THREAT MODELING

Identifying, enumerating, and prioritizing potential threats to the business.

ABOUT
ME

Senior Software Engineer
Calero Software

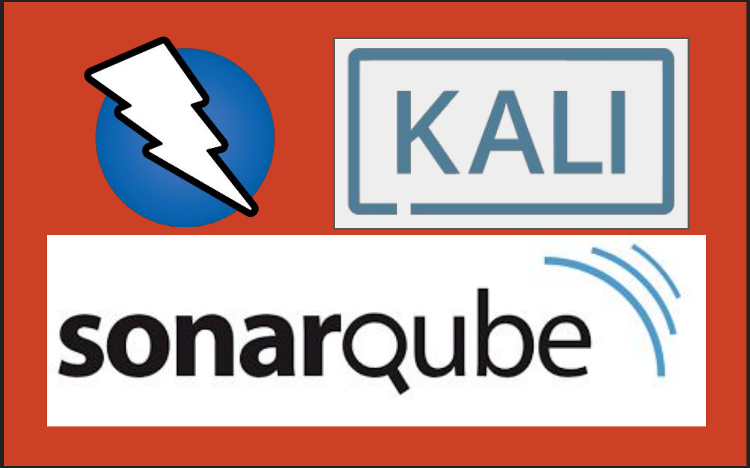
Rochester Chapter Leader
OWASP

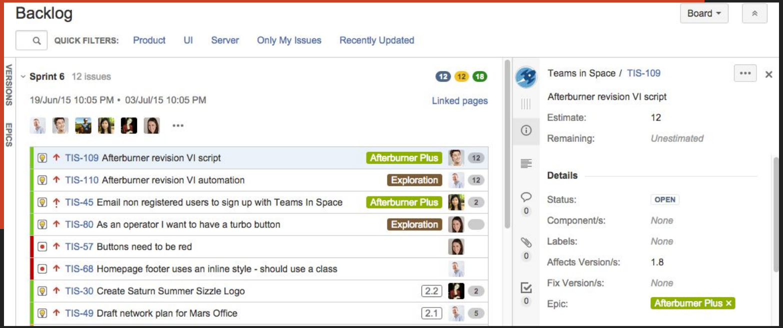
🐦 @jimkeeler

✉ jim.keeler@owasp.org

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





Backlog

QUICK FILTERS: Product UI Server Only My Issues Recently Updated

Sprint 6 12 issues 12 12 18

19/Jun/15 10:05 PM • 03/Jul/15 10:05 PM Linked pages

TIS-109 Afterburner revision VI script	Afterburner Plus		12
TIS-110 Afterburner revision VI automation	Exploration		12
TIS-45 Email non registered users to sign up with Teams In Space	Afterburner Plus		2
TIS-80 As an operator I want to have a turbo button	Exploration		
TIS-57 Buttons need to be red			
TIS-68 Homepage footer uses an inline style - should use a class			
TIS-30 Create Saturn Summer Sizzle Logo		2.2	2
TIS-49 Draft network plan for Mars Office		2.1	5

