RSAConference2019
San Francisco | March 4–8 | Moscone Center

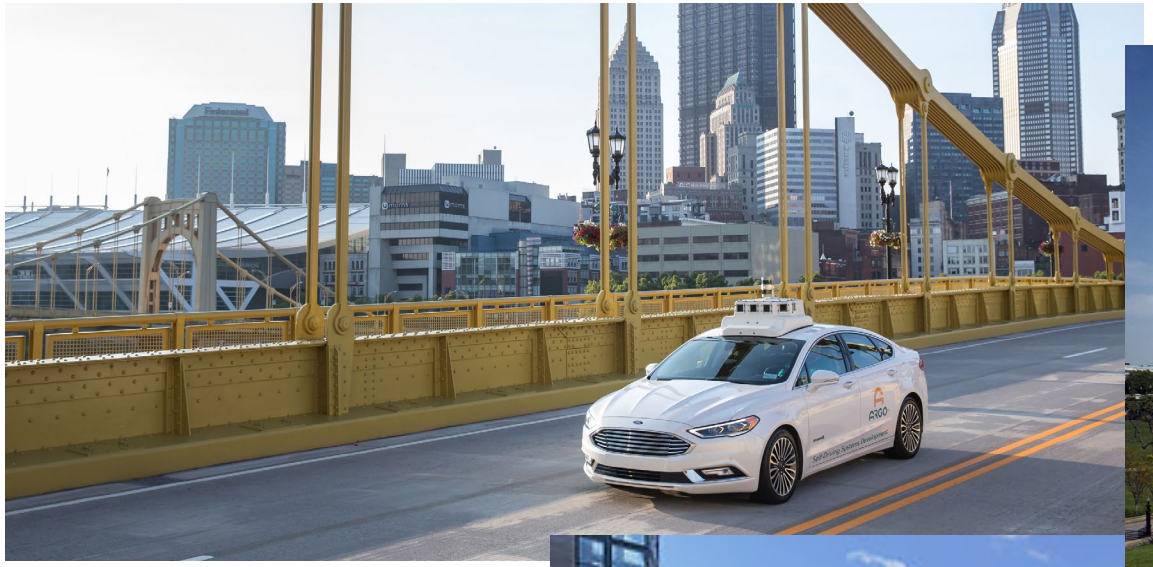
SESSION ID: AIR-W12

Prosilience: Moving Beyond Resilience

Bobbie Stempfley
Managing Director
CERT
@bobbiestempfley

Summer Craze Fowler
Chief Security Officer
Argo AI
@sumfowler

Experience spans Industry, Academia, Government



Argo.ai

Congress.gov

Cmu.edu

What We Want You to Get Out of This Presentation

- Lesson/Review on Resilience
- Introduction to Proactive Resilience
- Insight into Hybrid Threat Modeling Method
- Action Plan to use immediately
- New buzzword to impress your friends and family

https://www.johnogroat-journal.co.uk/News/Fantastic-crowd-wowed-by-90s-rockers-GUN-at-B-Fest-in-Wick-23082011.htm

