OCT 29
Washington, D.C

THREAT MODCON 2023

THREAT MODELING IS FOR EVERYONE

Speakers//

Brenna Leath

Software Security Principal
Navy Federal Credit Union

Lisa Cook

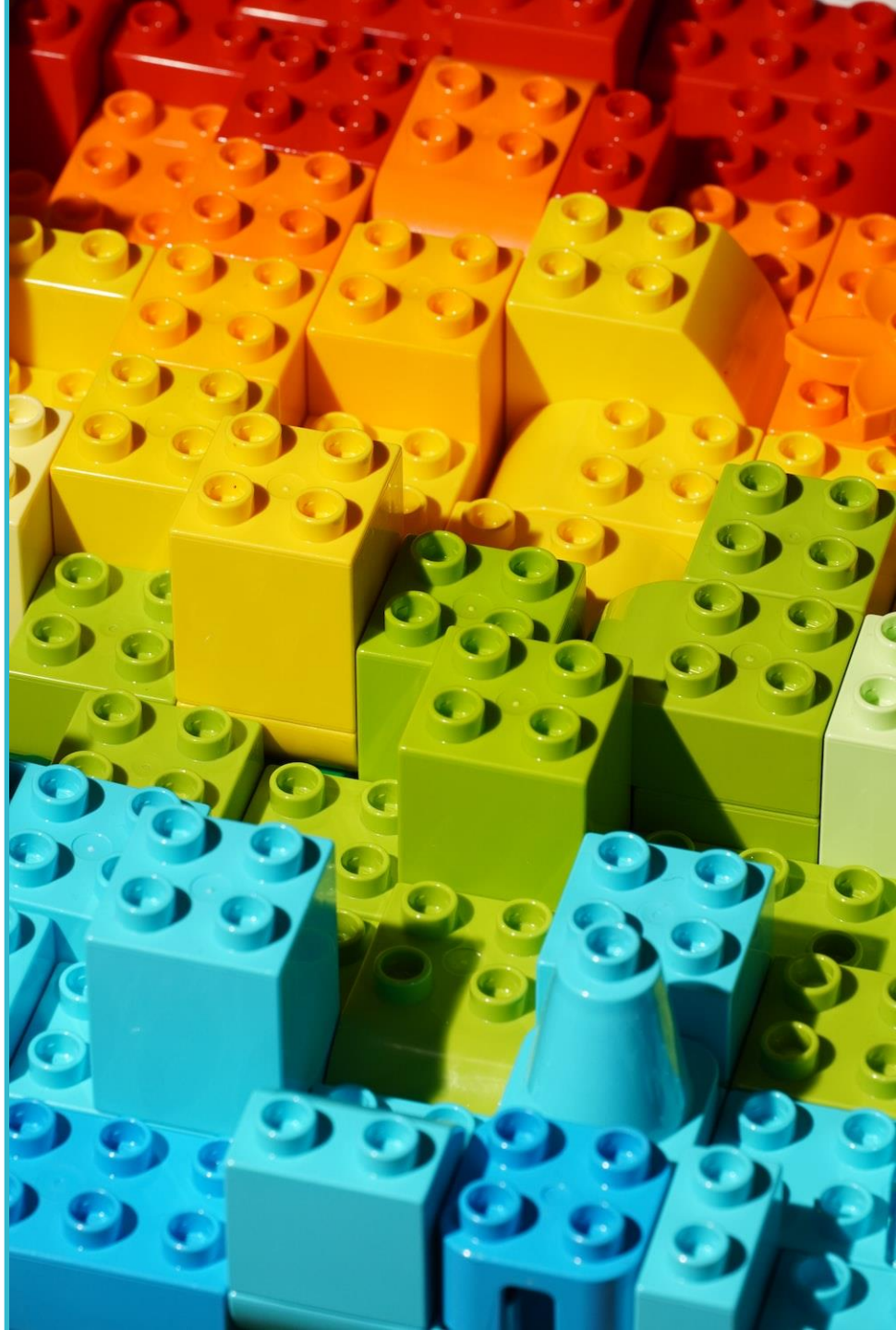
Product Security Lead
SAS

Hosted by
THREAT MODELING CONNECT

THREAT MODCON 2023

Threat Modeling Program Milestones

A Journey to Scale



AGENDA

- Introductions
- The Journey Begins
- An Identity Crisis
- Our Journey to Scale
  - 0.0 The Checklist
  - 1.0 The Hero
  - 2.0 The Heroes
  - 3.0 Justice League: By Size
  - 4.0 Justice League: By Skill
  - 5.0 Justice League: By Risk
  - 6.0 Self-Defense
- Lessons Learned
- Q&A

INTRODUCTIONS

THREAT MODCON 2023

LISA COOK

CSSLP, PMP, CC, CAMS

BRENNA LEATH

CISSP, CSSLP, CISA, PMP, CSM

THE JOURNEY BEGINS