Teams in Space / TIS-109

Afterburner revision VI script

Estimate: 12

Remaining: *Unestimated*

Details

Status: OPEN

Component/s: *None*

Labels: *None*

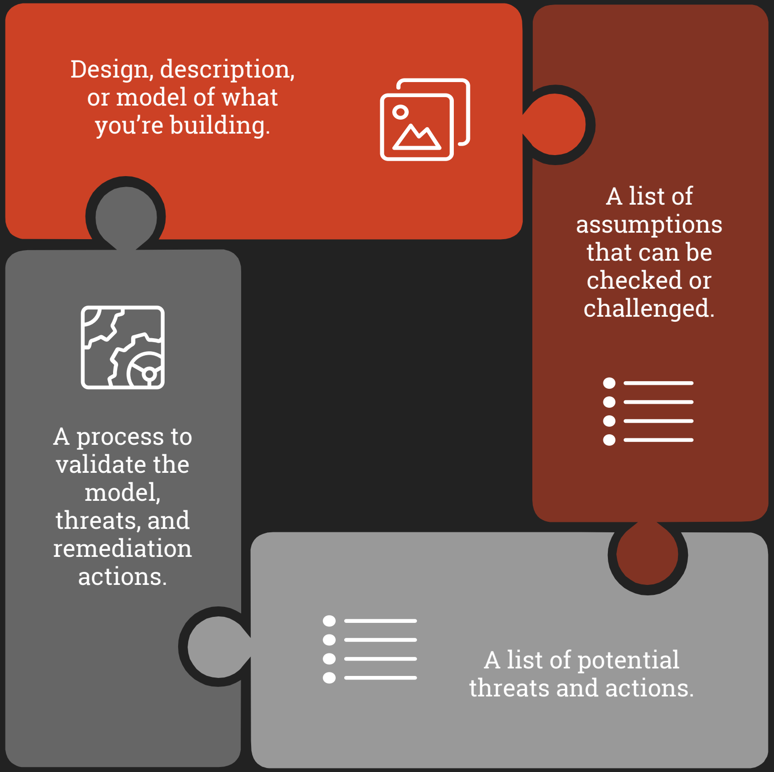
Affects Version/s: 1.8

Fix Version/s: *None*

Epic: Afterburner Plus ×

WHAT IS THREAT MODELING?

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



Design, description, or model of what you're building.

A list of assumptions that can be checked or challenged.

A list of potential threats and actions.

A process to validate the model, threats, and remediation actions.

WHY THREAT MODEL?

Build a secure design

Create required controls

Efficient investment of resources

Balance risks controls, and usability

Shared understanding

Documented threats and mitigation

Threat and compliance risk

Business goals are protected

FOUR QUESTIONS

What are we building?

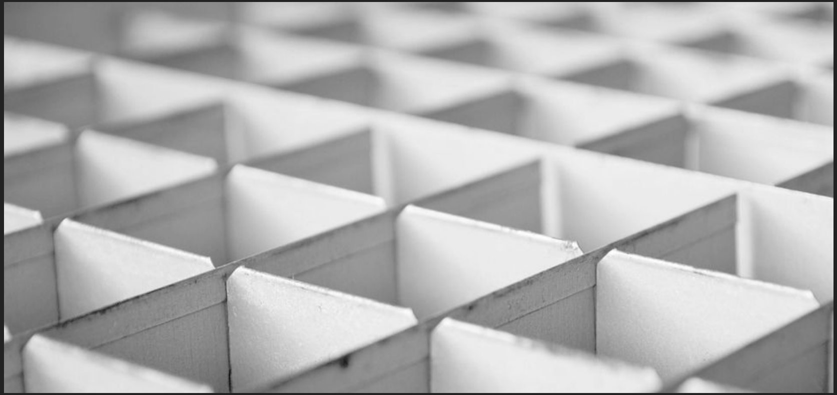
What can go wrong?

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?

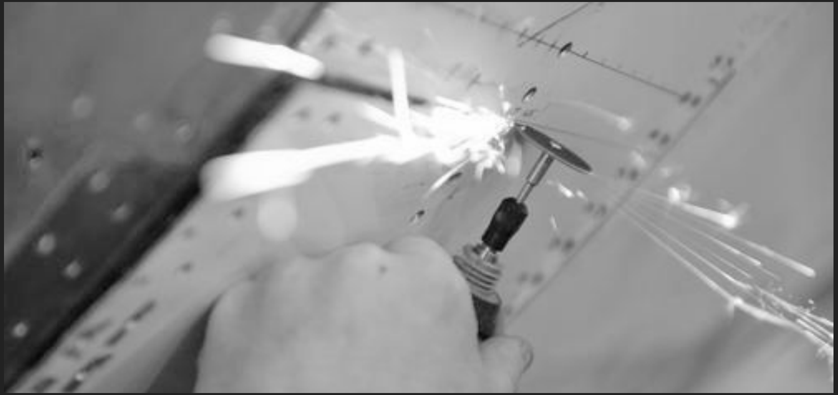
We research the main threats that apply to our scope.

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.



RISK RATING

Estimating risk that vulnerabilities bring to the business.

