December Community Meetup

Threat vs Mitigation: Which to Prioritize and How

December 14, 11 a.m. - 12 p.m. ET

Hosted by:

Jonathan (Jono) Sosulska
Principal Security Engineer, Aquia

About the Community Meetup

- **Our Goal**
  Exchange real-world experience, share practical knowledge, validate ideas to improve our own practice.

- **Chatham House Rule**
  Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

- **Video is optional but highly recommended :)**

📅 Agenda of Today

11:00	Welcome and intro
11:05	Presentation
11:35	Open Q&A, Discussion
11:55	Photo, Chappylosing & Announcements

About me

Jonathan (Jono) Sosulska

Principal Application Security Architect

Aquia Inc

In a prior life

- 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

Overview - Threat vs Mitigation - What to prioritize and how

- What is priority?
- Threats, Mitigations, and Applications - a complicated relationship
- Exec buy-in - Building an environment where we can be successful
- Tools vs toil

What is Priority and Triage?

“Something given or **meriting attention before competing alternatives**”
-*Priority Definition & Meaning - Merriam-Webster*

“**Prioritization is the activity that arranges items or activities in order of importance relative to each other.** In the context of medical evaluation it is the establishment of the importance or the urgency of actions that **are necessary to preserve the welfare of client or patient**.
-*https://en.wikipedia.org/wiki/Prioritization*

In medicine, **triage** (/ˈtriːɑːʒ/, /triˈɑːʒ/) is a process by which … [those with] knowledge determine the **order of priority** for providing treatment and/or **inform the rationing of limited supplies** so that they go to those who can most benefit from it.
-*https://en.wikipedia.org/wiki/Triage*

Prioritization Reminders:

1. Priority **is a relative concept** to the group of people discussing it. It’s mutable and highly subjective.

2. Assigning Priority **is a practice** that needs to balance multiple, and sometimes contradictory, objectives simultaneously

3. Prioritization conversations normally are comprised of:

- **Limited Resources** (People, Time)
- **Knowledge**
- **Who can most benefit** from the solution

How do organizations decide on priority?

Common prioritization factors in an organization

- Ability to drive value to the customer - Heart
  - Uptime of services
  - Competitive features
  - Differentiation from competitors
- Ability to protect data - Brain
  - Data Protection
  - Physical Asset Security
  - Cloud, Application, and Operational Security
- Ability to experiment quickly and securely - Body
  - Developer Productivity
  - Application Environment Stability
- Ability to meet compliance requirements - Law
  - FedRAMP/HIPAA/PCI
  - GDPR

What are my team’s priorities?

Priorities are affected by ...

The size of the organization - number of people on the project, number of applications, number of customers served

Availability of access to source code - Are you COTS dependant, or custom built software? Both have pros and cons around velocity of change and resource availability

The target of the threat model - Are you assessing a home grown greenfield application? Are you threat modeling in response to a threat in your industry? Has a new technology or mitigation arose to solve your issue?

What lense drives your organization’s priorities?

Questions to drive Application Priorities

- Is the application you’re threat modeling your “golden goose”?
- What is the limiting resource for this system?
- Is your application public or private facing?
- Does your application provide a service in a highly regulated space?
- Does your application store, transmit, or process data that affects people’s lives if it is not functional?
- Does your application suffer from legacy software issues - Application uptime availability, designed in an defunct language/technology, difficulties in scaling?
- What is your application’s logging story?

Questions to drive threat priorities

- Do we understand the technology or vector leveraged by this threat?
- Do we have any experience dealing with a threat like this?
- What is the likelihood of this happening to our core application?
- What is the cost of experiencing 1%, 10%, and 100% of a similar fallout?
- Would we see this threat exposed by our current logging?

