PUBLIC

MWR InfoSecurity

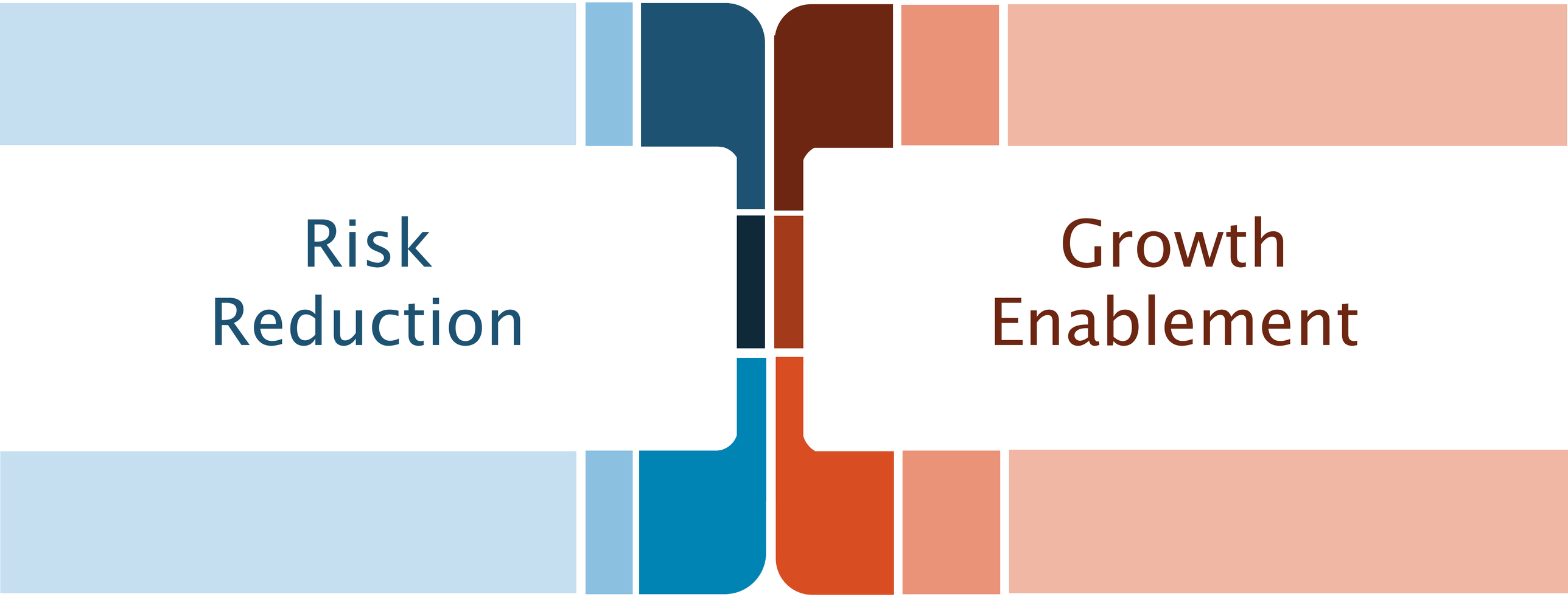
# VOYAGES

## of the (Security-Driven) Enterprise

BASC 2018
October 27th, 2018

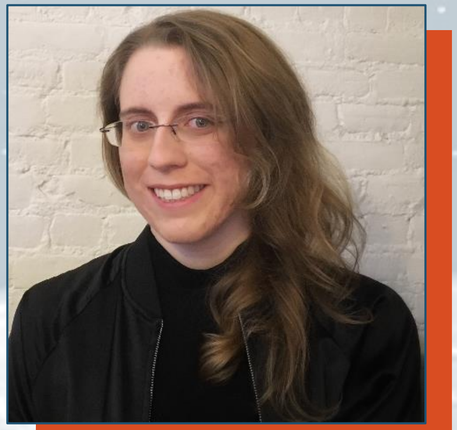
MWR InfoSecurity

# What is Security's Primary Role?



MWR InfoSecurity

# Speaker Bio



Katie Knowles (@_sigil)
*Security Consultant,*
*MWR NY*

- **Currently:** Pentester
- **Previously:** Blue Team of many hats for a large aerospace company
- **Passion:** Making my job (attacker) more difficult by helping defense improve as effectively as possible

