Incident Report

GreenAnimalsBank

Time Period: 2020/10/19 - 2021/10/19 | Report Date: 2021-10-19

4000 Legato Road, Suite 1100
Fairfax, VA 22033 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.

Gartner peerinsights™

4.9 OUT OF 5 STARS
IN 14 REVIEWS
AS OF 11/2020

Table Of Contents

Classification: [Confidential] Only For Designated Individuals

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Incident Summary

The Incident Report has been prepared for GreenAnimalsBank between 2020/10/19 - 2021/10/19 by SOCRadar Attack Surface Management, Digital Risk Protection, and Cyber Threat Intelligence Platform. This report is a summary of company-specific alarms and the cyber world events sent by SOCRadar. The data used for this analysis has been collected by scanning a wide variety of sources across Surface, Deep and Dark Web using non-intrusive OSINT methodologies. With this report, you can get actionable intelligence into your organization's attack surface to better predict and defend against cyber-attacks.

Actionable Alerts

147

Attack Surface Management

87
alert(s) have been generated

Digital Risk Protection

60
alert(s) have been generated

Reporting

0
report(s) have been prepared

Notifications

50

Cyber Threat Intelligence

50
notification(s) have been sent

- Weekly Vulnerability Digest
- Threat Share
- Deep & Dark Web News
- Cyber Security News

⋮

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Alert Type | Severity Level Distribution

The goal of this alert summary is to provide a clear intelligence overview of the cyber threats your company was confronting during 2020/10/19 - 2021/10/19.
The intelligence findings are based on alerts that were detected and provided via the portal. Distribution of alerts by alert types and severity levels:

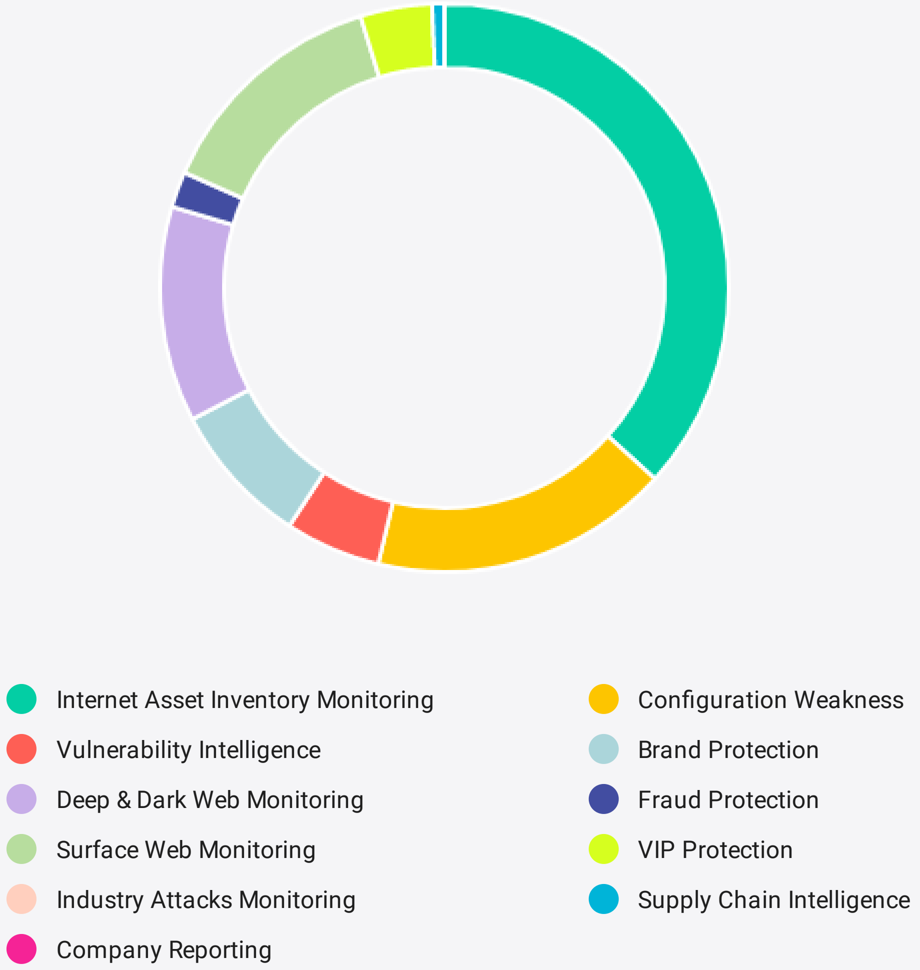
TYPE / SEVERITY	High	Medium	Low	Info	Total
Internet Asset Inventory Monitoring	2	9	0	43	**54**
Configuration Weakness	20	4	1	0	**25**
Vulnerability Intelligence	7	1	0	0	**8**
Brand Protection	5	4	3	0	**12**
Deep & Dark Web Monitoring	12	6	0	0	**18**
Fraud Protection	3	0	0	0	**3**
Surface Web Monitoring	17	2	0	1	**20**
VIP Protection	6	0	0	0	**6**
Industry Attacks Monitoring	0	0	0	0	**0**
Supply Chain Intelligence	1	0	0	0	**1**
Company Reporting	0	0	0	0	**0**
Total	**73**	**26**	**4**	**44**	**147**

