Welcome to Threat Modeling Lab!

Tell us a bit about yourself

📍 Share in the chat: Where are you based?

✅ Take the poll: What threat modeling framework(s) do you use?

THREAT MODELING | LAB

Creating your first threat model using a spreadsheet

February 22nd | 11:00am-1:00pm ET

Shankar Chebrolu

Director of Security Architecture, Red Hat

Agenda

	Details	
11:00 - 11:05	Welcome and introduction	
11:05 - 12:00	Presentation	● What’s threat modeling ● The six-step spreadsheet template demo
12:00 - 12:10	Break	
12:10-12:35	Hands-on Lab	Saas, PaaS, IaaS
12:35 - 12:50	Group Presentation	Each team will present your work (5 mins/team)
12:50 - 01:00	Wrap-up, Q&A	

Ground Rules

- **Be present:** Close off emails, Slack, other unnecessary windows to keep distractions at bay :)
- **Turn on your video if possible** **(except during individual exercise):** Help yourself and others stay engaged!
- **Be back on time:** So we can maximize the two hours together and finish on time

Learning Objectives

By the end of this workshop, you'll:

- A good understanding of what threat modeling is and isn't
- A good understanding of the four threat modeling elements and threat categories (STRIDE)
- A basic threat model built by you for a cloud application (SaaS, PaaS, IaaS)

Assumptions:

- Basic understanding of a Threat, Vulnerability and Risk
- Basic understanding of NIST CSF (Cybersecurity Framework)

What’s threat modeling?

- A structured and repeatable process to identify threats and mitigate them against valuable assets in a system
- Secure systems cannot be build without understanding the potential threats
- Threat modeling could be used for:
    - Modeling a system
    - Identify Threats
    - Analyze Vulnerabilities
    - Design, Implement & Verify Mitigations

Alignment to NIST-CSF

Function	Category	Sub-category
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-3: Threats**, both internal and external, are **identified** and **documented**

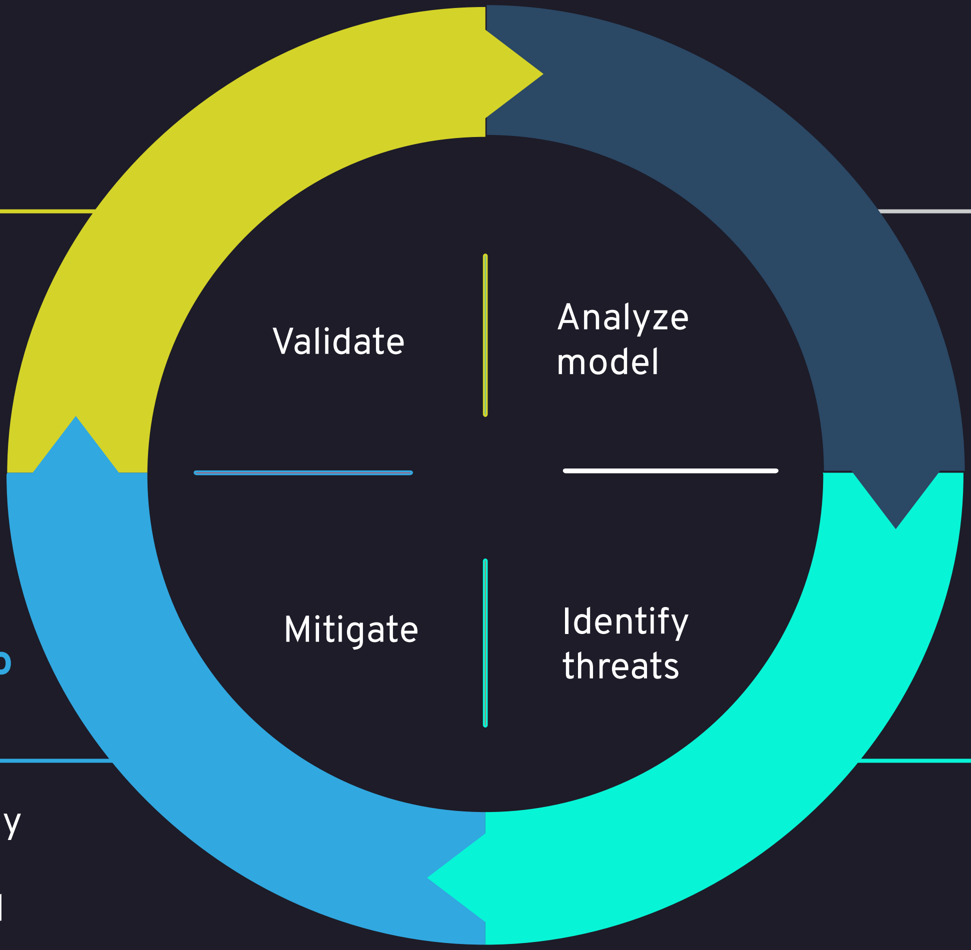
Threat Modeling Vs Threat Intelligence

	Threat Modeling (TM)	Threat Intelligence (TI)
Alignment	Security architecture / design portion of secure development lifecycle (SDL)	Security operations
Relevance	Identifying threats in a particular system before it is deployed in production	Comprehensive list of threats to a whole organization w.r.t. Systems already in production/laptops/workstations, etc
What’s in Common	Both TM and TI maps into NIST CSF: IDENTIFY (ID) → Risk Assessment (RA) → Threats are identified and documented (ID.RA-3)	