Certifications: OSCP, GPEN, CREST CRT
BS Electrical Engineering, RIT

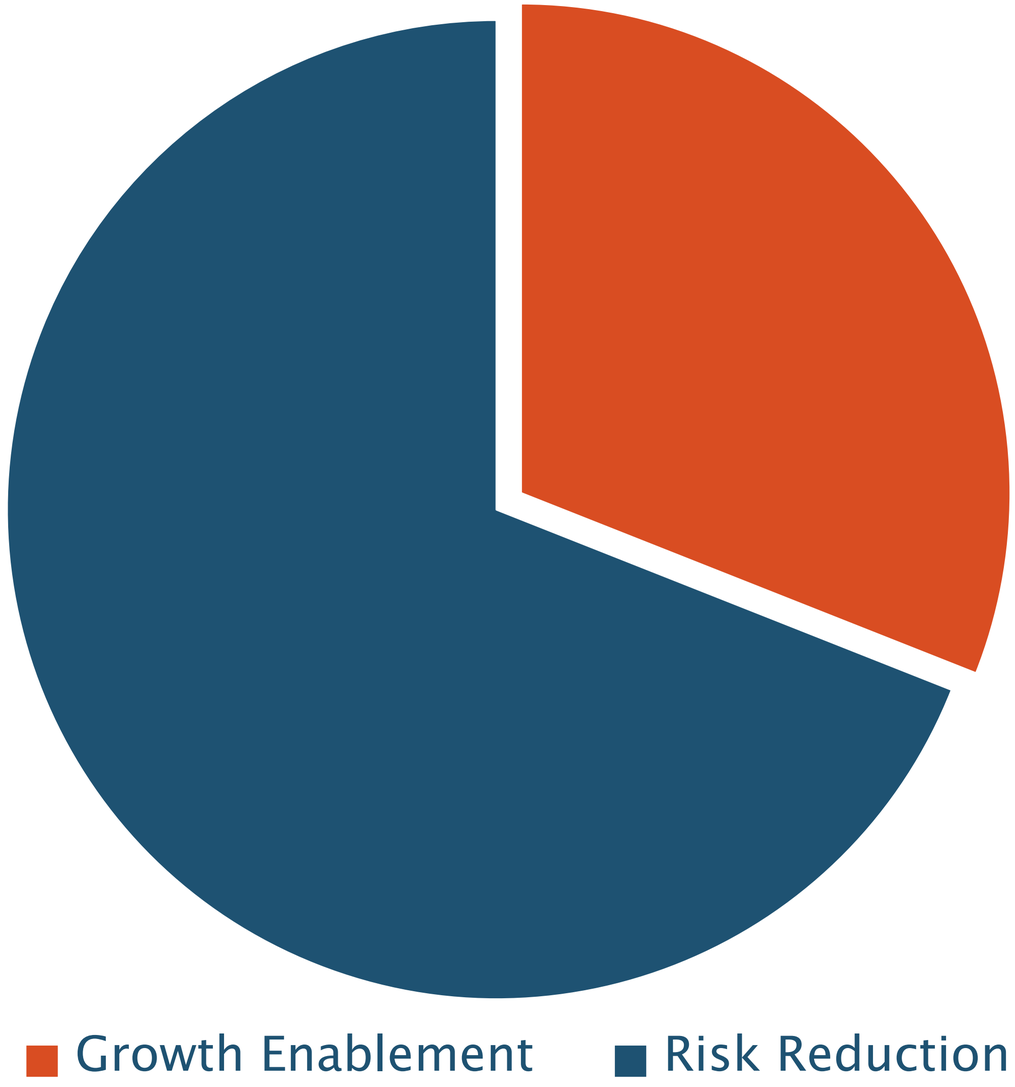
MWR INFOSECURITY

# Agenda

+ Why should security enable the business?
+ 3 Roles
  1. Translator:
     Learning New Languages
  2. Negotiator:
     Mapping the Impact
  3. Motivator:
     Enabling New Directions &
     Dealing with Obstacles
+ Takeaways

# Diverging Opinions

- Recent Cisco survey:
  "What is security's primary role?"
- 1014 senior & executive responses
- Growth Enablement: 31%
  Risk Reduction: 69%
- Additionally, 39% percent had **halted a mission-critical initiative** due to cybersecurity concerns.




https://connectedfutures.cisco.com/report/cybersecurity-as-a-growth-advantage/

# 8%

## Shared Responsibilities

- Survey of over 100 Financial CISOs:
  - Only 8% reported to the CEO
  - 39% reported to the CIO

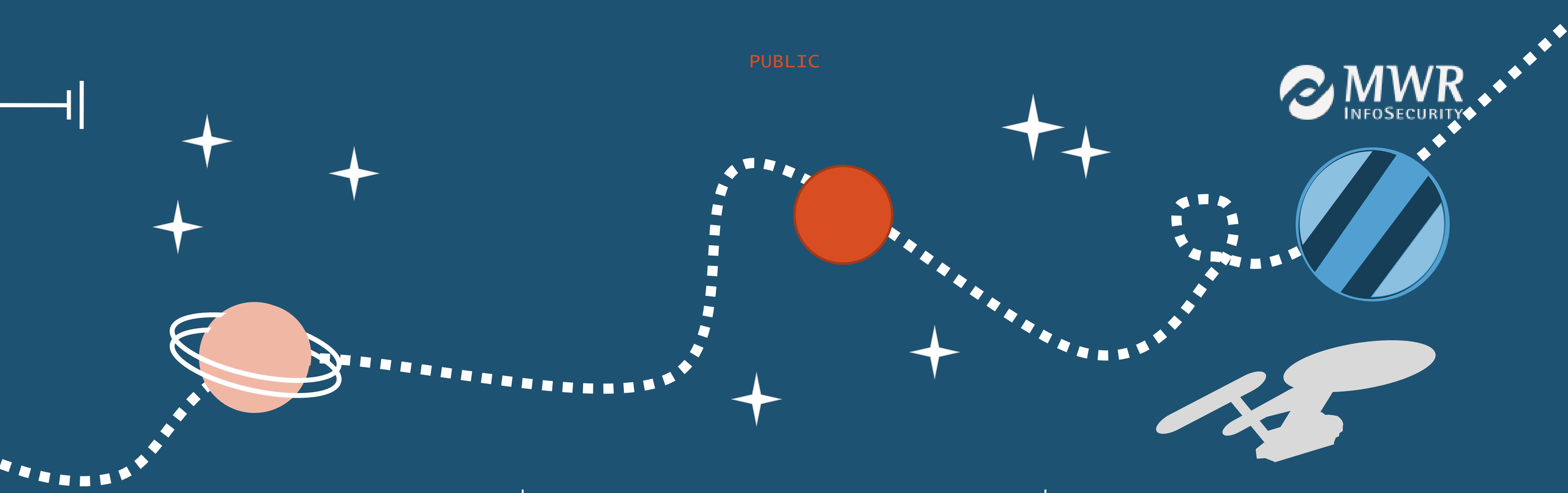
- "Offensive problems are largely technical, defensive problems are largely political." – Halvar Flake

https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

MWR INFOSECURITY

# Rethinking Perspectives

| Outlooks | | Reframing |
|---|---|---|
| Security is overloaded with responsibilities | → | Prevention & Planning > Crisis & Firefighting |
| Security's role is to represent security to the business | → | Security's role is to represent security ~~to~~ **for** the business |
| Compliance will ensure we stay secure | → | Compliance doesn't always mean commitment |



MWR InfoSecurity

## 1. Translator

Identify motivations, risks, and expectations of teams that security's work has an impact on.