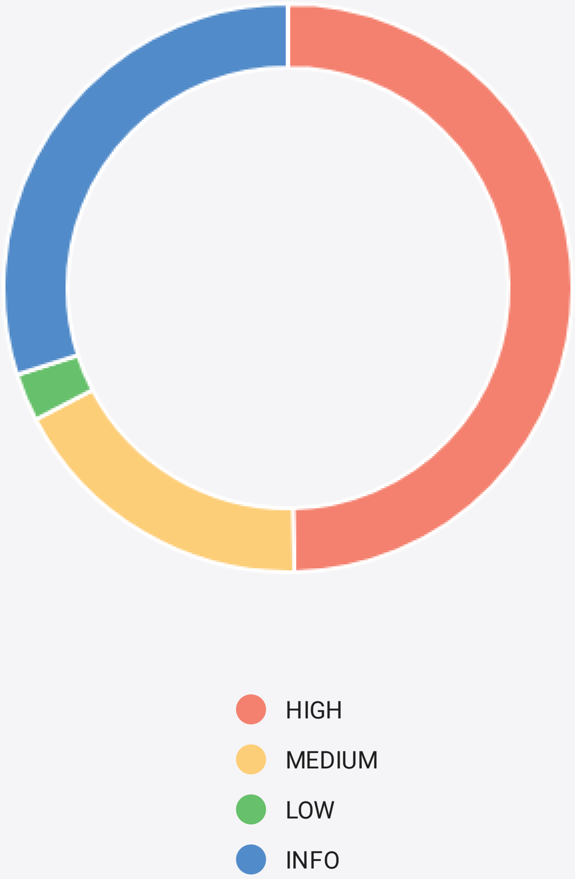
TLP:RED

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Alert Type | Severity Level Graphs

By analyzing the charts below, you can evaluate the top incident categories for your company and the severity of risks.





©SOCRadar Cyber Intelligence Inc. All rights reserved.

Weekly Alerts Severity Trending

The intensity and the severity of the alerts of the alarms day-by-day in the last week can be analyzed on the chart below.

