THREAT MODELING CONNECT

THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE

THREAT MODELING CONNECT

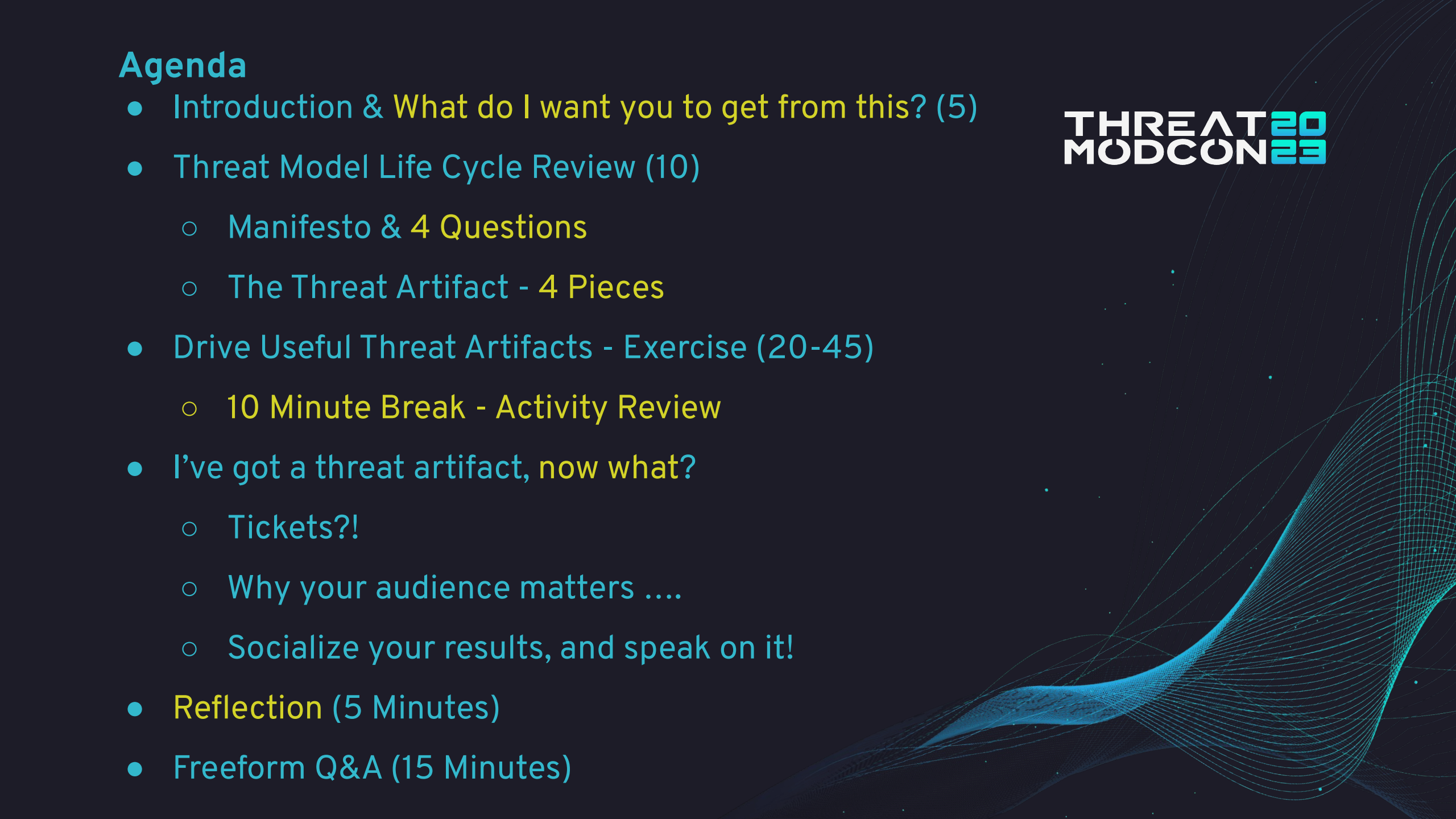
THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE

