SOCRadar®
Your Eyes Beyond

# EDUCATION THREAT LANDSCAPE REPORT:

"13,800 public school districts with 55 million students is under cyber threat in the US "

# Table of Contents

# Executive Summary

The education industry covers a diverse range of organizations, including K-12 education, higher education, private and public education, science research institutes, and tutoring ranging from exam preparation to hobby courses. Furthermore, educational technologies are integrally linked to other industries due to numerous related services, such as educational technologies and educational publishing. The users include students, parents, teachers, administrators, and consultants.

In the 2017 Census of Governments, the United States Census Bureau enumerated the number of school district governments as 12,754. The K-12 Cybersecurity Resource Center reported 1,331 publicly disclosed cyber incidents affecting U.S. school districts (and other public educational organizations) from 2016 to the end of 2021, and 166 of these school incidents affected schools in 162 school districts across 38 states in the calendar year of 2021.

The COVID-19 pandemic effects speed up this digital transformation process even more due to the need for distance education and online teaching systems. Therefore, this sudden increase in interest and demand for digital transformation brings more cyber security concerns. As a result, we do not expect this trend to change soon. It is high time for K-12 education institutions to protect themselves against the looming cyber threats.

Public school districts should be informed about all possible cyberattack scenarios, their attack surface, and security posture to prevent these cyber attacks. With the raise cyber incidents, public schools should pay close attention to cyber security and threat intelligence solutions.

New regulations in education are aimed at shifting the whole security paradigm towards a “zero trust approach”, whereby access to applications and data is denied by default. At this point, risk elimination is achieved by only granting access to networks and workloads utilizing policy informed by continuous, proactive, and contextual, across users and their devices in educational institutions.

SOCRadar's industrially tailored cyber security approach also undertakes these tasks enriched with External Attack Surface Management and Digital Risk Protection. Maximize the efficiency of your SOC team with false-positive free, actionable, and contextualized threat intelligence.

# Key Findings

•Cyber threats are threatening approximately **13,800 public school** districts with almost 55 million students in the United States.

•Public school districts have been one of the most popular victims for threat actors in both 2021-2022 in the United States.

•Threat actors intentionally target K-12 districts since they can pressure school or district administration and demand the ransom confidently since the data is even more critical than usual.

•Ransomware poses a great threat to K12 organizations. **SOCRadar's DarkMirror detected 24 ransomware incidents** targeting K-12 organizations in the US. Twelve unique ransomware gangs perpetrated these attacks, and the Vice Society group was the most active in targeting K-12 organizations.

•According to data from SOCRadar, we observe four main APT groups targeting US educational organizations: "Earth Lusca, APT41, Earth Berberoka, Bronze Spring." These prominent APT groups are all China-backed.

**•SOCRadar detected more than 1,100 phishing attempts** targeting organizations in the US education sector during 2022, which clearly indicates that phishing also remains to be a significant threat to K-12 organizations.

•According to SOCRadar's phishing data, **60.5 % of all phishing domains impersonating US education websites** within the last year were using the HTTPS protocol. This situation shows us that threat actors increasingly use HTTPS to trick victims into clicking malicious URLs using the trust generated by the little padlock icon.

•The number of ransomware attacks on the education industry detected by SOCRadar dark web analysts **increased by 234 %** in 2022 compared to 2021.

# Student Data Privacy Laws

The Family Educational Rights and Privacy Act (FERPA), is the primary federal law that protects the privacy of student education records. As stated on the U.S. Department of Education website, the law applies to all schools that receive funds under an applicable program of the Department of Education. The law regulates what data schools can gather, keep, and share with or without the consent of students, their parents, or guardians.

The Children's Internet Protection Act (CIPA) is mainly overlooked in regulating student data privacy and security. Most of the time, preventing students from reaching harmful content via content filtering is thought to be enough for complying with C.I.P.A. However, "unauthorized disclosure, use, and dissemination of personal information regarding minors" is also one of the CIPA requirements. Content filtering can not protect student data when stored in the cloud.

The Protection of Pupil Rights Amendment (PPRA), which establishes limitations on student privacy in federally financed surveys or evaluations, is another pertinent statute. Additionally, the confidentiality and privacy of personally identifiable information must be guaranteed by schools receiving funding under the Individuals with Disabilities Education Act (IDEA). In addition to federal laws, there are more than 100 privacy laws by states and the District of Columbia.

**Since education institutions retain student data for a long time, and some of the data belong to children and teenagers, the data requires all the protection it can get. However, according to experts, school IT staff and leadership often cannot be held personally accountable for a data breach. On the other hand, schools and districts can be liable for cyber incidents, and there could be consequences after the K–12 Cybersecurity Act became law in October 2022. Before, since FERPA is a funding law and does not have a private right of action (parents, guardians, or students cannot sue the schools), the worst possible outcome for schools was to lose their funding which rarely happened.**

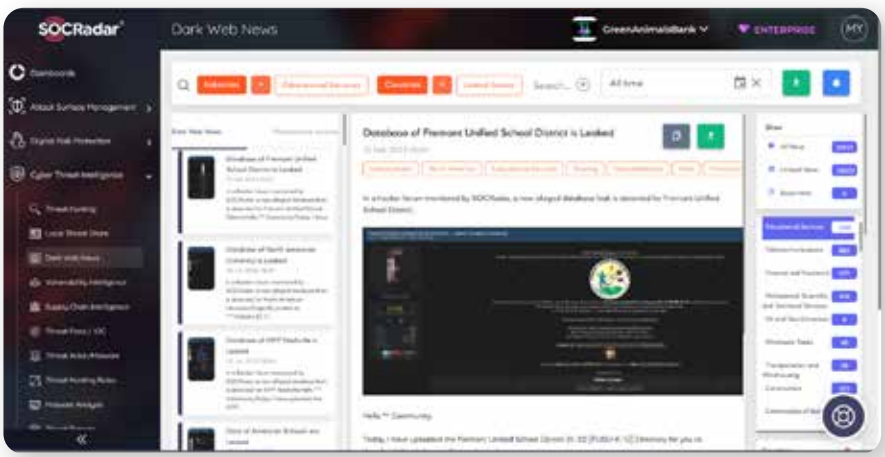
# Cyber Attacks Against Schools Are Rising

Despite all legal regulations, schools continue to be the target of cyber attacks. Within the last 24 months, data breaches and ransomware attacks into a district or school's computer systems and backups were increased. Threat actors intentionally target K-12 districts since they can pressure school or district administration and demand the ransom confidently since the data is even more critical than usual.

