XTI Solutions Brief

An Innovative Approach to Conventional Solutions: Extended Threat Intelligence (XTI)

SOCRadar's XTI represents a cutting-edge evolution of the traditional threat intelligence platform, featuring **advanced capabilities** that offer superior **threat detection** and **visibility.** This state-of-the-art solution utilizes powerful **machine learning technologies** to analyze vast amounts of threat data sourced from a multitude of **open sources, social media and the dark web.** By leveraging this comprehensive approach SOCRadar's XTI can help security teams to quickly identify and prioritize threats providing them **proactive security.**

The platform combines **External Attack Surface Management, Digital Risk Protection and Cyber Threat Intelligence** modules.

External Attack Surface Management

External Attack Surface Management (EASM) module helps customers **acquire broader visibility** and context regarding the severity of unknown **external-facing digital assets** in an automated manner.

Digital Risk Protection

Digital Risk Protection Service (DRPS) module enables organizations to check their **sensitive data** and **attack surface** by regularly monitoring it.

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) sustains the processes of gathering, analyzing, and sharing information about potential cyber threats in order to protect against them by **collecting data from various sources.**

EXTENDED
THREAT INTELLIGENCE

With XTI's combination of three cybersecurity modules, organizations can **monitor hacker forums, black markets** and instantly be informed about the sales of **databases,** vulnerabilities, etc., that concern the organization, country, or industry while generating instant alerts to prevent data breaches and credential thefts.

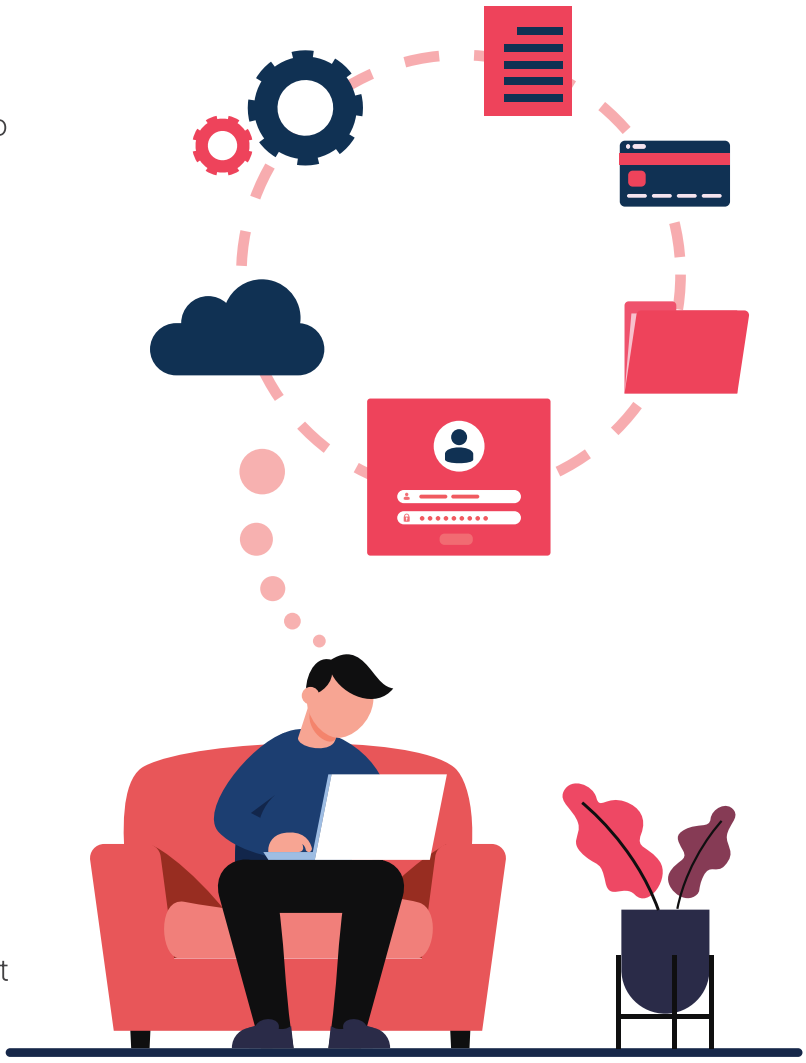
With **customizable dashboards** and user friendly design security teams can easily monitor and **manage threats** based on their specific requirements without the need for third party installations.

SOCRadar XTI offers seamless integration with a **range of security tools,** such as **SIEMs, threat intelligence platforms, endpoint detection and response (EDR) solutions** enabling organizations to create a **robust cyber defense.** It also has capabilities of offering advanced **threat hunting mechanisms** that enable security teams to **proactively identify** and respond to threats before they cause any damage. SOCRadar's commitment to staying ahead of emerging threats is demonstrated through its constant updates to its threat intelligence database ensuring that security teams have access to the most up-to-date information.

Why Now?

Over the past decade, **the rapid advancement of digitization** and the **growing reliance on digital platforms** have brought cybersecurity to the forefront as a critical concern. The inherent and residual risks associated with global connectivity pose significant threats to every industry integrated with digital networks. As a result of the increasing dependence on cutting-edge technologies and the extensive transmission of data through digital channels, cybersecurity has emerged as a top priority on the global stage.

