SOCRadar®

ALL-IN-ONE SOLUTION BRIEF

Threat Intelligence. Contextualized.

ThreatFusion

Cyber Threat Intelligence

SOCRadar®

KEY FEATURES

Global dark web coverage

Blackmarkets, darknet and TOR network

Precise API integration

For ticketing, SIEM and SOAR solutions

A timely, enriched IOCs

Rapid, relevant and enriched IOCs and IOAs

In-depth threat analysis

Uplevel your threat intelligence capabilities

Make better-informed decisions through contextualized intelligence.

Monitoring a wide variety of internet sources and layers pose difficult challenges, but ThreatFusion's autonomous technology accurately crawls, analyzes, and interprets data from many sources to identify leaked credentials and other confidential data.

ThreatFusion's historical precision and growing robust database help analysts cut through the noise, narrowing down relevant security items and prioritizing SOC analyst time and energy on the most critical security incidents.

The cloud-based platform provides API-ready realtime information on a broad range of cyber threats giving customers the power to get prepared for tactical and strategic responses proactively.

Realtime trends intelligence

Better-understand existing and emerging global cyber threats.

30K+ critical vulnerability alerts generated annually.

3M+ phishing attacks classified.

Vulnerability Intelligence

Better prioritize patches.

To prevent adversaries disrupt your business, see which vulnerabilities are being leveraged by threat actors. Get actionable insights and context on potentially vulnerable technologies to speed up the assessment and verification processes.

Global Phishing Radar

Get proactive on the phishing threat landscape.

Understanding and monitoring how the phishing threat landscape looks like is key to achieve a solid security program. ThreatFusion proactively monitors phishing threat landscape and brings you the latest in global phishing statistics and attacks from the wild.

Threat Actors Monitoring

Stay one step ahead of APT groups.

Through automated data collection, classification and AI-powered analysis of hundreds of sources across deep/dark web, SOCRadar's ThreatFusion keeps you alerted on APT groups' activities, helping you define use cases to detect and prevent malicious activities.

CyberSec News Monitoring

Digital footprint centric cyber security news.

To prevent you from losing focus, ThreatFusion CyberSec News module features the latest cyber security news you'd not want to miss. Auto-aggregated from credible RSS, Twitter and Telegram channels to bring you the most relevant news.

KEY BENEFITS

Near-zero false positives

Get actionable intelligence filtered through advanced technology

STIX/TAXII support

Collect and send STIX-formatted threat intelligence

Shed light on APT actors

Get essential insights into the latest activities of APT groups

Immediate start

Start in hours with minimal input

CTIA support

Ready to work with clients, helping them build in-house skills

Superior 3rd party integration

Smooth integration with SIEM, SOAR and ticketing platforms for faster incident response and investigation.

McAfee™ IBM MICRO FOCUS Jira Service Desk splunk>

Threat investigation module:

ThreatHose

SOCRadar's ThreatFusion provides a big-data powered threat investigation module **ThreatHose** to enable threat intelligence teams search for deeper context and realtime threat analysis. The module is fed by massive number of data sources across surface, deep and dark web.

> SOCRadar made a significant contribution to our security maturity and posture with its advanced cyber intelligence capabilities.
>
> **CISO, Retail Industry**

How ThreatFusion works?

Malware archives

Honeypot sensors

HUMINT sources

APT groups

Vulnerability databases

Industry-specific CERTs

Cybersecurity media

Big Data + Analysts + Artificial Intelligence + Domains, IPs... ThreatHose Investigation

FEEDS

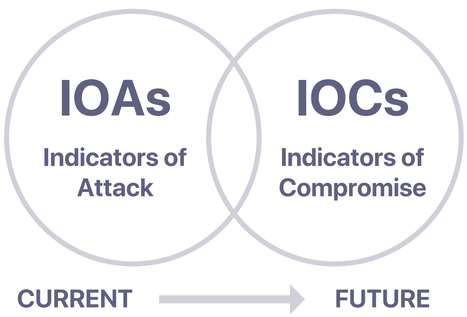
IPs / URLs
Phishing domains
DDoS Attackers
Hashes

REALTIME TRENDS

Vulnerability Intelligence
Threat Actors Monitor
Phishing Radar
CyberSec News

OUTPUT

THREATS



REPORTS

APT groups' activities
Malspam campaigns
Massive DDoS attacks
Global ransomware outbreaks
Significant hacking incidents

RiskPrime

Digital Risk Protection

KEY CAPABILITIES

Detect sensitive data belonging to employees, customers, or 3rd parties

Compromised credentials
Personal data (PII)
Proprietary code
Credit card information
Data breaches
Intellectual Property
Confidential documents
DLP identifiers

Identify upcoming threats & attacks

Crimeware-as-a-service
Typosquatted/phishing domains
Malicious mobile applications
Impersonating social accounts
Rogue SSL/TLS certificates

Protect your customers, employees and hard-earned brand reputation.

