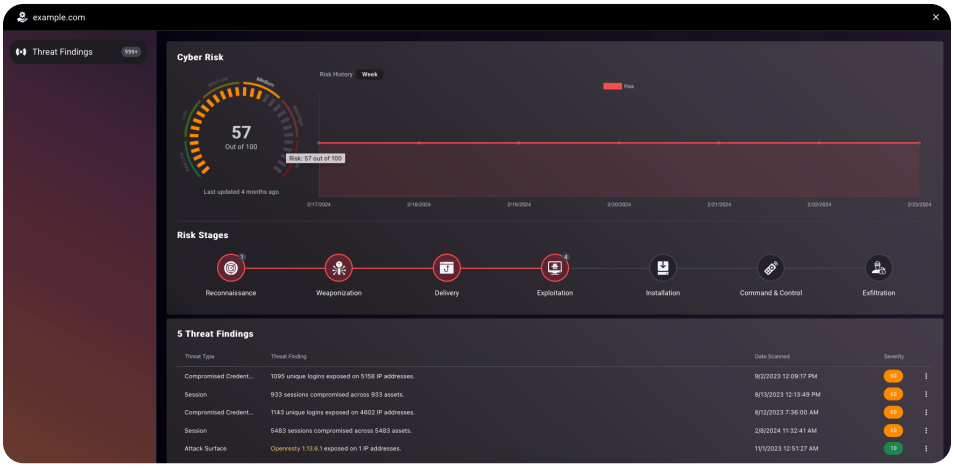
DATASHEET

Cogility TacitRed™

Tactical Attack Surface Intelligence

Summary

Today, over 80% of security breaches[1] originate from threat actors successfully conducting phishing, session, and malware attacks, and exploiting vulnerable internet-facing assets. An organization's external attack surface, including the third parties they work with, is the "soft target" for cyber criminals and nation-state threat actors because already over-stretched security teams have limited operational visibility and are inundated with a deluge of potential exposures, alerts, and threat intelligence noise.



Challenge

Security operations teams are tasked to prevent exposures, respond to threats, and defend assets and sensitive data, while infrastructures are growing rapidly in both size and complexity, with multi-cloud, modern application, IoT, and digital supply chain technologies. In this environment, traditional tools produce an overwhelming volume of potential threats and false alarms, making it impossible to identify real, high-priority threats, let alone respond before it's too late.

Solution

TacitRed™ empowers security teams to take immediate, decisive actions to mitigate exposures with real-time tactical attack surface intelligence – fully curated, specific, and detailed. Compromised and at-imminent-risk assets are prioritized and presented with full context of why they are at risk, accelerating triage and investigation, so organizations can optimize resources, mitigate data breach exposure, proactively improve their security posture, and help reduce supply chain risk.