## 2. Negotiator

Map security impact against business goals and objectives of impacted teams.

## 3. Motivator

Define projects of maximum benefit & search for additional support based on mappings.

# BUSINESS AREAS

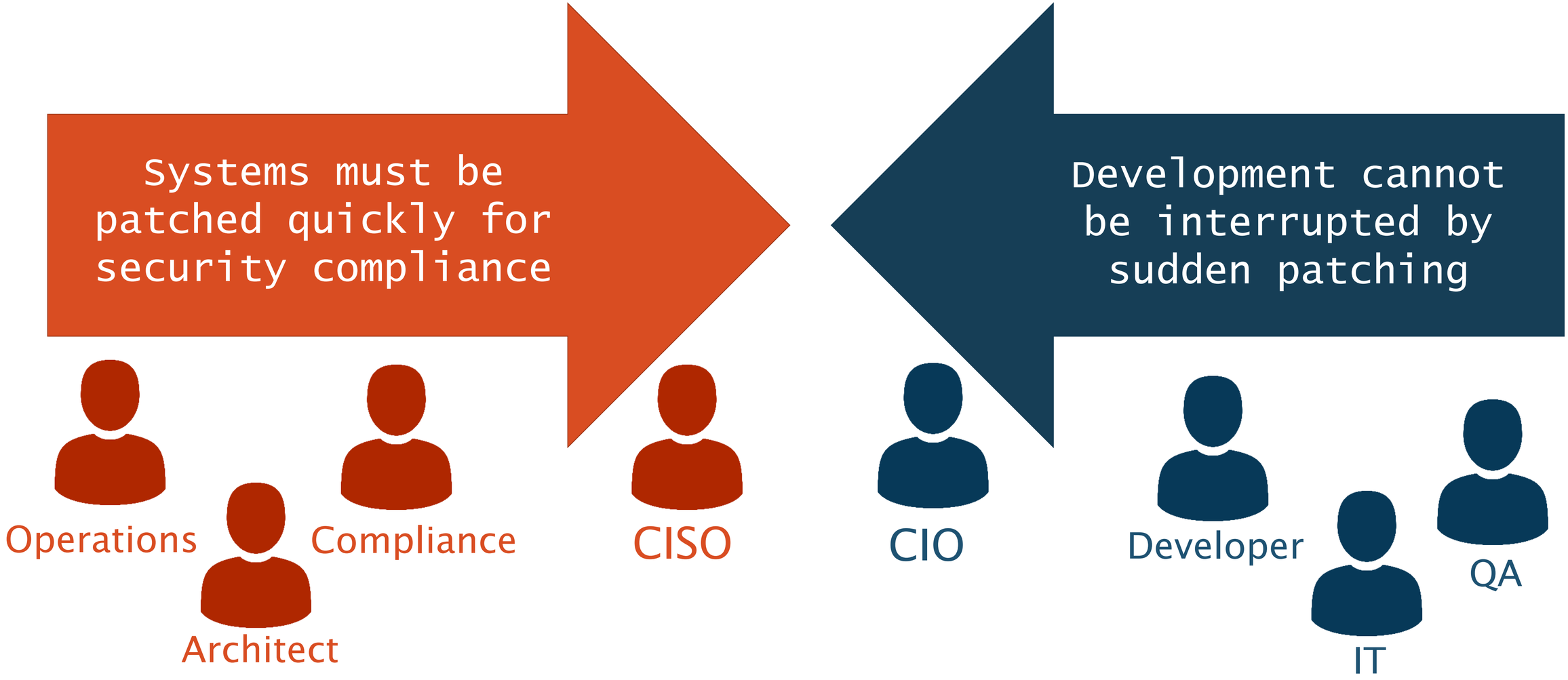
# COLLABORATIONS

Explore strange new ~~worlds~~.
Seek out new life and new ~~civilizations~~.
And boldly go where no ~~man~~ has gone before.

