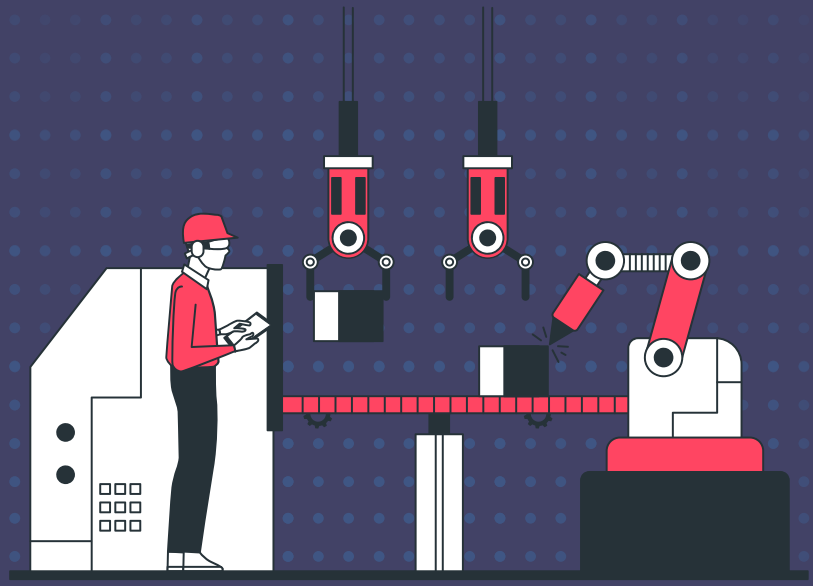
SOCRadar LABS



Industry Threat Landscape Report

Finance

Time Period: 2024/11/06 - 2025/11/06 | Report Date: 2024-11-06

SOCRadar® Your Eyes Beyond

651 N Broad St, Suite 205
Middletown, DE 19709

+1 (571) 249-4598

info@socradar.io

www.socradar.io

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence — all automated and supported by a global team of qualified intelligence analysts — provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle.

Gartner Peer Insights™

5/5

Agenda

SOCRadar®

01 Dark Web Threats

02 Ransomware Threats

03 Top Target Industry

04 Phishing Threats

05 APT Groups

2979 Dark Web Threats

in last one year.

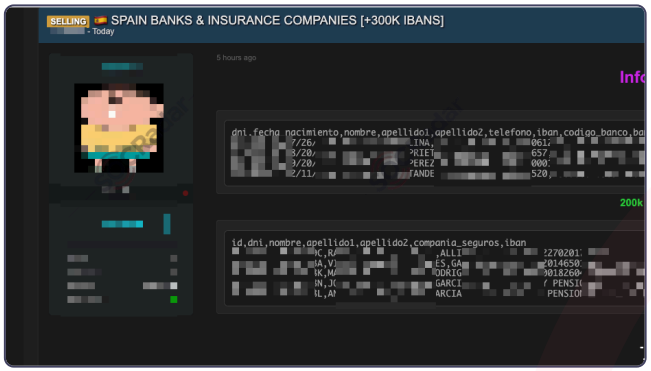
Most category are Selling and Sharing

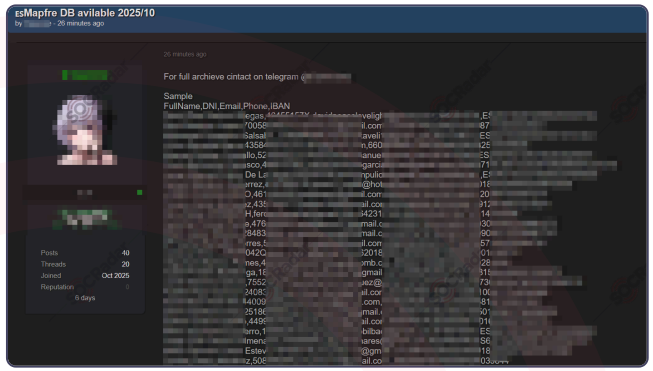
SOCRadar CTIA team has monitored the dark web to find trends and essential links. Throughout the this year, Finance enterprises were bombarded with cyber attacks. Various threat actors have tried to sell and sometimes share the fruits of these successful cyberattacks on dark web hacker forums.