Questions to drive mitigation priorities

- Do we understand the technology or processes that protect us from this threat?
- How much of this mitigation is due to what we don’t know?
- Does implementing this mitigation increase our risk in other areas?
- What would be a limiting resource that could impact our mitigation effectiveness?
- What logging are we leveraging to show this mitigation was activated, and what details do we capture?

How do you protect priority in an organization as part of threat modeling?

Protect Priority with Executive Buy-In

- Executives need to protect the execution of priorities from changes in scope.
- Executives who purchase a product or create a contract with a vendor have a responsibility to help build a relationship that is conducive to the developer experience of their team.
- Executives should participate on threat models of previous incidents in the company, and contribute to understanding how doing a threat model could have helped.
- Executives should understand the systems and data they maintain, and be able to leverage technical data to drive decisions

Tools vs Toil

I have a SAST/DAST scans of my application, I don’t need to threat model!

I’m compliant, I don’t need tools that send me hundreds of vulnerabilities!

My company can’t afford to threat model with tooling, and we have to rush to deliver value!

None of the above sentiments are true! Tools **supplement** human ingenuity for a complete picture of your threat landscape!

How to make your tools less toilsome

- Spend time tuning your tools after installing them, and plan for a longer tuning phase as part of implementation.
- Correlate across multiple data sources, rather than a single tool.
- Decide if the point of a threat modeling exercise is to validate tool data, or if tool data is informing an exercise machines don’t have the capability to do.

In the search of tools to minimize toil, don’t let tools become toil.

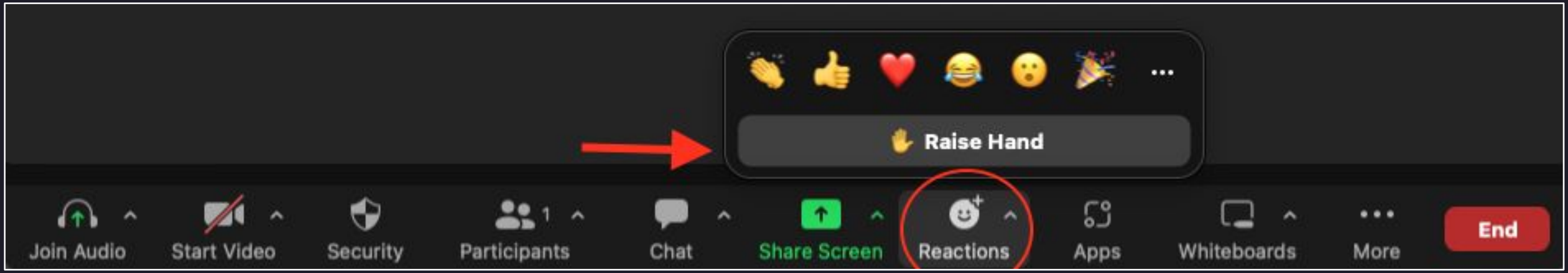
Recap

- What are my team's priorities relative to the rest of the organization?
- Prioritization is comprised of:
  - Limited Resources (People, Time)
  - Knowledge
  - Who can most benefit from the solution
- Priority in an organization *is driven* by the need to provide value, to protect data, to meet regulation, and to experiment quickly and securely.
- Priority in threat modeling *targets* an application, a threat, or a mitigation, and each has a different modality around being addressed.
- Turning priority into reality *is impacted* by the size of the organization, the availability of access to resources, and the target of what's been prioritized.
- Priority *is protected* by executive buy-in, data, and tooling informed decisions.

Discussion

- **Question 1:** How does the maturity and size of an organization impact the recommendations we discussed today?
- **Question 2:** What does a security champion's responsibility look like as part of prioritization?
- **Question 3:** How do _you_ prioritize within your organization, and how large is the organization you're working within?

Use "✋ Raise Hand" feature to let the hosts know you have something to share.



Happy
Birthday

Photo Time!

Next Meetup

Topic: High Assurance Threat Modelling

Date: January 19, 2024

Register: threatmodelingconnect.com/events