# TEAM

MWR InfoSecurity

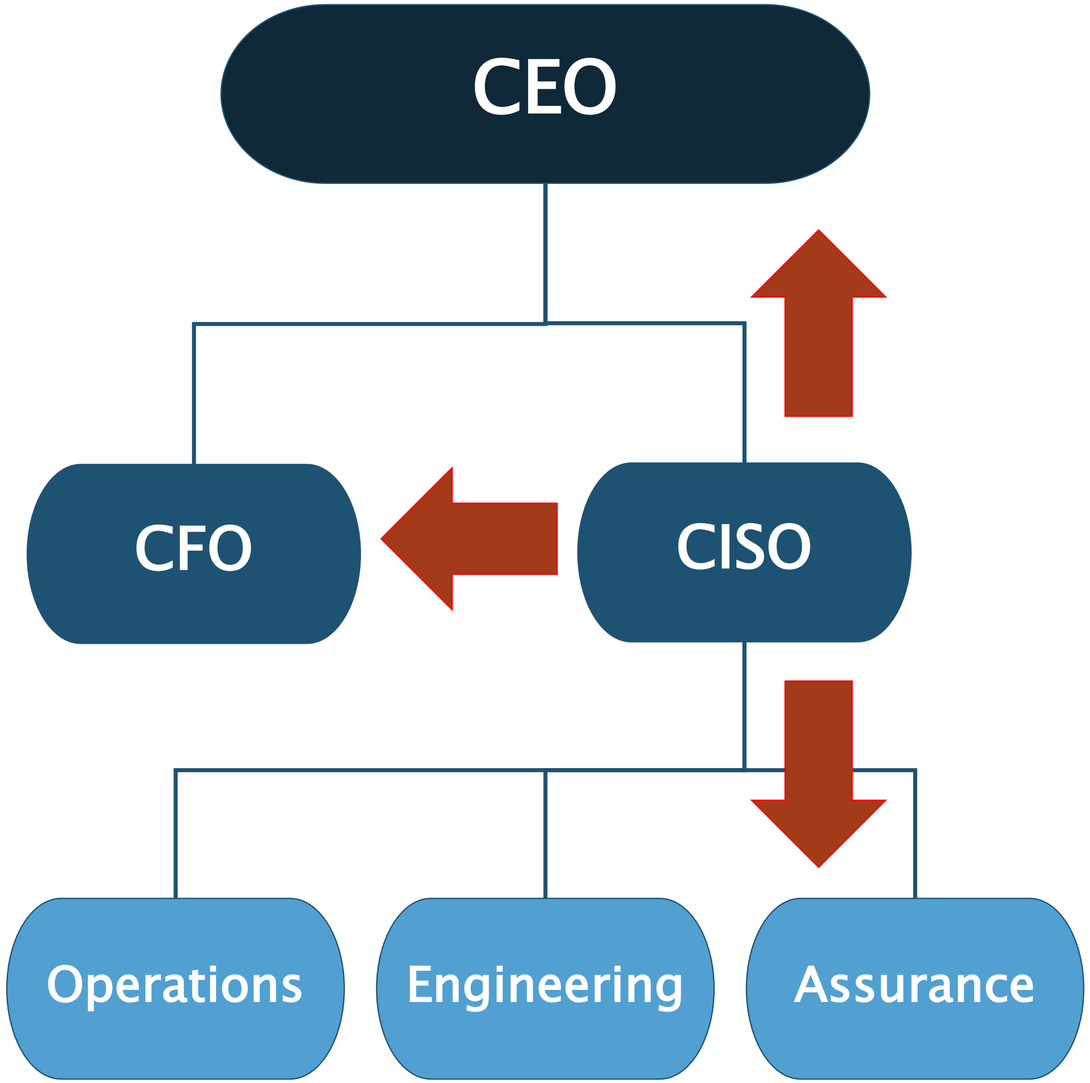
1. Translator
2. Negotiator
3. Motivator


Systems must be patched quickly for security compliance
Development cannot be interrupted by sudden patching
Operations
Compliance
CISO
CIO
Developer
QA
Architect
IT

MWR InfoSecurity

| | Information Security | Engineering Team |
|---|---|---|
| Motive | “We can’t let these systems get breached” | “We can’t let the app go down from patching” |
| Concerns | Breach:<br>• Loss of system availability<br>• Possible ongoing compromise<br>• Work hours devoted to remediation | Patching:<br>• Loss of system availability<br>• Ongoing issues with new software<br>• Work hours devoted to testing |
| Sentiment | “We can’t let the business be impacted by this” | “We can’t let the business be impacted by this” |

# Tool: Translating Perceptions




## Answer 3 Questions:

1. What output defines the success of this person's role?
2. Related to security, what would the "worst day ever" look like from this person's perspective?
3. What are the 2-3 most important things security can do/does for this person?

## Information Sources:

Emails, tickets, conversations, interactions with peers

MWR InfoSecurity

1. Translator
2. **Negotiator**
3. Motivator

# OWASP Risk Rating *(Example)*

| Likelihood and Impact Levels | |
|---|---|
| 0 to <3 | LOW |
| 3 to <6 | MEDIUM |
| 6 to 9 | HIGH |

| Overall Risk Severity | | | | |
|---|---|---|---|---|
| Impact | HIGH | Medium | High | Critical |
| | MEDIUM | Low | Medium | High |
| | LOW | Note | Low | Medium |
| | | LOW | MEDIUM | HIGH |
| | Likelihood | | | |

| Threat agent factors | | | | | Vulnerability factors | | | |
|---|---|---|---|---|---|---|---|---|
| Skill level | Motive | Opportunity | Size | | Ease of discovery | Ease of exploit | Awareness | Intrusion detection |
| 5 | 2 | 7 | 1 | | 3 | 6 | 9 | 2 |
| Overall likelihood=4.375 (MEDIUM) | | | | | | | | |