TRENDING OVER TIME

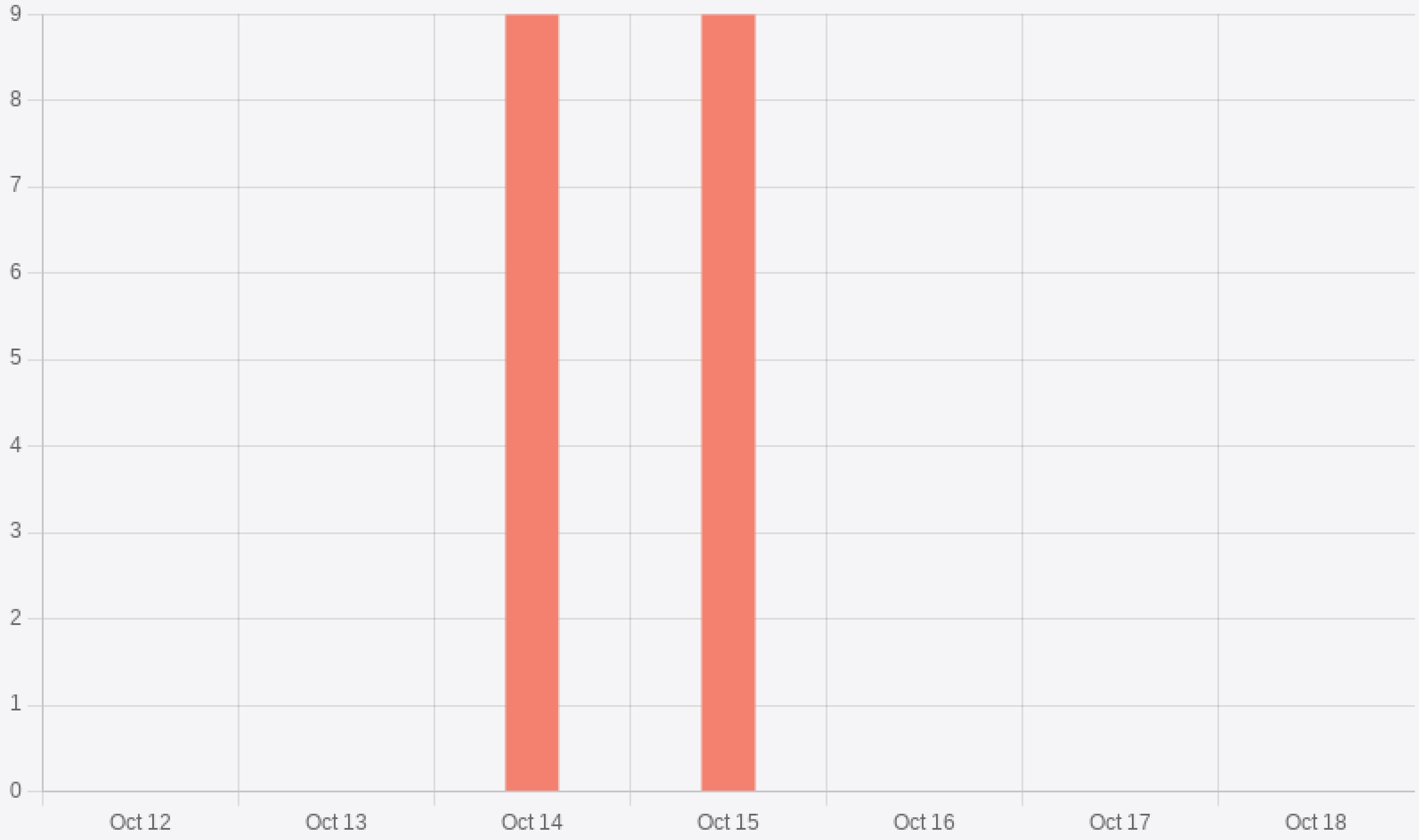
Total: 18

18
HIGH

0
MEDIUM

0
LOW

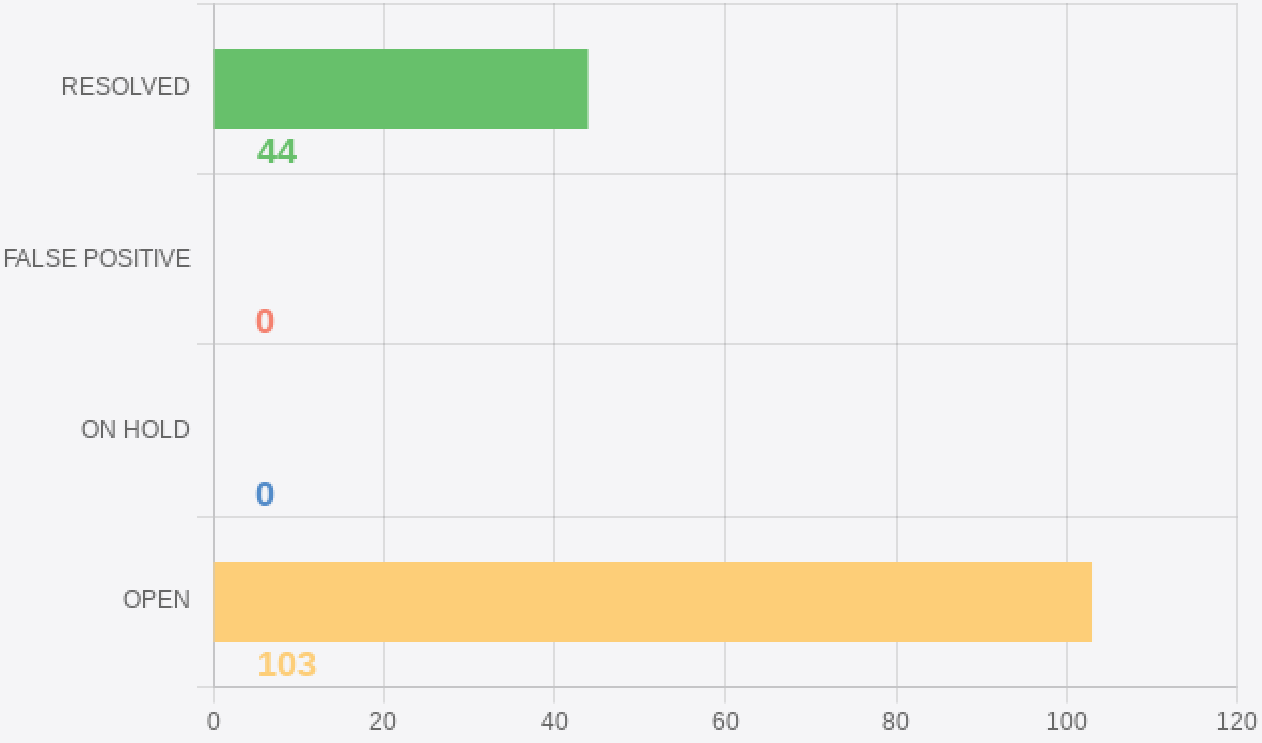
0
INFO



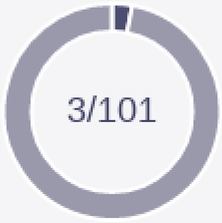
TLP:RED

©SOCRadar Cyber Intelligence Inc. All rights reserved.

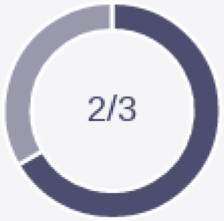
Remediation actions number (resolved, false positive, on hold) by the alert and also requested takedown number is presented in the chart below. High alerts are the most common alerts that require remediation.



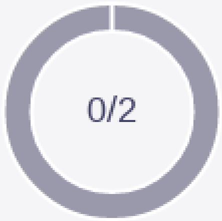
Phishing Request Takedown



Rogue Mobile App Request Takedown



Source Code Request Takedown



©SOCRadar Cyber Intelligence Inc. All rights reserved.