A Disturbance in the Force

AN IDENTITY CRISIS

THREAT MODCON 2023

COMPLIANCE

SECURITY

…NO MORE BAD COP

Compliant but Insecure

- “The Destination”
- Control focused
- Standards focused
- “Check the Box”
- Audit traceability

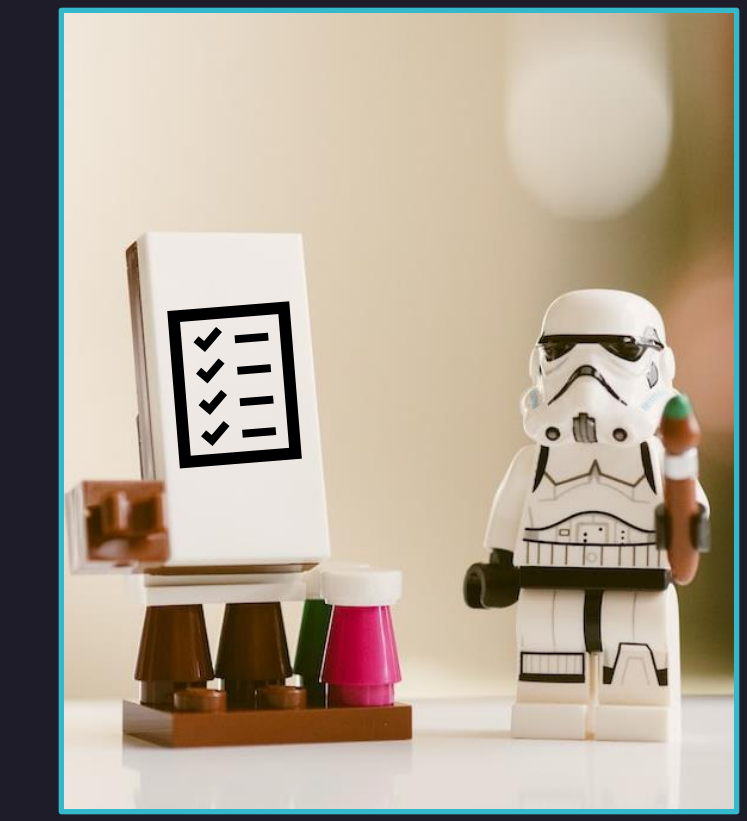
Secure but Non-Compliant

- “The Journey”
- Practice focused
- Results focused
- Development Partner
- Deep understanding of design weaknesses

OUR JOURNEY TO SCALE

The Checklist, The Hero, and The Heroes

THREAT MODCON 2023



OUR JOURNEY TO SCALE

Introducing... The Justice League

3

THREAT MODCON 2023

Who Participates – and Who Drives

Product Mgt

R&D Mgt

Dev Mgt & Leads

Perspective of use and abuse, misuse cases; Understand configuration mgt requirements, operational and maintenance expectations