General Definitions

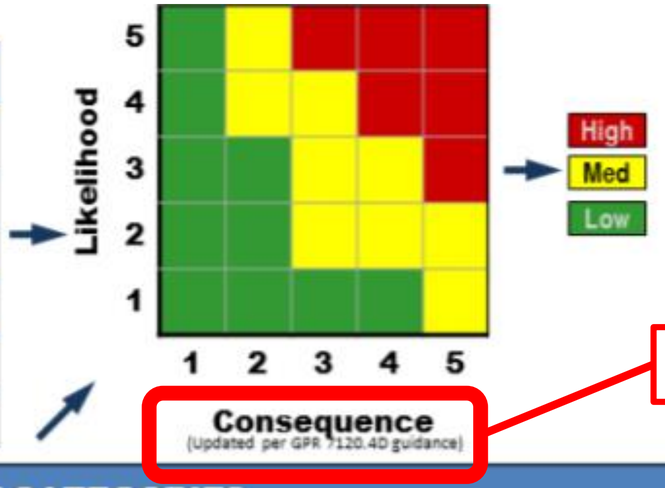
| Technical Impact | | | | | Business Impact | | | |
|---|---|---|---|---|---|---|---|---|
| Loss of confidentiality | Loss of integrity | Loss of availability | Loss of accountability | | Financial damage | Reputation damage | Non-compliance | Privacy violation |
| 9 | 7 | 5 | 8 | | 1 | 2 | 1 | 5 |
| Overall technical impact=7.25 (HIGH) | | | | | Overall business impact=2.25 (LOW) | | | |

Unweighted Scoring

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

# Ex. NOAA, NASA

| LIKELIHOOD CATEGORIES | | | |
|---|---|---|---|
| **Rank** | **Technical** | **Cost/Schedule** | **Safety** |
| **5 – Very High** | $P_T > 50\%$ | $P_{CS} > 75\%$ | $P_S > 10^{-1}$ |
| **4 – High** | $25\% < P_T \leq 50\%$ | $50\% < P_{CS} \leq 75\%$ | $10^{-2} < P_S \leq 10^{-1}$ |
| **3 – Moderate** | $15\% < P_T \leq 25\%$ | $25\% < P_{CS} \leq 50\%$ | $10^{-3} < P_S \leq 10^{-2}$ |
| **2 – Low** | $2\% < P_T \leq 15\%$ | $10\% < P_{CS} \leq 25\%$ | $10^{-5} < P_S \leq 10^{-3}$ |
| **1 – Very Low** | $0.1\% < P_T \leq 2\%$ | $2\% < P_{CS} \leq 10\%$ | $10^{-8} < P_S \leq 10^{-5}$ |




Impact

| CONSEQUENCE CATEGORIES | | | | | |
|---|---|---|---|---|---|
| **Rank** | **1 – Very Low** | **2 - Low** | **3 - Moderate** | **4 - High** | **5 – Very High** |
| **Technical** | No impact to meeting KPPs and/or other mission objectives.<br>No technology development or modifications required. | Minor impact to meeting KPPs and/or other mission objectives.<br>Minor impact to full mission success criteria.<br>No new technology development required.<br>May require minor modifications to existing technologies. | Moderate impact to meeting KPPs and/or other mission objectives.<br>Minimum mission success criteria is achievable with margin.<br>May require some new technology development. | Significant impact to meeting KPPs and/or other mission objectives.<br>Minimum mission success criteria is achievable.<br>Moderate new technology development is required. | Key Performance Parameter (KPP) and/or other mission objectives cannot be met.<br>Minimum mission success criteria is not achievable.<br>Major new technology development is required |
| **Cost** | < 2% increase over allocated Program or Segment/Sub segment funding, and can be handled within available reserves. | ≥2% but ≤ 5% increase over allocated Program, Project or Segment funding, and can be handled within available reserves. | >5% but ≤ 7% increase over allocated Program, Project or Segment level funding, and can be handled within available reserves. | >7% ≤10% increase over allocated Program, Project or Segment level funding, and/or threatens to reduce reserves below prudent levels. | >10% increase over allocated Program, Project or Segment funding and/or exceeds available reserves. |
| **Schedule** | inimal or no slip in non-critical ath elements.<br>o impact to schedule reserve | Any slip in non-critical path elements of ≥1month ≤2 month | Any slip in non-critical path elements of >2 months ≤3 months, accommodated within reserves | Moderate impact to critical path or any slip in non-critical path elements of >3 months ≤4 months or major milestones that threatens to reduce reserves below prudent levels. | Major slip in the critical path or any element on the critical path that exceeds reserves<br>Major slip that affects the award of the follow-on phase<br>Major slip that affects the launch date or delays scheduling to other segments |
| **Safety** | egligible or no safety impact | Could cause the need for only minor first aid treatment | May cause minor injury or occupational illness or minor property damage | May cause severe injury or occupational illness or major property damage | May cause death or permanently disabling injury or destruction of property |