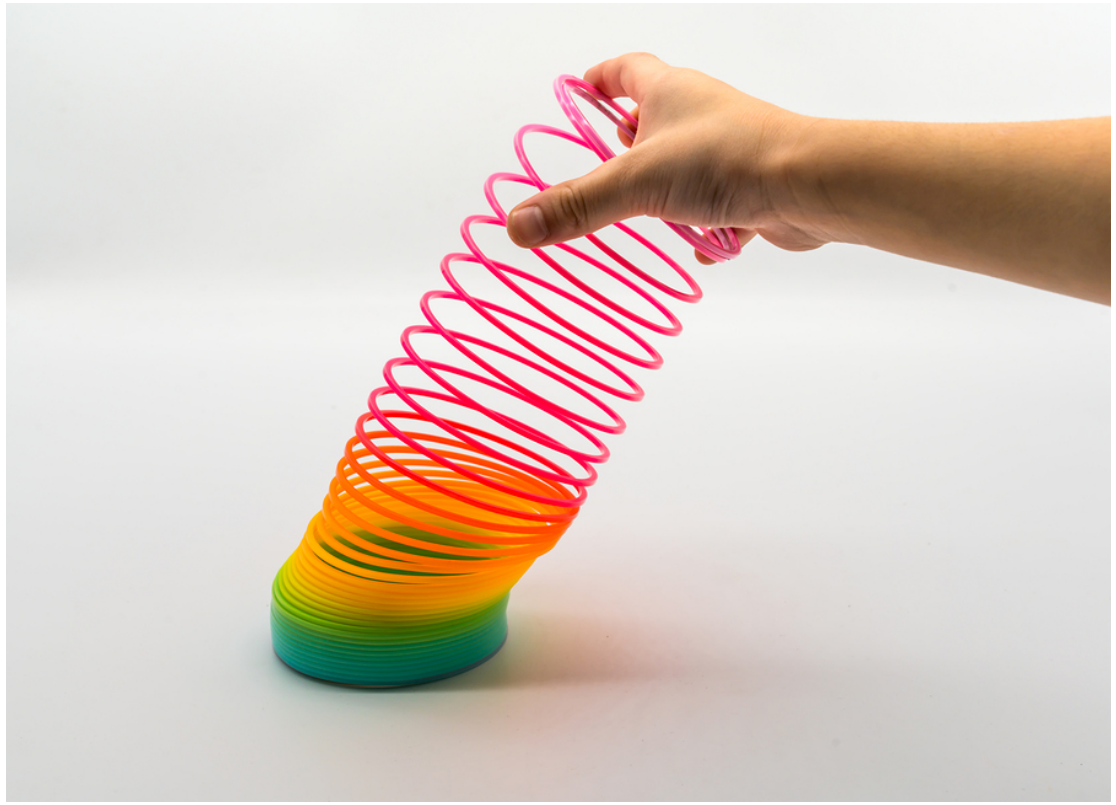
Disruption and Resilience

smithsonianmag.com

- An individual event is like a few grains of sand.
- A flow of grains of sand, even over a short time, can cause a disruption.
- A disruption can grow into a sandstorm of trouble.

To survive a sandstorm of trouble, an organization needs resilience.

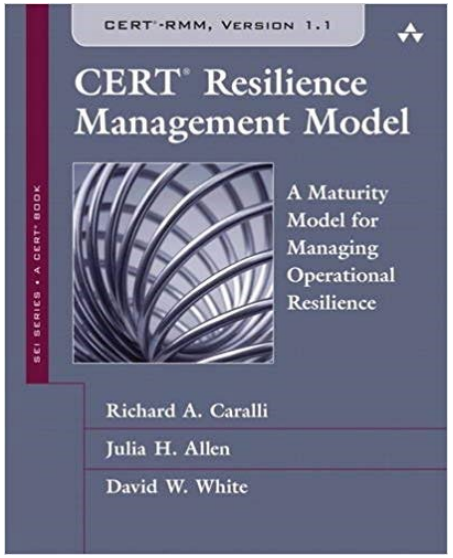
Resilience



Enables ability for an organization or system to operate before, during, and after a disruptive event…

AND return to normal operating mode following any degradation of capability

CERT-RMM Defines Elements of Resilience



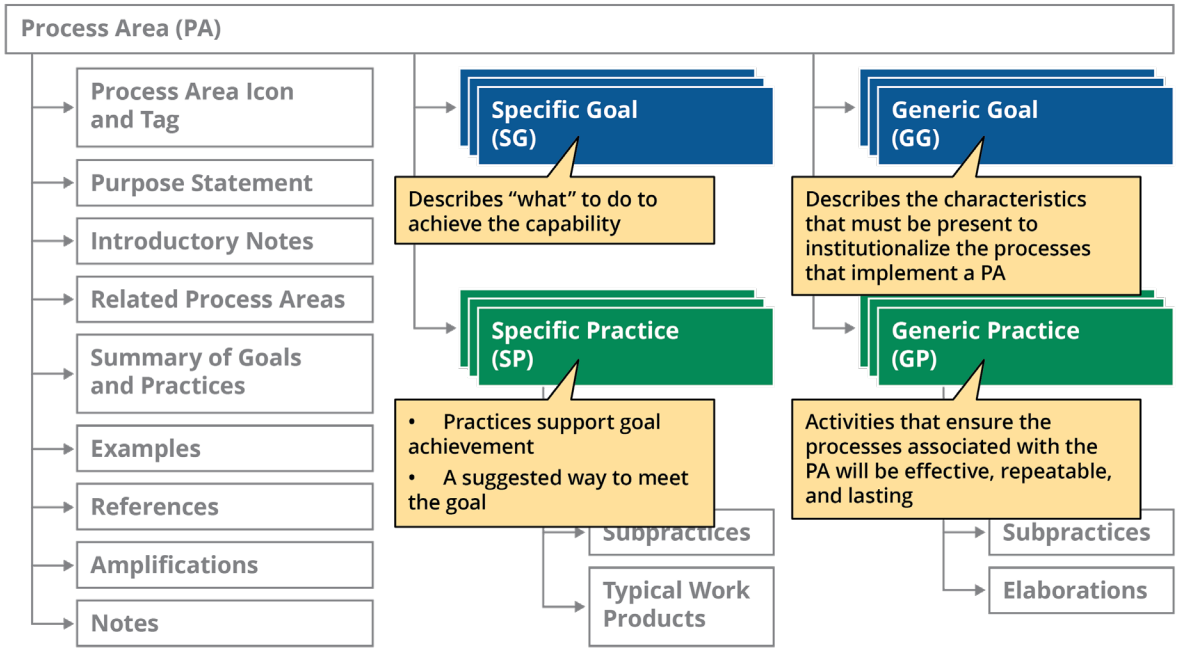
Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