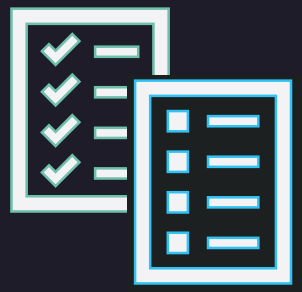
Threat landscape, attack surface knowledge; SCA & SAST

Active use of DAST and IAST tools; Architecture and design choices, To context coding and integration evaluation; security SMEs

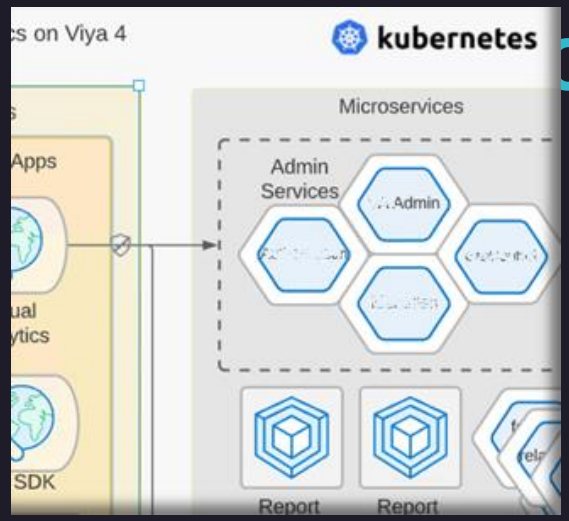
Test Leads

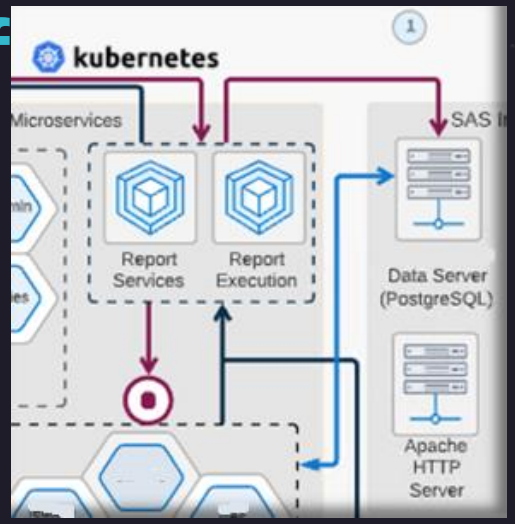
Build & Deploy

Security Specialists



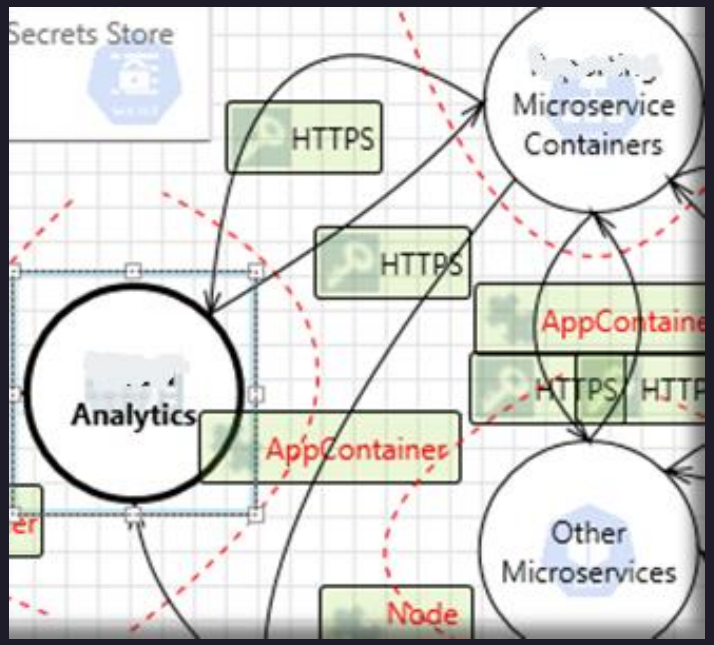
Security Reqs, Use & Abuse Cases





Ports & Protocols
IAST/DAST
PenTest and CRPs

- Product Overview; Fxl, non-fxl, and Security Requirements
- Security Architecture Diagram
- Data Flow & Persistence
- Technical Analysis
- Threat Model
- Risks & Recommendations



