THREAT MODELING

Identifying, enumerating, and prioritizing potential threats to the business.
In addition to my day-to-day software development work at Calero, I participate on an internal security team to promote secure development practices, conduct threat modeling, and support security initiatives.
VULNERABILITY MANAGEMENT
WHAT IS
THREAT MODELING?

Threat modelling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.
WHY THREAT MODEL?

- Build a secure design
- Efficient investment of resources
- Shared understanding
- Threat and compliance risk
- Create required controls
- Balance risks controls, and usability
- Documented threats and mitigation
- Business goals are protected
FOUR QUESTIONS

What are we building?

What can go wrong?

What are we going to do?

Did we do a good enough job?
WHAT ARE WE BUILDING?

We must define the scope of the threat model using architecture diagrams, data flow transitions, data classifications, and people from different roles.
WHAT CAN GO WRONG?

We research the main threats that apply to our scope.
WHAT ARE WE GOING TO DO?

We will turn our findings into specific actions.
DID WE DO A GOOD ENOUGH JOB?

We will examine the quality, feasibility, progress, and planning.
Estimating risk that vulnerabilities bring to the business.
Risk = Likelihood * Impact
FACTORS FOR ESTIMATING LIKELIHOOD

**Threat Agent**
An individual or group that can manifest a threat.

**Vulnerability**
A weakness which can be exploited by a threat agent, such as an attacker, to perform unauthorized actions.
# Threat Agent Factors

## Skill Level
- How technically skilled is this group of agents?

## Motive
- How motivated is this group of agents to find and exploit this vulnerability?

## Opportunity
- What resources are required for this group of agents to find and exploit this vulnerability?

## Size
- How large is this group of threat agents?
## VULNERABILITY FACTORS

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ease of exploit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **How easy is it for this group of threat agents to discover this vulnerability?**
- **How easy is it for this group of threat agents to actually exploit this vulnerability?**
- **How well known is this vulnerability to this group of threat agents?**
- **How likely is an exploit to be detected?**
FACTORS FOR ESTIMATING IMPACT

**Technical**
These factors are aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability.

**Business**
Business impacts are dependent on what is important to the business. Common areas include financial damage, reputation damage, non-compliance, and privacy violation.
<table>
<thead>
<tr>
<th>TECHNICAL IMPACT FACTORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of confidentiality</td>
</tr>
<tr>
<td>Loss of integrity</td>
</tr>
<tr>
<td>Loss of availability</td>
</tr>
<tr>
<td>Loss of accountability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How much data could be disclosed and how sensitive is it?
How much data is corrupted and how damaged is it?
How much service could be lost and how vital is it?
Are the threat agents’ actions traceable to an individual?
# BUSINESS IMPACT FACTORS

<table>
<thead>
<tr>
<th></th>
<th>Financial damage</th>
<th>Reputation damage</th>
<th>Non-compliance</th>
<th>Privacy violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- How much financial damage will result from an exploit?
- Would an exploit result in reputation damage that would harm the business?
- How much exposure does non-compliance introduce?
- How much personally identifiable information could be disclosed?
DETERMINING
SEVERITY

Threat Agent

Vulnerability

Technical

Business

L

I₁

I₂

19
LIKELIHOOD AND IMPACT LEVELS

LOW

0 to < 3

MEDIUM

3 to < 6

HIGH

6 to 9
## OVERALL RISK

### SEVERITY

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>HIGH</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIUM</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>LOW</td>
<td>Note</td>
<td>Low</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LIKELIHOOD</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
</table>

OVERALL RISK

SEVERITY
Our software has a URL tampering vulnerability that allows users in a specific role to view and user profile data on a multi-tenant system; including tenants that they do not belong to.

There are only a small handful of people assigned to this role and we log all access to this data. Unfortunately the logs are not reviewed regularly and the message does not include which user accessed the data.

Engineering is estimating that a rewrite of the entire role based access controls is necessary to fix this vulnerability.
### Threat Agent Factors

<table>
<thead>
<tr>
<th>Skill Level</th>
<th>Motive</th>
<th>Opportunity</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

### Vulnerability Factors

<table>
<thead>
<tr>
<th>Ease of Discovery</th>
<th>Ease of Exploit</th>
<th>Awareness</th>
<th>Intrusion Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>6</td>
<td>9</td>
<td>2</td>
</tr>
</tbody>
</table>

### Technical Impact

<table>
<thead>
<tr>
<th>Loss of Confidentiality</th>
<th>Loss of Integrity</th>
<th>Loss of Availability</th>
<th>Loss of Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>7</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>

### Business Impact

<table>
<thead>
<tr>
<th>Financial Damage</th>
<th>Reputation Damage</th>
<th>Non-Compliance</th>
<th>Privacy Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

---

**Example**
DETERMINING SEVERITY

Threat Agent: 4.375 - MEDIUM
Vulnerability: 7.25 - HIGH
Technical: 2.25 - LOW
## Determining Severity

<table>
<thead>
<tr>
<th>Impact</th>
<th>Overall Risk Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Note</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
</tr>
</tbody>
</table>

- **Overall Risk Severity:**
  - High
  - Medium
  - Low

- **Likelihood:**
  - Low
After the risks to the application have been classified there will be a prioritized list of what to fix. As a general rule, the most severe risks should be fixed first. It simply doesn't help the overall risk profile to fix less important risks, even if they're easy or cheap to fix.
CUSTOMIZING THE RISK RATING MODEL

Adding factors
Choose factors that better represent what's important for the organization.

Customizing options
The options associated with each factor will be much more effective if customized to the business.

Weighting factors
You can weight factors to emphasize the factors that are more significant for the specific business.
WHAT’S NEXT?

Don’t stop threat modeling!

Work through existing applications and systems

Model all new system designs

Integrate it into your SDL
Credits

Shapes & Icons
Vectorial Shapes in this Template were created by Free Google Slides Templates and downloaded from FreePik.com.
Icons in this Template are part of Google® Material Icons and flaticons.com.

Fonts
The fonts used in this template are taken from Google fonts. (Trebuchet, Arial)
You can download the fonts from the following url: https://www.google.com/fonts/

Backgrounds
The backgrounds were created by Free Google Slides Templates.

Images
Photos in this template were downloaded from pixabay.com Attribution is located in each slide notes and the Credits slide.

Color Palette
The Template provides a theme with four basic colors:
- #cc4125ff
- #999999ff
- #ffffff
- #222222ff

Trademarks
Microsoft® and PowerPoint® are trademarks or registered trademarks of Microsoft Corporation.
© 2015 Google Inc, used with permission. Google and the Google logo are registered trademarks of Google Inc.
Google Drive® is a registered trademark of Google Inc.