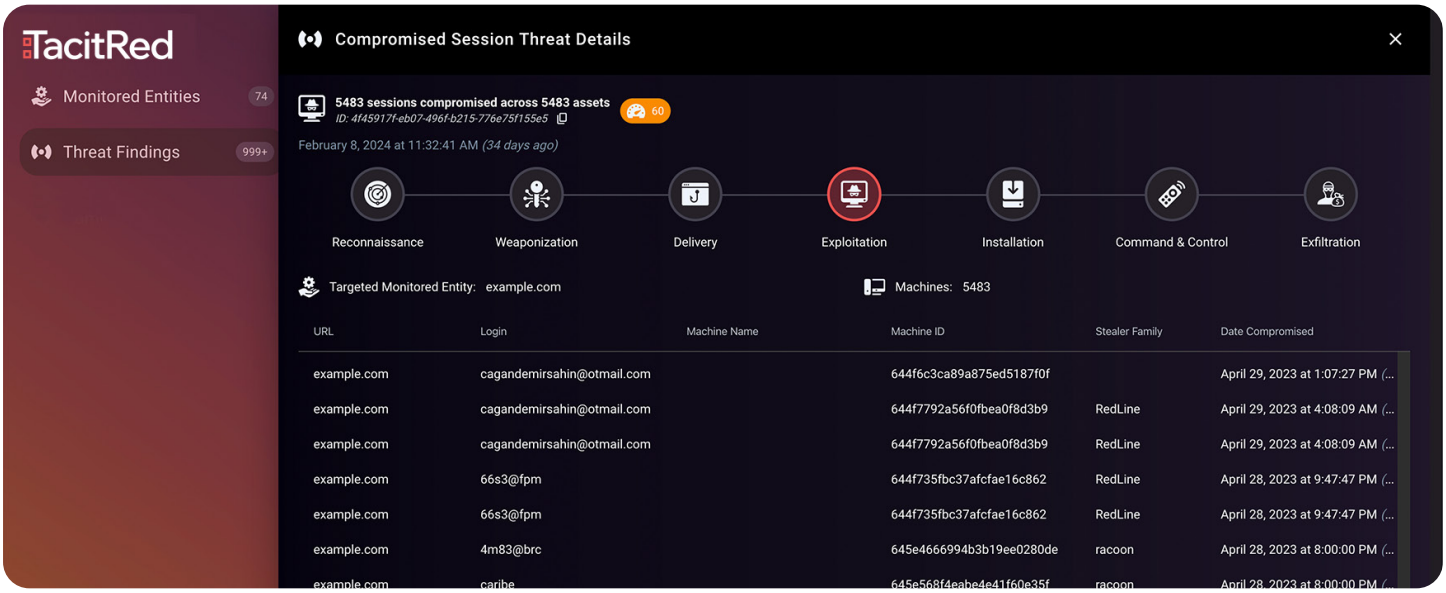
Benefits

- Immediate time-to-value; enables rapid, decisive, and informed threat mitigation
- Continuously analyzed, active attack surface intelligence; focus on impactful exploits and threats with full evidence
- Increase security analyst productivity
- Expedite mean time to resolution, attack impact containment, and proactive measures
- Gain accurate security posture risk insight
- Reduce attacker dwell time and costly data breach exposure
- Obtain true, actionable third-party risk – at scale

1 2024 Verizon DBIR

Exploit Insights

Understand active exploits and at-imminent-risk assets, and where they are on the cyber attack chain stage: reconnaissance, weaponization, delivery, exploitation, installation, command & control, and exfiltration.



Patented Technology

Unlike conventional Attack Surface Management (ASM) approaches, Cogility TacitRed provides Tactical Attack Surface Intelligence that empowers security analysts to take immediate, prioritized, and decisive actions to quickly mobilize mitigation processes for attacked and high target assets. TacitRed uniquely delivers fully curated results, not volumes of additional threat data to query insignificant threats to chase – all the relevant information is at the security analyst fingertips and can be easily integrated into existing tools. As a result, organizations can increase analyst productivity, expedite mean time to resolution, gain accurate security posture risk insight, and reduce costly data breach exposure.

TacitRed goes well beyond mapping an entity's internet-facing assets. Security analysts readily gain an accurate overall threat score and substantiated list of compromised and at-imminent-risk assets with detailed exposure evidence. Severity ratings are offered based on immediacy of the threat, and categorized by threat type and cyber attack chain stage. Now security teams have full context, such as affected machines, IP addresses, and users, needed to streamline investigation, containment, resolution, and prevention processes. In addition, operators can readily obtain tactical attack surface intelligence of third-party entities; to share threat scores and critical security exposures with their subsidiaries, agents, partners, and suppliers to further reduce extended attack surface risk.