Resilience Management at a Practical Level



- Each process area has a series of goals for organization to achieve along with examples
- Measures two dimensions of each process area
  - completeness
  - institutionalization

CERT-RMM Elements Correlate with other Frameworks

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

ISO 31000: 2009
BS25999-1:2006
CobiT 4.1
CMMI –DEV v1.2
CMMI –SVC v1.2
FFIEC BCP Handbook
ISO 20000-2:2005(E)
ISO 24762:2008(E)
ISO 27002:2005
ISO 27005:2008
PCI DSS v1.2.1: 2009
NFPA 1600:2007
ANSI/ASIS SPC.1-2009

NIST SP 800-18
NIST SP 800-30
NIST SP 800-34
NIST SP 800-37
NIST SP 800-39
NIST SP 800-53
NIST SP 800-53A
NIST SP 800-55
NIST SP 800-60
NIST SP 800-61
NIST SP 800-70
NIST SP 800-137

Resilience has Limits

- Learns from prior experience but can be limited to that knowledge
  - Darktrace: ML identifies previously unknown zero-day and other exploits
- Doesn't know what it doesn't know
- More reactive than proactive

Does your organization's resilience practice match the pace of potential disruption?

Prosilience is Possible

Resilience

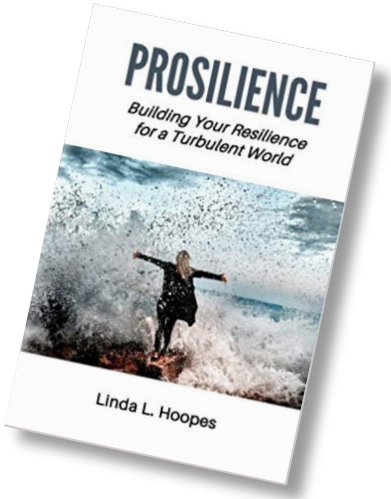
+

Proactivity

=

Prosilience

- Resilience is how you respond to challenges
- A *resilient* organization can achieve its objectives despite a disruption
- Prosilience is how you **intentionally prepare** to deal with them
  - Draws on psychology, neuroscience, physiology, and spirituality
- A *prosilient* organization is resilient and prepares for and anticipates disruptions



Suggested reading

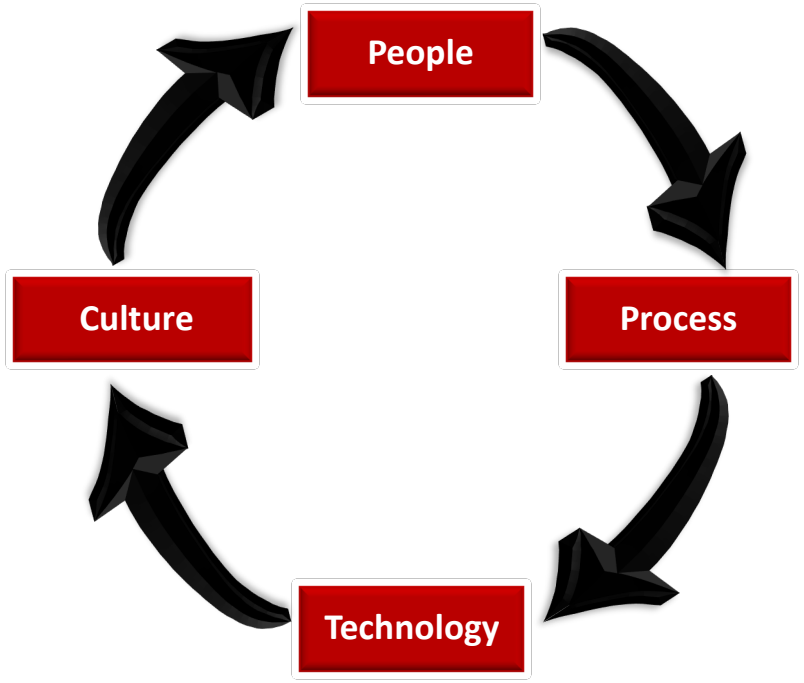
Prosilience takes Advantage of the Interconnected World

https://blog.storagecraft.com/hurricane-checklist-data-protection/

Function	Resilience	Prosilience
Identify	Today's, weather report indicates a chance of rain	The month is April and daily rain average is 70%
Protect	Grab umbrella as you run out the door	In anticipation of rainy days, rain gear has been stored in car and office
Detect	Rain starts falling	Observe clouds; Alerts of humidity, barometer, and rain probability by phone
Respond	Open umbrella, after sensing rain on head	Open umbrella JUST BEFORE rain starts
Recover	Dry off	Close umbrella, having been notified that rain threat ceased