1690 Dark web Threat Actors

- bochan
- Cayenne
- torveyino
- Cleverly
- doznon

Dark Web Threats





2025-11-01

Alleged Database of Spanish Banks and Insurance Companies are on Sale

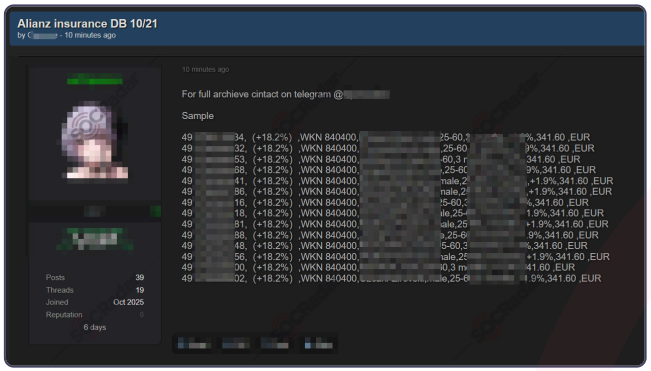
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Spanish banks and insurance companies. https://image.socradar.com/screenshots/2025/10/31/df2c7113-2299-46cb-8cbf-cfaeedb44475.pngInformation of the pack 100k Banks d...

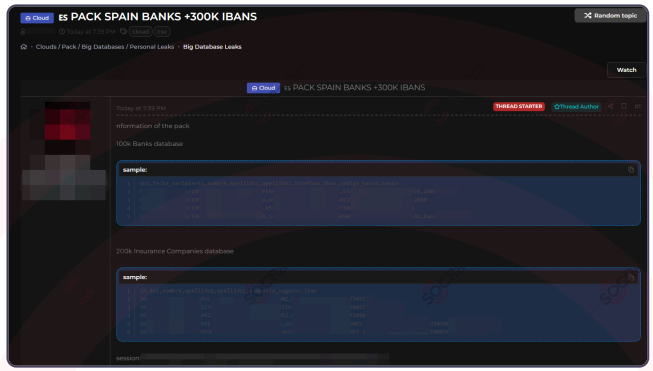
2025-10-31

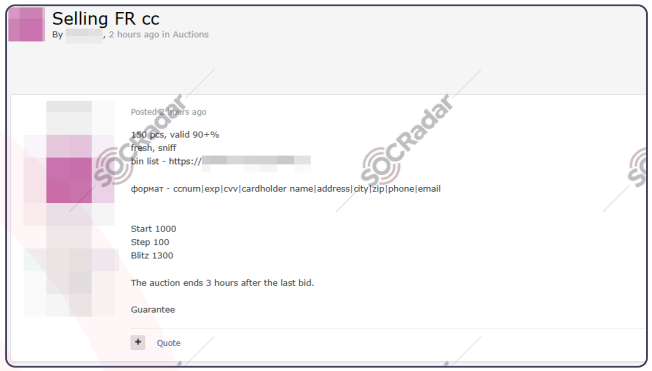
The Alleged Database of Mapfre is on Sale

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Mapfre. https://image.socradar.com/screenshots/2025/10/31/b5af52b0-6f24-4316-b77c-befe2556a64f.pngFor full archieve cintact on telegram @**** SampleFullName, DNI,Emai...

Dark Web Threats







2025-10-31

The Alleged Database of Allian...

In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Allianz. https://image.socradar.com/screenshots/2025/10/31/bc181f55-8fc3-4b29-86e2-261b6c66f84d.pngFor full archieve cintact on telegram @**** Sample ******

2025-10-31

The Alleged Data of Spainish B...

In a hacker forum monitored by SOCRadar, a new alleged data sale is detected for Spanish banks. https://image.socradar.com/screenshots/2025/10/31/911692d1-f9f1-4ece-b682-562fe4350620.pngnformation of the pack 100k Banks database sample: dni,fecha_nac...

2025-10-31

The Alleged Credit Card Data o...

In a hacker forum monitored by SOCRadar, a new alleged credit card data sale is detected for France. https://image.socradar.com/screenshots/2025/10/31/ca96f11c-fc53-4d55-9725-3d4623b01410.png150 pcs, valid 90+% fresh, sniff bin list - https://***** ф...