From Threat Discussion to Completed Mitigation: Making your Threat Model Useful! (Workshop)

Agenda

- Introduction & What do I want you to get from this? (5)
- Threat Model Life Cycle Review (10)
  - Manifesto & 4 Questions
  - The Threat Artifact - 4 Pieces
- Drive Useful Threat Artifacts - Exercise (20-45)
  - 10 Minute Break - Activity Review
- I've got a threat artifact, now what?
  - Tickets?!
  - Why your audience matters ....
  - Socialize your results, and speak on it!
- Reflection (5 Minutes)
- Freeform Q&A (15 Minutes)



Who is Jono?

THREAT MODCON 2023

- Principal Application Security Architect @ Aquia, Inc.
- Community Technical Manager & Developer Advocate (Consul) @ HashiCorp
- DevOps Dojo Coach @ Liatrio
- Platform Infrastructure Engineer @ Apple
- AWS SRE @ Zeta Global

ThreatModelConnect: Jono-131

LinkedIn: **jsosulska**

Whether development, operations, advocacy or education ... Every role I have ever had, has benefited by taking the time to Threat Model - Jono

What is Aquia?

THREAT MODCON 2023

Aquia

Aquia is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that specializes in transformative cloud and cybersecurity professional services for the public and private sectors. Learn more at **aquia.us**.

aws 50 CERTIFIED

aws PARTNER Advanced Tier Services

- Public Sector
- Authority to Operate

Trusted by

VA | U.S. Department of Veterans Affairs

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF INSPECTOR GENERAL

PLATFORM ONE — WATERFALL. ONLY YOU CAN PREVENT

U.S. AIR FORCE

Nava

KESSELRUN

DATALOCK CONSULTING GROUP

VALLEY IT SOLUTIONS

coforma

RegScale

noblis

Excella

cantaloupe

BIGBEAR.AI

What do I want for you to get out of this activity?

THREAT MODCON 2023

- *Threat Modeling is for **Everyone**.*
- *So long as you have a **threat description**, a **potential mitigation**, some **action items**, and **questions**, it doesn't matter how you got here. What matters is **what you do with that information.***
- *Engage, and re-engage, with your Threat Models to improve value beyond your team.*

Concepts Review: 4 Questions and the Manifesto

THREAT MODCON 2023

THREAT MODELING MANIFESTO

What is threat modeling?

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions:

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

https://www.threatmodelingmanifesto.org/

Concepts Review: Threat Ideation and Identification

THREAT MODCON 23

Threat Description
An attacker can inject a command that the system will run at a higher privilege level - ♔ **King** ♔ *Elevation of Privilege Suit*
An attacker can use a shared key to authenticate as different principals confusing information in the logs - **Nine** *Repudiation Suit*

Do we understand “what [threat] is being worked on”, **based on our role**?

Do we know “what could go wrong” … **based on the description** as is?

What are we going to do to improve the description?

Elevation of Privilege Card Game

Concepts Review: Threat Ideation and Identification

THREAT MODCON 2023

Threat Description
An attacker can inject an unknown command via a tampered container image being uploaded to an image registry, and deployed into a Kubernetes cluster to run at a higher privilege level, by squatting on the tag of an open source dependency - **Modified ♚King♚** *Elevation of Privilege Suit*
An attacker can use a shared key to authenticate as different principals to a shared development account, confusing information in the logs - **Modified Nine** *Repudiation Suit*

Concepts Review: Improving Threat Ideation and Identification

THREAT MODCON 2023

What can we improve about our descriptions?

- ***Consider your audience!***

  Tech Writing? Sales (Eng)/Marketing? Inter-team Dependencies?

- ***Support asking and recording questions!***

  Shared doc/wiki? Slid.io? Sticky notes?

Advice: If only 2 people understand the work described, only 2 people can do the work described.

