SOCRadar®
Your Eyes Beyond

US MANUFACTURING THREAT LANDSCAPE REPORT

"300% Increase in the Number of Dark Web References to Manufacturing Organizations"

socradar.io

The Rising Tide of Cyber Threats in the US Manufacturing Industry

In recent years, the manufacturing industry has increasingly become a hotbed for cyber-attacks due to its extensive networks and significant data assets. As digitization and globalization continue to grow, manufacturing sectors are becoming more interconnected and, consequently, more susceptible to cyber threats. The complexity of networks in the manufacturing industry, as well as the valuable data they manage, makes them a prime target for hackers

.

The COVID-19 pandemic further complicated the scenario by accelerating the adoption of remote operations and industrial control systems, thereby stretching IT security practices thin and creating more opportunities for cyber-attacks. IBM's X-Force cybersecurity intelligence division reported that in 2021, the manufacturing industry surpassed finance and insurance to become the "most attacked" industry. Ransomware and email compromise attacks particularly surged. In this blog, we will delve into the data collected from the SOCRadar Extended Threat Intelligence platform, focusing on the timeframe from July 2021 to June 2023.

Key Cyberattacks in US Manufacturing

Tracking the trajectory of cyber threats over the years offers essential insights into cybercriminals' evolving tactics and impact. The following timeline outlines some major cybersecurity incidents in the US manufacturing industry from 2020 to 2022, illustrating the escalating challenge of safeguarding sensitive data and essential operations against increasingly sophisticated threats.

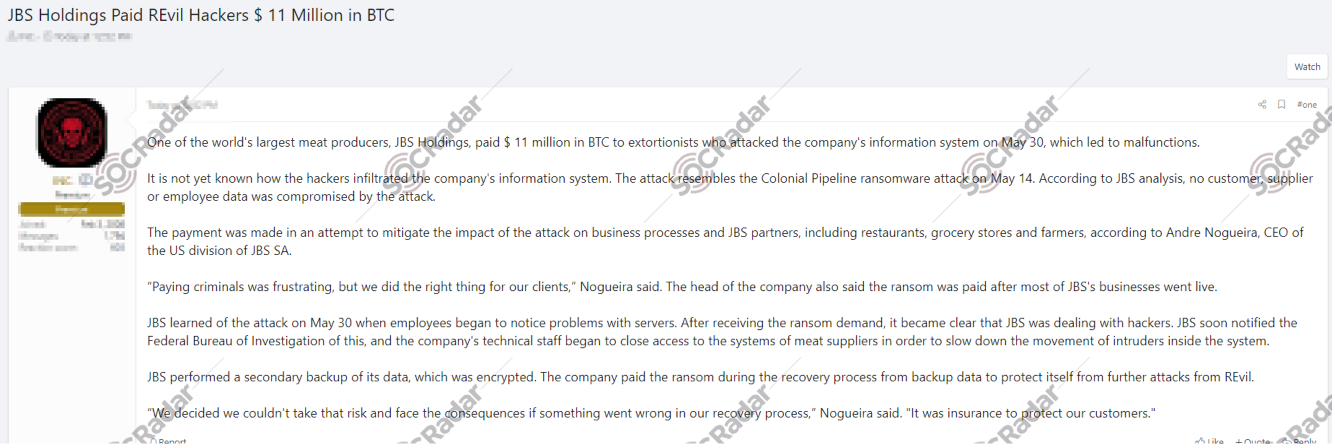
2020

Tesla: In August 2020, a Russian citizen attempted to recruit a Tesla employee to install malware into Tesla's Nevada Gigafactory. The plan was to extract data and launch a ransomware attack. However, the employee reported the attempt to the company, and the FBI apprehended the perpetrator.

Key Cyberattacks in US Manufacturing

2021

Cybersecurity in the manufacturing sector has become an issue of pressing concern over recent years. As manufacturers transition to digital operations, they present an enticing target to cybercriminals due to the complex networks they employ and the rich troves of valuable data they store. A prominent example of this escalating trend is the recent $70 million ransomware attack on Taiwan Semiconductor Manufacturing Company (TSMC), an Apple supplier, orchestrated by the Russian ransomware gang, LockBit.



JBS Holdings Paid REvil Hackers $ 11 Million in BTC

One of the world's largest meat producers, JBS Holdings, paid $ 11 million in BTC to extortionists who attacked the company's information system on May 30, which led to malfunctions.

