Torq and Black Kite

Integrate to automate third-party cyber risk detection and response

BUSINESS CHALLENGE

Third-party cyber risk has outpaced the manual processes built to manage it. Vendor onboarding, ongoing monitoring, and incident response remain fragmented across spreadsheets, questionnaires, and disconnected tools — leaving security teams with stale visibility and delayed reactions when a vendor's risk posture changes. By the time a ransomware event, breach, or critical exposure surfaces in the supply chain, the window to act has often already closed.

SOLUTION

Torq + Black Kite makes third-party risk management smarter and faster by turning continuous intelligence into action. Black Kite continuously monitors the vendor ecosystem and delivers AI-powered cyber ratings, Ransomware Susceptibility Index™ (RSI™) scores, and FocusTag® alerts the moment a vendor's risk posture changes. Torq takes those signals and automates the next steps — classifying risk, opening cases, enriching context, notifying stakeholders, and orchestrating response across the SOC and risk stack. Together, they shrink third-party incident response from days to minutes.

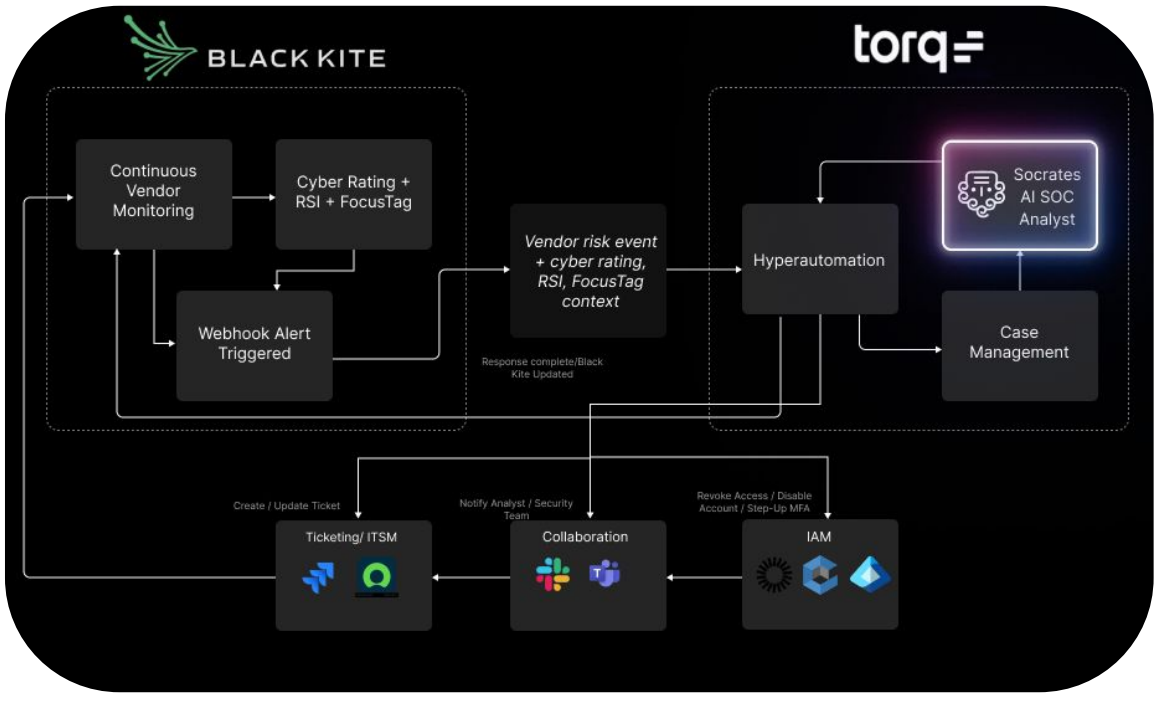
VALUE

With Torq and Black Kite working together, third-party risk moves from manual triage to automated orchestration. Vendor risk events arrive enriched with cyber rating, RSI™ score, FocusTag® context, and breach signal details. Response then flows seamlessly through the SOC and risk stack — whether via automated case creation, stakeholder notification, scheduled reporting, or analyst review when needed.

