DATASHEET

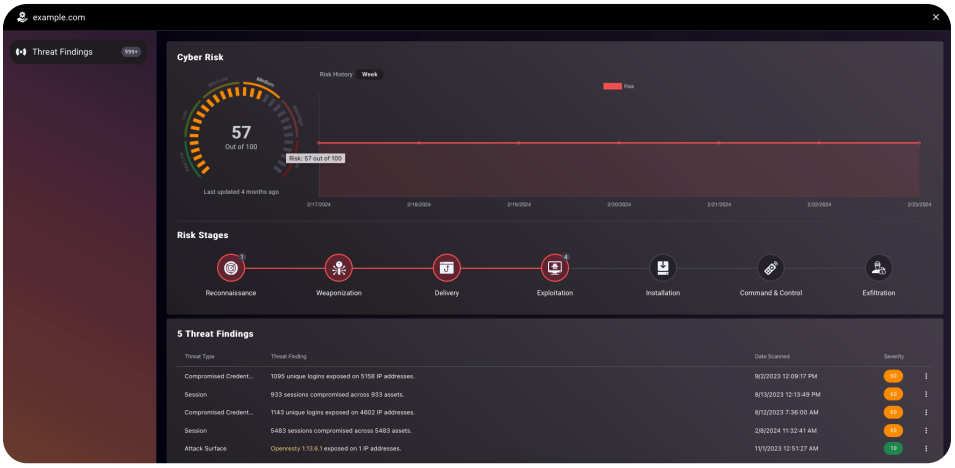
TacitRed

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. Modern infrastructures are growing rapidly in both size and complexity, with multi-cloud, distributed applications, IoT, and 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 issues, let alone respond before it's too late.

Solution

TacitRed™ empowers security teams to take immediate, decisive actions to mitigate active exposures with real-time tactical attack surface intelligence — fully curated, specific, and detailed. Compromised and at-imminent-risk assets are prioritized, visualized, and presented with full context of why they are at risk to accelerate triage and investigation processes.As a result, 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 prioritized exposures with full evidence
- Increase security analyst productivity
- Expedite mean time to resolution, attack impact containment, and proactive remediation
- 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

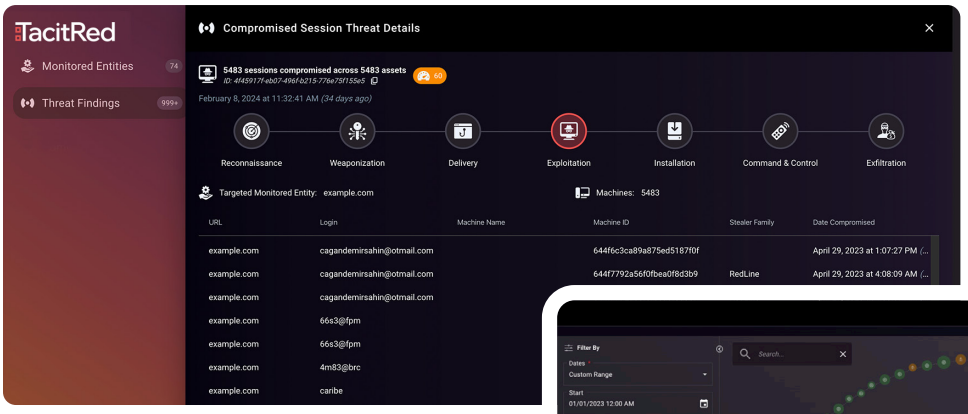
Comprehensive, Fully Curated Intelligence On-Demand

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 or a list of insignificant threats to chase — all the relevant information is delivered through an on-demand SaaS and can be 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.

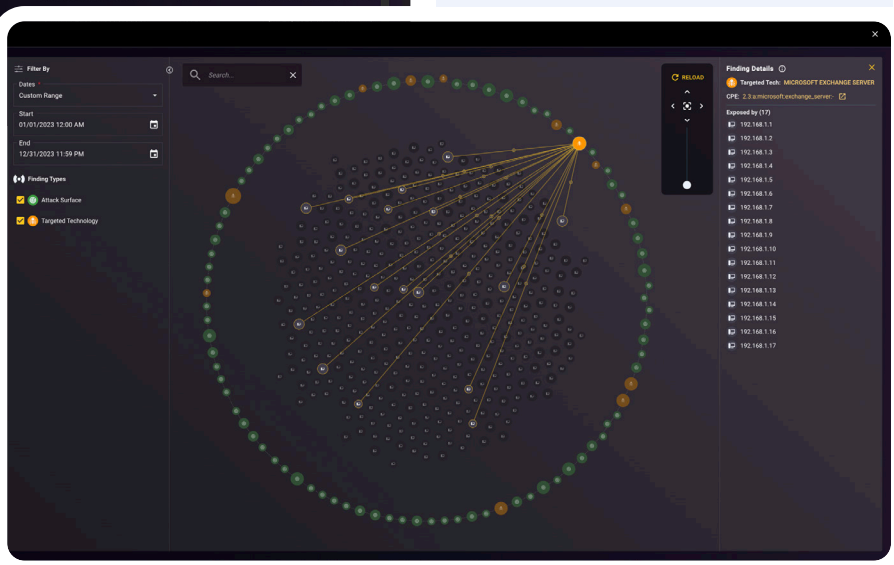
TacitRed provides an interactive visualization and finding dashboard of an entity's external attack surface. Security analysts readily gain an accurate overall threat score and substantiated list of compromised and at-imminent-risk assets with detailed exposure evidence. Analysts can quickly see attack relationships in the Attack Surface Explorer, and examine severity ratings, based on the type and immediacy of the threat, threat type categorization, and cyber attack chain stage — as well as threat and attack details. Now security teams have full context, such as affected machines, IP addresses, and users, needed to streamline investigation, containment, resolution, and prevention processes. Analysts gain high-fidelity first-party and third-party cyber risk insights and can share security issues with subsidiaries, agents, partners, and suppliers.