It is not yet known how the hackers infiltrated the company's information system. The attack resembles the Colonial Pipeline ransomware attack on May 14. According to JBS analysis, no customer, supplier or employee data was compromised by the attack.

The payment was made in an attempt to mitigate the impact of the attack on business processes and JBS partners, including restaurants, grocery stores and farmers, according to Andre Nogueira, CEO of the US division of JBS SA.

“Paying criminals was frustrating, but we did the right thing for our clients,” Nogueira said. The head of the company also said the ransom was paid after most of JBS's businesses went live.

JBS learned of the attack on May 30 when employees began to notice problems with servers. After receiving the ransom demand, it became clear that JBS was dealing with hackers. JBS soon notified the Federal Bureau of Investigation of this, and the company's technical staff began to close access to the systems of meat suppliers in order to slow down the movement of intruders inside the system.

JBS performed a secondary backup of its data, which was encrypted. The company paid the ransom during the recovery process from backup data to protect itself from further attacks from REvil.

“We decided we couldn't take that risk and face the consequences if something went wrong in our recovery process,” Nogueira said. "It was insurance to protect our customers."

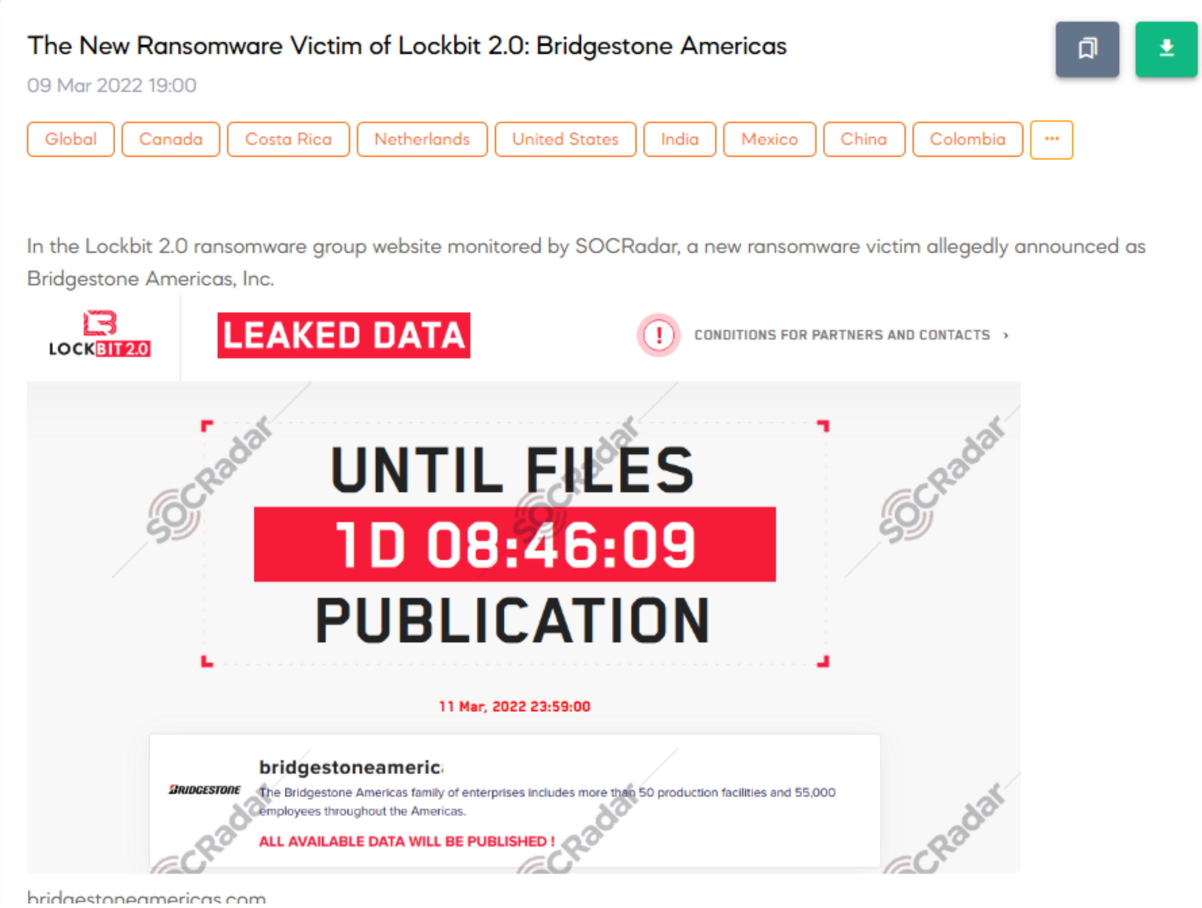
Quanta Computer: Quanta Computer, a Taiwan-based manufacturer that supplies several large tech companies in the US, like Apple, was targeted by a ransomware attack from the REvil group in April 2021.