Specific Definitions

https://www.goes-r.gov/syseng/docs/Risk_Mgmt_Plan_v2-0.pdf

# ++ Tool: Negotiating Priorities

## Likelihood:

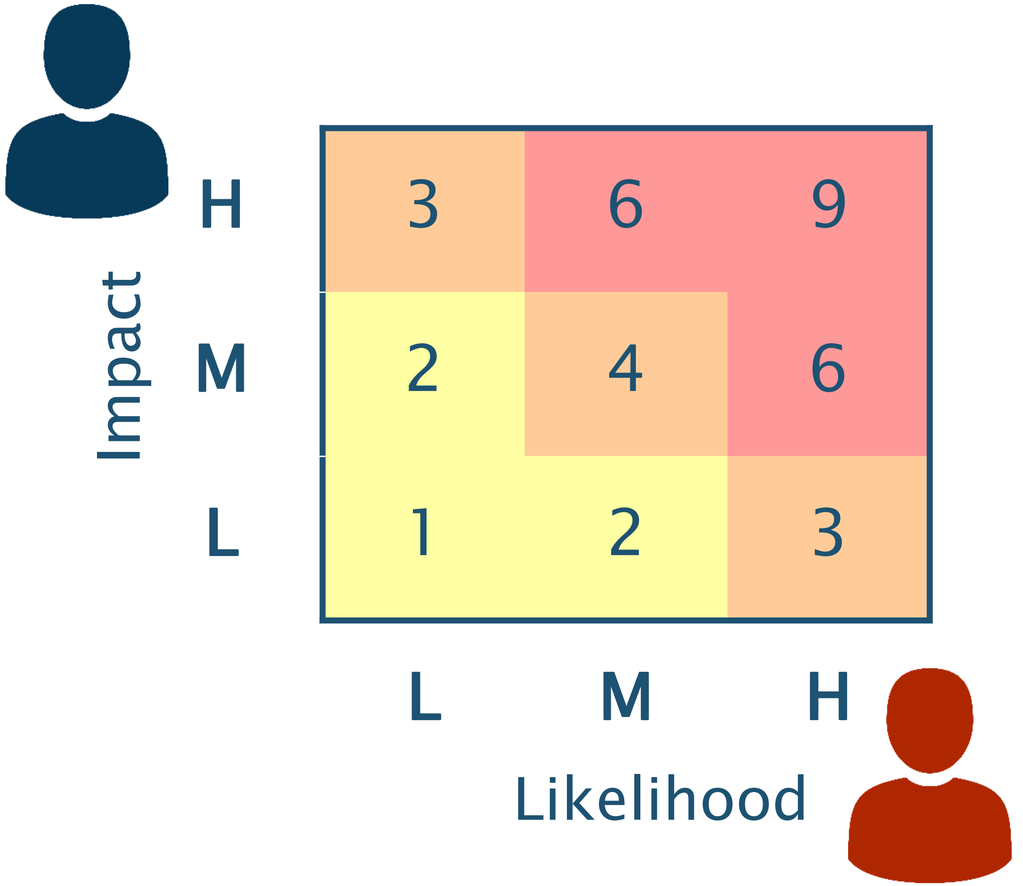
Define security likelihood

*(Ease of exploit, ease of detection, etc.)*

## Impact:

Define…

1. How would ~~CIA~~ **success** in this area of the business be impacted?
2. Would this delay the “critical path”?
3. Would this result in a worst-case scenario for this area of the business?



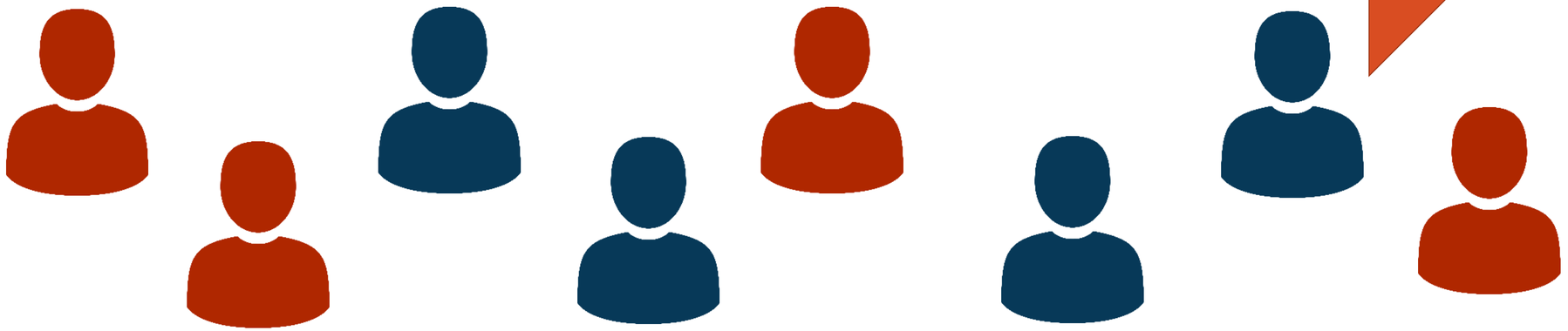
MWR InfoSecurity

1. Translator
2. Negotiator
3. Motivator

# Group Objective: Improve Patching Process

Development cannot be interrupted by sudden patching

Systems must be patched quickly for security compliance



MWR InfoSecurity

++

# Enabling Growth

## 1. Situations of Mutual Benefit

+ Build security in where objectives overlap
+ Reach new objectives with support from additional groups

Ex. SDLC

+ Security:
  Security reviews during development
+ Development:
  Quick testing & deployment of new releases

## 2. Projects Facing Pushback

+ Look for strength in numbers & common enemies
+ Make security easy, then work towards mandatory

Ex. Mandatory Logging

+ Security:
  Detection of suspicious behavior, response to security incidents
+ IT:
  Troubleshooting info. for uncommon system errors

MWR InfoSecurity

# The Complete Voyage

## 1. Translating Perceptions

Define areas of success, concern, & most important things security can do for this area of business

## 2. Defining Priorities

1. Likelihood: Security likelihood
2. Impact: Business impact for this area of the business

## 3. Enabling Growth

Identify situations of:

1. Mutual Benefit
2. Projects Facing Pushback


# Closing Thoughts

1. Use conflict as an opportunity to define resilient, meaningful goals
2. Turn “adversaries” into allies to unite the business against common issues
3. Mandating change wins at first, but influencing change will get us further in the long run

# Questions?

Or reach out at:
@_sigil
Katie.Knowles@mwrinfosecurity.com

MWR INFOSECURITY

## 3 Questions: Translating Perceptions

1. What output defines the success of this person's role?
2. Related to security, what would the "worst day ever" look like from this person's perspective?
3. What are the 2-3 most important things security can do/does for this person?