Ransomware Threats

182 ransomware attacks

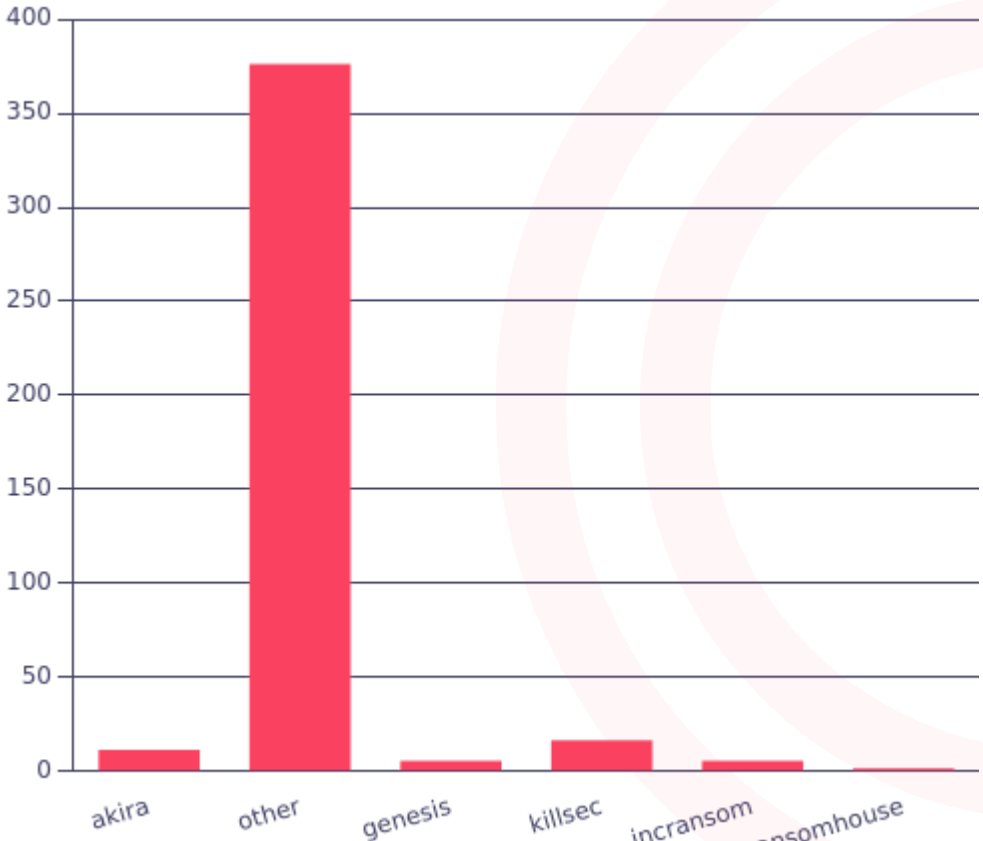
in Finance.