Threat modeling classification: STRIDE

Classification	Definition	Sample Threats
Spoofing	Impersonating someone or something else	❑ Pretending to be valid user ❑ Pretending to be another web server
Tampering	Modifying code or data	❑ Modifying code (or library), data on a system ❑ Modifying a packet as it traverses the network
Repudiation	Claiming to have not performed an action	❑ Remove record of modification of a file ❑ Remove record of deletion of a system resource
Information disclosure	Exposing information to someone not authorized to access	❑ Sniffing network traffic to read sensitive data in transit ❑ Launching SQL injection attack to read sensitive data from DB table(s)
Denial of service (DoS/DDoS)	Deny or degrade service to users	❑ Crashing a website ❑ Sending data absorbing CPU cycles or storage resources
Elevation of privilege	Gain capabilities without proper authorization	❑ Allowing a limited user to switch to an admin user without authorization or validation logic

Threat modeling process
(The four-question framework by Adam Shostack)



Validate

Analyze model

Identify threats

Mitigate

1 **What are we working on?**

Create an architectural diagram

2 **What can go wrong?**

Analyze the model to identify potential threats

3 **What are we going to do about it?**

Indicate which threats are already mitigated and determine how the remaining threats would be mitigated

4 **Did we do a good job?**

Validate the system against recorded threat model. Continue to mitigate any open issues

Threat modeling elements

- **Actor:** Users (typically humans)
- **Datastore:** Databases, Filesystems, LDAP, Cookies, Memory-Cache
- **Data Flow:** HTTPS, IPSEC, RPC
- **Process (runs code):** Web application/service, OS process, any business logic running in a server (web server, app server, database)

STRIDE applicability threat modeling elements

	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Actor	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Datastore		✓	✓	✓	✓	
Dataflow		✓		✓	✓	

Cloud Threat Modeling: understanding shared responsibility matrix

- Cloud Threat Modeling expands on standard threat modeling practices to account for unique cloud services and an application’s qualities and considerations.
- Cloud Threat Modeling exercise involves understanding the shared responsibility matrix between cloud provider and cloud consumer

	IaaS	PaaS	SaaS
Security Governance, Risk & Compliance	Cloud Consumer	Cloud Consumer	Cloud Consumer
Data Security	Cloud Consumer	Cloud Consumer	Cloud Consumer
Application Security	Cloud Consumer	Cloud Consumer	Shared Responsibility
Platform Security	Cloud Consumer	Shared Responsibility	Cloud Provider
Infrastructure Security	Shared Responsibility	Cloud Provider	Cloud Provider

Demo 💻

Break ☕

See you all again at 12:10pm ET!

Hands-On Lab

12:10-12:35m ET (25 mins)

Group Presentation

12:35-12:50pm ET (5 mins/group)