360° monitoring of surface, deep and dark web

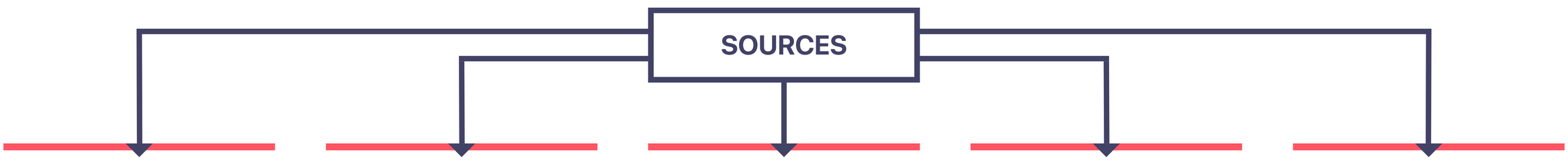
Every day, threat actors launch thousands of attacks targeting businesses, employees and their customers resulting in brand reputation and financial loss. SOCRadar's RiskPrime builds on industry-leading instant phishing domain detection, internet-wide scanning, and compromised credential detection technologies by aggregating and correlating massive data points into intelligence-driven alerts. This enables organizations to swiftly understand how particular risks have evolved and what to do for mitigation.

Autonomous Process

Continuous monitoring → **Accurate detection** → **Realtime alerting**

Unrivaled, curated data sources

As the threat landscape grows, SOCRadar Labs is constantly qualifying new data sources and channels. SOCRadar's RiskPrime draws on a growing collection of data from these sources then through advanced analytics algorithms and a team of talented analysts, alerts organizations to know if their sensitive data, documents, financial information or customers' PII have been compromised.



Social media / Chat

Twitter, Linkedin, YouTube
Facebook, Instagram
IRC, Chatters
ICQ, Discord, Telegram
Hacker channels