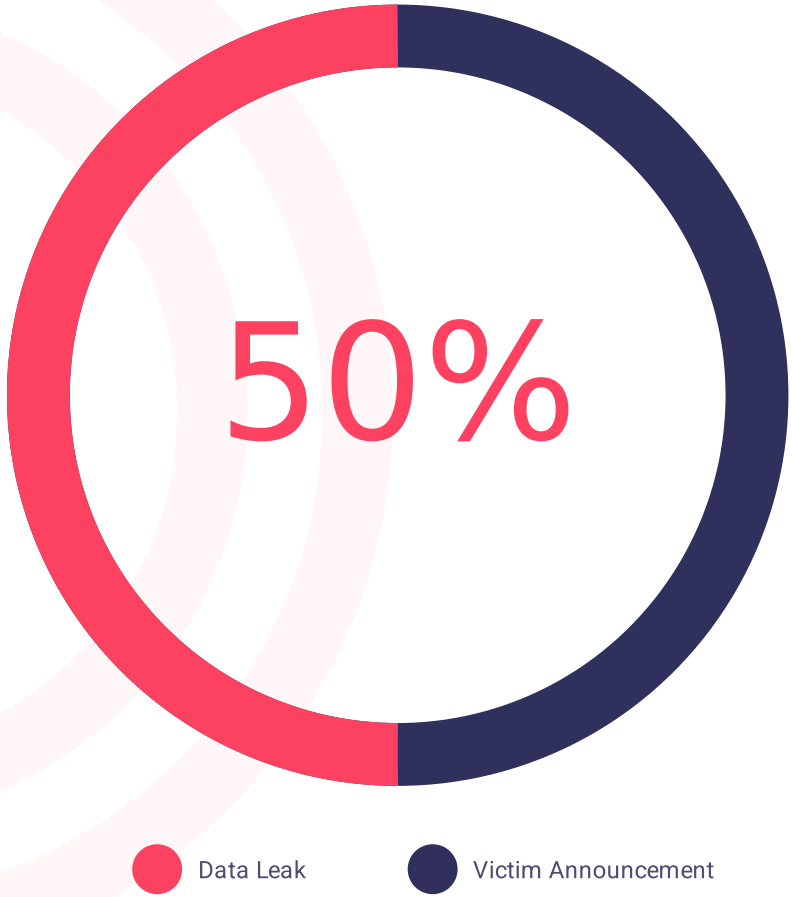
Ransomware attacks are among the most critical cyber attacks an organization can experience. The results can be destructive for an organization and lead to massive data loss and leaks of the victim company's sensitive data.

98 Ransomware Gangs

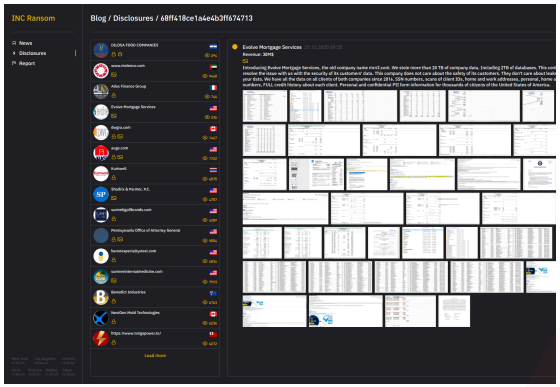
- qilin
- killsec
- akira
- everest
- incransom

Ransomware Threats





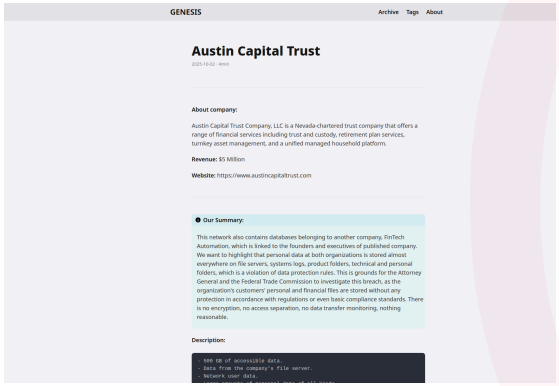
Ransomware Threats



The New Ransomware Victim of incransom: Evolve Mortgage Services

2025-10-30

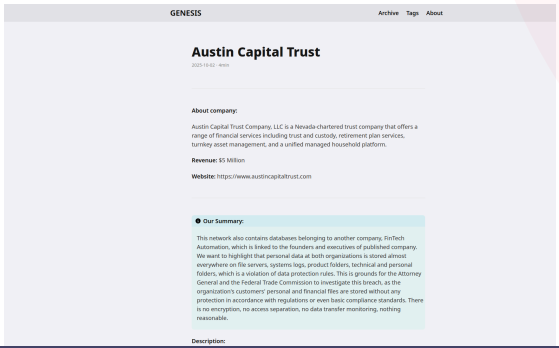
In the incransom ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Evolve Mortgage Services https://image.socradar.com/screenshots/2025/10/30/99e1a85e-f2f3-42d0-a75a-8346eee461ae.pngIntroducing Evolve Mort...



The New Ransomware Victim of genesis: Austin Capital Trust

2025-10-30

In the genesis ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Austin Capital Trust https://image.socradar.com/screenshots/2025/10/26/47f43508-cf53-47e0-9326-0f7d9237b3f9.pngThe Trust company that offers...