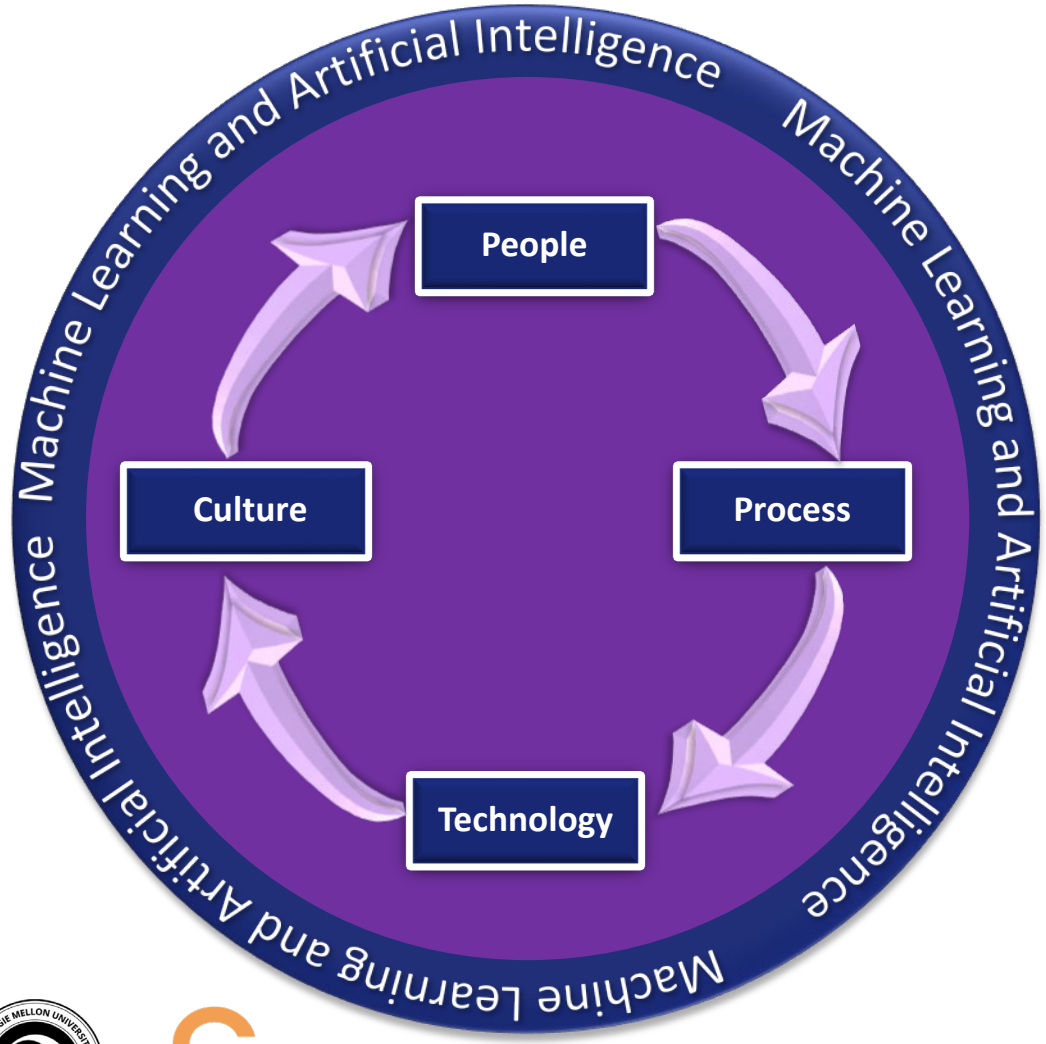
Can we apply prosilience to cybersecurity?

Cybersecurity & Resilience Balance People, Processes, Technology, and Culture



- Ensures completeness of practices in each area
- Measures institutionalization of practice
- Goal is survivability DESPITE disruption