I

## Identify Situations: Enabling Growth

1. Maximum Mutual Benefit
   - Build security in where objectives overlap
2. Projects Facing Pushback
   - Look for strength in numbers, common foes wherever possible
   - Make security easy, then work towards mandatory

III

II

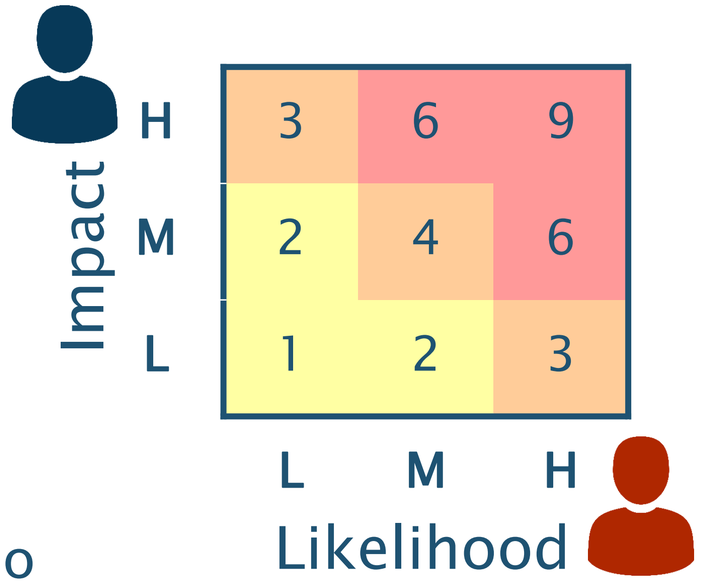
## Likelihood & Impact: Defining Priorities

Likelihood: Define security likelihood

*(Ease of exploit, ease of detection, etc.)*

Impact: Define…

1. How would success in this area of the business be impacted?
2. Would this delay the critical path?
3. Would this result in a worst-case scenario for this area of the business?