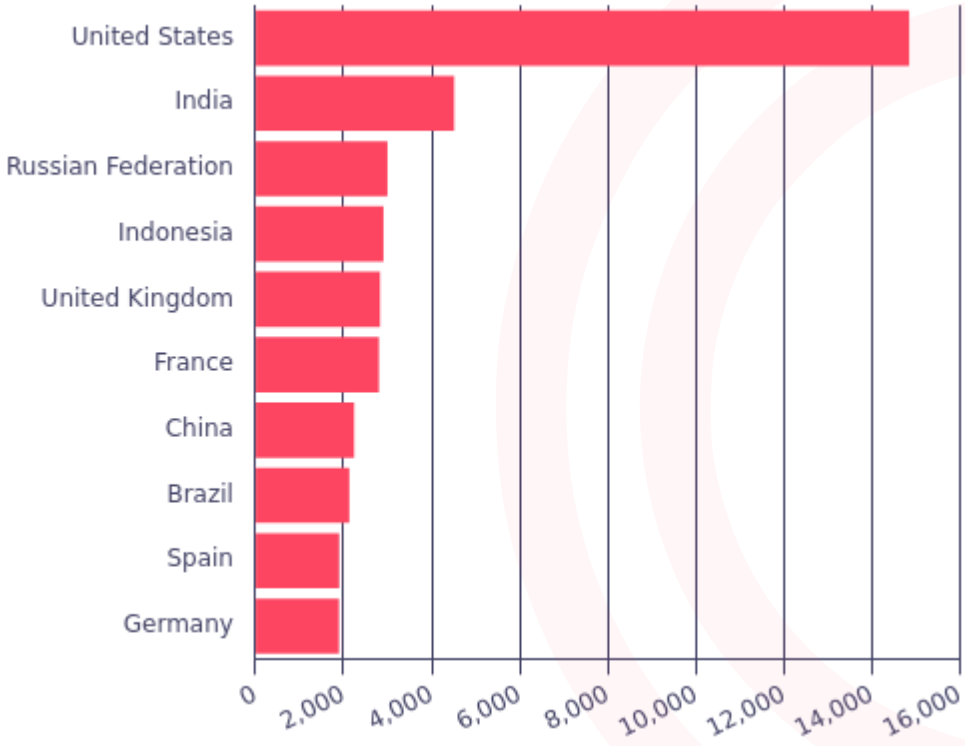
The New Ransomware Victim of genesis: Austin Capital Trust

2025-10-28

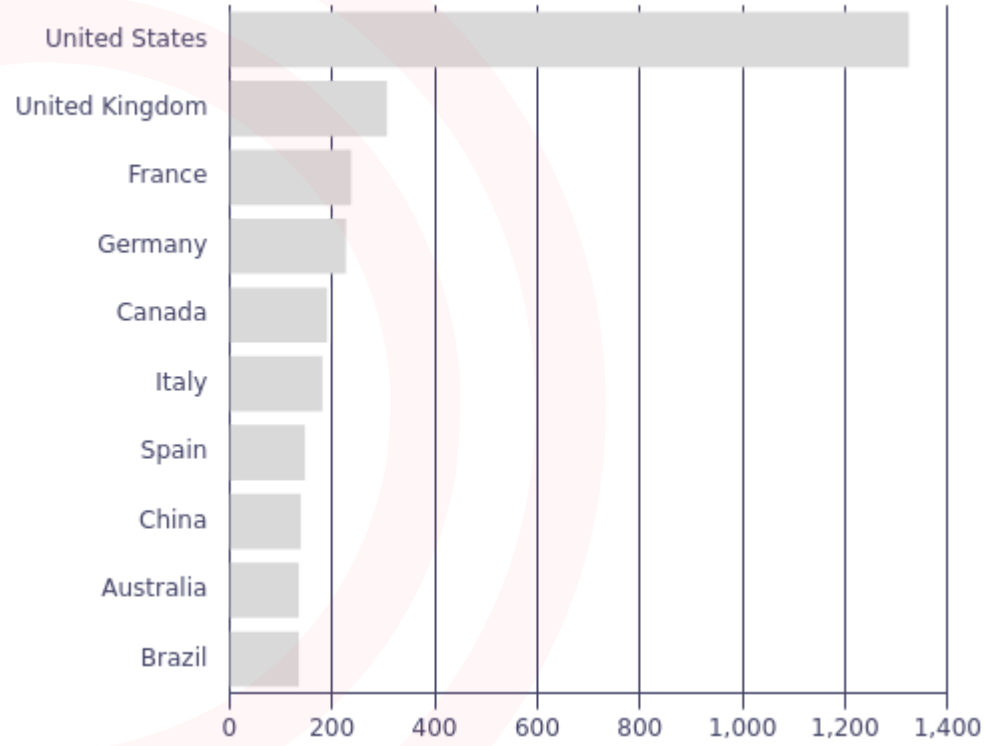
In the genesis ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Austin Capital Trust https://image.socradar.com/screenshots/2025/10/27/8455241c-d055-4668-81bf-3407a18f4e47.pngThe Trust company that offers...

