lema

Proactive 3rd-Party Risk Intelligence

Proactively Mitigate 3rd-Party Risk Without Chasing Down Information

Tomer Roizman

lema

CTO & Co Founder @ Lema

lema.ai

linkedin.com/company/**lema-ai**/

Slides

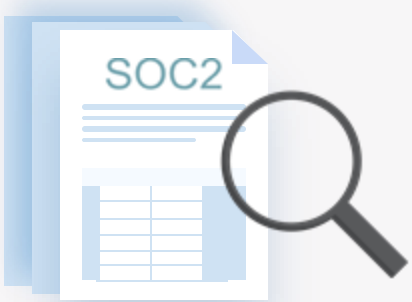
- Storytime
- Control in TPRM
- The Solution

Story Time | My first third-party assessment

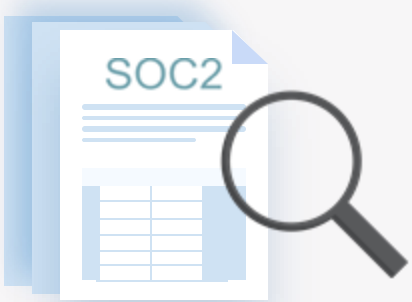
Story Time | Communicating with business owners

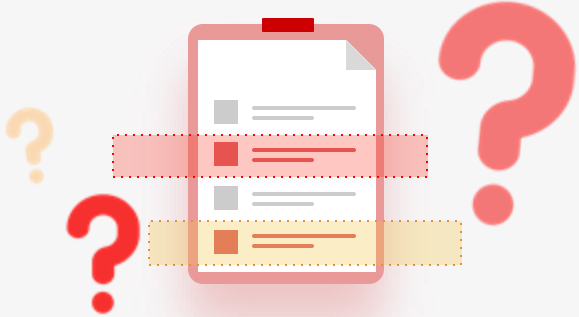
Story Time | Researching the third-party: who are they?

Story Time | Meticulously analyzing their SOC2 report

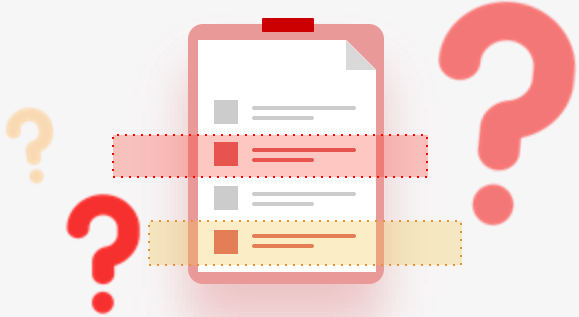


Story Time | Sending the third-party questionnaires





Story Time | Compiling the list of resulting third-party risks




REPEAT THAT,
x10,000

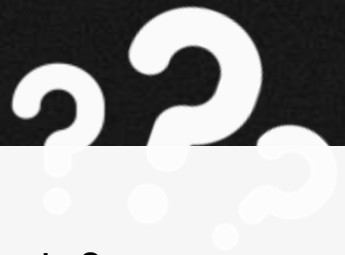
The plot thickens...

A third-party was breached

Do we engage with the third-party?

How much does it damage us?

Loss of Control



- Do we even engage with this third-party?
- When did we assess them?
- Did they have access to our customer's data?
- Did they have a backup policy?
- Do they encrypt our sensitive data?
- Did they use MFA for their production environment?

Loss of Control

- 400 Questions - **BUT THEY** were **never logged in a system of record**
- SOC 2 Type II Report - **BUT IT** was **2 years old**
- IRQ states ‘no access’ to our data - **BUT THEY** actually **DID** have access

Why didn’t we have the tools to be proactive?

The human need for control

> ***Control*** - Creating a sense of predictability, stability and order.

In TPRM:

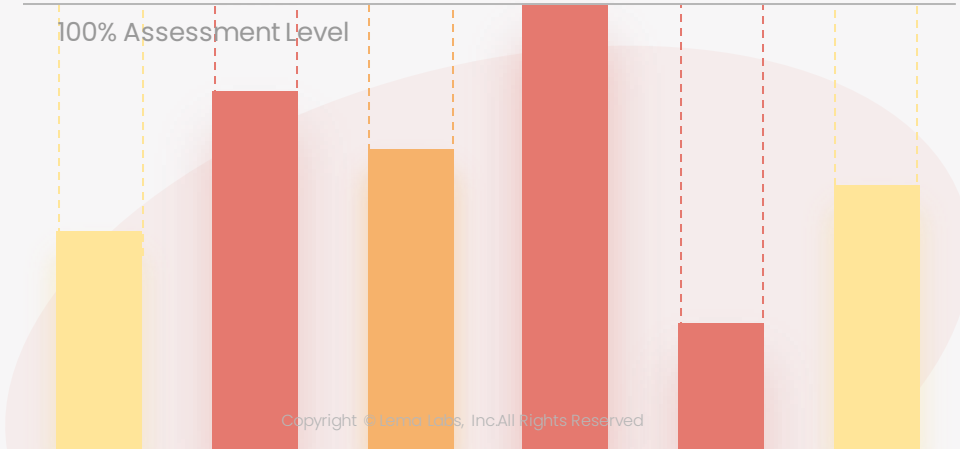
creating visibility, stability, and pro-activity with all our third-party relationships

What was missing? | Visibility

- We didn't have a **standard** third-party assessment repository
- We **only** assessed what **seemed** to be high-risk third-parties
- We were **swamped** by third-party assessments

What was missing? | Stability

- We were missing stability: assessment level wasn't standardized
- 100% assessment level per third-party wasn't guaranteed