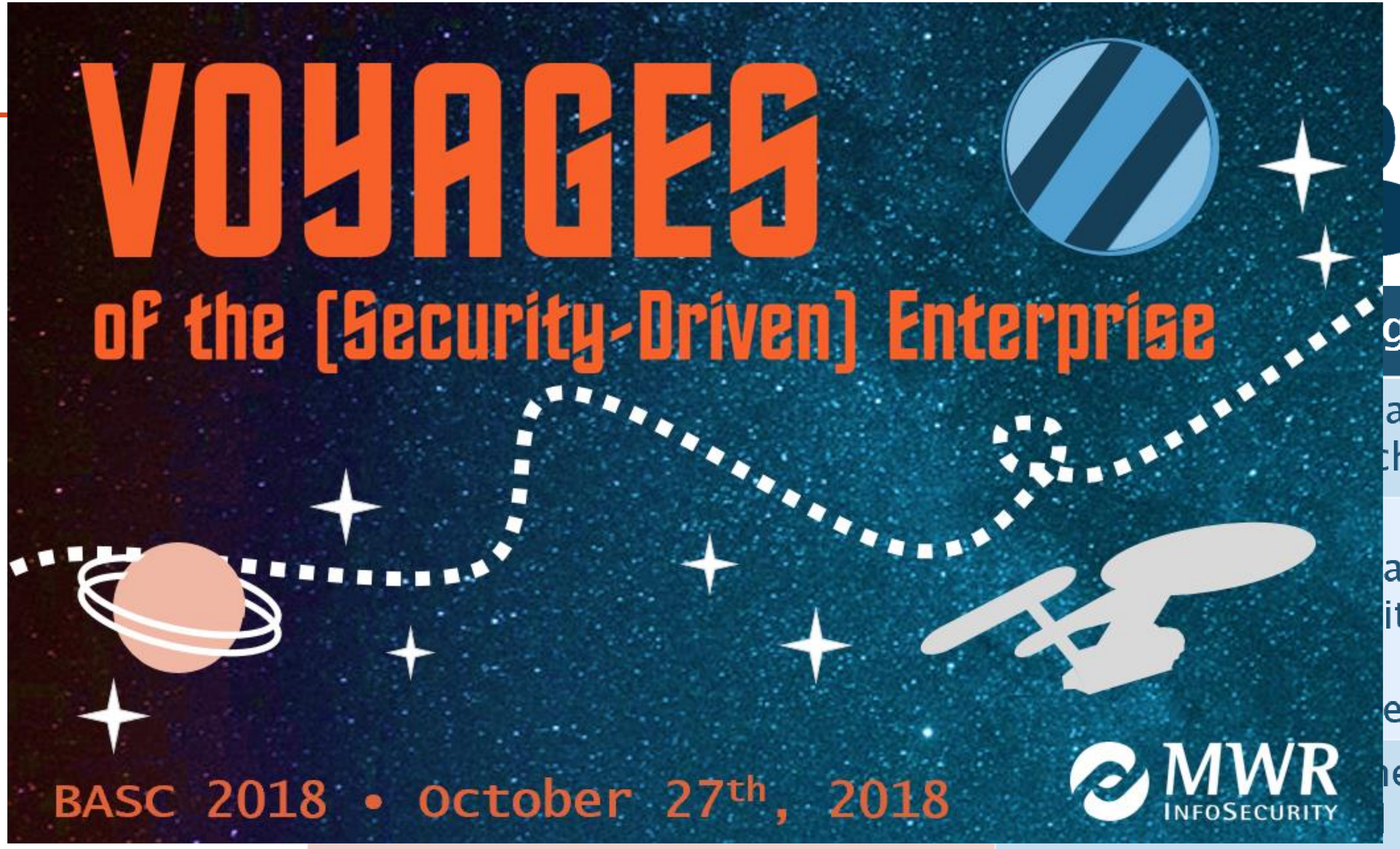


MWR InfoSecurity

# VOYAGES

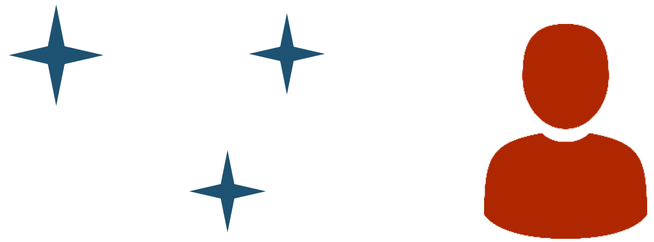
## of the (Security-Driven) Enterprise

BASC 2018
October 27th, 2018




| g Team |
| --- |
| app go down<br>ching” |
| ailability<br>ith new |
| ed to testing |
| e business<br>by this” |

MWR
INFOSECURITY

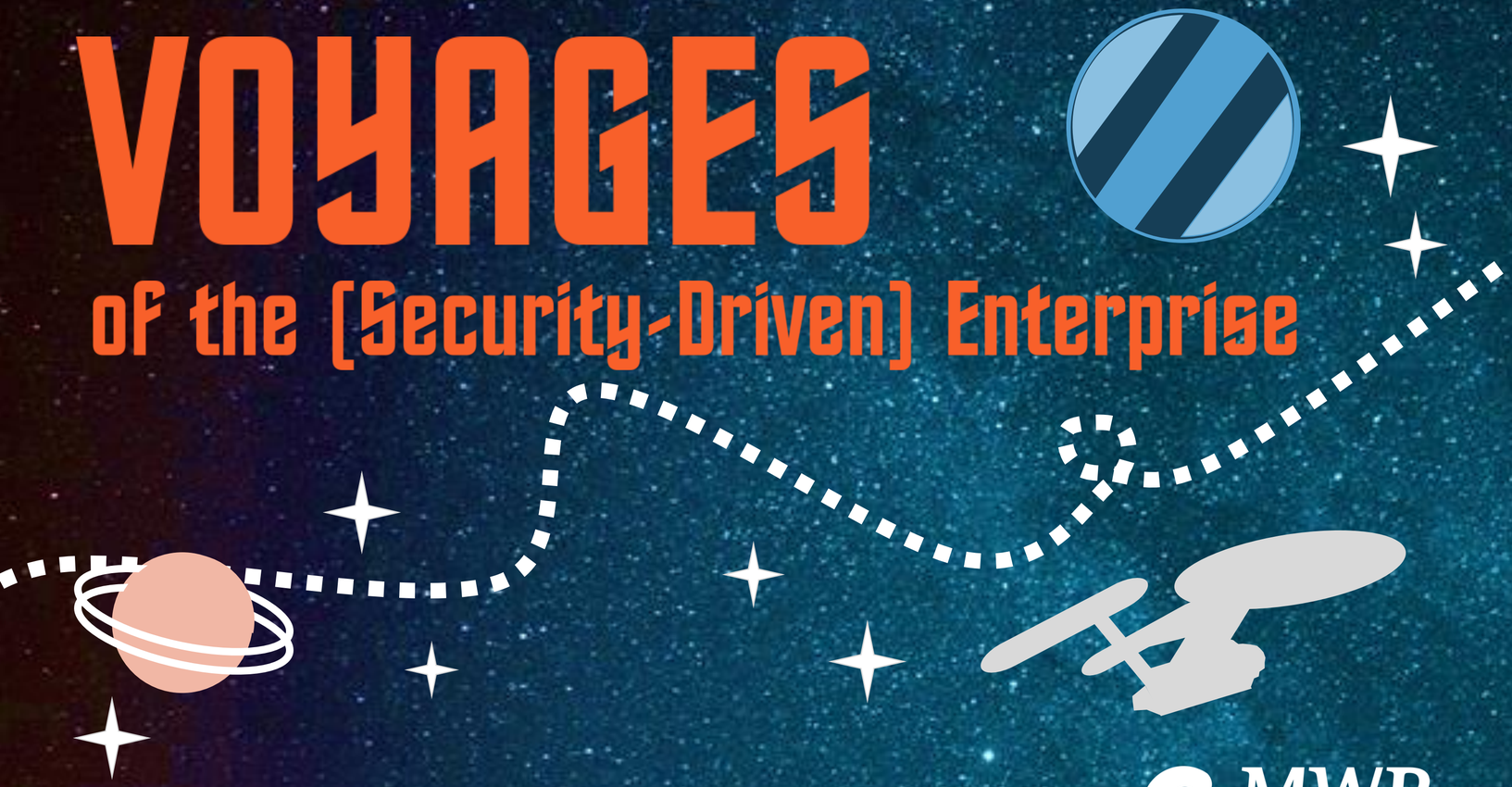


| | Information Security | Engineering Team |
|---|---|---|
| Motive | "We can't let these systems get breached" | "We can't let the app go down from patching" |
| Concerns | Breach:<br>• Loss of system availability<br>• Possible ongoing compromise<br>• Work hours devoted to remediation | Patching:<br>• Loss of system availability<br>• Ongoing issues with new software<br>• Work hours devoted to testing |
| Sentiment | "We can't let the business be impacted by this" | "We can't let the business be impacted by this" |

MWR INFOSECURITY

# VOYAGES

## of the (Security-Driven) Enterprise



BASC 2018 • October 27th, 2018

MWR InfoSecurity