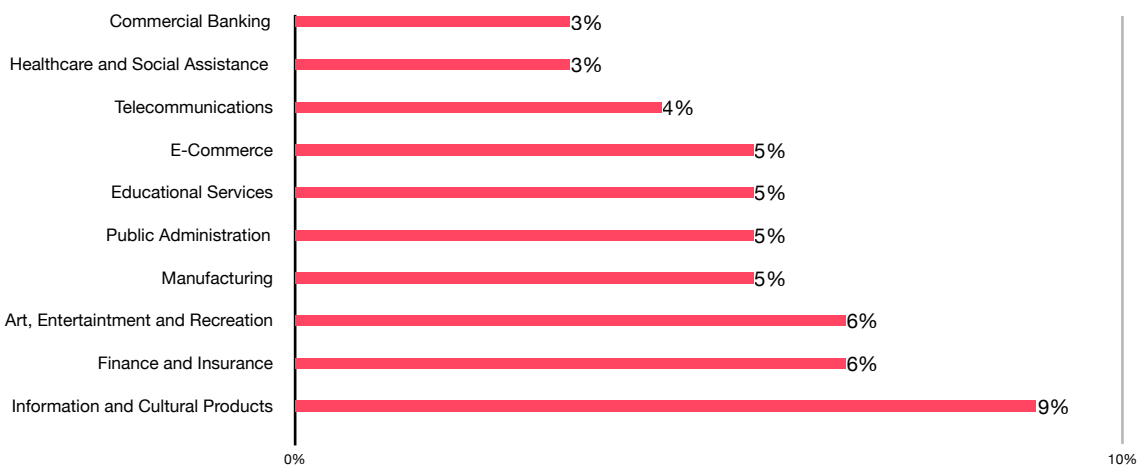
To prevent or minimize the losses from cyberattacks, the federal government started to direct its attention to K-12 cyberattacks. Congress recently passed the Infrastructure Investment and Jobs Act in addition to K–12 Cybersecurity Act discussed above. The former Act provides 1 billion dollars in funding to help states and local school districts combat cyber attacks.

This report provides an analysis of cyber incidents faced by school districts, as well as recommendations that school districts can utilize to minimize the effects of cyber incidents.

In 2022, **736 education industry-related posts** were reported in SOCRadar Platform dark web news module. The number of education industry-related postings shared on **underground forums increased by 61 % in 2022** compared to 2021. The most active threat actors were **"Jitter," "Kelvinsecurity,"** and **"Flowercower."** According to the distribution of 2022 dark web posts on the SOCRadar XTI platform by industries, the education services rank sixth with a rate of **4.59 %.**




You can follow and subscribe to the latest cyber security incidents in your region, country, and industry using the filters on the right-hand side of our Dark Web News page.




*(Source: SOCRadar)*

# K-12 Cyber Incidents: Analysis and Trends

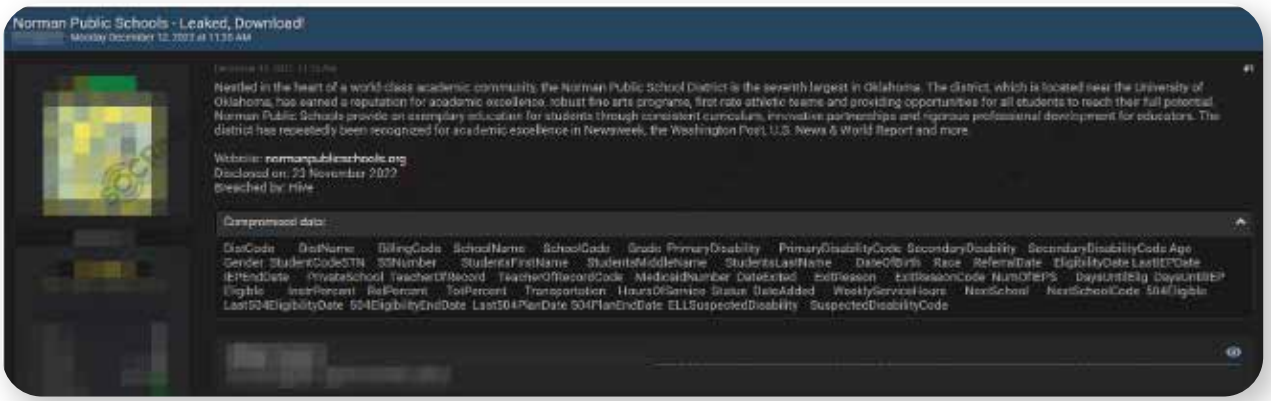
## Recent Events

Everyone worked to overcome the negative effects of COVID-19 in 2022, while threat actors merely sought to get more money from these efforts. International crises like the diplomatic conflict about Taiwan and Russian invasion of Ukraine have also inspired threat actors. Let us take a look back at the top cyber incidents of 2022.

**December 11 2022**

### Database of Norman Public Schools is Leaked:

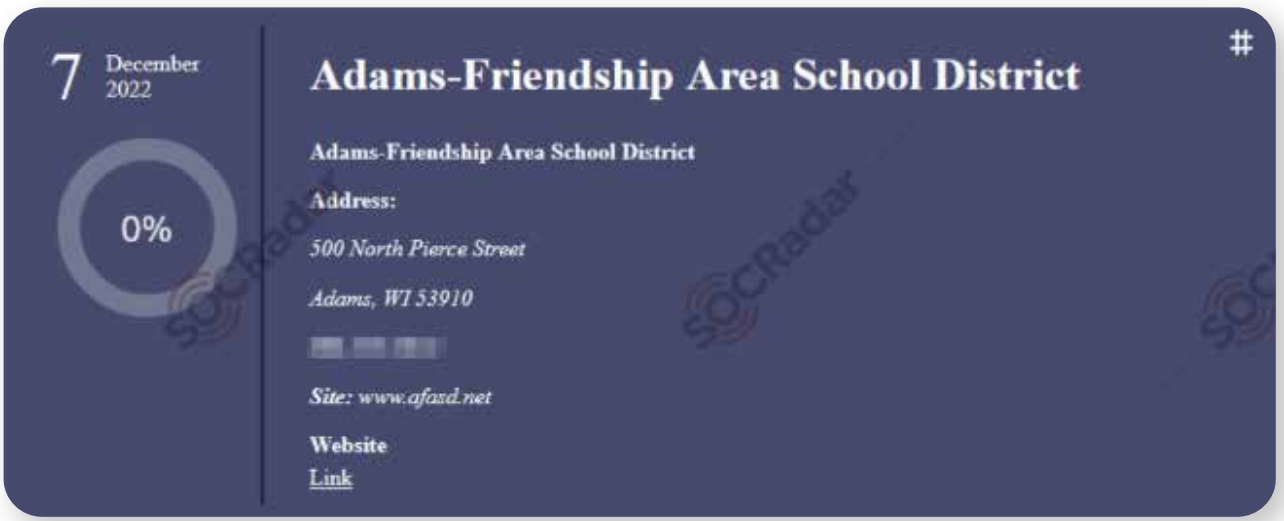
In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Norman Public Schools. (Source: SOCRadar)




