

FAIR & Cyber Intelligence at Fannie Mae

Samantha Chamberlin

Cyber Intelligence Analyst

Fannie Mae

Samantha_Chamberlin@fanniemae.com

Table of contents

1. Our Journey
2. Parallel Lifecycles
3. Reciprocal Relationship between FAIR and Intel
4. Putting it in Practice

Fannie Mae's Journey



2020

Maturing FAIR Program

Spreading FAIR as way of thinking across the organization.

2019

Maturing FAIR Program

Establishing Risk as a Service

2018

Relaunched FAIR program

Coupled Cyber Risk and Cyber Intelligence

2017

Risk Management with FAIR

Leveraged RiskLens platform with goal of assisting project prioritization.

2016

Risk Management without FAIR

Primarily Compliance based risk responses

Why It Works



Comfortable working in uncertainties



Serving as an advisory function

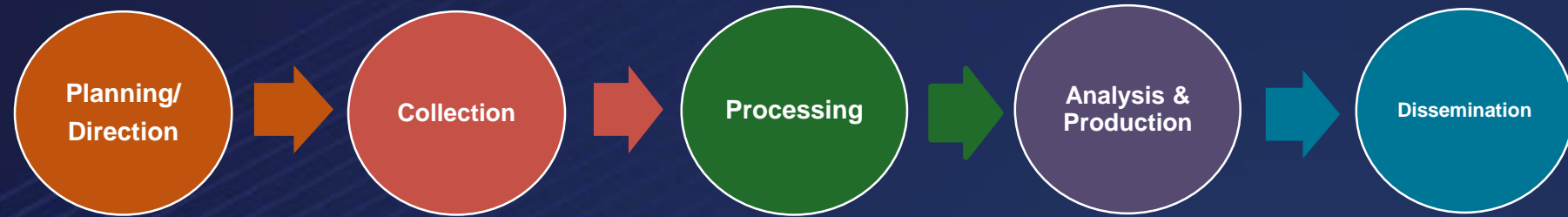


Similarities between FAIR and Intel Lifecycles

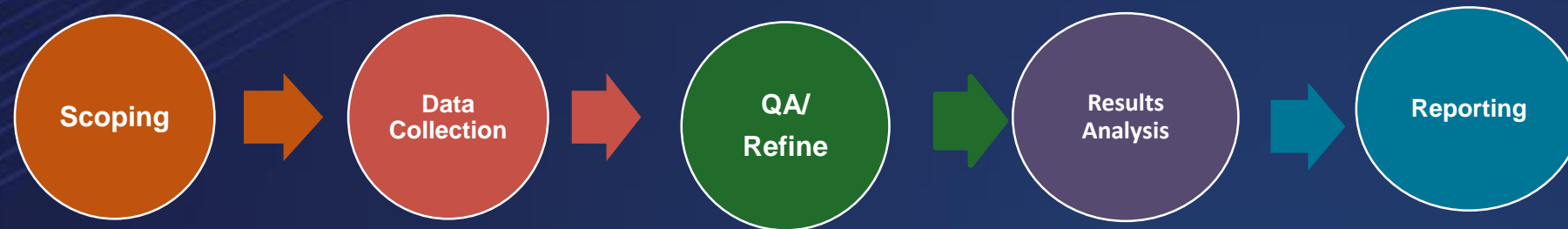
Inserting FAIR into an already credible team entrusted with providing recommendations to leadership proved successful.