Colonial Pipeline: In May 2021, the Colonial Pipeline, which supplies nearly half of the US East Coast's fuel, was forced to halt operations due to a ransomware attack, resulting in widespread fuel shortages and flight cancellations. The company ended up paying a $4.4 million ransom to restore its network.

JBS USA: In June 2021, JBS USA, a leading processor of beef, pork, and other prepared foods, was hit by a ransomware attack believed to be carried out by REvil. The attack led to shutdowns at the company's US-based meat processing plants.

Key Cyberattacks in US Manufacturing

2022



The New Ransomware Victim of Lockbit 2.0: Bridgestone Americas

09 Mar 2022 19:00

Global | Canada | Costa Rica | Netherlands | United States | India | Mexico | China | Colombia | ···

In the Lockbit 2.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Bridgestone Americas, Inc.

bridgestoneameric

The Bridgestone Americas family of enterprises includes more than 50 production facilities and 55,000 employees throughout the Americas.

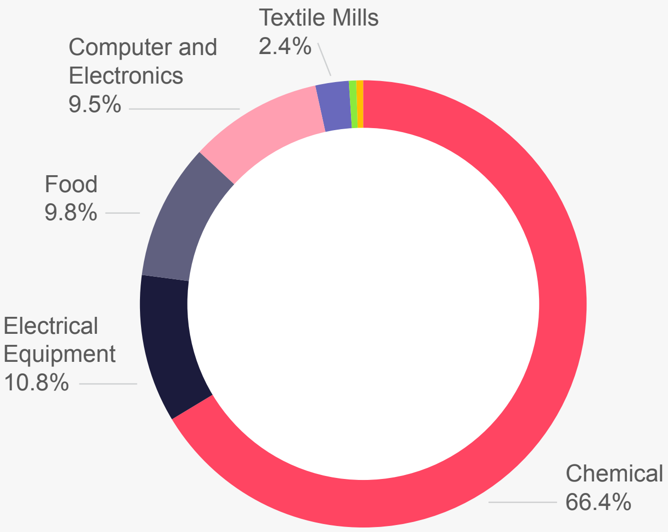
ALL AVAILABLE DATA WILL BE PUBLISHED !

bridgestoneamericas.com

Bridgestone Americas: In February 2022, Bridgestone Americas, a tire producer, suffered a cyberattack from the LockBit ransomware group. The company had to disconnect computer networks and halt production at several facilities across North America. This timeline represents some of the most notable cyberattacks on manufacturing companies directly affecting the US over the past few years. As cyber threats evolve, manufacturers must stay vigilant, adopt robust cybersecurity practices, and seek dynamic solutions to mitigate these attacks.

Dark Web Activities Concerning the US Manufacturing Industry

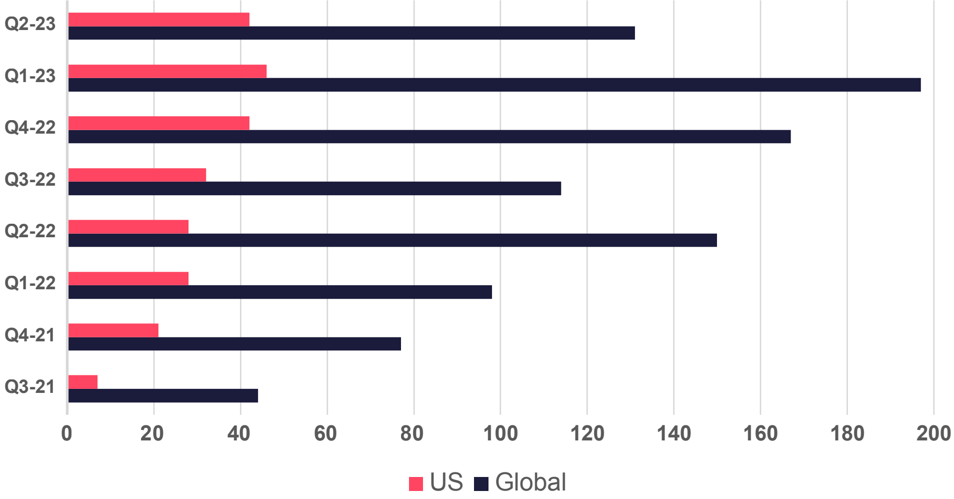
SOCRadar analysts examined posts mentioning the Manufacturing Industry and uncovered he breakdown of posts by sub-industry. Notably, just over 30% (295 out of 978) had secondary tags. As illustrated in the pie chart below, Chemical Manufacturing emerges as the primary target for threat actors in the US manufacturing industry.