**December 7 2022**

### The New Ransomware Victim of Royal: Adams Friendship Area School District

In the Royal ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Adams-Friendship Area School District. (Source: SOCRadar)



# K-12 Cyber Incidents: Analysis and Trends

November 22, 2022

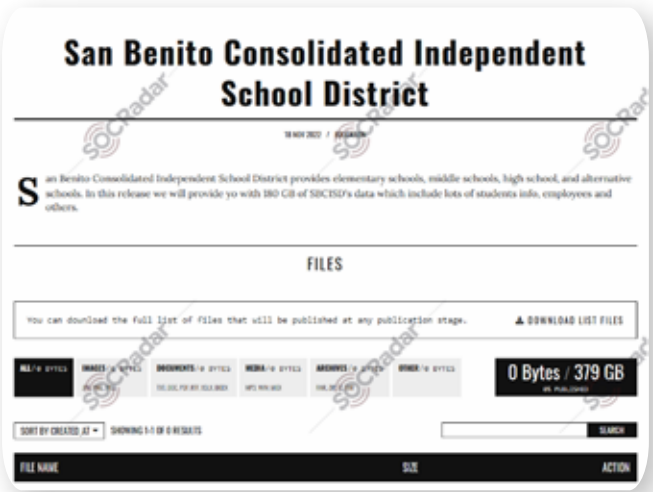
## HiveLeaks Ransomware Group Leaked The Data of Norman Public Schools

In the HiveLeaks ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Norman Public Schools. (Source: SOCRadar)


November 18, 2022

## The New Data Breach Victim of Karakurt:

San Benito Consolidated Independent School District: In the Karakurt cyber criminals website monitored by SOCRadar, a new data breach victim allegedly announced as San Benito Consolidated Independent School District. For more information, you can read the detailed analysis by the SOCRadar Research Team. (Source: SOCRadar)




October 1, 2022

## Database of Mansfield Independent School District is Leaked:

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Mansfield Independent School District. (Source: SOCRadar)

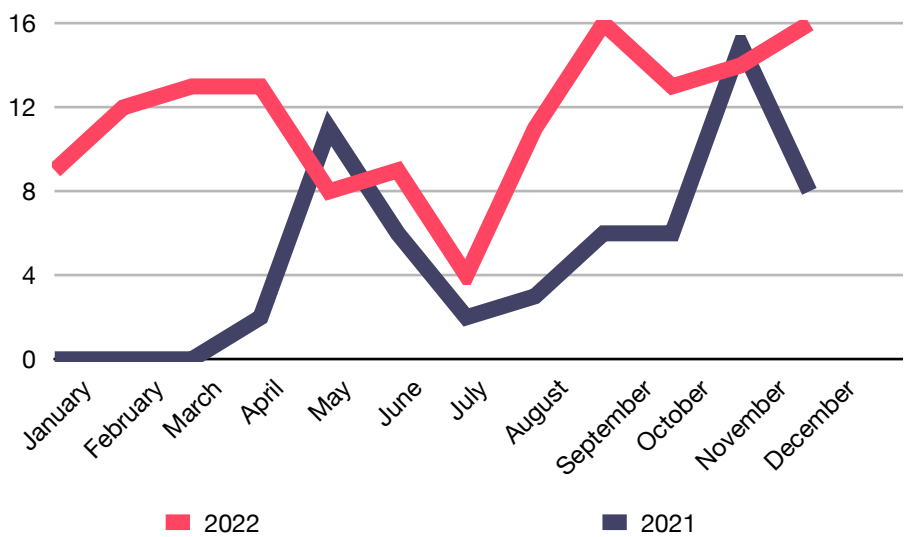
# Ransomware Attacks Against Educational Institutions in 2022

Ransomware attacks are a type of cyberattack that threat actors use to exploit victims financially. In a ransomware attack, the threat actor first gains access to the victim's system and loads the necessary tools and software into the system.

After the threat actor is ready, an encryption process is started, and all the data in the victim system is encrypted, no longer accessible by the victim. Generally, the threat actor copies the victim's data and blackmails the victim by threatening to release all stolen data unless a ransom is paid.

**After the attack, the victim has two choices: either pay the ransom, which can be up to millions of dollars, and hopefully get all the data back, or do not pay the ransom and never be able to access the encrypted data and risk the chance of all sensitive data, including student information, getting leaked.**

The number of **ransomware attacks** on the education industry detected by SOCRadar dark web analysts increased by **234% in 2022** compared to 2021. The distribution of ransomware attacks in the education industry in 2021 and 2022 are as follows.


*Distribution of Ransomware attacks against the education industry in 2021 and 2022 (Source: SOCRadar XTI Platform)*

# Ransomware Attacks Against Educational Institutions in 2022

The ransomware groups that have targeted education systems are **"Vice Society," "LockBit ( 2.0 )",** and **"Hive."** US authorities seized the servers of the Hive ransomware group on 26 January 2023. For more about the Hive ransomware group, click here.

