CTI Solution Brief

Cyber Threat Intelligence

The process of collecting, analyzing and disseminating data of threats

Cyber Threat Intelligence (CTI) is the collection of data gathering, analyzing, and deducing processes regarding **potential cyber threats,** outcoming attacks, threat actors, their mindsets, strategies, skills, tactics, techniques, and procedures.

In the ever-evolving cyber threat landscape, having insights into a threat actor's **next move** is paramount. It enables organizations to proactively customize their defenses, staying one step ahead to prevent potential attacks. This is where Cyber Threat Intelligence (CTI) emerges as a pivotal tool for businesses aiming to prevent financial loss, **reputational damages** and market credibility that may be adversely affected by cyber incidents. By leveraging the up-to-date intelligence on cyber risks and vulnerabilities, organizations can significantly enhance their capacity to combat threats and efficiently respond to incidents, ultimately strengthening their cybersecurity posture.

Cyber Threat Intelligence

CTI uses several techniques and resources, including open-source intelligence, **dark web surveillance,** social media analysis, to obtain raw data that can help ensure security operations. By evaluating 'the intelligence,' CTI analysts can spot patterns, trends, and **indications of compromise (IOCs),** which can assist enterprises in recognizing and avoiding cyberattacks. **Security teams,** threat hunters, and incident responders frequently use CTI to immediately identify and neutralize risks.

Establishing a robust **CTI process** poses significant challenges for organizations. Some daunting issues, such as data overload, integration, and prioritization, might be a bit overwhelming for the capabilities of organizations' security teams. However, investing in the **right CTI solutions** can let organizations leverage the full potential of threat intelligence, ultimately enhancing their defense against a **dynamic threat landscape.**

SOCRadar's CTI

The actionable intelligence against cyber threats

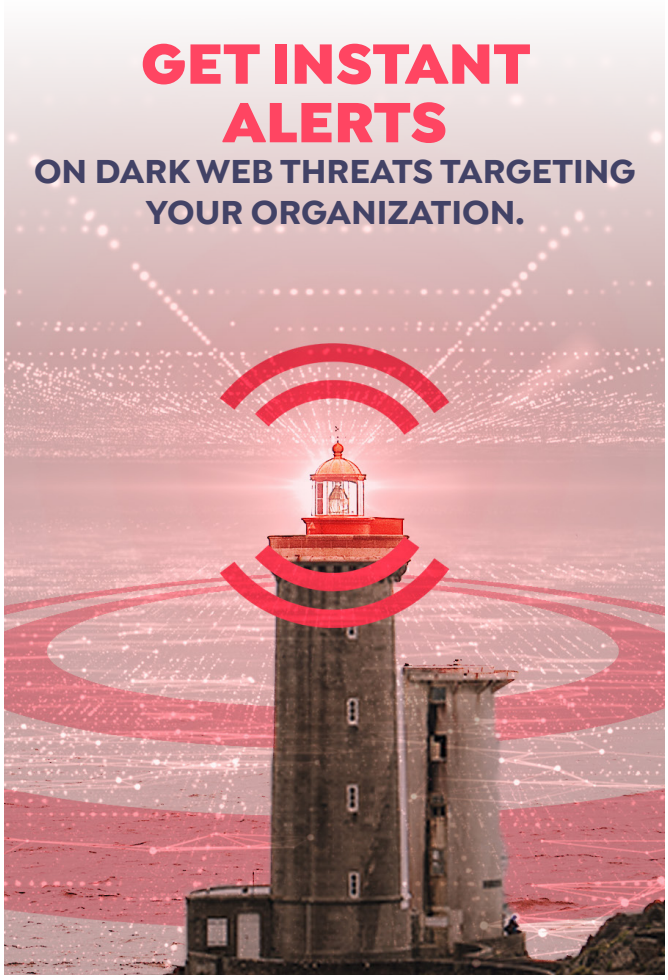
SOCRadar's Cyber Threat Intelligence module is a part of the SOCRadar Extended Threat Intelligence platform that provides **actionable, contextual,** and **real-time intelligence** and analysis to help SOC teams.

SOCRadar CTI is fed by massive data sources across surface, deep, and dark web including paste sites, underground markets and public available source, and provides actionable intelligence incorporating information from these feeds.

SOCRadar's Cyber Threat Intelligence provides extended **API-ready tools** for security teams. The platform presents all the insights covering leaks, breaches, phishing domains, and the threat landscape in an easy-to-read interface for cybersecurity experts.

SOCRadar CTI module helps to keep track of cybersecurity incidents and offers more effective threat hunting and threat actor tracking capability with behavioral analytics, **AI,** and **ML-powered algorithms.** Organizations can stay up-to-date with comprehensive incident reports focusing on attackers' **TTPs and IOCs.**

Security teams can monitor hacker forums and black markets and instantly be alerted about the sales of databases and vulnerabilities concerning their organizations. The CTI module tracks malicious file hashes, domain registrations, suspicious IPs etc. and provides intelligence reports, customizable dashboards, and real-time threat alerts.



Supply Chain Monitoring

A supply chain attack is a form of cybersecurity threat that targets you through a **3rd party partner or provider** that has access to your organizational data or resources. Weak security measures within third-party organizations can potentially compromise the security of entire supply chains, posing significant risks. Recognizing this, SOCRadar CTI strongly focuses on supply chain intelligence to provide effective solutions in this critical area.

SOCRadar's supply chain monitoring extends to various critical areas:

Dark Web Supply Chain Monitoring:

This includes monitoring activities on hacker forums, ransomware forums, and black markets on the dark web.

Surface Web Supply Chain Monitoring:

Cover a wide range of platforms on the surface web, including GitHub, project management tools, data buckets.

Supply Chain Vulnerability Detection:

Employ passive scans to detect vulnerabilities within your supply chain.

SOCRadar CTI offers integrations with various product groups, including **SIEM, SOAR, EDR, firewalls, Threat Intelligence Platforms, Vulnerability Management, Ticketing systems,** and **Team Meeting tools.** These integrations enable feeding security solutions like EDR, SIEM, Firewall, and SOAR products by IOC feeds. So organizations can significantly lighten the load on their security teams and swift action and efficient management, ensuring a vigilant response to alarms concerning their company's cybersecurity.

Gartner

Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

GET
SOCRadar Demo
See Extended Threat Intelligence at work