Dark web

TOR/I2P network
Cyber criminal forums
Breaches, dumps
Blackmarkets
Autoshops

Content / File sharing

Paste sites
Amazon s3 buckets
Code repositories
Torrent
Trello

News

Blogs
Security news
Hacktivism news
Mainstream news
Geopolitical news

Technical

Google Dorks
Web hack archives
VirusTotal
Hybrid analysis
Bug bounty sites

KEY FEATURES

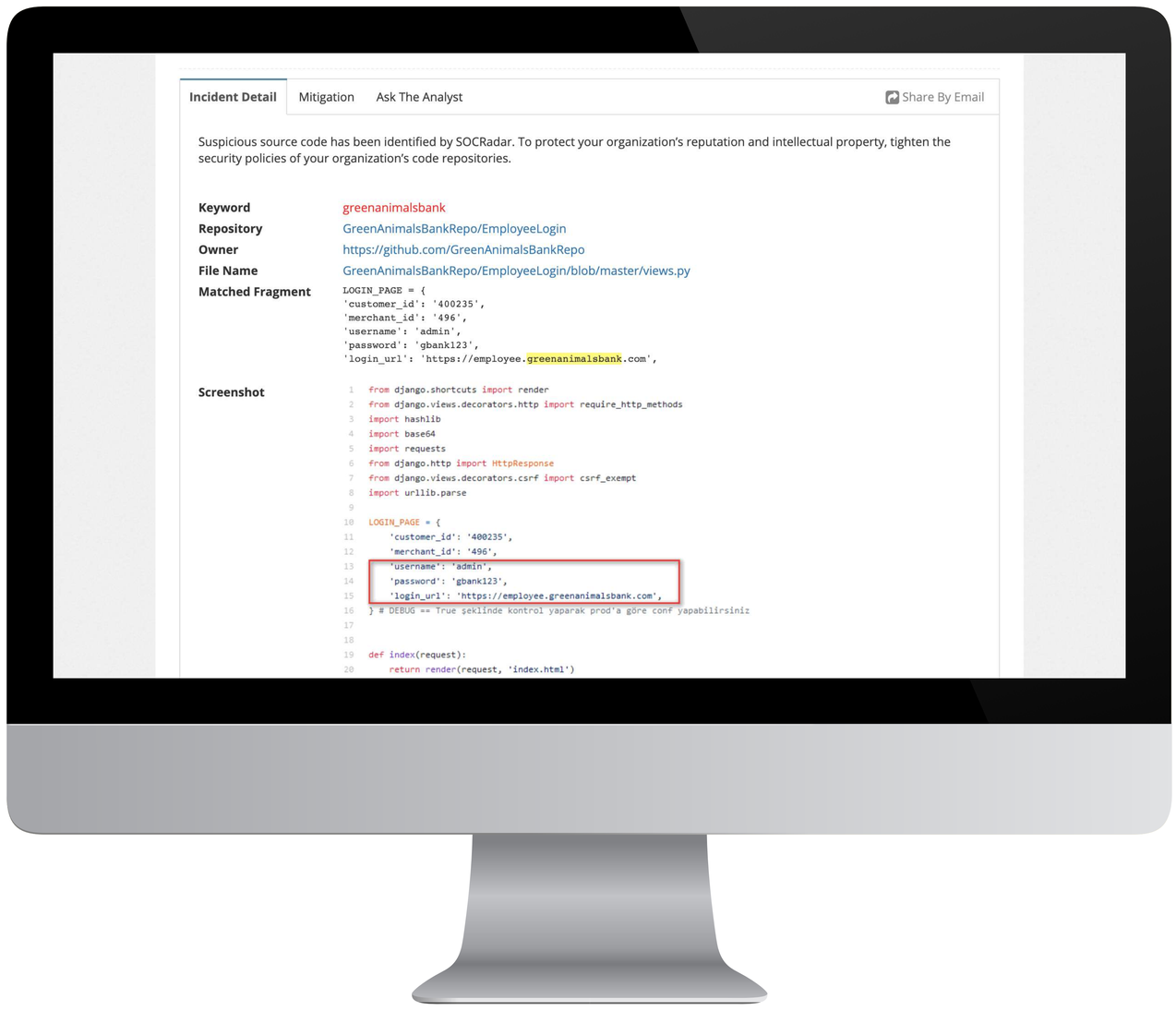
Improve your overall security posture.

Get proactive with actionable threat intelligence.

Identify and remediate faster.

Reduce risk of...

- IP theft
- Brand reputation loss
- Data breaches
- GDPR/CCPA penalties
- Business Email Compromise attacks
- CEO Fraud
- Credential stuffing attacks



All-in-one digital risk protection platform

4M+ domains analyzed per week.

Detect newly-registered phishing domains

AI-enabled SOCRadar Digital Risk Protection platform analyzes millions of domains every day across most major domain registrars to detect malicious or look-alike domains targeting your brand and entire business network.

Get proactive to block credential stuffing and

Empower your existing login security mechanisms to prevent hackers from stealing your customer's trust. Enhance your credit card fraud prevention mechanisms with SOCRadar Digital Risk Protection platform's AI-powered intelligence at scale.

Use playbook to handle prioritized alerts

SOCRadar's historical precision, accurate playbook and growing robust database help analysts cut through the noise, narrowing down relevant security items and prioritizing SOC analyst time and energy on the most critical security incidents.

5.5B+ breach dataset records processed.

Secure your C-level executives

SOCRadar enables you to search & monitor critically important email addresses, PII, SSNs or credit card details of C-suite executives whether it's indexed somewhere in the growing database of major worldwide breaches that may be sought by your adversaries.

Autonomous dark web intelligence

RiskPrime provides thorough dark/deep web monitoring solution that enables organizations to identify and mitigate threats rapidly. Using unparalleled, autonomous reconnaissance and crawling technology, we help you proactively secure your organization.

Integrated remediation & takedown service

SOCRadar provides on-demand takedown services for phishing, malware, social media, mobile apps, and brand abuse sites. Completing the protection offering, with one-click you can initiate takedown process without any additional legal and procedural burden to security teams.