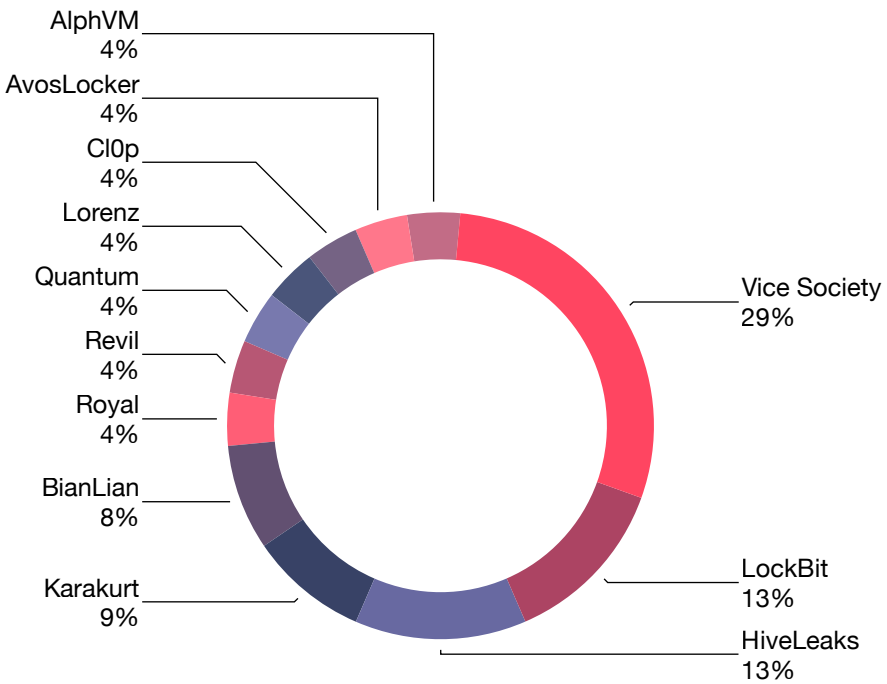

*The top ransomware families targeted the education industry, In 2022 (Source: SOCRadar)*

The ransomware groups that have targeted education systems are **"Vice Society," "LockBit ( 2.0 )",** and **"Hive."** US authorities seized the servers of the Hive ransomware group on 26 January 2023. For more about the Hive ransomware group, click here.

SOCRadar protects K-12 organizations by preventing cyber-attacks in the reconnaissance phase of the cyber kill chain. SOCRadar crawls through both the surface web and the dark web to find the compromised credentials of employees with access to the organization's network, which the threat actors can leverage to gain initial access into the victim system with the help of brute force and dictionary attacks.

Within the last year, SOCRadar's DarkMirror has detected 24 ransomware incidents targeting K-12 organizations in the US. Twelve unique ransomware gangs perpetrated these attacks, and the Vice Society group was the most active in targeting K-12 organizations.

**Ransomware attacks can disrupt services, costing the valuable time, effort, and resources of K-12 organizations. In some cases, we have seen that school districts had to cancel classes for some time to recover from a fresh ransomware attack. In addition, the ransom paid to threat actors to decrypt the encrypted files is another factor to consider while discussing the costly consequences of ransomware attacks.**




*Most active ransomware gangs targeting K12 organizations within the last 12 months (Source: SOCRadar)*

# APT Groups

APT groups are another type of threat actors posing significant threat to companies, government organizations, critical infrastructures, and in our case, K12 organizations and school districts. Unlike ransomware gangs, APT groups are not financially motivated. They aim to carry out their nation's malicious cyber objectives by crippling the target nation's government agencies and critical infrastructures.
State-sponsored APT groups do not care whether their targets are school districts. According to data from SOCRadar's ThreatFusion, we observe four main APT groups targeting US educational organizations.

## APT Groups Targeting the Educational Institutions in US

The primary purpose of APT groups attacking K12s is to steal data. Spear phishing attacks can be designed with stolen data and can create a background for spying activities. The stolen data can be the core of future cyber espionage. Also, prominent APT groups are all China-backed. China has also carried out attacks targeting the personal data of US citizens in the past. For example, the hacking of the Office of Personnel Management was a significant event in the history of cyber security.

### Earth Lusca

Earth Lusca is a threat actor believed to be supported by the Chinese government. Earth Lusca mainly targets government organizations and academic institutions.

### APT41

APT41 (Double Dragon) is another threat actor believed to be supported by China. According to Mandiant's report, APT41's targets are aligned with China's 13th five-year plans.

### Earth Berberoka

Earth Berberoka (also known as GamblingPuppet) is a new APT group known for targeting gambling websites and educational institutes. According to TrendMicro's research, the group uses malware families historically attributed to former Chinese threat actors.

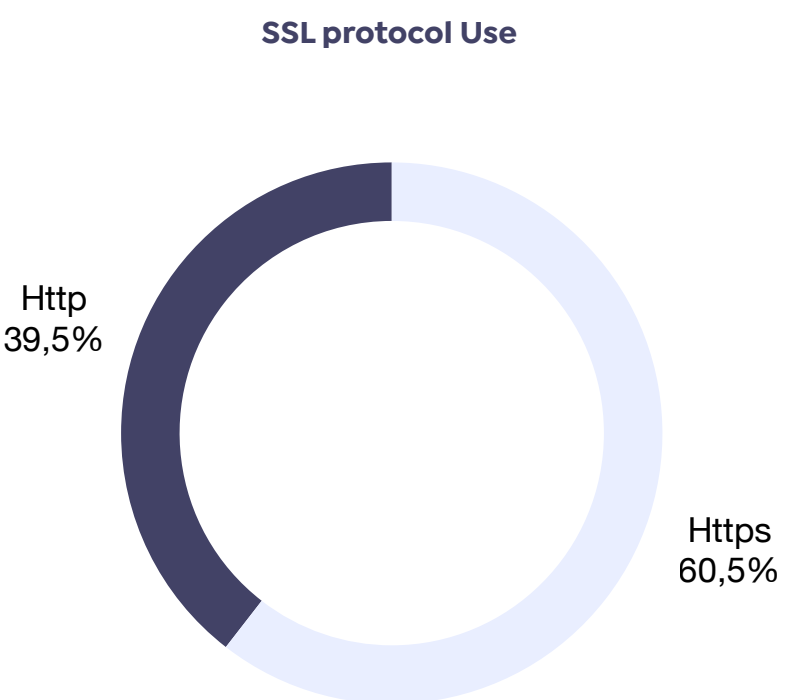
### Bronze Spring

BRONZE SPRING is another Chinese APT group that has previously targeted US educational organizations. In addition to the education sector, the group has also targeted the defense industry and medical institutes.