Prosilience Wraps Cybersecurity Practice in Advanced Analytics



Characteristics

- Predictive
- Adaptive
- Evolutionary

Goal is analytics to AVOID disruption

Developed through

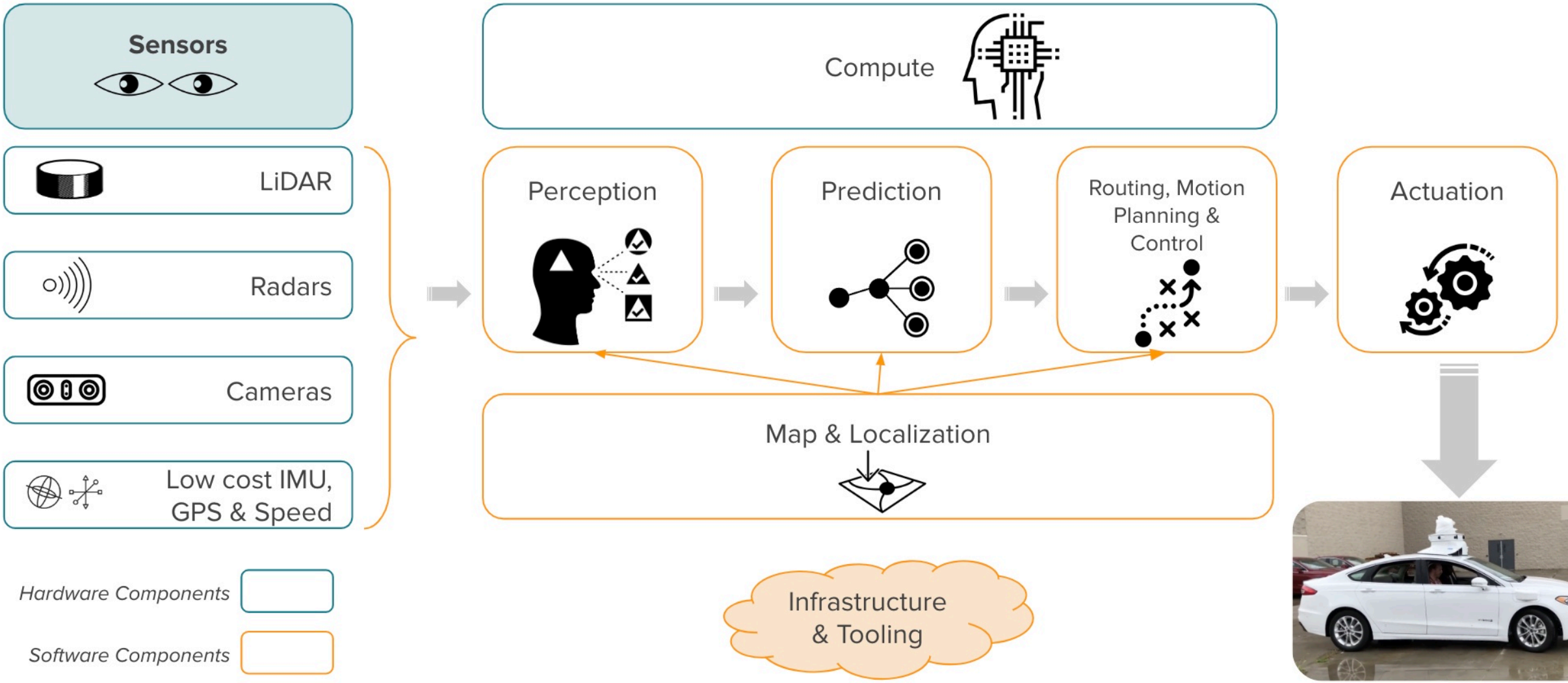
- Scenario planning
- Continuous exercises
- Incorporating real-time and real-world indicators

Meet Disruptions with New Science

Becominghuman.ai

- Machine Learning
  - ML Concepts
- Artificial Intelligence
  - AI Concepts

Application Example



Disruption and Prosilience

smithsonianmag.com

- Can Machine Learning and AI help and organization predict each grain of sand in your organization?
- Do we even know WHAT or HOW to apply these concepts?
- AI and ML first require human intelligence and learning models

Baby Steps --> Prosilient Concepts in Resilience

- Resilience:
  - Completeness of practices
  - Institutionalization of practices
- Prosilience anticipates rather than reacts
- Let's start low-tech with our own neural network of threats
  - Identify and Prioritize, Assets, Connections, Actors, Vectors, and Vulnerabilities.
    - *"Where are the high-value assets?"*
    - *"Where am I most vulnerable to attack?"*
    - *"What are the most relevant threats?"*
    - *"Is there an attack vector that might go unnoticed?"*
-

Hybrid Threat Modeling Method (hTMM)