Parallel Lifecycles

Intel Lifecycle



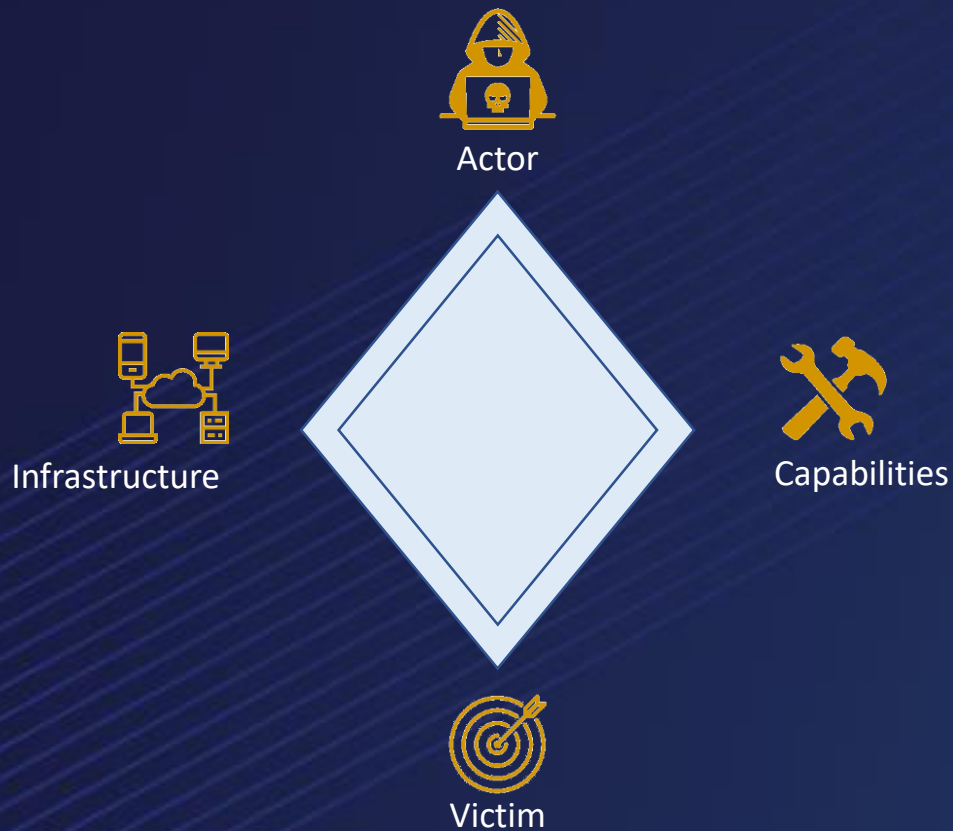
FAIR Scenario Lifecycle



FAIR & Intel: A Reciprocal Relationship



Cyber Intelligence



Adversary-based collection helps answer:

1. What entities/assets are being targeted?
2. What are their motivations?
3. How capable are the threat actors?
4. What tools, tactics, and procedures (TTPs) are they using to conduct attacks?

Factor Analysis of Information Risk



FAIR assessments help answer:

1. How probable is it that a loss event will occur over a given timeframe?
2. Where do I expect loss to materialize in the company?
3. How much monetary loss is expected to be incurred for a given scenario?
4. How strong are our controls against a given threat actor?

Reciprocal Relationship

INTEL

- Follows trends in activity
- Enables understanding of various attack vectors
- Adds indicators and observables from reporting to detection and blocking controls



FAIR

- ✓ Create FAIR scenario's grounded in real-world events
- ✓ Better communication and engagement with technical SME's
- ✓ Informs TCAP, RS and/or LM

Reciprocal Relationship

FAIR

- Identify ceiling risks based on quantified Loss Magnitude
- Form trusted relationships across the organization
- Identify gaps in security posture
- Quantify traditional intel monitoring



INTEL

- ✓ Inform PIR collection
- ✓ Strengthens defensible recommendations based on FNMA sources/breaks silos
- ✓ Examines ways to strengthen security against threats
- ✓ Makes intel more consumable to leadership

Putting it in Practice



Put in Practice – Example Scenario



EXTERNAL ACTOR deploys RANSOMWARE on WORKSTATIONS



Availability

- Caused outage on workstations
- Became ceiling risk scenario
- Added to daily collection cycles

[Insert Intel]

- Over last year regulations on data privacy tightened (GDPR, CCPA)
- Shift in attack method from 7 day ransom increase to 7 day data released publicly

Confidentiality

- Caused outage on workstations + exposed data publicly

Strengthening Trusted Partnerships



Breaking silos and spreading the methodology can bridge the gap between the business and information security.

Questions?

Sources

- <https://www.flaticon.com/>
- <https://soccerdrawing.com/five-top-risks-of-soccer-goal-clipart-soccer-goal-clipart/9-soccer-goal-free-clipart-9-soccer-goal-clipart/>
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.pngitem.com%2Fmiddle%2FhbRjwTi_4-hands-putting-together-puzzle-pieces-hands-putting%2F&psig=AOvVaw03zptWMh5kdQODOXW5ziip&ust=1580930539069000&source=images&cd=vfe&ved=2ahUKEwj4heuqz7jnAhUEA98KHcr4BnAQr4kDegQIARBe
- https://www.google.com/imgres?imgurl=http%3A%2F%2Fimages.clipartpanda.com%2Fexchange-clipart-parcel-exchange-2409261.jpg&imgrefurl=http%3A%2F%2Fwww.clipartpanda.com%2Fcategories%2Fexchange-clip-art&tbnid=V2XCyOO4bEob9M&vet=12ahUKEwie7e_Uz7jnAhVZZ98KHfzgCo4QMyglegUIARCCAg..i&docid=x-hHL4VmVyFTgM&w=1300&h=1220&q=exchange%20clip%20art&safe=active&ved=2ahUKEwie7e_Uz7jnAhVZZ98KHfzgCo4QMyglegUIARCCAg