# Phishing Attacks Against the US Educational Institutions in 2022*

Phishing is a critical cyber-attack scheme that threat actors use to steal sensitive information including credentials to gain initial access to a victim's network. Phishing is another lethal threat vector for K-12 organizations. SOCRadar detected more than 1,100 phishing attempts targeting organizations in the US education industry during 2022, which shows us that phishing also poses a significant threat to K-12 organizations.

According to SOCRadar's phishing data, 60.5 % of all phishing domains impersonating US education websites within the last year were using the HTTPS protocol. This situation shows us that threat actors increasingly use HTTPS to trick victims into clicking malicious URLs using the trust generated by the little padlock icon.




*SOCRadar detects phishing schemes against your organization and automatically requests the takedown of all phishing attempts, which protects employees and customers of K-12 organizations against phishing schemes.*

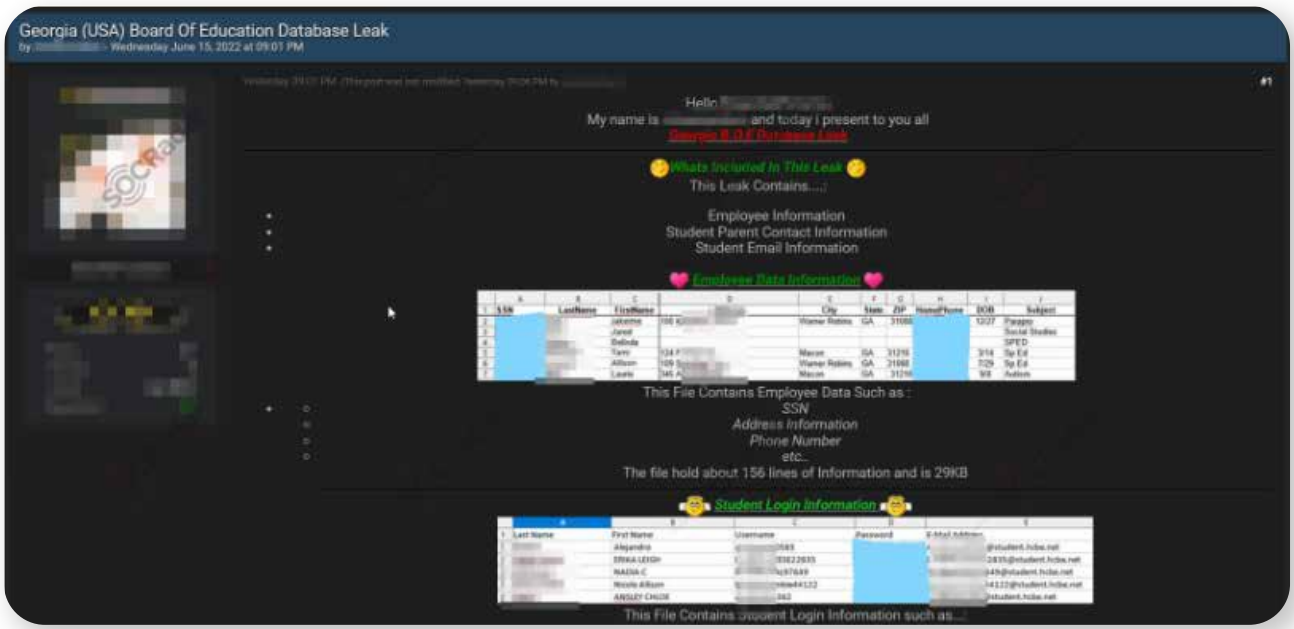
*Phishing Research Scope: Within the last year (January - December 2022), educational institutions in the US wit the total of 1.148 phishing attempts.*

# Data Breaches in US Educational Institutions in 2022

Within the last three years, public school districts have had to deal with data breaches. These data breach incidents are mostly detected in the Dark Web hacker forums that are continuously being monitored by SOCRadar. Some of the incidents monitored are listed as follows.

### • Database of Georgia Board of Education is on Sale

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for the Georgia Board of Education.



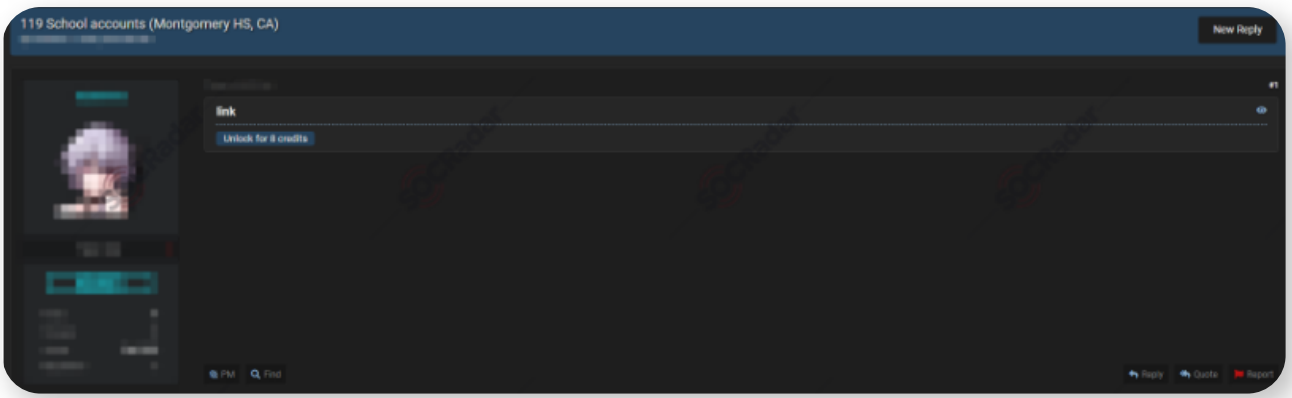

### • Database of Chicago Public Schools is Leaked

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Chicago Public Schools.