- Combines agility, repeatability, and threat model coverage needed for our overall systems architecture and operation process.
- Combination of SQUARE, security cards, and Personae non Gratae (PnG) activities
- Characteristics of hTMM
  - Intuitive and iterative process
  - No false positives
  - No overlooked threats
  - Consistent results regardless of who is doing the threat modeling
  - Cost-effective (doesn't waste time)
  - Empirical evidence to support its efficacy

hTMM Steps

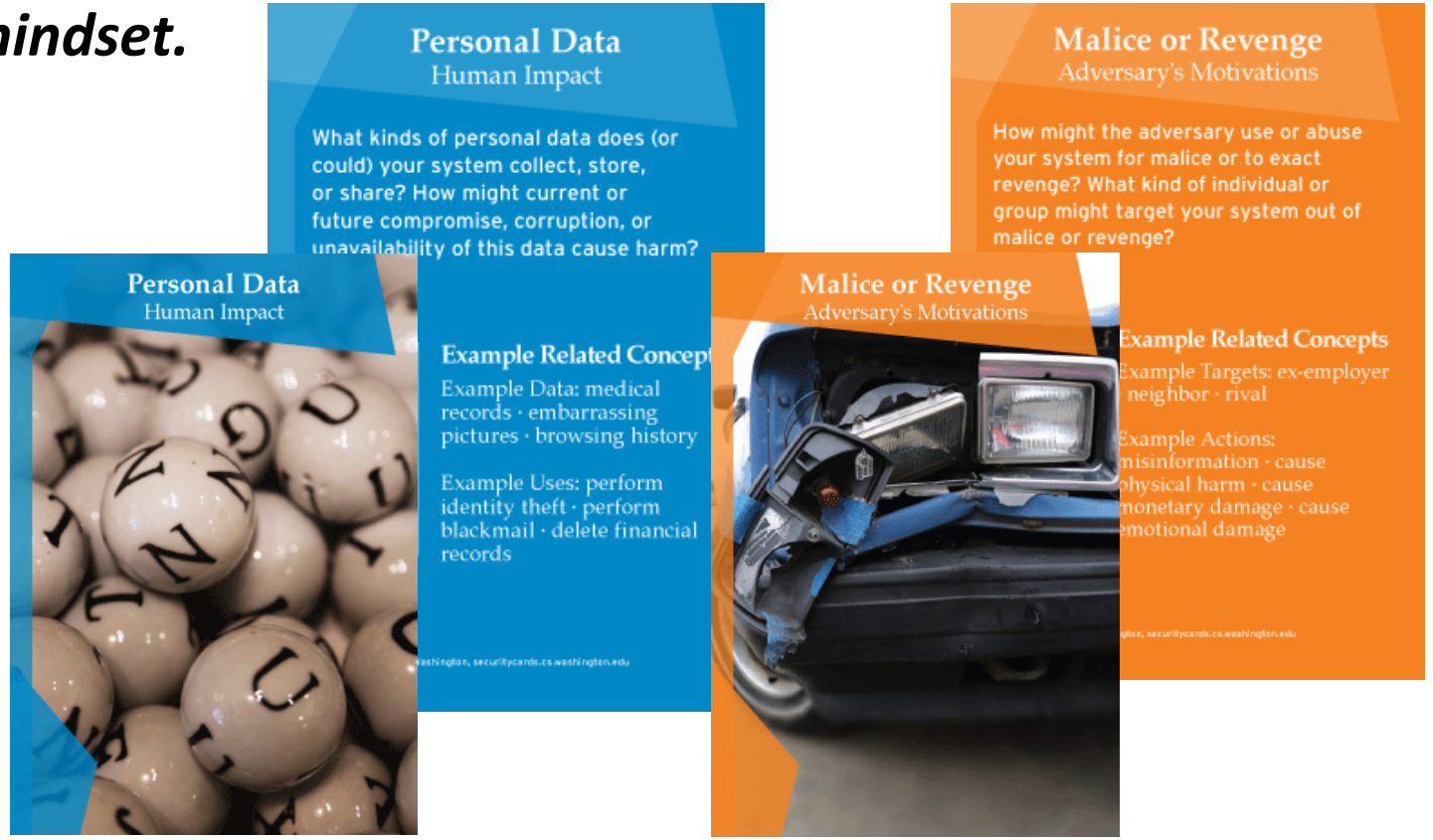
1. Identify the system you will be threat modeling.
   - Complete steps 1-3 of SQUARE threat model method
2. Apply Security Cards according to users' or developers' suggestions.
   - Review dimensions and identify likelihood rankings
3. Prune PnGs that are unlikely or for which no realistic attack vectors could be identified.
4. Summarize results from the above steps, utilizing tool support.
5. Continue with a formal risk assessment method (FAIR).