Detailed Incident Summary

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Internet Asset Inventory Monitoring

Internet asset inventory monitoring detects the blind spots of the public digital attack surface with using non-intrusive OSINT methodologies. It helps customers gain additional visibility and context regarding the severity of unknown external-facing digital assets in an automated manner. Through SOCRadar's advanced internet-wide monitoring algorithms, Internet Asset Inventory monitoring provides security teams with direct visibility into all internet-facing technological assets in attributed to IP, DNS, Domain.

Incident ID	Sub Type	Title	Severity	Date
260896	Domain Information	Domain Information Change(s) Detected	INFO	2021-08-24
240904	SSL Information	Company SSL Certificates are About to Expire!	MEDIUM	2021-06-08
239256	Website Information	Website Connection Timeout Detected	INFO	2021-06-03
239250	Website Information	Website Connection Timeout Detected	INFO	2021-06-03
239249	Website Information	Website Connection Timeout Detected	INFO	2021-06-03
239248	Website Information	Website Connection Timeout Detected	INFO	2021-06-03
237505	Website Information	Website Connection Timeout Detected	INFO	2021-05-28
237504	Website Information	Website Connection Timeout Detected	INFO	2021-05-28
236702	SSL Information	Company SSL Certificates are About to Expire!	MEDIUM	2021-05-25
235529	Website Information	Website Title Change Detected	INFO	2021-05-20

* This table shows the last 10 incidents in the selected date range.

TLP:RED

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Configuration Weakness

Much of the success of cyberattacks or any prevalent threat is due to weakness of cyber assets visible to cybercriminals and threat actors. For instance, threat actors frequently target internet-exposed RDP servers millions of which are protected by no more than a username and password.

Incident ID	Sub Type	Title	Severity	Date
276416	Network Security	Critical Open "445 SMB" Port Detected	HIGH	2021-10-15
276415	Network Security	Critical Open "135" Port Detected	HIGH	2021-10-15
276414	Network Security	Critical Open "3389 RDP" Port Detected	HIGH	2021-10-15
276413	Network Security	Critical Open "21 FTP" Port Detected	HIGH	2021-10-15
276412	Network Security	Critical Open "3306 MySQL" Port Detected	HIGH	2021-10-15
276411	Network Security	Critical Open "22 SSH" Port Detected	HIGH	2021-10-15
276410	Network Security	Critical Open Port Detected	HIGH	2021-10-15
276079	Network Security	Critical Open "22 SSH" Port Detected	HIGH	2021-10-14
276078	Network Security	Critical Open "135" Port Detected	HIGH	2021-10-14
276077	Network Security	Critical Open "21 FTP" Port Detected	HIGH	2021-10-14

* This table shows the last 10 incidents in the selected date range.

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Vulnerability Intelligence

SOCRadar continuously monitors your perimeter from an external perspective to spot critical internet-facing vulnerabilities to be exploited.

Incident ID	Sub Type	Title	Severity	Date
276409	Network System Vulnerability	Network Application "XXXX" Vulnerability Detected	HIGH	2021-10-15
276408	Thirdparty Product Vulnerability	Thirdparty Product "XXXX" Vulnerability Detected	HIGH	2021-10-15
276071	Network System Vulnerability	Network Application "XXXX" Vulnerability Detected	HIGH	2021-10-14
235292	Network System Vulnerability	Critical Unsupported Python Version Detected	HIGH	2021-05-19
235291	SSL Certificate Vulnerability	Vulnerability Detected On SSL Certificate	MEDIUM	2021-05-19
233470	Network System Vulnerability	Critical Rce Vulnerability In Microsoft Exchange Servers Detected	HIGH	2021-05-10
232640	Network System Vulnerability	Multiple Critical Vulnerabilities Affecting Your Exim Mail Server	HIGH	2021-05-07
231111	Network System Vulnerability	Network Service Vulnerability Detection	HIGH	2021-05-02

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Brand Protection

Threat actors are using every tool at their disposal to impersonating companies and sell counterfeit goods through online marketplaces and social media platforms. SOCRadar tracks impersonating domains, social media accounts, and mobile apps as well as if the company's assets are on bad reputation lists to protect your brand.

