Cogility TacitRed

Monitor, Manage, and Mitigate Cyber Third-Party Risk

Executive Summary

Adversaries actively target third parties in the supply chain to gain access to entities that are otherwise secure, thus making third-party risk management a critical priority. Existing solutions for third-party risk have failed to go beyond point-in-time snapshots and do not provide enough actionable details and transparency for full mitigation. Cogility offers a completely cloud-based third-party risk management product—Cogility TacitRed—to fill this market need.

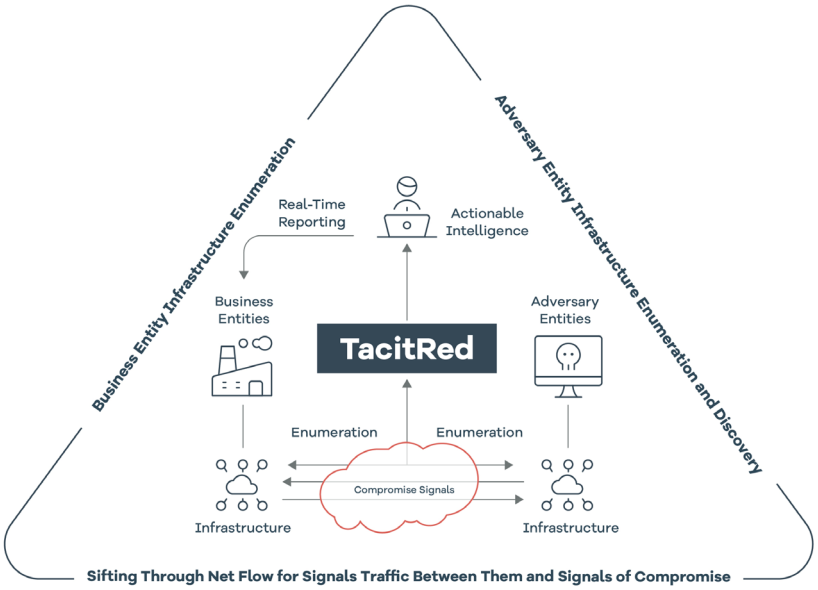
Problem

Despite vendor vetting processes, contractual obligations, robust internal cyber security controls and teams, and even security compliance standard certifications, risks remain. Even the most advanced analytic platforms struggle to solve the complete set of challenges—automated entity enumeration, internet scale NetFlow signals processing, and automated malware intelligence analysis—in single comprehensive platform capability.

Solution

Cogility TacitRed continuously monitors internal and external cyber risks on an always-on basis in near real-time. It not only identifies targeted technologies, but also actively detects malware compromises and network interactions related to ongoing threat actor operations. All of the most damaging, headline-grabbing hacks of recent years—Colonial Pipeline, Maersk, Okta, Target, SolarWinds—would have been flagged by TacitRed.

How Does It Work?



By combining our unique understanding of the threat actors, detailed insight into the current vulnerabilities of that entity, and actively tracking compromised systems and networks; we calculate and rank the likelihood of that entity becoming a victim of a cyber-attack, and provide actionable intelligence—including specific compromise details. For the TacitRed product offering, Cogility has sourced factual signals based on NetFlow, observed threat actor targeting patterns, validated post-compromise telemetry, threat actor communications, and malware botnet logs collected directly from threat actor infrastructure.

Key Product Features

- Advanced cyber situational awareness for your entire third-party cyber threat landscape
- Cloud / SaaS / “turnkey”
- Highly-scalable
- Transparent Risk Scores
- View active compromise details with powerful investigative tools allowing your IT / security staff to coordinate mitigating actions

Benefits

- Streaming analytics; not query-based
- Stateful results; not a snapshot
- Highly tunable results using Bayesian risk
- Automatic enumeration of vendor sub-domains and IP ranges—no need for vendor data input
- Provides full provenance for all data sources

Proven Results at Scale

Tacit Red sampled 30K US companies over 30 days of telemetry data—TacitRed discovered:

4.7M	Affiliated Domains
177K	Unique Affiliated IP Ranges
6.9K	Exposed Attack Surfaces
190	Companies with Malware
443	Compromised Web Sessions
445	Being Surveilled
365	Persistent Traffic to Threat Actors

Data Sources/Data Partners

Hudson Rock, Shodan, IPInfo, WhoisXML, Team Cmyru, SAM.GOV

sales@cogility.com | (949) 398-0015

COGILITY