1. What is SQUARE?

1. Agree on Project Definitions
   - **Input:** Candidate terminology and definitions compiled from expertise and knowledge of Argo systems, technologies and threats, compiled from public resources and stakeholder interviews.
   - **Techniques:** Stakeholders, requirements team in focus group, interviews
   - **Output:** Argo threat model lexicon
2. Identify Business Goals for the System, Assets and Threat Model
   - **Input:** Definitions, candidate goals, business drivers, policies and procedures, examples
   - **Techniques:** Stakeholders, engineers in work sessions, surveys, interviews
   - **Output:** Primary and prioritized supporting goals of the threat model project
3. Gather Artifacts
   - **Input:** Potential artifacts (e.g., diagrams, scenarios, mis/use cases, templates)
   - **Participants:** Stakeholders, engineers, requirements team
   - **Output:** Useful diagrams, scenarios, mis/use cases, models, and templates

2. Security Cards

- Security Cards were developed at the University of Washington to help emphasize creativity and brainstorming over more structured approaches such as checklists.
- ***Security Cards develop a security mindset.***
- The 4 Security Dimensions:
- Human Impact (9 Cards)
- Adversary's Motivations (13 Cards)
- Adversary's Resources (11 Cards)
- Adversary's Methods (9 Cards)

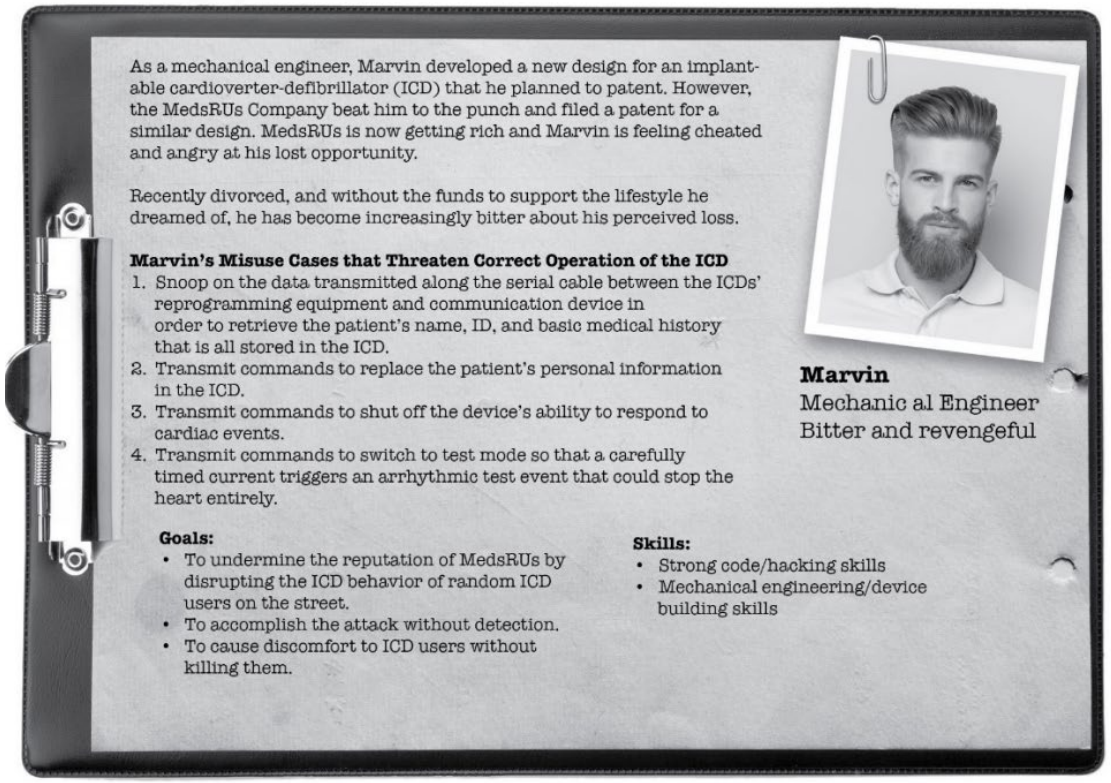


3. Prune Personae Non Gratae (PnGs)

Once data has been collected, prune PnGs that are unlikely or for which no realistic attack vectors could be identified. Itemize their misuse cases.

This expands on HOW the adversary attacks the system.

For the likely misuse cases provide the supporting detailed information on how the attack takes place.



As a mechanical engineer, Marvin developed a new design for an implantable cardioverter-defibrillator (ICD) that he planned to patent. However, the MedsRUs Company beat him to the punch and filed a patent for a similar design. MedsRUs is now getting rich and Marvin is feeling cheated and angry at his lost opportunity.

Recently divorced, and without the funds to support the lifestyle he dreamed of, he has become increasingly bitter about his perceived loss.

Marvin's Misuse Cases that Threaten Correct Operation of the ICD

1. Snoop on the data transmitted along the serial cable between the ICDs' reprogramming equipment and communication device in order to retrieve the patient's name, ID, and basic medical history that is all stored in the ICD.
2. Transmit commands to replace the patient's personal information in the ICD.
3. Transmit commands to shut off the device's ability to respond to cardiac events.
4. Transmit commands to switch to test mode so that a carefully timed current triggers an arrhythmic test event that could stop the heart entirely.

Goals:

- To undermine the reputation of MedsRUs by disrupting the ICD behavior of random ICD users on the street.
- To accomplish the attack without detection.
- To cause discomfort to ICD users without killing them.