This reduces manual triage by eliminating repetitive vendor risk reviews and surfacing changes with the context teams need to act fast. It accelerates response, closing the gap between a vendor risk signal and meaningful action. Most importantly, it strengthens the third-party risk program by ensuring vendor exposures are continuously detected, validated, and addressed before they become incidents.

Torq + Black Kite Benefits

- **Automated intelligence to action:** Black Kite webhook alerts flow directly into Torq workflows, turning every FocusTag®, RSI™ threshold, and breach signal into instant, automated response.
- **Context-rich decisions:** Pull cyber ratings, RSI™ scores, and FocusTag® details from Black Kite directly into Torq workflows to prioritize the highest-risk vendors.
- **Seamless SOC integration:** Black Kite alerts trigger Torq workflows that connect seamlessly to Case Management, Jira, ServiceNow, Slack, or Microsoft Teams.
- **Reduced analyst fatigue:** Torq automatically gathers vendor, rating, and ransomware context, freeing security and risk teams to focus on real exposure instead of manual review.
- **Proactive risk reporting:** Scheduled Torq workflows turn Black Kite's multi-dimensional cyber ratings into automated, always-current reports for stakeholders and leadership.



HOW IT WORKS

Black Kite continuously monitors the vendor ecosystem, scoring third parties across 20 risk categories and surfacing changes through real-time webhook alerts — including FocusTag® events, RSI™ threshold crossings, and data breach signals. When Black Kite emits an alert, the event flows into Torq, where Hyperautomation enriches it with vendor, rating, and ransomware context pulled directly from Black Kite's APIs.

Socrates AI SOC Analyst evaluates the enriched event, correlates it against historical signal, and decides the right path. High-confidence risk events trigger automated response — opening cases, notifying vendor owners through collaboration channels, or routing tickets in Jira or ServiceNow. Higher-impact or ambiguous events route to Case Management with full context, so analysts and risk owners can decide in seconds rather than hours.

On a continuous schedule, Torq also pulls Black Kite's multi-dimensional cyber ratings and RSI™ data into automated reporting workflows — surfacing top-risk vendors, trending exposures, and supply-chain ransomware signals to stakeholders without manual effort.

Torq + Black Kit Use Cases

Accelerated Third-Party Incident Response: When Black Kite emits a FocusTag®, RSI™, or breach alert, Torq pulls vendor context, opens a case, and orchestrates response across the SOC stack — turning months of advance notice into immediate action.

Automated Vendor Risk Reporting: Torq pulls Black Kite's multi-dimensional cyber ratings on a daily or weekly schedule, generates risk reports, and delivers them to stakeholders — replacing manual reviews with always-current visibility.

Proactive Ransomware Risk Monitoring: Torq analyzes the vendor population through Black Kite's RSI™, surfaces vendors trending in the wrong direction, and notifies risk owners with context — moving teams from reactive to proactive.

About Black Kite

Black Kite is a leading third-party cyber risk management platform, fueled by AI-powered intelligence to deliver automated vendor cyber risk monitoring and assessments. With multi-dimensional cyber ratings across 20 risk categories, the Ransomware Susceptibility Index™ (RSI™), and FocusTag® intelligence, Black Kite gives organizations always-on visibility and trusted intelligence to act confidently — reducing the exposure and impact of potential third-party threats.

For more information, visit blackkite.com.

About Torq

Torq is the AI SOC platform transforming how enterprises manage risk. Using adaptive agentic reasoning and automation, Torq identifies, prioritizes, and remediates critical threats at machine speed, slashing MTTI and MTTR while amplifying productivity. Global leaders like PepsiCo, Procter & Gamble, Siemens, Telefónica, and Virgin Atlantic trust Torq to power the next generation of AI-driven security operations.

For more information, visit torq.io.