# Data Breaches in US Educational Institutions in 2022

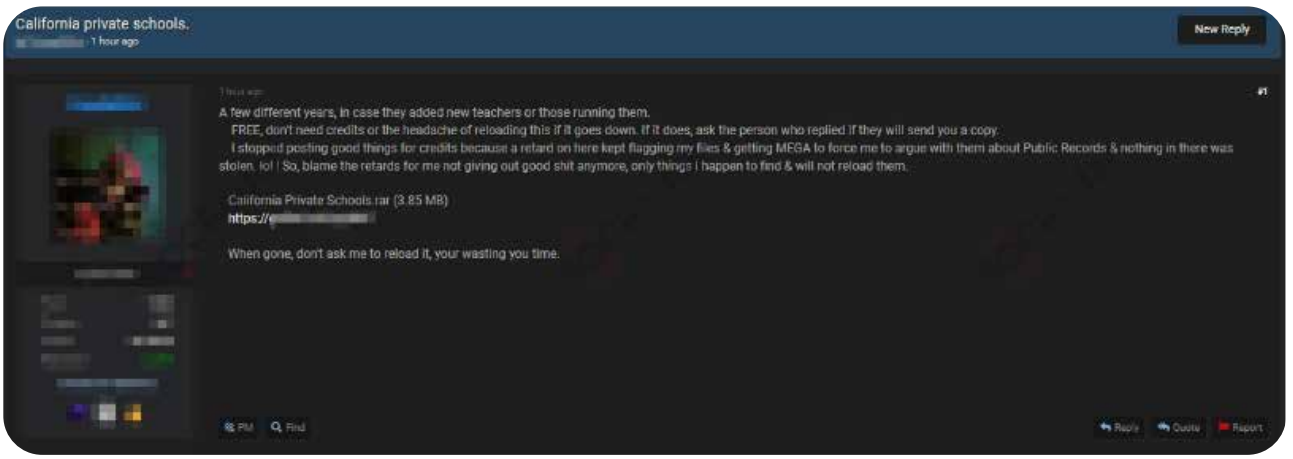
**• Accounts of Montgomery High School are Leaked**

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Montgomery High School.




**• Data of California Private Schools is Leaked**

In a hacker forum monitored by SOCRadar, a new alleged data leak is detected for private schools, operating in California.




**• Massive CPS data breach exposes records of 560,000 students, employees**

The staff and student information were exposed after a CPS vendor was targeted in a ransomware attack on December 1, 2021, the district said.

# Lessons Learned from Cyber Attacks Against Educational Institutions


## Lesson 1: Paying Ransom is not a solution

Lincoln College, one of the historical colleges of the U.S., was the target of a ransomware attack on December 19, 2021. All registration, academic, finance, admissions, and fundraising systems were impacted and shut down. The school officials agreed to pay the $100,000 ransom after almost 2 months of negotiating with the ransomware group. The first decryption key given by the threat actors did not work after accepting the ransom; some part of the data could be recovered with the second decryption key sent later.

The systems could be fully recovered in March 2022, but the school, which had difficulty maintaining operations after COVID-19, could not overcome the challenges caused by the ransomware attack. On May 13, 2022, the school officially announced the end of its 157-year existence as an educational institute.

# Lessons Learned from Cyber Attacks Against Educational Institutions

## Lessons Learned

**There is no guarantee that the victim will receive the decryption key or that the decryption key will restore all data once the ransom has been paid.** Furthermore, the time required for discussions and subsequent recovery can have an irreversible impact on the organization's operations. As a result, backups must be optimized to allow faster recovery of the most critical data and services in case of a ransomware attack. It is necessary to reestablish access to systems and data rapidly.

## Lesson 2: Rapid Digital Transformation Leads Wider Attack Surface

Digitalization has recently increased in the education sector, as in many other industries. The COVID-19 pandemic, in particular, forced the education system to shift to remote education rapidly. The digitalization of the system with solutions such as online courses, online meeting tools, smart classrooms with smart whiteboards, and student tracking tools has expanded the attack surfaces of educational institutions. The uncontrolled expanding attack surface exposed new weak points for threat actors.

## Lessons Learned

***Educational institutions' digitalization without adequate resources and security posture, using various online platforms and supporting tools, should take advantage of advanced threat intelligence tools to monitor their expanding attack surface.***

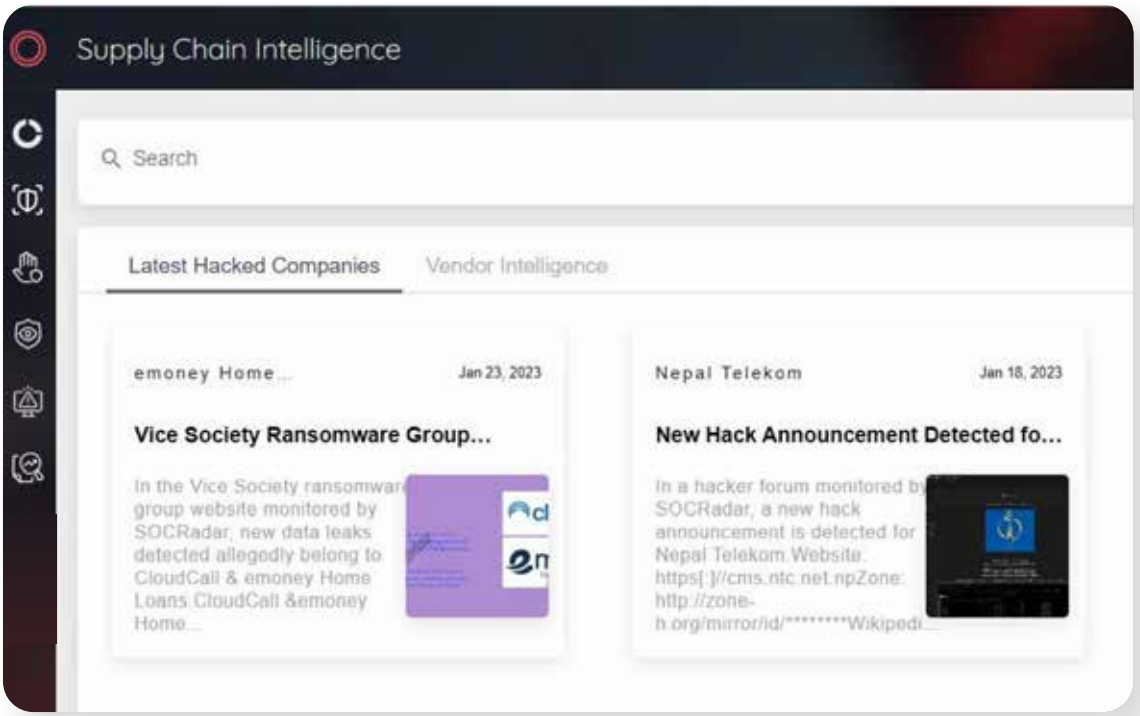
# Lessons Learned from Cyber Attacks Against Educational Institutions

## Lesson 3: Supply Chain Security is Critical for the Education Industry

The New York City Department of Education (NYDOE) reported in March 2022 that threat actors got unauthorized access to the personal information of 820,000 current and past New York City Public School System students. The vulnerability was discovered in the Skedula and PupilPath software, which tracks grades and attendance. A California-based Illuminate Education company owns both platforms. The breach occurred in January 2022, but the third-party software vendor informed the NYDOE in March 2022.