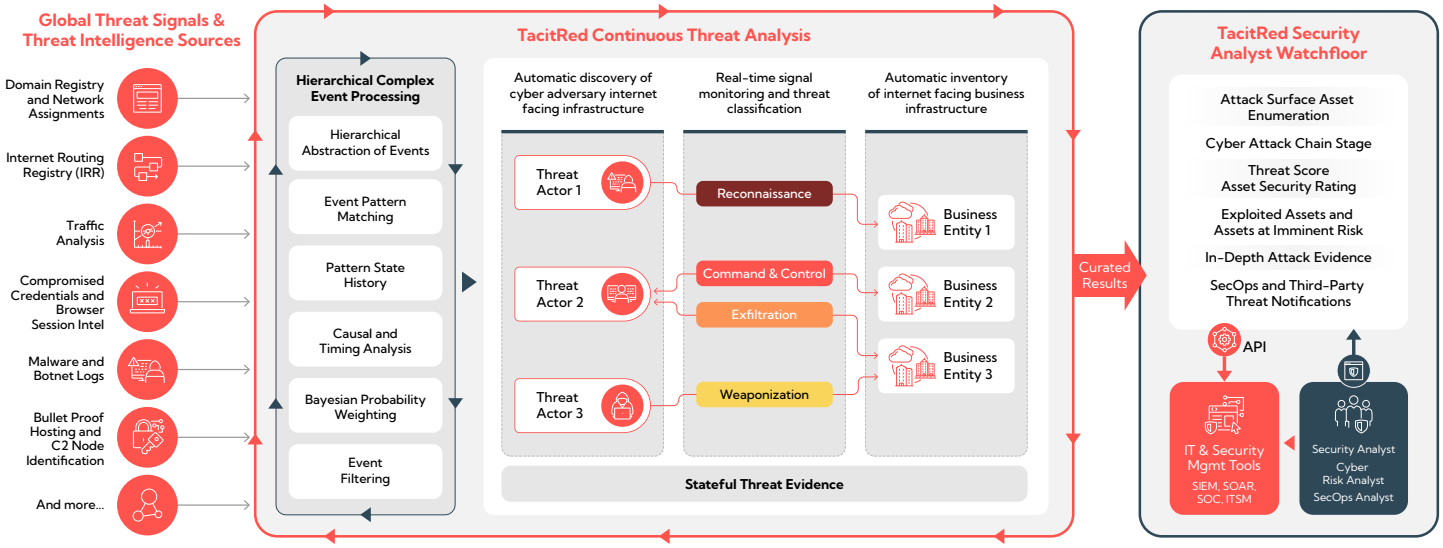
Features

- Constant, pertinent attack surface intelligence – instant, extensive, and at global scale
- Continuous monitoring and analysis of over 18 million U.S. entities – findings available instantly
- Active attack surface mapping with dynamic calculated threat score
- Curated intelligence – full context with no need to filter noise or conduct iterative querying
- In-depth findings categorized by threat type and attack stage, prioritized by severity rating
- Security exposures for third-party entities: agents, partners, acquisition targets, suppliers, etc.

Inner Workings

Offered as a turnkey SaaS solution, TacitRed continuously analyzes massive streams of internet traffic, and attack signals, and a broad array of threat intelligence sources through its patented Hierarchical Complex Event Processing (HCEP) engine to achieve global attack surface asset-to-entity associations, dynamic threat actor reconnaissance, and deep exploitation activity monitoring. TacitRed provides on-demand, tactical attack surface intelligence for over 18 million US companies. Just put in your or a third-party domain to instantly examine curated results.

Tactical Attack Surface Intelligence



Fortify External Attack Surface Management

1 Inventory
Continuously maps and analyzes your internet-facing assets and connections.

2 Discover
Identifies compromised and at-imminent-risk assets and applies proprietary threat score.

3 Investigate
Curates and prioritizes threats, providing full contextual details using patented technology.

4 Respond
Expedites mitigation efforts by sharing curated findings with incident response teams.

5 Extend
Easily extends to protect your subsidiaries, partners, suppliers, agents, and service providers.

TacitRed's approach to active attack surface intelligence closely aligns to the principles of Gartner's Continuous Threat Exposure Management (CTEM) model, which serves to anticipate and mitigate potential threats before they can escalate.

TacitRed

Visit **www.tacitred.com** to take a tour, request a demo – or better yet, to register to try TacitRed for free.

TacitRed
15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015