**CHALLENGE**
Misconfigured Cloud Storage

**SOLUTION**
Automated cloud monitoring

CUSTOMER STORIES

## SENSITIVE DATA LEAKAGE WAS PREVENTED WITH 3RD PARTY CLOUD MONITORING

One of SOCRadar's customers active in the European digital media industry, faced sensitive information leak while in a business cooperation with a 3rd party **insurance company.**

Documents, including several Personally Identifiable Information **(PII)** along with the plate number and vehicle type, insurance contracts, signings and all digital paperwork related with the company's car fleet, were stored into a **publicly available cloud storage** due to a misconfiguration.

SOCRadar's client experienced a grave security lapse. They were receiving insurance services from a third-party provider, which might lead to an inadvertent **data breach.** The personal information of **senior managers and executives,** including those who used company cars, might have been stolen in a publicly accessible **data bucket** due to inadequate security measures.

**REGION**
Europe

**INDUSTRY**
Digital Media

**CHALLENGE**
Personally Identifiable Information (PII) leakage, Cloud Security

**SOLUTION**
Automated cloud storage monitoring

Thanks to SOCRadar's Cloud Security Module's (CSM), **automated monitoring systems** detected the misconfigured cloud bucket owned by the insurance company and the customer was immediately alerted by SOCRadar to take necessary precautions.

The case was **successfully closed** without having any reputational or financial damages

## Why is this important?

Securing PII (Personally Identifiable Information) is vital for preserving **privacy,** preventing **fraud,** building trust, and ensuring **compliance** with relevant laws and regulations. It holds immense importance both for enterprises and individuals so ensuring the security of PII is essential to safeguarding the data.

Breaches or unauthorized access to PII can lead to **financial loss, fraudulent transactions,** and compromised **credit cards.** Due to the strict **data protection regulations, compliance** with these rules is essential for avoiding legal repercussions.

**Third party service** providers may cause the organizations to face significant cybersecurity risks. We are going through a new chapter in the digital era, where any **security risk** related to one of your **suppliers** may potentially pose a security risk to your own company causing exponential enlargement of the attack surface. SOCRadar's Extended Threat Intelligence (XTI) approach efficiently contributes to the organizations' cyber security posture by including **third party intelligence** to its large portfolio of contextualized intelligence.

## CHALLENGE
Misconfigured Cloud Storage

## SOLUTION
Automated cloud monitoring

CUSTOMER STORIES

The move towards cloud-based systems, on the other hand, has amplified these risks, as **misconfigurations**, weak **access controls,** system **vulnerabilities,** or shared credentials can cause unintentional or intentional data leaks in the public cloud storages.

Misconfiguration of the cloud storage settings can be considered as the one of the main causes of data leaking. Any data stored in that bucket becomes **accessible** to the public, including **unauthorized users** or **bots,** if a third-party administrator does not properly configure the bucket's permissions. Also employees of a 3rd party with access to the customer's **cloud infrastructure** run the **risk** of accidentally changing access restrictions or moving data to a **publicly accessible** area, which would make it available to unauthorized users. **Malicious actors** may use these flaws to access the public bucket and leak data if the cloud architecture of the **third party** has any holes or weaknesses.

SOCRadar's Cloud Security Module (CSM) strives to shield the clients' data **from exposure** in the cloud. SOCRadar employs various strategies and methods in order to manage and **reduce the risks** connected with **third-party vendors,** suppliers, contractors, and partners. It entails evaluating and keeping track of the cybersecurity posture of third-party organizations to guarantee the security of sensitive data and reduce vulnerabilities.

SOCRadar also keeps track of the customers' own public cloud buckets and **alerts** them when any of those cloud **buckets' statuses change,** allowing our customers to avoid any security problems resulting from misconfigurations of the cloud buckets.

**1** Documents belonging to our customer, including Personally Identifiable Informations (PII), were leaked from a cloud storage due to a misconfiguration.

SOCRadar's Cloud Security Module's (CSM) and automated monitoring systems detected the misconfigured cloud bucket and alerted the customer. **2**

**3** SOCRadar successfully prevented the issue and the case was solved without having any reputational or financial damages.