Incident ID	Sub Type	Title	Severity	Date
274309	Impersonating Domain	Impersonating Domain Registration Detected	HIGH	2021-10-08
235522	Social Media Risk	Impersonating Twitter Account Detected	MEDIUM	2021-05-20
235520	Social Media Risk	Impersonating Instagram Account Detected	HIGH	2021-05-20
235261	Impersonating Domain	Impersonating Domain IP Change Detected	LOW	2021-05-19
235086	Impersonating Domain	Impersonating Domain MX Record Change Detected	LOW	2021-05-18
231888	Impersonating Domain	Impersonating Domain Parked Status Change Detected	LOW	2021-05-04
231329	Impersonating Domain	Impersonating Domain Registration Detected	HIGH	2021-05-03
230058	Social Media Risk	Impersonating LinkedIn Account Detected	HIGH	2021-04-28
228410	Social Media Risk	Impersonating Instagram Account Detected	MEDIUM	2021-04-21
216574	Social Media Risk	Company Name Detected Across Web Platforms	MEDIUM	2021-02-27

* This table shows the last 10 incidents in the selected date range.

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Deep & Dark Web Monitoring

SOCRadar provides a thorough Dark & Deep Web Monitoring solution that enables organizations to identify and mitigate threats across the surface, deep, and dark web.

Incident ID	Sub Type	Title	Severity	Date
259243	Dark Web Suspicious Content	Company Related Information Detected on Hacker Forum	HIGH	2021-08-19
233494	IM Platform Suspicious Content	Company Related Information Detected on Telegram Channel	HIGH	2021-05-10
233492	Dark Web Suspicious Content	Company Related Information Detected on Hacker Forum	MEDIUM	2021-05-10
233491	Dark Web Suspicious Content	Company Related Information Detected on Hacker Forum	MEDIUM	2021-05-10
233490	Dark Web Suspicious Content	Company Related Information Detected on Hacker Forum	MEDIUM	2021-05-10
233489	Dark Web Suspicious Content	Company Related Information Detected on Hacker Forum	MEDIUM	2021-05-10
233260	IM Platform Suspicious Content	Company Related Information Detected on Telegram Channel	HIGH	2021-05-10
232829	IM Platform Suspicious Content	Company Related Information Detected on Telegram Channel	HIGH	2021-05-07
232828	IM Platform Suspicious Content	Company Related Information Detected on Telegram Channel	HIGH	2021-05-07
232827	IM Platform Suspicious Content	Company Related Information Detected on Telegram Channel	HIGH	2021-05-07

* This table shows the last 10 incidents in the selected date range.

TLP:RED

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Fraud Protection

Online fraud has become big business for threat actors because sophisticated tools and breached data are readily available for attacks. SOCRadar actively monitors black markets and detects stolen credit cards. It also detects and reports fraud content on hacker forums.

Incident ID	Sub Type	Title	Severity	Date
266066	Stolen Credit Card Detection	Credit Card(s) Detected on Hacker Forum	HIGH	2021-09-13
266064	Stolen Credit Card Detection	Credit Card(s) Detected on Hacker Forum	HIGH	2021-09-13
266063	Stolen Credit Card Detection	Credit Card(s) Detected on Hacker Forum	HIGH	2021-09-13

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Surface Web Monitoring

SOCRadar provides a thorough Surface Web Monitoring solution that enables organizations to identify and mitigate threats across the deep, and dark web.

Incident ID	Sub Type	Title	Severity	Date
260897	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-24
260892	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-24
260785	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-24
260784	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-24
260783	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-24
260398	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-23
260397	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-23
260396	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-23
260395	Code Repository Data Leak	Company Related Information Detected on Code Reporsitory	HIGH	2021-08-23
259838	Code Repository Data Leak	Company Related Information Detected on Github	HIGH	2021-08-21

* This table shows the last 10 incidents in the selected date range.