Features

- Constant, pertinent attack surface intelligence — instant, extensive, and at global scale
- Continuous monitoring and analysis of over 18 million U.S. entities — findings on-demand
- Interactive, searchable, and filterable active attack surface visualization
- Curated intelligence — full context with no need to filter noise or do iterative queries
- In-depth findings categorized by threat type and attack chain stage, prioritized by severity
- Security exposures for third-party entities: agents, partners, acquisition targets, suppliers, etc.



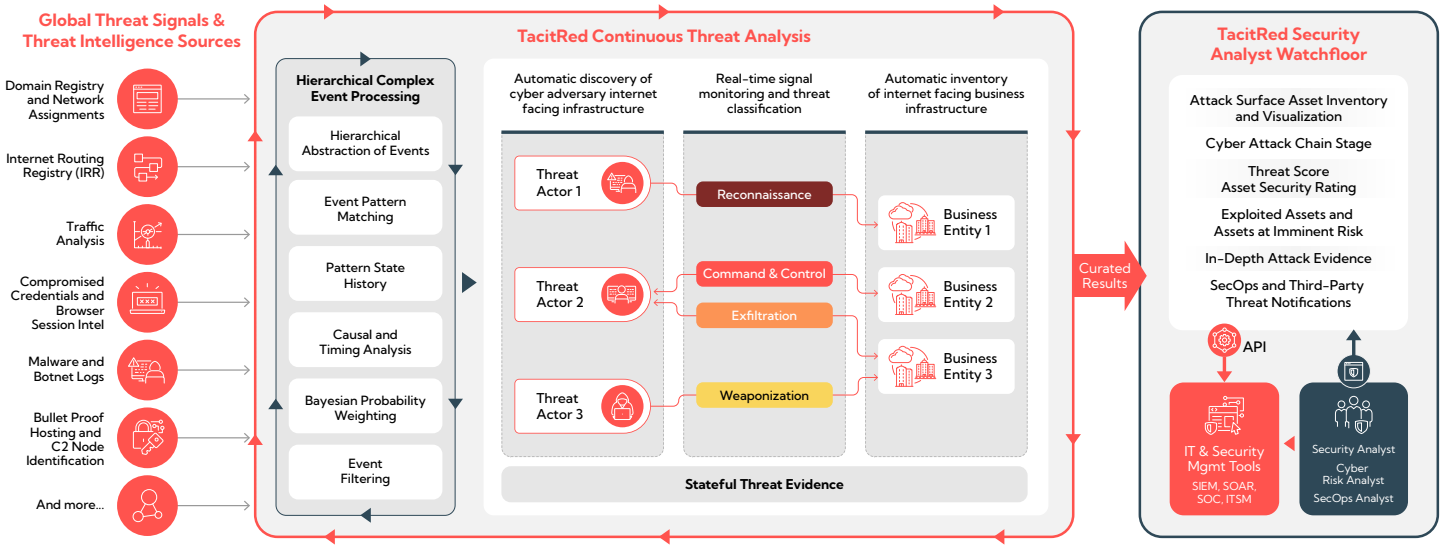
Comprehensive Attack Surface Insights: Interactively visualize and examine active exploits and at-imminent-risk assets with high-fidelity context.



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, threat actor activity monitoring, and comprehensive exposure and exploitation visuals and context. 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 discovers and analyzes your internet-facing assets and security issues.

2 Discover
Identifies, visualizes, and applies a threat score to compromised an imminent-risk assets.

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

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

5 Extend
Easily extend risk analysis to your subsidiaries, partners, suppliers, agents, and service providers.

TacitRed's active attack surface intelligence aligns to the principles of Gartner's Continuous Threat Exposure Management (CTEM) model that serves to anticipate and mitigate cyber exposures before they can escalate.

TacitRed Attack Surface Explorer, Visualize the Features:

Features by Edition

Features	Essentials	Advanced	Professional	Enterprise
User License(s)	1[3]	2	4	Custom
Monitored Entities[2]	5[3]	20	50	Custom
API Service	No	No	Yes	Yes
Continuous Attack Surface Findings	Free[3]	Yes	Yes	Yes
Attack Surface Explorer	Free[3]	Yes	Yes	Yes
Total Threat Score	Free[3]	Yes	Yes	Yes
Findings Severity Rating	Free[3]	Yes	Yes	Yes
Cyber Attack Chain Stage	Free[3]	Yes	Yes	Yes
Reconnaissance Findings	Free[3]	Yes	Yes	Yes
Targeted Technology Findings	Free[3]	Yes	Yes	Yes
Advanced Persistent Threat Findings	Free[3]	Yes	Yes	Yes
Compromised Credentials Findings	Yes[4]	Yes	Yes	Yes
Compromised Sessions Findings	Yes[4]	Yes	Yes	Yes
Malware Infections Findings	Yes[4]	Yes	Yes	Yes
Technical Support	Online	Online	Online	Dedicated

2 Domain names entered for Monitored Entities can be changed after a 90-day period

3 Remains free after Trial Period, however, account will be terminated after 60-days of inactive use

4 Detailed findings are only included during Trial Period or within paid subscription Order term

TacitRed

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

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

sales@cogility.com
+1 949.398.0015