Over the past two years, our data from SOCRadar Platform has revealed a notable surge in dark web activity concerning the manufacturing industry. Between July 2021 and June 2023, we recorded 27,214 posts on the platform. Of these, 978 posts, specifically related to the manufacturing sector. A detailed review of these posts indicates an upward trajectory over time.

In the third quarter of 2021 (Q3 2021), only 44 posts discussed the manufacturing industry and a mere 7 of those targeted US-based organizations. Fast forward to the first quarter of 2023 (Q1 2023), and these figures ballooned to 197 manufacturing-related posts in total, with 46 explicitly directed at US firms.

Number of the Dark Web Posts Mentioning Manufacturing Industry US vs. Global



Interestingly, the second quarter of 2023 (Q2 2023) showed a mixed picture. While the total number of manufacturing-related posts declined to 131, the number of posts targeting US entities dipped slightly to 42. This trend led to a peak in the proportion of posts aimed at the US, which jumped to an all-time high of 32%. For context, this ratio was only 16% in Q3 2021.

This sharp rise shows an alarming shift towards a higher representation of US organizations within dark web threats to the manufacturing industry.

Dark Web Activities Concerning the US Manufacturing Industry

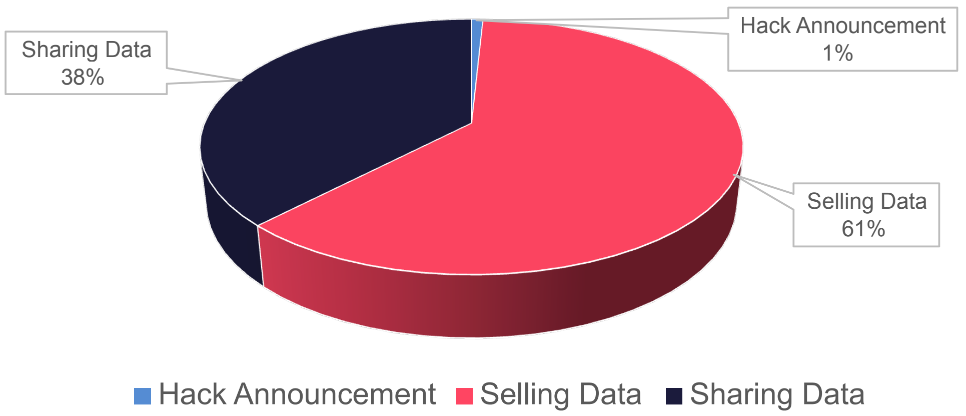
Zooming in on the geographical distribution of these threats, the United States topped the list as the most frequently mentioned target in dark web posts about the manufacturing sector. Over the two years examined here, 20.55% of manufacturing-related posts specifically targeted the US, excluding posts referencing multiple organizations in different countries.

India and the Russian Federation came in next, albeit significantly behind the US, with 5.11% and 4.4% of such posts directed at them, respectively.

A breakdown of the content within dark web posts referencing the US manufacturing sector identified three primary themes: announcements of hacks, data selling, and data sharing. What's notable here is the stark difference in the distribution among these categories.

Hack announcements made up only a tiny fraction of posts (2 or about 0.8%), while the majority of posts were related to selling data (151 or about 61.4%) and sharing data (93 or roughly 37.8%). A comparison with global averages, which can be found in SOCRadar's Manufacturing Threat Landscape Report, reveals that selling data is approximately 10% higher for posts about US companies. This suggests that threat actors view data from US companies as more valuable.