What was missing? | Proactivity

- Tools, assessments, business owners, & third-parties **overwhelmed** us
- We spent **too much time** collecting data
- In the end, we lost the ability to make decisions

Finding a solution

- Three step program to boost our third-party risk program
- Empower practitioners
- Enable the business
- Reduce risk

Step 1: Automation

Staying up to date

- **Recording events:**
  Every breach, lawsuit, vulnerability, financial event, M&A, Layoffs, Geopolitical event

- **Recording procurement:**
  Every request to go into procurement automatically creates a record in the system

Step 2: Automation

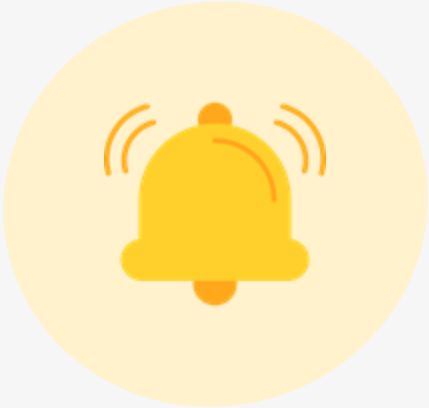
Automatic assessment

- **Ai assesses** every question, report, & contract
- **Cross correlate** data from all the different artifacts to find gaps
- With high quality assessments, we can make **better decisions**

Step 3: Automation

Relationships change

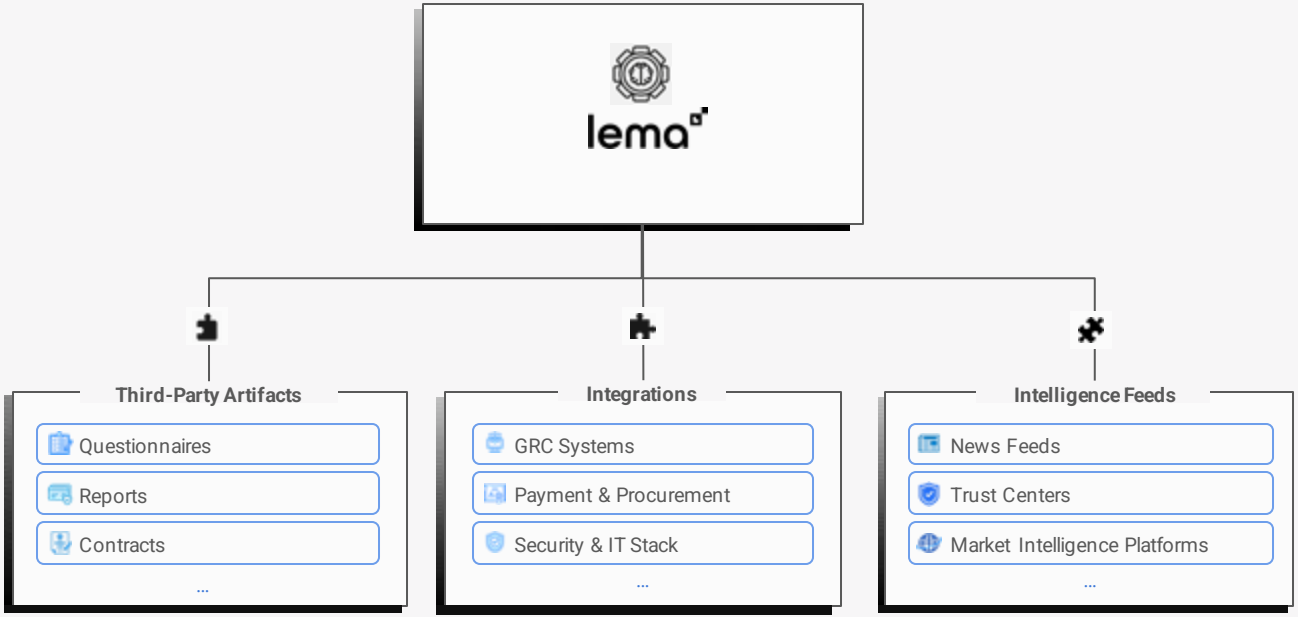
- We receive **notifications** each time a third-party:
  - Gains new access
  - A line of business gets new features
  - Spend goes up



- Automatically **assesses** the **dangers** in each action

Step 4 - Control

Always knowing what is going on everywhere in the business



How Can We Evolve?

Your TPRM Now

Your TPRM's Final Form

Payment & Procurement

What is it?

- Contains all third-party procurement requests
- Every software purchase with corporate card
- Business owner, purpose and service provided

Payment & Procurement

What can we get from it?

- Tracking the entire procurement life cycle
- Triggering assessment in real time
- Tracking all paid businesses and accounts payable

Identity Providers

What is it?

- Provides identity / enterprise email services
- Tracks all Single-Sign-On
- Each external contractor or identity is logged

Identity Providers

What can we get from it?

- Who is using which third party?
- What permissions do they have?
- How often do they access the service?
- Who are our external identities?

Cloud Environment & Cloud Security Platforms

What is it?

- Service Accounts
- Roles and Permissions
- Identity and Access Management

Cloud Environment & Cloud Security Platforms

What can we get from it?

- Which service account belongs to which third party?
- Can they access my data?
- Can they affect my production environment?
- When did they last use their permissions?
- Are their roles separated?

CASB / DLP / New Gen Firewalls

What is it?

- Brokering each access and data sent out of the organization
- Outbound traffic data mapping
- Third-party domains and applications

CASB / DLP / New Gen Firewalls

What can we get from it?

- Who sends exchanges data with third-parties
- What type data is being exchanged
- How many records?
- What is the domain/email address on the other side
- Blocking specific data types

Tomer Roizman

lema

CTO & Co Founder @ Lema

lema.ai

linkedin.com/company/**lema-ai**/