ surfaces indicators of compromise (IOCs), suspicious behavior, and anomalies across your ecosystem, enabling deeper risk intelligence, stronger cyber ratings, and more targeted vendor outreach.

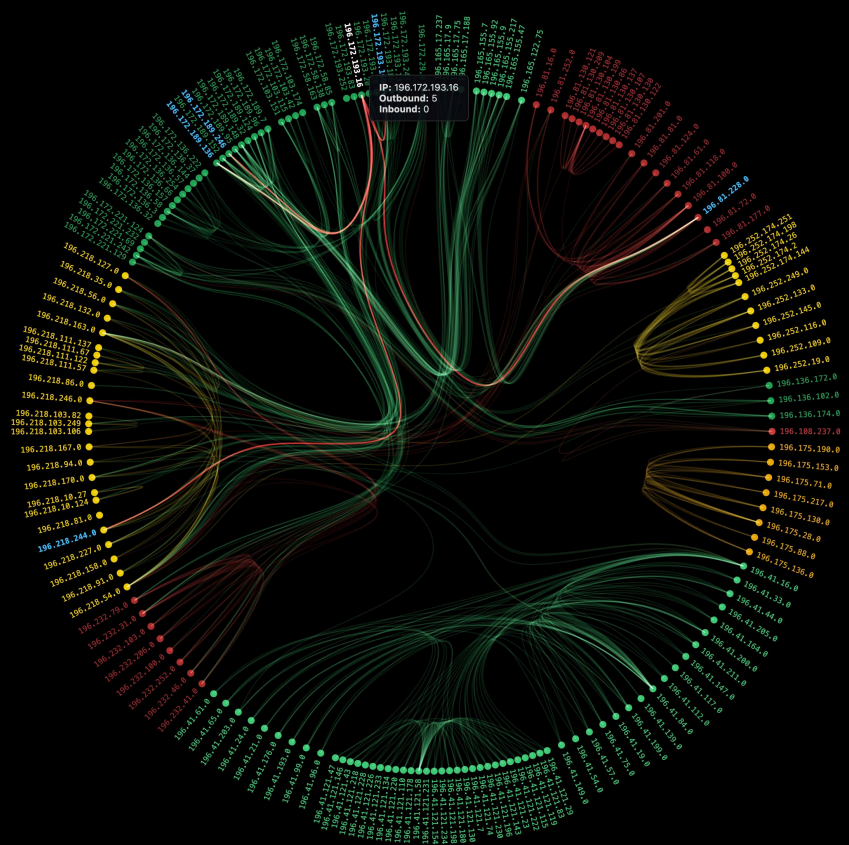
Business Impact

- → Earlier detection of compromise
- → Stronger cyber ratings
- → More targeted vendor outreach

How It Works

ThreatTrace™ analyzes internet traffic flows using NetFlow and DNS telemetry. The type of visibility this telemetry provides is similar to what you would see on a phone bill. It shows who connected to whom, when, how often, and for how long - not what was said. While internet traffic analysis doesn't inspect packet content, it reveals powerful behavioral signals that can indicate potential compromise.

With ThreatTrace, TPCRM teams can detect Indicators of Compromise (IOCs) and anomalies, including Botnet infection, suspicious outbound activity, traffic baseline deviations, threat actor targeting, and more.



What ThreatTrace™ Delivers

Stronger Cyber Intelligence
Adds new controls informed by NetFlow and DNS telemetry to the IP Reputation risk category, which are factored into cyber ratings.

Broader IOC/Anomaly Detection
Enables detection of botnet infection, suspicious outbound traffic, active threat actor targeting, traffic baseline deviations, and more.

Greater Supply Chain Visibility
Enhances digital footprinting by uncovering new subdomains and connected third-party service providers.

Key Detection Capabilities

BOTNET INFECTION
Identifies IP addresses blacklisted by multiple threat intelligence sources as malicious or compromised, potentially associated with botnet activity including spam campaigns, DDoS attacks, or C2 operations.

SUSPICIOUS OUTBOUND ACTIVITY
Correlates DNS queries to high-risk domains - such as Tor sites, hacker forums, or known C2 servers - with outbound network traffic from company IPs.

ACTIVE THREAT ACTOR TARGETING
Detects known malicious IPs actively interacting with an organization's digital assets, signaling live reconnaissance or attack activity.

TRAFFIC BASELINE DEVIATIONS
Flags abnormal traffic patterns including unusual data volume spikes, connections to previously unseen high-risk IPs, or abnormal port usage - common indicators of data exfiltration.

GEOPOLITICAL & SERVICE RISK
Identifies unauthorized services and suspicious data flows to high-risk or sanctioned regions, helping uncover compliance violations and potential data leakage.

Black Kite is a leading third-party cyber risk management platform trusted by thousands of customers to manage every supplier and every risk across their extended ecosystem.

To learn more, visit: www.blackkite.com

Gartner Peer Insights. Customer First

IT Vendor Risk Management Solutions

4.8 ★★★★★