> By monitoring thousands of surface/dark web sources, SOCRadar helped us to be more informed and resilient against cyber attacks.
>
> **CISO, Finance Sector**

AttackMapper

Attack Surface Management

SOCRadar®

KEY BENEFITS

Detect hacker-exposed vulnerabilities early

Identify shadow digital assets

Monitor essential IT infrastructure

Identify major cryptographic threats

Eliminate the blind spots like:

- Open ports
- Unpatched software
- DNS misconfiguration issues
- Invalid, expired certificates
- Publicly-found employee data
- Unauthorized social profiles
- Vulnerable JavaScript frameworks
- Outdated CMS applications
- Shadow cloud services
- Forgotten domains
- Forgotten subdomains
- Blacklisted IP addresses

Sharpen your view outside your perimeter.

Take control of your ever-evolving attack surface.

Threat actors use thousands of entry points to launch ever-sophisticated attacks. Using an advanced, AI-enabled asset identification and classification algorithm, SOCRadar's AttackMapper enables enterprise security teams to automatically detect and view all external-facing digital assets with infrastructure including IP addresses, DNS configurations, network software, domains, and cloud applications. It enables organizations to detect and eliminate unknown threats and vulnerabilities by providing extensive, continuous visibility in an automated manner.

Gain visibility into hackers' perspective.

Prevent RDP exposure and ransomware attacks.

The successful cyberattacks are due to open ports and cyber assets visible to cybercriminals and threat actors. Threat actors frequently target internet-exposed RDP servers millions of which are protected by no more than username and password.

From an external monitoring perspective, SOCRadar enables you to gain continuous visibility into critical or dangerous open ports which can be abused for exploiting vulnerable services or malicious traffic via worms or malware.

Adapt to the age of machine-speed vulnerability exploitation.

The possibility of discovering an unknown asset or vulnerability that could be exploited by adversaries keeps the security teams up at night. Verizon's 2020 data breach investigations report states that vulnerability exploitation is the second most common type of hacking in breaches. AttackMapper continuously monitors your perimeter from an external perspective to spot critical internet-facing vulnerabilities to be exploited.

Highly-precise scanning engine alerts you when a critical vulnerability is cross-referenced to your digital assets like:

Web application firewalls	**SSL/TLS certificates**	**Software**
VPN appliances	**Web applications**	**CMS applications**
Network services	**JavaScript libraries**	**Operating system**

KEY FEATURES

Power of automation

Skyrocket team efficiency by automating time-consuming manual tasks

On-time alerting

Get alerted by email or through API for faster remediation

Intuitive web portal

Find what you’re looking for with precise asset categorization and interactive maps

Real-time inventory

Maintain real-time asset inventory through continuous, automated discovery

3rd party visibility

Scalable underlying technology to maximize the ecosystem visibility rapidly

Accurate asset inventory

Easily find the digital assets you're looking for

Monitor digital-footprint-centric risks.

SOCRadar helps solving today’s toughest attack surface discovery challenges through monitoring every digital asset for any change.

From the actionable threat intelligence perspective, get alerted on any suspicious incident or baseline change to respond faster.

Attack surface alert types:

Website uptime	SSL/TLS Certificate Grading	Malware / CryptoMining Risk
Domain Expiry/WHOIS	Perimeter Appliance (FW/WAF/IPS)	Dynamic Forms / Skimming Code
DNS Records	IP Reputation / Torrent traffic	BGP Hijacking Risk
Domain TakeOver	SMTP MX Blacklist	IP Routing / MiTM / Hijack
Subdomain TakeOver	Website Defacement	DDoS Amplification Target
Domain Shadowing	Website Title-Content Change	PortMap Malicious Port/Service

> By monitoring and reporting on all public-facing assets of us at large scale, SOCRadar generates actionable insights for our SOC team.
>
> **CISO, Finance Sector**

The SOCRadar Advantage

Consolidated architecture for operational efficiency and unmatched ROI.

SOCRadar combines attack surface management, digital risk protection, and threat intelligence capabilities to protect your entire business against sophisticated multi-vector cyber attacks.

ThreatFusion
Cyber Threat Intelligence

- Threat actor / APT tracking
- API-ready threat feeds
- Multilingual CTI support
- Threat hunting & investigation

RiskPrime
Digital Risk Protection

- Sensitive data leak detection
- Phishing domain detection
- Compromised account detection
- VIP protection

AttackMapper
Attack Surface Management

- Continuous scanning
- Digital footprint discovery & mapping

Start your free trial now!

Sign up for a test drive to try out SOCRadar free for 14 days.

SOCRadar®

Gartner peerinsights™ 4.9 OUT OF 5 STARS IN 7 REVIEWS AS OF 06/2020

8609 Westwood Center Dr.
Vienna, VA 22182 USA

+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.