Subject of Dark Web Posts



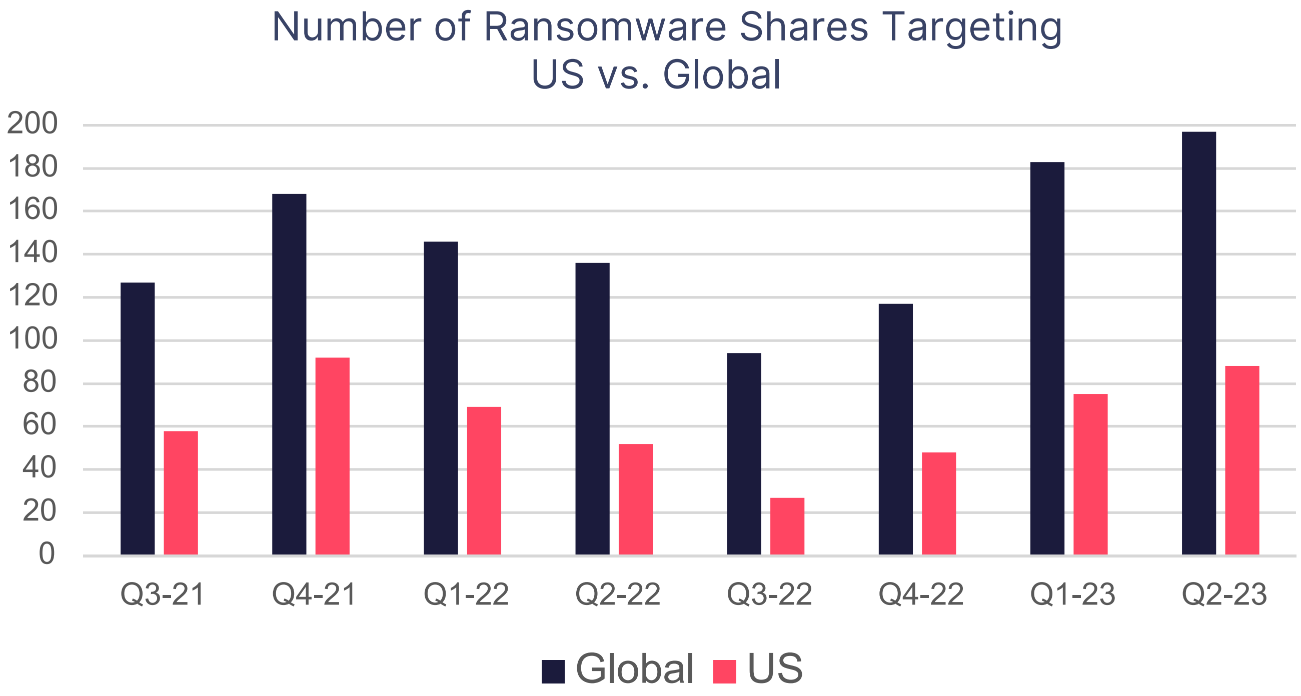
Beyond what's displayed in the pie chart, we also apply tags to denote announcements of targets and offers for cooperation. The pie chart demonstrates that the dark web market seems saturated with shared and sold manufacturing industry data. Consequently, there appears to be a lack of interest in buying data or databases related to this industry.

This oversupply of data could potentially lower the demand and, subsequently, the price. Another interpretation could be that the threat actors have already obtained the required data. Hence, they don't post about purchasing specific data sets or seeking cooperation or partnerships.

Customer data and databases were quite popular regarding the type of shared or sold, with Remote Desktop Protocol (RDP) and VPN access being the most common types of shared or sold accesses. Other kinds of accesses offered included the admin panel and Citrix credentials. This wide array of access points can grant hackers significant control over the victim's systems, making it a concern for the manufacturing industry.

Cyber Siege: Nearly Half of 2023's Ransomware Attacks Targeted the US in Manufacturing

Over the past two years, between July 2021 and June 2023, there have been 6,081 shares related to ransomware on the dark web. A significant 1,168 of these, nearly one in five, mentioned the manufacturing industry. Of these, 509 shares, or 43.6%, were explicitly focused on the manufacturing industry within the United States. As the bar graphic illustrates, there have been varying degrees of activity across different quarters, with the number of dark web posts mentioning the U.S. manufacturing industry peaking in Q4 of 2021 (54.8%) and showing another noticeable surge in Q1 and Q2 of 2023.