In today's interconnected world, data has become a crucial element for businesses, necessitating robust protection against **malicious actors.** Cybersecurity revolves around safeguarding against **data breaches** and **mitigating** any risks that may result in harm. As the volume of data generated, stored, and shared across various platforms continues to grow exponentially, the importance of cybersecurity becomes increasingly paramount. Furthermore, with the rise of new technologies such as **artificial intelligence** and **the Internet of Things,** the complexity of potential cyber threats also increases, making it imperative for businesses to prioritize and invest in **comprehensive cybersecurity strategies.**



The shift to **cloud-based services** offers numerous advantages, including **cost reduction,** increased **scalability,** and e**nhanced flexibility.** However, this migration also exposes organizations to a **new range of cyber threats and vulnerabilities.** Transferring digital assets, such as **IT infrastructure, applications, databases, and servers** to the cloud demands meticulous planning to prevent potential breaches and leaks. Consequently, businesses must prioritize and invest in robust cybersecurity measures to **protect their critical assets** while harnessing the benefits of cloud computing.

The widespread use of digital technologies and the internet has created a universal vulnerability that transcends traditional boundaries. Cybercriminals are not constrained by the same limitations as conventional criminals, enabling them to launch targeted or indiscriminate attacks from any corner of the world. This means that no organization is immune to the risk of cyber threats, and even small-scale businesses or those operating in niche sectors must prioritize cybersecurity to protect their sensitive data, systems, and networks.

Cybercrime inadvertently turned into an increasingly lucrative business for cybercriminals. In 2022 alone, cyber attacks experienced **a surge of 38% compared to 2021.** Furthermore, the financial impact of these attacks is staggering, with **global losses estimated to exceed $10.5 trillion between 2015 and 2025.** This trend highlights how the rapid expansion of global connectivity has created a thriving market for threat actors, who can now capitalize on the widespread digital dependency to launch instant attacks and reap significant profits.

The rise of the **remote workforce,** exacerbated by the **COVID-19 pandemic,** has significantly transformed the cyber threat landscape, introducing new challenges and vulnerabilities for organizations to address. As more employees work remotely, the reliance on virtual private networks (VPNs) and other remote access technologies has increased, expanding the potential attack surface for cybercriminals. This shift has led to a greater risk of unauthorized access, data breaches, and targeted phishing campaigns aimed at exploiting the remote workforce.

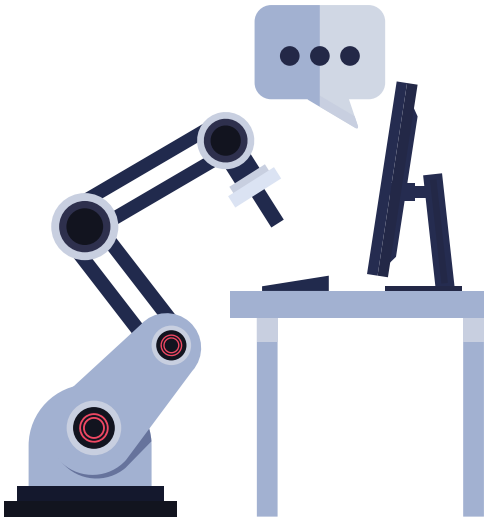
The ever-evolving landscape of cybersecurity requires an unconventional approach to effectively combat these challenges. The lack of skilled professionals in the cybersecurity domain further intensifies the difficulty businesses face in countering cyber threats.

Organizations must adopt a comprehensive strategy that encompasses the hacker-mindset to anticipate and understand potential threats, implement early warning system for proactive defense, and **leverage automation to reduce human errors and enhance security measures.** By embracing these innovative approaches, businesses can better protect their digital assets and stay ahead of the curve in a world where the complexity and scope of cyber threats continue to expand.

Why SOCRadar?

As a cybersecurity company, SOCRadar provides **comprehensive threat intelligence** and **security automation capabilities** to help organizations detect, investigate and respond to cyber threats in real-time. The company aims to provide a **safer digital world** and **sustain a better security surface** while prioritizing **proactive security** with analyzing the hacker-mindset constantly. SOCRadar supports enterprises to maximize the efficiency of their security teams with **false-positive, free, actionable and contextualized threat intelligence.**

Cyber threat intelligence involves routine tasks that are often performed manually. These tasks may include data collection from various sources, analysis of collected data, and identification of potential threats. While automation and machine learning can significantly reduce the manual workload, human expertise remains essential for recognizing the context, validating the accuracy of intelligence, and making strategic data-driven decisions.



XTI

SOCRadar's major product, **XTI platform,** is designed to assist organizations to proactively identify, analyze and mitigate cyber threats through an effective approach. **Utilizing sophisticated analytics, machine learning, and the expertise of human analysts,** our CTI platform offers **contextualized and actionable intelligence** to help organizations in safeguarding their digital assets and minimize the risk of cyberattacks.

SOCRadar XTI represents a successful **fusion of automation** and **human expertise.** As the 'extension of security teams' SOCRadar automates critical tasks such as **data collection, threat detection, and initial analysis.** However, the true strength of XTI Platform lies in its seamless integration of human expertise. Skilled analysts validate the tool's findings, putting into a context and clarify the tactics of threat actors. This unique **combination of automation and human touch** not only streamlines the threat intelligence process but also ensures that organizations **receive false-positive free alerts.**

As a **SaaS and cloud-based company,** SOCRadar allows users to easily scale their software usage up or down based on their needs, making it an ideal choice for businesses with fluctuating needs. Discovering digital assets without any demand from the customer, **generating alerts for early warning systems and hunting leakages,** SOCRadar aims to **ensure the security surface and leverage the customer's durability** against external attacks. The XTI platform, the main service of SOCRadar, offers numerous advantages including accessibility from any location simply with an internet connection, **scalability** to adapt an organization's needs and cost-effectiveness due to lower upfront costs, eliminating infrastructure expenses. Additionally, rapid deployment, seamless integration with other security tools, and ongoing support from expert teams are among XTI platform's multitude of advantages.