Concepts Review: Threat Mitigation

THREAT MODCON 2023

Threat Description	Threat Mitigation
An attacker can inject an unknown command via a tampered container image being uploaded to an image registry, and deployed into a Kubernetes cluster to run at a higher privilege level by squatting on the tag of an open source dependency.	1. Create a pipeline to gate uploading images to artifact repository 2. Remove human access to upload to artifact repositories 3. Implement Kubernetes logging to identify if privileged containers are launched
An attacker can use a shared key to authenticate as different principals to a shared development account, confusing information in the logs.	1. ?

Concepts Review: Identifying Action Items & Questions

THREAT20 MODCON23

Threat Description	Threat Mitigation	Action Items & Questions
An attacker can inject an unknown command via a tampered container image being uploaded to an image registry, and deployed into a Kubernetes cluster to run at a higher privilege level by squatting on the tag of an open source dependency.	1. Create a pipeline to gate uploading images to artifact repository 2. Remove human access to upload to artifact repositories 3. Implement Kubernetes logging to identify if privileged containers are launched.	1. Do we have an established pipeline for artifact creation? How would we verify if there were any unexpected artifacts? 2. Has anyone tried to manually access the artifact repository lately? If so, what does that look like in the logs?
An attacker can assume a shared administrative role in a shared development account on a service or platform, confusing information in the logs.	1. No existing mitigation in dev. (Prod has confirmed no human access)	1. We will need to spike on improvements to separating shared access to resources for experimentation. 2. Look into tagging strategies within the standardized logs we use.

Drive Useful Threat Artifacts Exercise

THREAT MODCON 2023

Activity Time! Please get out your phones, and go to the pages on each of the following slides. Each activity has a unique QR code and window for participation!

After-workshop note: The following slides will be proxies of the activity, as well as some of the responses included. There is no QR codes, but the questions and responses are recorded

*They will be broken down into **the question**, **audience responses**, and **facilitator add-ons.***

Several questions extend across multiple slides. Slides 17-22 all apply to a single activity. See (Con't) in the title.

Drive Useful Threat Artifacts: Improve the Threat Description

THREAT MODCON 2023

What would you do to improve this threat description?

An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID" **E.g. "name the endpoints**

- **Response:** Add more info on the attacker (authenticated/non-authenticated, local, acting as a sysadmin, dev, etc.).
  - **Add on:** Correct! This applies more detail relative to the role, as well as the context of the Threat
- **Response:** who the potential attackers might be
  - **Add on:** See Above
- **Response:** Detail the functionality of the endpoints
  - **Add on:** Correct! Specific endpoints may care more about a certain type of threat actor or attacker based on their business, operational, or support functions
- **Response:** Explain why
  - **Add on:** Correct! Explaining a bit more about what specifically may be targeted or why is valuable to the scope

Drive Useful Threat Artifacts: Describe Potential Mitigations (3 or Higher Votes)

THREAT MODCON 23

What are some mitigations based on an AWS EKS architecture? E.g. "implement service mesh with internal CA"

- **Response (4) :** service to service authentication and authorization and have different clusters **AND** mtls/mutualTLS
  - **Add on:** As mitigations go, these are technically correct. For Threat Modeling Sessions, spend a little time going over technologies like mtls in a lunch-and-learn style, or demo. Having context of this technology touched on as part of a threat model goes a long way to uplifting everyone in the session.
- **Response (3) :** Are you enforcing tenant isolation?
  - **Add on:** This question got upvoted a lot, and I'm happy to see it in this section. For a lot of teams, they may not *know* exactly what specific configurations may be.

Drive Useful Threat Artifacts: Describe Potential Mitigations (1 Vote - Con't)

THREAT MODCON 23

What are some mitigations based on an AWS EKS architecture?
E.g. "implement service mesh with internal CA"

- **Response:** Ingest audit logs to a siem, get container level visibility, implement irsa, turn off public access, use authorized images and nodes, manage base node ami, NSP, audit SA accounts
  - **Add on:** This is a strong list of potential mitigations that could be implemented in an EKS architecture. For each on of these, a small description to accompany the mitigation would go a long way to support a Threat Model's (re)use!
- **Response:** Don't store sensitive information in logs, is persistent store
  - **Add on:** It may be easier to identify actions or activities not to take. As part of recording a mitigation of non-action, include potential other mitigations as well!
- PAM
  - **Add on:** Privilege Access Management - A challenge for any Kubernetes System
- Clear policy and owners, procedures
  - **Add on:** Are your current policy and procedures adapted to your platform specifics?