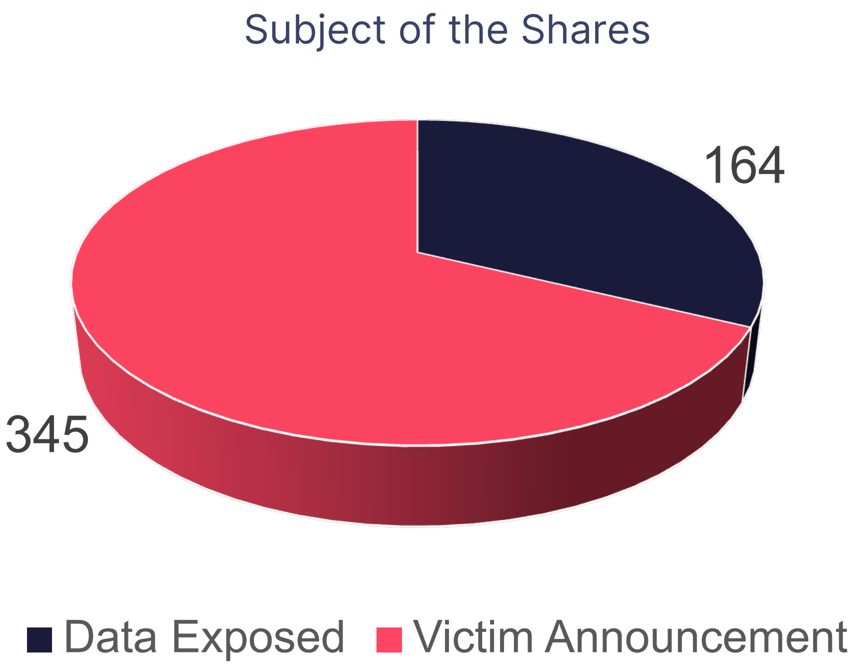


Regarding geographic distribution, the United States has been the most targeted country, accounting for 36.82% of shares mentioning the manufacturing industry. Germany and Italy follow, with 5.99% and 4.54% respectively. It's worth noting that despite Russia featuring prominently in the overall list of dark web posts, it has been largely untouched regarding ransomware attacks, with only two incidents, a mere 0.17%, recorded over the two years.

Different ransomware groups have varying levels of activity over the years. Among the 61 active groups involved in the 509 attacks, the most active have been LockBit 3.0&2.0, responsible for 94 incidents, followed by Conti with 72 incidents and Black Basta with 40.

Cyber Siege: Nearly Half of 2023's Ransomware Attacks Targeted the US in Manufacturing

Lastly, the nature of the shares can be divided into two primary categories: “data exposure and victim announcements”. Of the 509 shares, 164 were related to data exposure, indicating that sensitive information was leaked, while a more significant number, 345, were victim announcements, indicating newly targeted organizations.



These statistics underscore the considerable threat that ransomware poses to the manufacturing industry and the urgent need for comprehensive security measures to counteract this ongoing cyber menace. The high concentration of attacks targeting the United States, in particular, demonstrates the critical need for American manufacturers to remain vigilant and proactive in their cybersecurity efforts.

Other Cyber Threats Confronting US Manufacturing

Manufacturers in the US face an increasingly intricate web of cyber threats as their operational processes become more digital. The burgeoning interconnectedness of Information Technology (IT), Operational Technology (OT), and Industrial Control Systems (ICS) has multiplied potential attack vectors for cybercriminals.

The Manufacturing Industry is the primary target for OT-related cyber threats, with over 50% of these incidents aimed at manufacturers, according to the 2023 IBM X-Force Threat Intelligence Index. Notably, the fallout from high-profile ransomware attacks, like the ones experienced by Bridgestone, AGCO, and Kojima Industries, frequently impacts more than just the digital infrastructure. These attacks can incapacitate production systems and necessitate broad-scale shutdowns, inflicting substantial financial burdens that can often exceed the demanded ransom.