### Lessons Learned

In the case of receiving support services from third parties and subcontractors, ***educational institutions need to ensure that their suppliers have robust cybersecurity protocols for the sensitive data in their systems.***




*SOCRadar's Supply Chain Module*

# Lessons Learned from Cyber Attacks Against Educational Institutions

## Lesson 4: Extended Threat Intelligence should be implemented

On September 6, 2022, LAUSD, the second-largest school system in the U.S., announced that it had been the target of a ransomware attack. It was discovered that the attackers, the Vice Society ransomware group, were active on LAUSD's networks from July 31, 2022, to September 3, 2022.


*Ransomware announcement of LAUSD (Source: Twitter)*

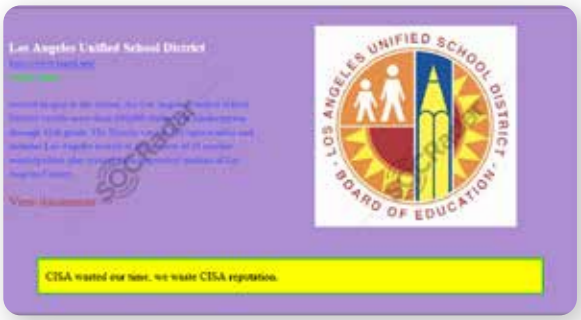
Meanwhile, the authorities took action. **The Federal Bureau of Investigation (FBI),** the **Cybersecurity and Infrastructure Security Agency (CISA),** and the **Multi-State Information Sharing and Analysis Center (MS-ISAC)** released a joint cybersecurity advisory about the **Vice Society Ransomware Group (AA22-249A)** on 06 September 2022. The advisory stated that Vice Society actors disproportionately target the education sector with ransomware attacks.

On September 30, the Vice Society announced they would publish LAUSD data on the leak site in a few days.


*Vice Society ransomware attack announcement*

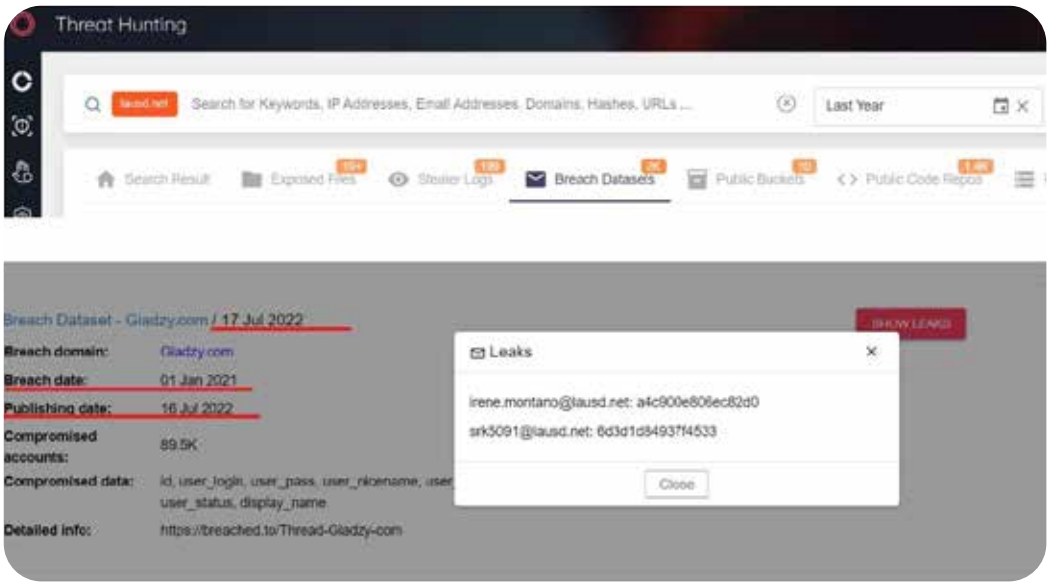
The group published sensitive data of LAUSD on October 2, 2022, with their response to the CISA.

# Lessons Learned from Cyber Attacks Against Educational Institutions




*Vice Society ransomware attack announcement*

How Vice Society gained access to the LAUSD networks is unknown. Still, it is believed that the group exploited leaked internal login credentials found on the dark web. It has been observed in the SOCRadar, Threat Hunting Module, that many breach data sets of the "lausd.net" domain were published on the dark web before the attack.




*SOCRadar Threat Hunting Module, "lausd.net" breach data sample*

## Lessons Learned

An extended threat intelligence solution that monitors the dark web, gathers intelligence, and alerts customers when critical data is released to the dark web is crucial. Thus, **the possibility of using compromised accounts in continued attacks is reduced.**

# **Before the Conclusion:** Reasons for the Increase in Cyberattacks Against the Educational Institutions

The educational system is responsible for storing considerable amounts of personal and confidential data. Personal data that can be gathered from various sources, such as PII (personally identifiable information), contact information, birth certificates, social security numbers, bank information, intellectual property, and research findings, can be found all together in the systems of educational organizations. As the timeline demonstrates, within the last few years, especially with the effect of the pandemic disease of COVID-19, cyber threats against public schools have increased.

**Some primary causes of the rise in cyber-attacks on the education industry are as follows:**

-Students, as participants in educational institutions, generally prioritize comfort over security, using their own devices, studying in shared spaces, and using public Wi-Fi.

-There is varying cyber security awareness among users of all ages.

-User's sensitive data and valuable intellectual property obtained from research programs in the higher education system are also helpful for threat actors.