STANDARD
RISK MODEL

Risk = Likelihood * Impact

FACTORS FOR ESTIMATING LIKELIHOOD

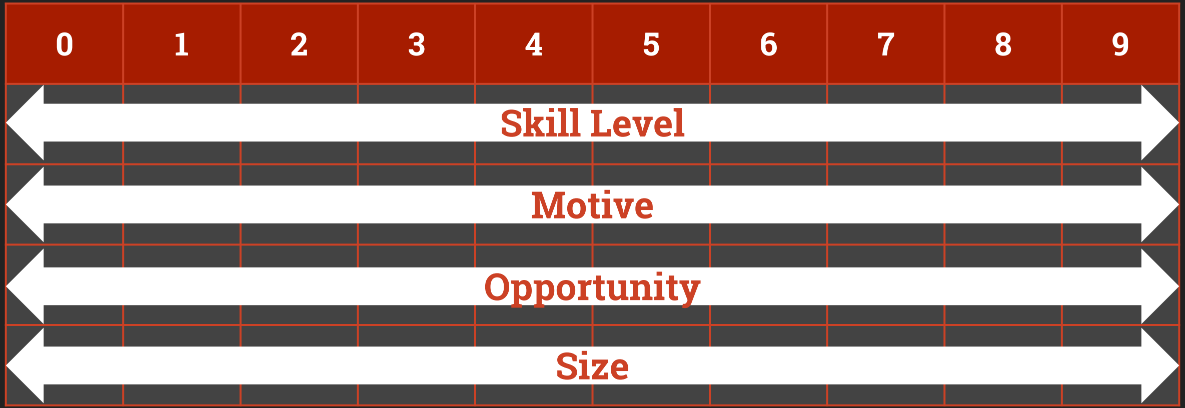
Threat Agent

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



0 1 2 3 4 5 6 7 8 9

Skill Level

Motive

Opportunity

Size

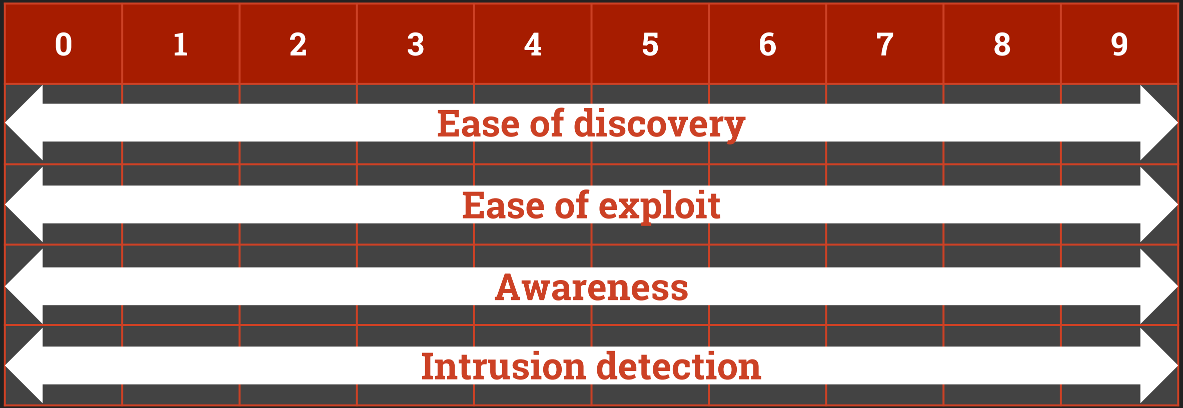
How technically skilled is this group of agents?

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

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

How large is this group of threat agents?

VULNERABILITY FACTORS



0 1 2 3 4 5 6 7 8 9

Ease of discovery

Ease of exploit

Awareness

Intrusion detection

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

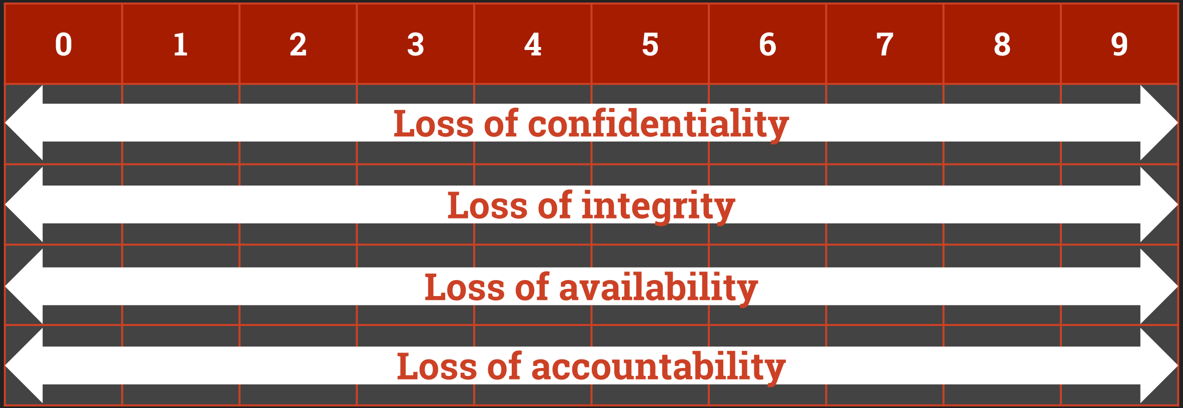
Technical

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.