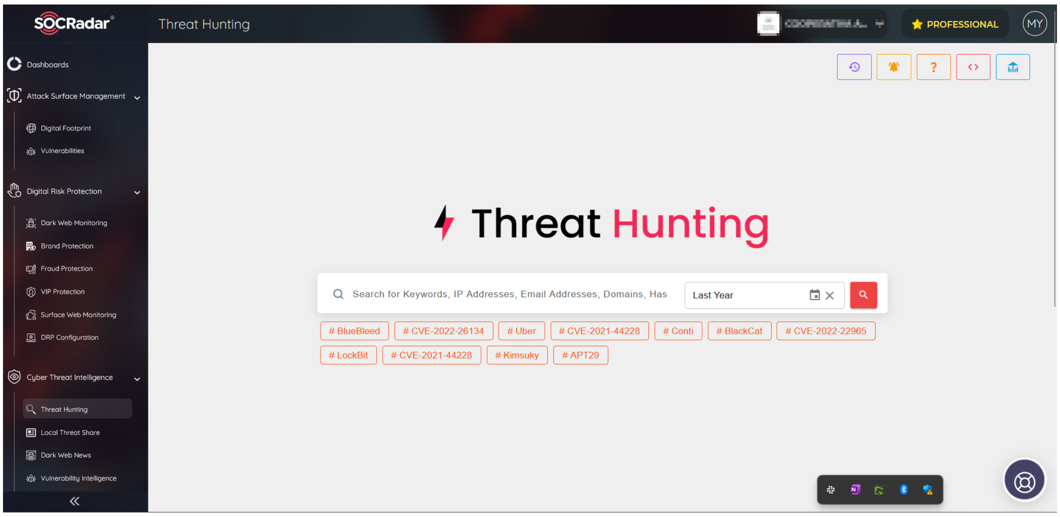
Despite the growing danger, many cyberattacks on the manufacturing sector go unreported due to limited compliance reporting requirements. Furthermore, supply chain threats, illustrated by the 2021 Microsoft Exchange email server vulnerability exploits and the 2020 SolarWinds software compromise, can wreak havoc on internal systems.

The illicit access and theft of intellectual property, along with supply chain cyber attacks, pose a significant threat to the manufacturing industry by causing severe disruptions and monetary damages. Additionally, the sectors of defense and critical infrastructure often fall prey to strategic cyber attacks orchestrated by nation-states. Moreover, the inadequate security protocols around Operational Technology (OT) devices and an increase in internal security breaches, especially in the context of remote work, compound the cybersecurity risks faced by the manufacturing sector.

Securing the Future of Manufacturing by Leveraging SOCRadar's Capabilities

The growing cybersecurity threats targeting the manufacturing industry present a significant challenge. These challenges, spanning from intellectual property theft, supply chain attacks, nation-state attacks, to equipment sabotage and internal breaches, require an in-depth and multi-layered security approach. It's clear that traditional defenses are insufficient, and a proactive, intelligence-driven strategy is needed to identify and mitigate threats before they escalate.

This is where SOCRadar's capabilities come into play. As a digital risk protection platform, SOCRadar can provide comprehensive visibility into an organization's digital footprint, unearthing potential risks, threats, and vulnerabilities that may compromise its security. Our platform can help manufacturing companies identify threats in real-time, allowing them to take swift action to protect their digital assets.



Threat Hunting Module of SOCRadar Platform`s Cyber Threat Intelligence suite.

By leveraging SOCRadar's advanced threat intelligence capabilities, manufacturing companies can proactively defend against various cyber threats. Our platform's ability to track threat actors, malware, ransomware, and emerging cyber threats, coupled with our comprehensive dark web monitoring, can provide the early warning needed to thwart cyberattacks. Additionally, our commitment to securing both IT and OT systems makes us a suitable choice for manufacturing companies looking to secure their interconnected systems.

Key to SOCRadar's approach is its Attack Surface Management capabilities. This robust service constantly analyzes digital assets associated with your organization across the Internet to identify potential risks. It also continually inspects your external infrastructure for misconfigurations, vulnerabilities, and exposed sensitive information. By providing real-time visibility into your external attack surface, SOCRadar ensures that potential threats are detected early and can be addressed promptly.

SOCRadar’s proactive and comprehensive strategy, combined with SOCRadar’s threat intelligence and digital risk protection, creates a powerful shield, ensuring that your manufacturing operations stay robust and secure in the face of an ever-evolving cyber threat landscape.

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar’s approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 6.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

8.400
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique dark web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers’ PII: Scan millions of data points on the surface, deep and dark web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner Peer Insights. Customer First

Gartner Peer Insights™

5/5 ★★★★★

Contact Us

✉ info@socradar.io

☎ +1 (571) 249-4598

651 N Broad St, Suite 205,
Middletown, DE 19709