Drive Useful Threat Artifacts: Generate Additional Questions - All Responses!

THREAT MODCON 2023

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

- How sensitive is the data at risk? Are there regulatory implications?
- Is sensitive data being transmitted?
- What type of data is sent?
- What is the data in questions? What do we accept and what do we return on this endpoint?
- What part of the user experience would break if we made it authenticated?
- What is the impact on the business if this happens?
- What is the impact of compromise?
- What is the impact of this attack? , e.g exposure of customer date, .. etc
- Would you talk through with me how this might affect my functional area?
- What is the likelihood for being able to attack / exploit?
- What does the attacker gain access to?
- what does the service behind the endpoints do?
- What other systems can the attacker access using the data captured from the endpoint?
- What asset is the attacker able to read/modify?
- Does the privacy also impact?
- What endpoints are involved? What data is involved?
- What are the conditions for this attack to be possible?

These are all broken out by groups in continuing slides!

- Where would an attacker be able to insert themselves to execute MITM in the first place?
- How likely is it that mitm will be successful?
- Where are the endpoints located? Internal, external or. Both?
- What is the position of the actor?
- What services are exposed in this end point?
- Have we got https anyway?
- Does the system requires to be compliant with a specific standard
- Who is the attacker? an insider or external?
- Is it a open network?
- Is this server or client side attack related?
- What is the full interaction (source, destination, comm protocol)
- who are your users, how do they access the system, from where do they access ?
- Can there be trust ensured between the systems?
- How could the attacker become a MITM
- Is the connection unencrypted?
- What is the associated risk/impact?
- Are we not enforcing TLS everywhere?
- Was there a reason why you didnt include authentication
- Why is this unauthenticated

Drive Useful Threat Artifacts: Generate Additional Questions - Technique-Based Questions (Con't)

THREAT MODCON 2023

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

- What is the likelihood for being able to attack / exploit?
- What does the attacker gain access to?
- What asset is the attacker able to read/modify?
- What endpoints are involved? What data is involved?
- What are the conditions for this attack to be possible?
- Where would an attacker be able to insert themselves to execute MITM in the first place?
- How likely is it that mitm will be successful?
- What is the position of the actor?
- What services are exposed in this end point?
- Have we got https anyway?
- What is the full interaction (source, destination, comm protocol)
- How could the attacker become a MITM?
- Is the connection unencrypted?

Drive Useful Threat Artifacts: Generate Additional Questions - Authentication Based Questions (Con't)

THREAT MODCON 2023

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

- Where are the endpoints located? Internal, external or Both?
- Who is the attacker? an insider or external?
- Is it a open network?
- Is this server or client side attack related?
- What is the full interaction (source, destination, comm protocol)
- who are your users, how do they access the system, from where do they access ?
- Can there be trust ensured between the systems?
- Are we not enforcing TLS everywhere?
- Was there a reason why you didnt include authentication
- Why is this unauthenticated
- what does the service behind the endpoints do?
- What other systems can the attacker access using the data captured from the endpoint?

Drive Useful Threat Artifacts: Generate Additional Questions - Privacy, Impact, & Risk Questions (Con't)

THREAT MODCON 2023

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

- How sensitive is the data at risk? Are there regulatory implications?
- What is the impact on the business if this happens?
- What is the impact of compromise?
- What is the impact of this attack? , e.g exposure of customer date, .. etc
- Would you talk through with me how this might affect my functional area?
- What is the likelihood for being able to attack / exploit?
- What does the attacker gain access to?
- What other systems can the attacker access using the data captured from the endpoint?
- Does the privacy also impact?
- Does the system requires to be compliant with a specific standard
- who are your users, how do they access the system, from where do they access ?
- What is the associated risk/impact?