TECHNICAL IMPACT
FACTORS



0 1 2 3 4 5 6 7 8 9

Loss of confidentiality

Loss of integrity

Loss of availability

Loss of accountability

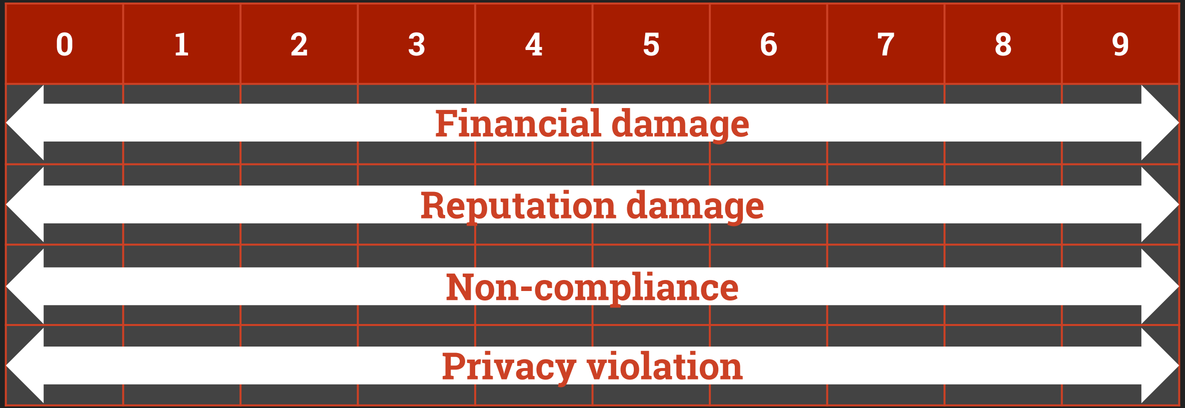
How much data could be disclosed and how sensitive is it?

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



0 1 2 3 4 5 6 7 8 9

Financial damage

Reputation damage

Non-compliance

Privacy violation

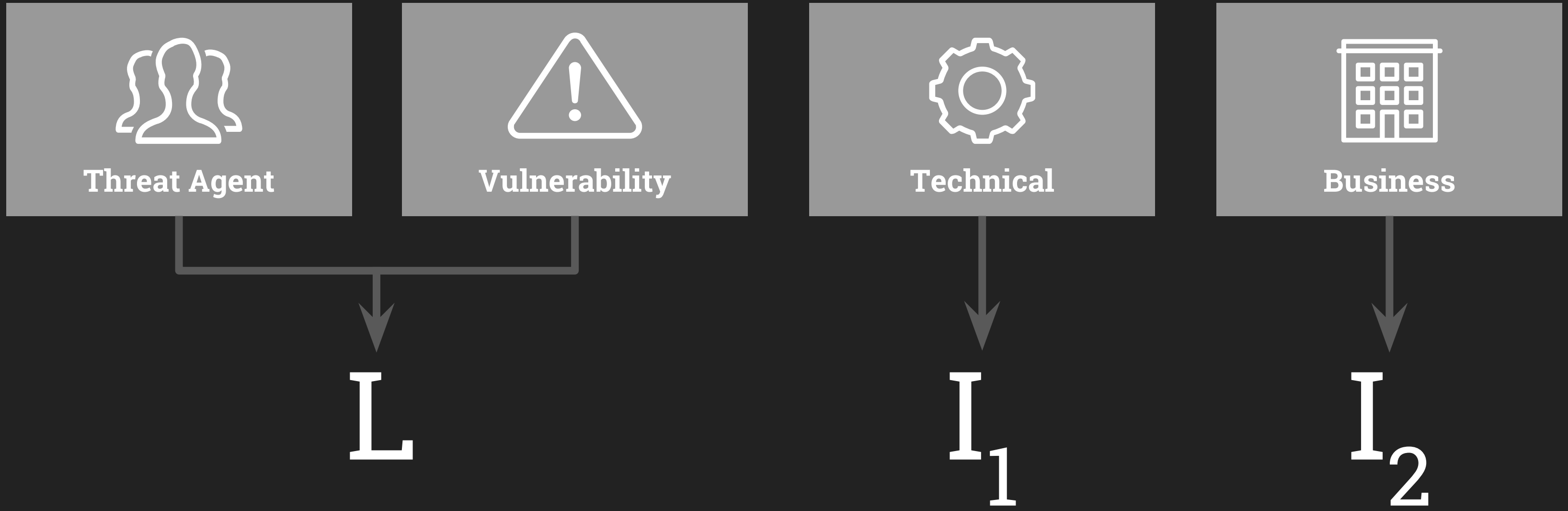
How much financial damage will result from an exploit?

