SOCRadar® Your Eyes Beyond

SANS | Research Program

PRODUCT BRIEFING

CTI with SOCRadar:
Insights from the 2025 SANS Institute CTI Survey

May 2025

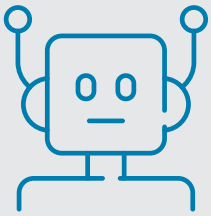
As credential theft and identity-based attacks surge, security teams need early visibility not just into where attackers are entering their networks, but how. The 2025 SANS CTI Survey results confirm that stealer logs, identity-driven threats, and threat intelligence overload have made early detection and actionable reporting more critical than ever.

SOCRadar Extended Threat Intelligence (XTI)

For midsize security teams facing enterprise-level threats, SOCRadar delivers Extended Threat Intelligence (XTI), a unified platform combining digital risk protection, attack surface management, supply chain visibility, and core cyber threat intelligence (see Figure 1). SOCRadar's core platform provides MITRE ATT&CK enrichment, threat actor visibility, and reporting. The newly introduced Copilot expands those capabilities by enabling users to ask simple questions and receive autonomous responses. The result is a faster, more focused response with the help of targeted alerts and AI-powered reporting that delivers the right information to the right people.

Figure 1. SOCRadar Extended Threat Intelligence (XTI)

Key Findings



33% of organizations now use AI in at least one part of their CTI workflow.

Most common AI use cases: data gathering, pattern recognition, and analysis support

Use of AI for reporting and dissemination still lags behind.

Clear, actionable communication is critical—CTI has little value if it isn't understood.

According to the survey, 80% of CTI teams now rely on written reports to share intelligence, up from 62% just three years ago. This shift away from raw data feeds reflects a demand for clearer, more actionable communication and smarter delivery systems. SOCRadar Copilot, an AI assistant built into the platform, addresses that need. It enables users to ask plain-English questions, enrich indicators with MITRE ATT&CK and campaign history, prioritize alerts based on real impact, and auto-generate reports customized by audience and industry. Copilot's AI agents support dynamic task automation, using contextual awareness and business risk to decide when to escalate, what to prioritize, and how to route alerts, creating a definite advantage to traditional rule-based triggers.

When SOCRadar sees a known IoC (indicator of compromise), such as a domain, IP, or file hash, it doesn't just flag it. It instantly adds context by showing which MITRE ATT&CK technique it relates to and whether it's been used in real-world campaigns. SOCRadar Copilot was designed to cut through digital clutter and deliver exactly the kind of AI-enabled support the SANS survey flagged as becoming critical and necessary for CTI maturity. Copilot automates and tailors reporting by audience, generating the right level of insight whether for a SOC lead, executive, or board member.

A core strength of SOCRadar is its deep visibility into stealer logs, collections of stolen credentials (emails, passwords, session cookies) that help attackers log in instead of hack in. These credentials often circulate on the dark web long before a breach is detected.

By surfacing this data early, SOCRadar helps security teams detect credential exposure, track identity-based threats across underground channels, and prevent downstream compromise.

SOCRadar simplifies security workflows by integrating essential capabilities into one pane of glass:

- Attack Surface Management to identify exposed assets and misconfigurations
- Digital Risk Protection to detect and remove impersonation, phishing kits, brand abuse, and initiate takedown actions
- Supply Chain Intelligence to assess third-party risk from surface and dark web sources
- Core CTI Engine to track threat actor behavior and campaign activity with ATT&CK mapping

Together, these capabilities provide full-spectrum external visibility, enriched with one-click takedowns, contextual alarms, and integrations with platforms such as JIRA, Splunk, and Cortex XSOAR.

More than 70% of survey respondents are now feeding CTI into detection and response systems, yet 41% still cite limited automation and integration as major blockers. Respondents also reported increasing pressure to prove CTI's value. SOCRadar tackles this by ensuring every part of the CTI process delivers measurable ROI at every step:

- Enriching raw IOCs with critical context
- Enabling dynamic task automation for alarm prioritization, routing, and false positive reduction
- Offering freemium access and modular pricing
- Auto-generating reports tailored to each audience and industry

The SOCRadar Copilot Light version is free, while Copilot Pro includes advanced AI agents for dynamic task automation, phishing site detection, and full analyst-level support.

Although SOCRadar supports large enterprises, its mission is to democratize CTI for the mid-market. With 15-minute onboarding, a freemium model, and one of the most comprehensive stealer log datasets in the industry, SOCRadar delivers high quality intelligence backed by an active global user community.

Its one-of-a-kind collection practices includes deep monitoring of Telegram and dark web markets to ensure fresh, relevant, and hard-to-find intelligence other platforms miss. From real-time alarms to auto-generated reports to executive-level insights, SOCRadar helps CTI teams get ahead of attackers, show value to leadership, and scale their efforts without scaling their team.

In a world where cybersecurity is everyone's problem but not everyone has the same resources, SOCRadar is making CTI smarter, simpler, and more accessible—one alert, report, and insight at a time.

To learn more, visit
www.SOCRadar.io