Identified Risk	Risk Resolution	Tracking Ticket	Target Cadence
Information Disclosure – API response contains more data than context warrants.	Mitigate via API filtering.	JIRA-43245	2022.09
Uploaded user file may contain malicious code	Mitigate: Verify file type by content; Segregate uploads to quarantine.	NCC-1701	2022.12

THREAT MODCON 2023

AIM: What do we want to accomplish?

Product Decomposition, Inherent Security & Compliance Reqs

VISUALIZE: What are we building?

Architecture and Sequence Diagrams, Data Flow & Persistence

IDENTIFY: What can go wrong?

Threat model, security scans, pen-test results

MITIGATE: What are we going to do about it?

Risk Identification & classification, recommended treatment

VALIDATE: Did we do a good job?

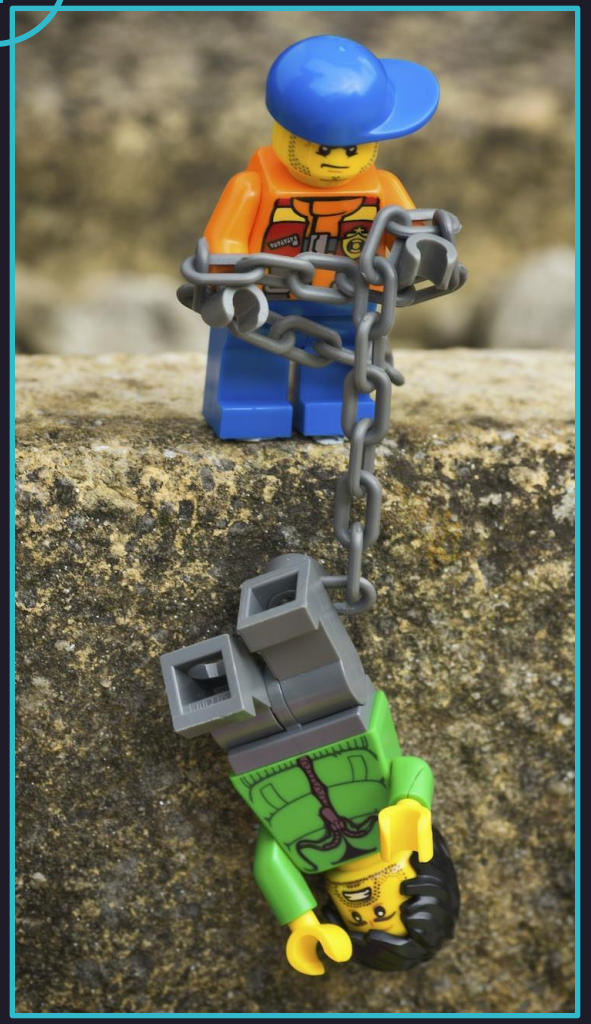
Track issues to resolution, update reviews and findings