Drive Useful Threat Artifacts: Generate Additional Questions - Data Questions (Con't)

THREAT MODCON 2023

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

- How sensitive is the data at risk? Are there regulatory implications?
- Is sensitive data being transmitted?
- What type of data is sent?
- What is the data in questions? What do we accept and what do we return on this endpoint?
- What is the impact of this attack? , e.g exposure of customer date, .. etc
- What asset is the attacker able to read/modify?
- What does the attacker gain access to?
- Does the privacy also get impacted?
- What endpoints are involved? What data is involved?

Drive Useful Threat Artifacts: Generate Additional Questions - Review (Con't)

THREAT MODCON 23

What questions do you have about this threat? An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection" - 7 ID

As was apparent from the multitude of questions, a lot of different areas of information can be covered and captured in asking and answering questions.

Grouping questions is effective in order to understand a topic more completely, while also keeping from distracting people from the larger issue at hand.

Capturing these questions means that a solution will be more well informed - even from 10 minutes of silently capturing this in a workshop!

Drive Useful Threat Artifacts: Common Action Items

THREAT MODCON 2023

How do we know a mitigation is working?

- *Create test cases, regression tests on a known environment or configuration, easily verifiable with a well-documented pointer to specific logs or errors*

How much of this threat is due to what we don't know?

- *Create focus areas with clear SMEs enabled to make decisions & educate team mates through demos and teachbacks.*

What factors affect impact and severity of this threat?

- *Document assumptions as part of the overall threat process and reassess frequently*

Break - 10 Minutes

THREAT MODCON 2023

The Threat Artifact -All Pieces Combined; An outline

THREAT MODCON 2023

Threat Description	Threat Mitigation	Action Items & Questions

If you are just getting started, please use this basic outline to guide your session for your team. As your team practices more, you'll definitely grow out of using this table!

The Threat Artifact -All Pieces Combined; Now What?

THREAT MODCON 2023

Create Tickets for the Dev Team

- Spikes
- Documentation & Runbook Creation/Updates
- Contextualized Mitigations and Features

Socialize your Threat Model Results

- Consider your Audience

Return to your Threat Model process often

- The time spent on your threat model is invested - what matters is what you do with the information created

I've got an Artifact, Now What? Create Sprint Tasks

THREAT MODCON 2023

Three-Part User Story:
As an audience, I would like a mitigation description, so that I may avoid threat description. To do this, I need to action item #1, action item #2, and spike on question #1.

Gherkin:
Feature: Mitigation Description

Scenario: threat actor performs threat description
When: audience performs threat description
And: …
Then: mitigation effect
And: additional validation of mitigation effect
…

I've got an Artifact, Now What? Socialize your results

THREAT MODCON 2023

Identify your audiences

- Management Stakeholders
- Downstream & Upstream Applications
- QA Team (if separate)
- Operations Team (if separate)
- Customers & Marketing
- Compliance & Regulations/Legal

Sage Advice From Rafiki

THREAT MODCON 2023

Sage Advice From Rafiki

THREAT MODCON 2023

Rafiki: And “what are you going” to do about it?

Simba: I’m going back … (to my threat model!)

I’ve got an Artifact, Now What? Return to your experiences

THREAT MODCON 2023

Return to Threat Models For Your Team:

- Drive onboarding new employees
- Drive and prioritize operational & security tabletop scenarios
- Inform your Demos
- Create Blog posts to retain or socialize a solution to your problem space
- Improve on the Threat Model system, documentation, and process for team velocity and flexibility

I've got an Artifact, Now What? Return to your experiences

THREAT MODCON 23

Return to Threat Models for Stakeholders and Dependencies:

- Drive new user documentation & training on your product
- Educate non-technical staff supporting your product
- Incentivize product acquisitions, contracts, and workflows
- Inform Pen Testing Engagements
- Create Blog posts to retain or socialize a solution to your problem space
- Improve on the Threat Model system, documentation, and process based on what audiences need

Review!