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



LIKELIHOOD AND IMPACT
LEVELS

LOW	MEDIUM	HIGH
0 to < 3	3 to < 6	6 to 9

OVERALL RISK
SEVERITY

IMPACT	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	LIKELIHOOD			

EXAMPLE

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.

EXAMPLE

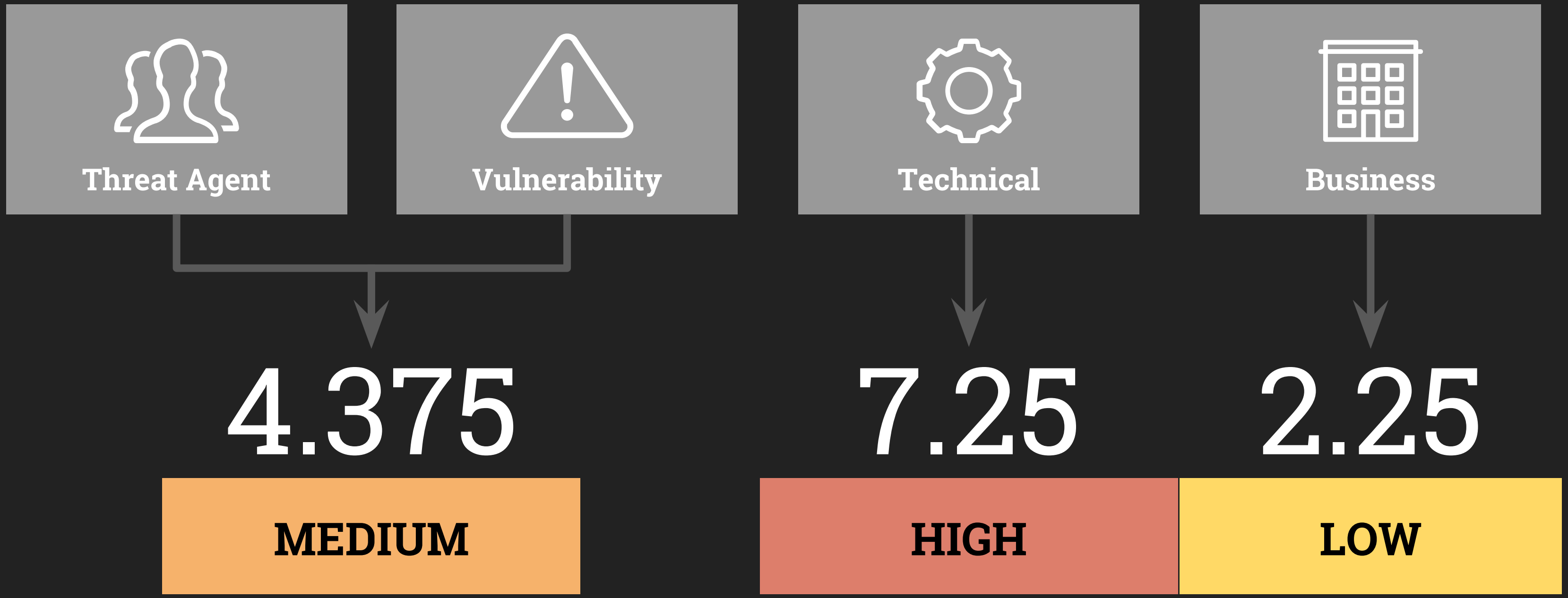
THREAT AGENT FACTORS			
SKILL LEVEL	MOTIVE	OPPORTUNITY	SIZE
5	2	7	1

VULNERABILITY FACTORS			
EASE OF DISCOVERY	EASE OF EXPLOIT	AWARENESS	INTRUSION DETECTION
3	6	9	2

TECHNICAL IMPACT			
LOSS OF CONFIDENTIALITY	LOSS OF INTEGRITY	LOSS OF AVAILABILITY	LOSS OF ACCOUNTABILITY
9	7	5	8

BUSINESS IMPACT			
FINANCIAL DAMAGE	REPUTATION DAMAGE	NON-COMPLIANCE	PRIVACY VIOLATION
1	2	1	5

DETERMINING SEVERITY



Threat Agent

Vulnerability

Technical

Business

4.375

MEDIUM

7.25

HIGH

2.25

LOW

DETERMINING SEVERITY

HIGH

LOW

OVERALL RISK SEVERITY				
IMPACT	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	LIKELIHOOD			

MEDIUM

DECIDING WHAT TO FIX

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**.

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.

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/

Color Palette

The Template provides a theme with four basic colors:

#cc4125ff	#999999ff
#ffffffff	#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.