THE JUSTICE LEAGUE

THREAT MODCON 2023

3 By Size

4 By Skill



OUR JOURNEY TO SCALE

5 By Risk

6 Self Defense (Future State)

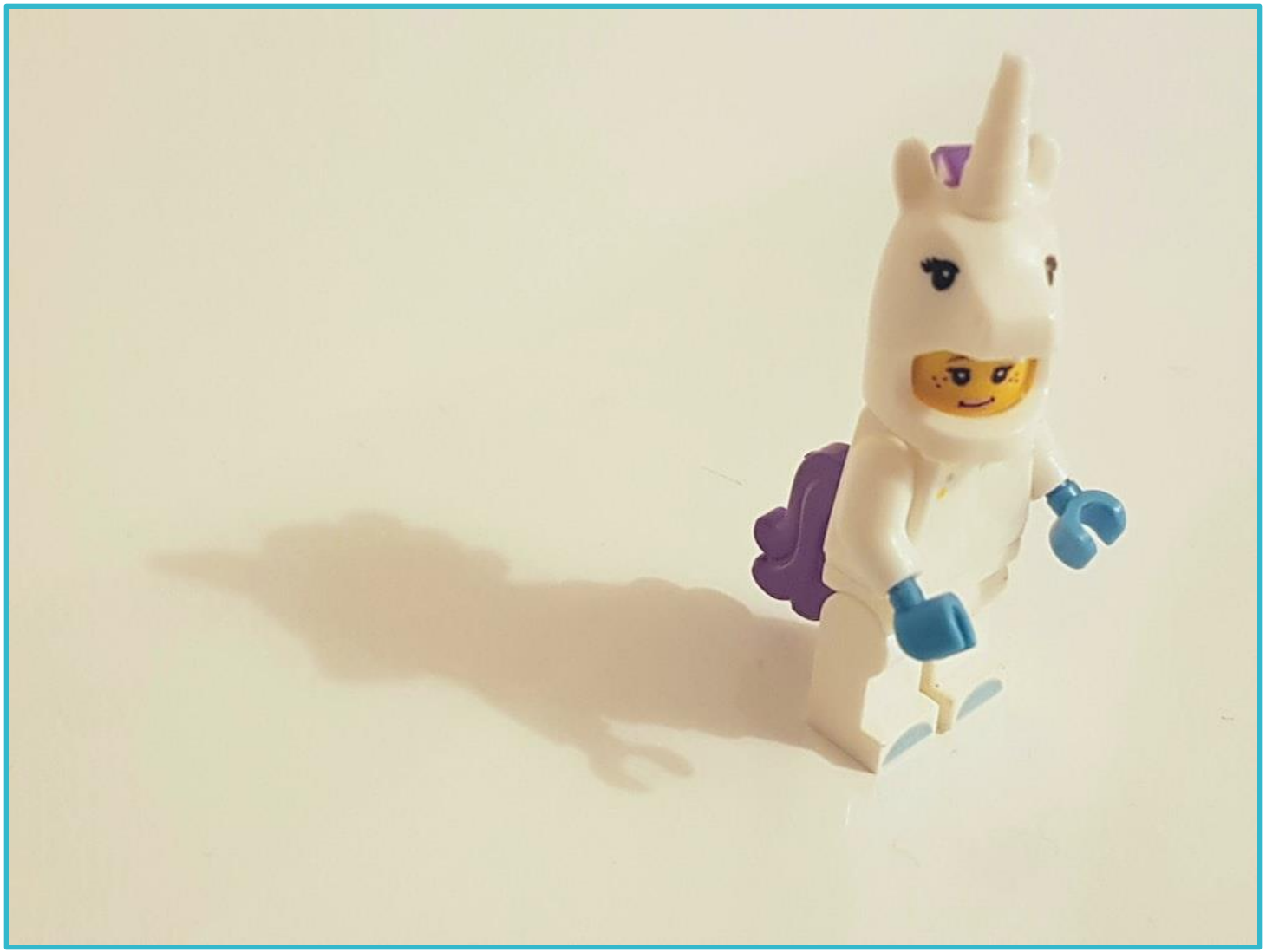
Threat Modeling Journey to Scale

From Hero to League of Champions

Lessons Learned

The Journey Continues

Q&A



https://www.linkedin.com/in/brennaleath/

https://www.linkedin.com/in/lisaweba11y

Creative Commons Images courtesy of Unsplash

- https://unsplash.com/license


THREAT MODELING
CONNECT
THREAT MODCON 2023
THREAT MODELING IS FOR EVERYONE