Top Target Countries

239 Different industries targeted in Finance



Dark Web Industry Threats



Ransomware Industry Threats

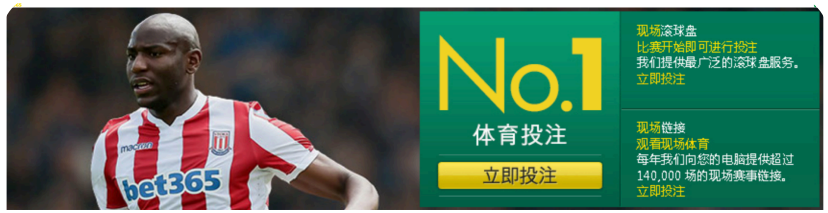
Phishing Threats

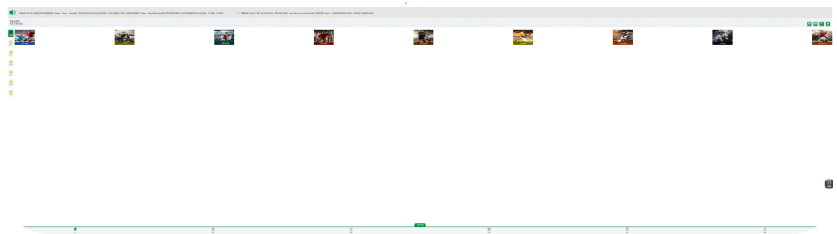
Brand impersonation takes place when a threat actor creates a social account pretending to be your brand. SOCRadar can spot fraudulent and fake domain. Also can spot fake social accounts by monitoring well-known social media platforms so that you can quickly take action to stop possible phishing scams.

Phishing Domain	Sector	Register Date
bet365e[.]sbs	Finance	2025-11-02
bet365e[.]sbs	Finance	2025-11-02
bet365005[.]cc	Finance	2025-11-02
mybet365[.]co	Finance	2025-11-02
mojdpd[.]si	Finance	2025-10-30
mojdpd[.]si	Finance	2025-10-30
pnfinancep[.]s3[.]eu-nort...	Finance	2025-10-30
weebly[.]com	Finance	2025-10-30

+992 Phishing Threats

10861 phishing domains detected in **Finance**





80 apt groups found in Finance

Group Name	Aliases	Country
Evilnum	TA4563 , Jointworm , G0120 Evilnum	Canada , Australia ...
Infraud Organization	Infraud Infraud Organization	Germany , India ...
UNC2891	UNC2891	-
APT 28	Threat Group-4127 , Fighting Ursa , Sofacy IRON TWILIGHT ...	Asia Pacific Economic Cooperation , European Commission ...
MageCart	-	-
Gold Ionic	ionic Gold Ionic	Germany , United Kingdom ...
MuddyWater	TA450 , MuddyWater , G0069 ATK 51 ...	Egypt , Georgia ...
Antlion	Antlion	Afghanistan , Belarus ...

+72 Threat Actors

Cyber Threat Intelligence for SOC Analysts

As an 'Extension to SOC Teams', CTI4SOC aims to provide you with actionable and contextualized TI with minimized false positives.
A unique assistant to SOC teams with 12 functional modules.

Sign Up for Free CTI4SOC

Get Free CTI4SOC

SOCRadar®
Your Eyes Beyond

Trusted by world's leading organizations

Gartner
Peer Insights™

5/5