©SOCRadar Cyber Intelligence Inc. All rights reserved.

VIP Protection

SOCRadar allows security teams to search and monitor critically important personal email addresses of C-suite people whether it’s indexed somewhere in the growing database of major worldwide breaches that may be sought by your adversaries.

Incident ID	Sub Type	Title	Severity	Date
260898	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-08-24
260891	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-08-24
231956	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-05-05
231378	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-05-03
231377	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-05-03
231376	VIP Credential	Company VIP Employee Credential Detected	HIGH	2021-05-03

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Supply Chain Intelligence

Supply chain providers are attractive targets for cyber criminals because many small and medium-sized enterprises have a shortage of proper security resources, facilities, and secure protocols. SOCRadar detect suspicious content of your supply chain organizations in dark web and surface web. In addition, important vulnerabilities that may create criticality are detected.

Incident ID	Sub Type	Title	Severity	Date
228712	Dark Web Supply Chain Monitoring	Supply Chain Related Content Detected on Dark Web	HIGH	2021-04-22

©SOCRadar Cyber Intelligence Inc. All rights reserved.

Notification Summary

SOCRadar informs your company about threats in the cyber world and sends notifications.

Notification ID	Title	Date
72127	SOCRadar Weekly Vulnerability Digest (2021/09/27 - 2021/10/04) [GREENANIMALSBANK][INFO]	2021-10-04
68798	SOCRadar Weekly Vulnerability Digest (2021/09/20 - 2021/09/27) [GREENANIMALSBANK][INFO]	2021-09-27
65352	SOCRadar Weekly Vulnerability Digest (2021/09/13 - 2021/09/20) [GREENANIMALSBANK][INFO]	2021-09-20
28859	SOCRadar Weekly Vulnerability Digest (2021/05/25 - 2021/06/01) [GREENANIMALSBANK][INFO]	2021-06-01
25479	SOCRadar Release v21.05 Yeni Eklenen Özellikler/Güncellemeler Hakkında Bilgilendirme	2021-05-18
24797	SOCRadar Release v21.05 Yeni Eklenen Özellikler/Güncellemeler Hakkında Bilgilendirme	2021-05-17
20014	SOCRadar Weekly Vulnerability Digest (2021/04/19 - 2021/04/26) [GREENANIMALSBANK][INFO]	2021-04-26
18057	SOCRadar Weekly Vulnerability Digest (2021/04/12 - 2021/04/19) [GREENANIMALSBANK][INFO]	2021-04-19
16147	SOCRadar Weekly Vulnerability Digest (2021/04/05 - 2021/04/12) [GREENANIMALSBANK][INFO]	2021-04-12
14121	SOCRadar Weekly Vulnerability Digest (2021/03/29 - 2021/04/05) [GREENANIMALSBANK][INFO]	2021-04-05

* This table shows the last 10 notifications in the selected date range.

©SOCRadar Cyber Intelligence Inc. All rights reserved.

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

RiskPrime
Digital Risk Protection

AttackMapper
Attack Surface Management

Power of automation

Skyrocket security team efficiency by reducing mundane tasks.

360° visibility

Gain in-depth visibility into your external-facing digital assets.

Precise API integration

Smooth integration with existing security stack and SIEM solutions.

Immediate start

Hitting the ground in hours, discovering, monitoring and alerting without requiring any input.

Optimized costs

Choose from the discovered assets only you want to monitor to reconcile license costs with real needs.

CTIA support

Ready to work with clients to identify and remediate threats, helping them build in-house skills and expertise.

SOCRadar®

Trusted by world's leading organizations

Gartner peerinsights 4.9 ★★★★★

Copyright © 2020 SOCRadar Cyber Intelligence Inc.
All rights reserved.