Skills:

- Strong code/hacking skills
- Mechanical engineering/device building skills

Marvin
Mechanic al Engineer
Bitter and revengeful

4. hTMM Summary

- **Actor (PnG):** Who or what instigates the attack?
- **Purpose:** What is the actor's goal or intent?
- **Target:** What asset is the target?
- **Action:** What action does the actor perform or attempt to perform?
  - Here you should consider both the resources and the skills of the actor. You will also be describing HOW the actor might attack your system and its expansion into misuse cases.
- **Result of the action:** What happens as a result of the action? What assets are compromised? What goal has the actor achieved?
- **Impact:** What is the severity of the result (high, medium, or low)
- **Threat type:** (e.g., denial of service, spoofing)

4. What Does It Look Like?

PnG	Purpose	Target	Action	Result	Impacts	Sev	Threat Type
Marvin	Revenge	Garage	Wifi Pineapple	Network Exploit, Denial of Service	Financial Wellbeing	Medium	Insider Threat
Susan	Corporate sabotage.	LiDAR	Laser Pointer	Data Corruption	Financial, Societal, (Bad Data)	High	Sensor Attack
Bob	Financial	ADP	Change Direct Deposit	Integrity	Emotional, Financial	High	Criminal
Jane	Curiosity	Corp Social Media	Access and post	Inappropriate messages posted	Emotional, Financial	Medium	Hacker

Identify the data you collect/establish the labels

5. Extra Credit – Monetize Impact

"Factor analysis of information risk (**FAIR**) is a taxonomy of the factors that contribute to risk and how they affect each other."

https://www.fairinstitute.org/about

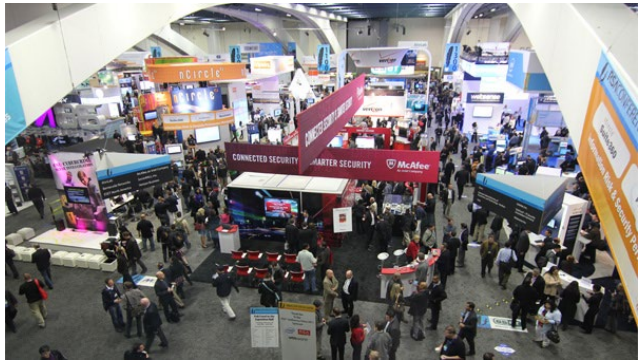
What Can You Do

- Start a conversation in your organization
- Identify most critical systems (resilience!)
- Gather stakeholders for 1 hour meeting on one system
- Follow hTMM steps and build profiles
- Work with teams to use these profiles to determine ways to address
  - Build the intelligence to ANTICIPATE the disruptions
- Survey the data you collect and leverage the profiles for analytics
- Learn more here: https://insights.sei.cmu.edu/sei_blog/2018/04/the-hybrid-threat-modeling-method.html

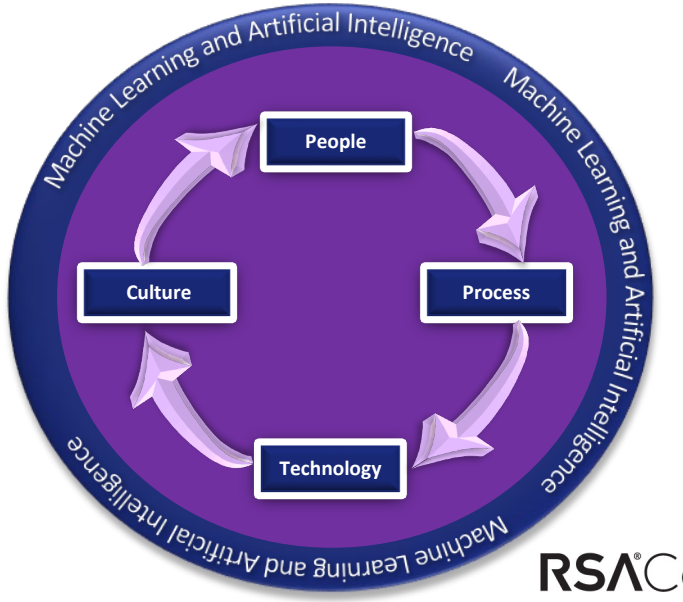
First steps in moving to Prosilience: modeling threats

How Does This Help You Today?

- Current buzzwords surround us – especially this week!
- Determining which of the new, shiny AI tools will work requires you to start with resilience concepts
- Build for prosilience with threat modeling using hTMM
- Use this new neural network to assess AI/ML tools that will help



http://thefreightdude.com/blog/tag/rsa-conference-2015/



RSAConference2019

RSA®Conference2019

RSAConference2019

Removed slides