THREAT MODCON 2023

- *Threat Modeling is for **Everyone**.*
- *So long as you have a threat description, a potential mitigation, some action items, and questions, it doesn't matter how you got here. What matters is **what you do with that information.***
- *Engage, and re-engage, with your Threat Models to improve value beyond your team*

Reflection (5 Min)

THREAT MODCON 2023

- **Who** can I partner with, outside of my application development team, to share and socialize my application threat model?
- **What's** stopping you from socializing your application in your organization?
- **How** can I close the loop between work identified by the threat model, and work completed in a reasonable time?
- What are some things you can do to improve the fidelity of your threat description, action items, and/or mitigations?

Interested in Learning More?

THREAT MODCON 2023

Send us a message

threatmodeling@aquia.us

Download our white paper

Freeform Q&A - Prioritization

- "It doesn't matter how you got there" - what if how you got there means you missed a bunch of threats?
  - Tools can generate a lot of generic threats. Before introducing a tool to a group, consider spending additional time defining your signal-to-noise.
- How long does this "threat refinement" for hundreds of generated threats from a tool, how do you prioritize which ones to focus on?
  - There's emerging frameworks to help prioritize your threats more effectively, but there is no "one-size fits all" approach. One framework we've found success adopting is Exploit Prediction Scoring System - I recommend you check out this blog for more info.
- Does security team ask for fixes only for critical and high threats? Thoughts on how to proceed with other threats identified?
  - As with the above, it's important to work with your security team to identify if there is an existent risk framework in place to help drive priority. Using things like "probability of exploitation"/more likely to happen as a key indicator on what to prioritize

Freeform Q&A

- Some companies consider threat model data restricted data / need to know. Your suggestion implies sharing the threat artifacts widely to more teams (doc, implementation). How would you reconcile this widening the audience / access to these artifacts with the principle of least privilege?
  - Work with your company to identify potential legal risks sharing your threat model externally.
  - Not every version of a threat model needs to be accessible to everyone. Choosing to expose different information from your threat model to different relevant groups is key. Consider your audience!
  - Frequently audit how you are allocating access to this data.
- How do you communicate the effect of a suggested countermeasure on the level of risk the threat represents?
- Can you show us several of hour completed threat models and how you organize your data and drive to conclusions

Freeform Q&A - Risk

THREAT MODCON 2023

- Are you risk rating the threats in your table?
  - This specific workshop avoids touching on risk as each field has a different way to assess, accept, and allocate risk. Government organizations, organizations with PHI, and Banks (as examples) can all have wide ranging ways they handle risk. Consult with your risk team in order to encourage a common lexicon between risk, security and application security (AppSec) organizations.
- Do you have a suggestion for a standardized, repeatable way to best prioritize threat remediation?
  - See prior slide with respect to EPSS, tooling choices, and how-to break a story out of a threat description. By translating a threat and remediation to actionable work, you can prioritize against level of effort (LOE), complexity-first, tech debt, or other organizational metrics.
- How do you communicate the effect of a suggested countermeasure on the level of risk the threat represents?
  - See “How do I know my mitigation is working?” slide. A countermeasure should be testable, repeatable, non-repudiable, and documented. The effect of the lack of a measure should be documented as part of the Threat Model Notes.

Freeform Q&A - General

- Shouldn't/Couldn't the questions and answers be captured as part of the threat model, not as questions/answers, but as part of the description of the system being threat modelled?
  - Yes! So long as the questions, and answers to those questions, are tied to documentation, process, or technology improvements, the exact location of the storage of that information can be customized to your organization. However, keep the questions close to the core Threat Model artifact, so those resources can be cross referenced during activities.
- Are there any publicly available Threat Model repositories?
  - hysnsec/awesome-threat-modelling has some fantastic examples in their repos!
  - K8s Threat Model
- Can you show us several of (your) completed threat models and how you organize your data and drive to conclusions
  - Reach out personally to talk more. While we can't share client data, we do have some tips and tricks for specific lines of business, depending on the maturity of the organization.