Wrap-Up

Q&A

Upcoming Threat Modeling Lab

THREAT MODELING | LAB

Security Threat Modeling Workshop

March 1st | 11am-1pm ET

Chris Romeo

CEO, Kerr Ventures

Upcoming Threat Modeling Lab

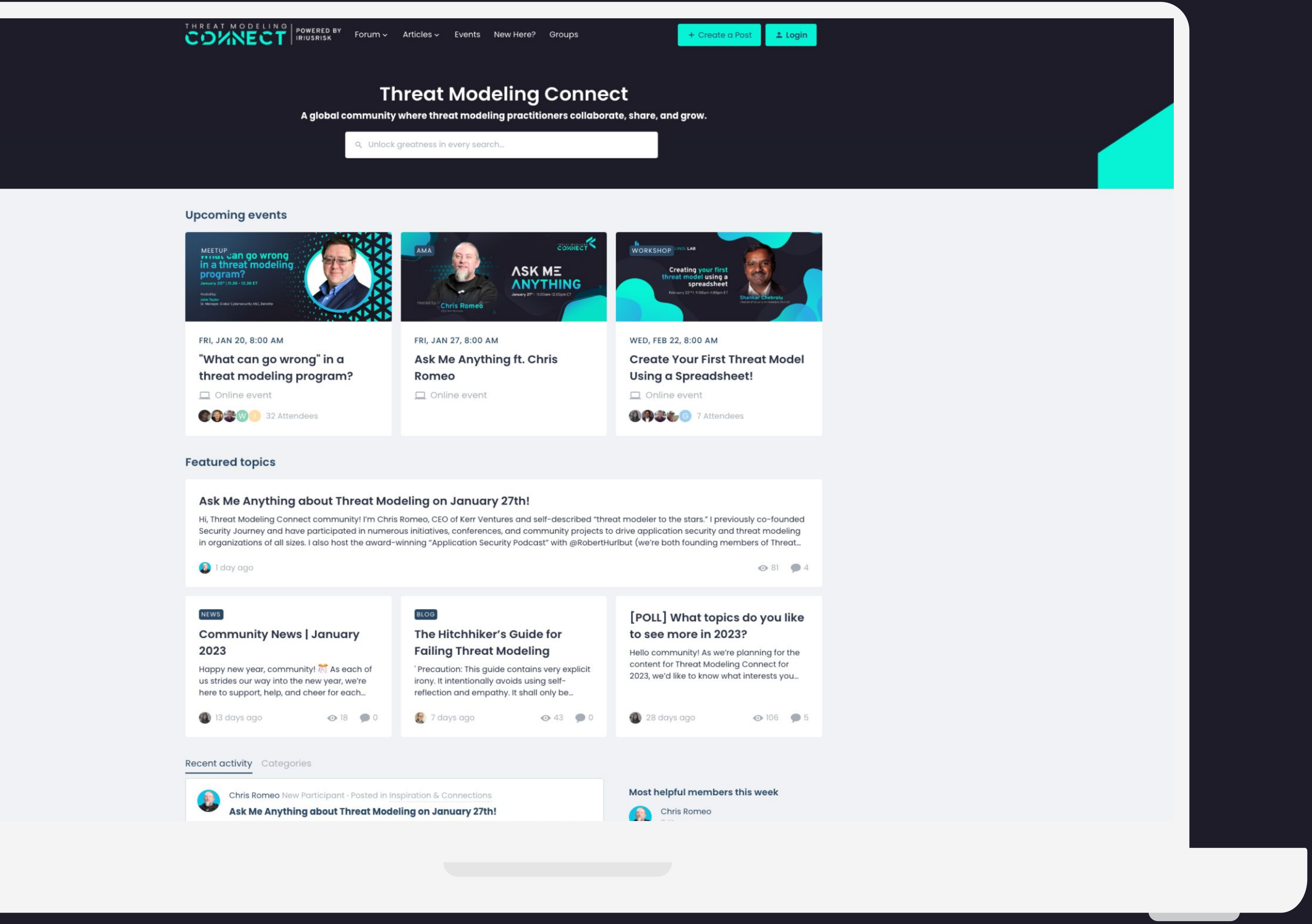
THREAT MODELING | LAB

Privacy Threat Modeling Workshop

March 9th | 10am-12pm ET

Kim Wuyts

Sr. Privacy Researcher, KU Leuven


THREAT MODELING CONNECT | POWERED BY IRIUSRISK
Forum
Articles
Events
New Here?
Groups
+ Create a Post
Login
MEETUP
What can go wrong in a threat modeling program?
AMA
ASK ME ANYTHING
Chris Romeo
WORKSHOP
Creating your first threat model using a spreadsheet
Shankar Chebrolu

Threat Modeling Connect

A global community where threat modeling practitioners collaborate, share, and grow.

Unlock greatness in every search...

Upcoming events

FRI, JAN 20, 8:00 AM
"What can go wrong" in a threat modeling program?
Online event
32 Attendees

FRI, JAN 27, 8:00 AM
Ask Me Anything ft. Chris Romeo
Online event

WED, FEB 22, 8:00 AM
Create Your First Threat Model Using a Spreadsheet!
Online event
7 Attendees

Featured topics

Ask Me Anything about Threat Modeling on January 27th!

Hi, Threat Modeling Connect community! I'm Chris Romeo, CEO of Kerr Ventures and self-described "threat modeler to the stars." I previously co-founded Security Journey and have participated in numerous initiatives, conferences, and community projects to drive application security and threat modeling in organizations of all sizes. I also host the award-winning "Application Security Podcast" with @RobertHurlbut (we're both founding members of Threat...

1 day ago 81 4

NEWS
Community News | January 2023
Happy new year, community! 🎊 As each of us strides our way into the new year, we're here to support, help, and cheer for each...
13 days ago 18 0

BLOG
The Hitchhiker's Guide for Failing Threat Modeling
' Precaution: This guide contains very explicit irony. It intentionally avoids using self-reflection and empathy. It shall only be...
7 days ago 43 0

[POLL] What topics do you like to see more in 2023?
Hello community! As we're planning for the content for Threat Modeling Connect for 2023, we'd like to know what interests you...
28 days ago 106 5

Recent activity Categories

Chris Romeo New Participant · Posted in Inspiration & Connections
Ask Me Anything about Threat Modeling on January 27th!

Most helpful members this week
Chris Romeo

Let's continue the conversation at Threat Modeling Connect

An **open threat modeling community** where you can collaborate, share, and grow with practitioners worldwide through forum discussions, expert content, and events.

👉 **Stay in touch between calls:**
https://www.threatmodelingconnect.com