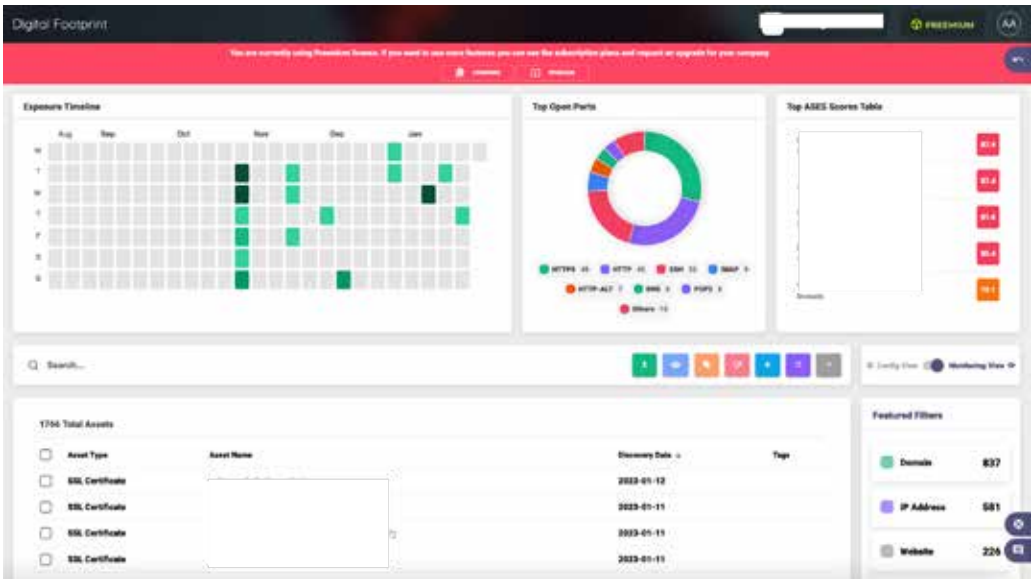
-Higher education institutions operate on more accessible networks due to the inherent information-sharing culture. The structure of networks is broad, allowing users to connect remotely. The open IT infrastructure policy also provides network access for external visiting students, teachers, and researchers, making it difficult to determine who is on the network at any time.

-Since educational institutions must operate on a small budget, outdated technologies with security vulnerabilities are used to provide cyber security infrastructure.

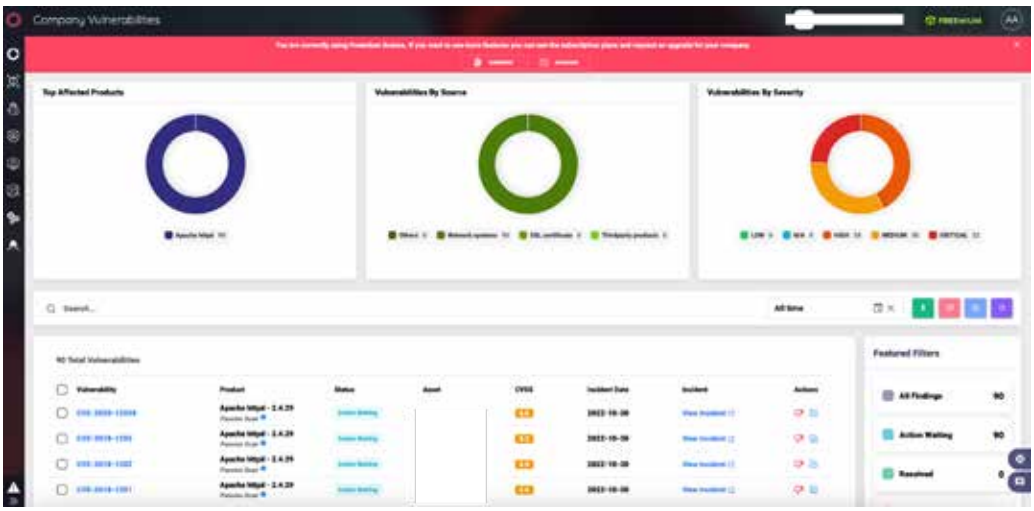
-Education shifted to online platforms during the COVID-19 pandemic, and threat actors targeted these platforms as a new entry point into educational systems. Although face-to-face education has returned after the pandemic, online media and personal device usage continue.

# How SOCRadar Can Help Educational Institutions?

**- Valuable intellectual property from campus research:** Software used on educational campuses may need to be constantly updated. "Get notified when a critical zero-day vulnerability is disclosed, **"GETTING STARTED WITH SOCRADAR DEMO".**




**-Student and employee personal information:** Every information is valuable in the digital world. If you do not want the data of your students, parents, and staff to be exposed on dark web forums, you can use SOCRadar to "Monitor your domain name on hacked websites and phishing databases."



# How SOCRadar Can Help Educational Institutions?

**-Computer processing power:** Devices are used more frequently than ever before. New applications, delays in patching and failing security controls added complexity and vulnerabilities to the environment. These environmental factors together with the type and amount of personal data maintained in education systems make primary and secondary schools and colleges a prime target for ransomware and placing student and school safety at risk. With SOCRadar, you can receive notifications against vulnerabilities. ThreatFusion is a part of the SOCRadar Extended Threat Intelligence platform and provides a big-data powered threat investigation module to help cyber threat intelligence teams search for deeper context, real-time threat research, and analysis.


**-Establish cyber-resiliency across endpoints, applications and your network:** Digital assets also should be tracked by using SOCRadar as an External Attack Surface Management products. In this way, your organization can gain visibility on all known and unknown assets.
SOCRadar's new stand-alone CTI solution CTI4SOC is a next-generation threat intelligence platform designed to simplify the work of SOC analysts. A unique assistant to SOC teams with 12 functional modules it contains. Powered by big-data, unlike traditional threat intelligence platforms, CTI4SOC presents all the data that analysts can obtain using several tools in an organized and contextual manner.

CTI4SOC

# GET ACTIONABLE INTELLIGENCE FOR FREE WITH MINIMIZED FALSE POSITIVES

SOCRadar®
Your Eyes Beyond

# 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 companies 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 4.000 companies from 150 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.

**5.600**
**Freemium Companies**

**Darknet and Deep 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.

**Protecting Customers' PII:** Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

**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.

**360-Degree Visibility:** Achieve digital resiliency 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 peerinsights™ 5.0

**Contact Us** info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709