RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Criticality Analysis & Supply Chain: Providing "Representational Assurance"

SESSION ID: STR-W04A

Dan Reddy (CISSP, CSSLP)
Sr. Consultant Product Manager & Supply Chain Assurance Lead
EMC Product Security Office
@danlj28

Problem

- Those who buy technology for a new system need to understand the risk there are taking on from their technology providers.
- Providers of technology don't want to unduly share details behind their technology that could compromise their product's security or their company's competitive posture.
- How to bridge the gap? **"Representational Assurance"**
  - Uses meaningful metadata about security practices that can be shared to build initial risk posture. Leveraging graphics help to analyze while scaling.
- You will see how to apply this concept to a Use Case.

Set the Stage for the Use Case - Actors:

Public Sector System Builder seeks to acquire technology from ICT COTS Providers

System Builder (Acquirer)

- Has overall system goal
- May acquire through Integrator
- Required to address Information & Communication Technology (ICT), Commercial Off-the-Shelf (COTS) risk as part of the system
  - Including Supply Chain Risk Management (SCRM)

Supplier (Provider)

- Builds highly functional products
- Cares about quality
- Builds secure products
- Good practices matter most
  - Strives to prevent “bugs”
  - Cares about product integrity
  - Invests in Certs & Accreditation
  - Has enterprise risk program

Today's Situation – Not on same page

Acquirer

- Guidance says:
  - Conduct *Criticality Analysis*
  - Assess overall risk of System
    - Many aspects to cover
  - Create visibility into supply chain of suppliers
  - Ask for supply chain map with traceable details of components and supplier locations and delivery !

Provider

- Builds high availability as feature
- Performs rigorous quality testing
- What do you mean by Criticality Analysis?
  - Sharing component tier Supplier details appears unreasonable
    - What is really needed?
    - Disclosing such info is a risk

Sidebar: What is Criticality Analysis? (CA)

- Originated by U.S. DoD; used by NASA
- Required by U.S. DoD in protection planning
- Extension of Failure Modes, Effects by adding *Criticality* Analysis (FMECA)
- Determine Impacts to Overall System based on Threats to System subsystems
- Decompose Architecture and align with Threats
- Among many threats, consider SCRM impacts
- Plan for mitigation and testing

(Resilient Technologies in Wausau WI)

Can my vehicle keep moving if tires are shot out?

Future State: Recommended Approach (+ few years)

Acquirer

- Begin *Criticality Analysis* internally
  - Decompose Design into subsystems and architectural elements (AE)
  - Issue RFI to Providers.
  - Ask for data about provider's products and any suppliers that contribute most critical components
- Import responses into analysis

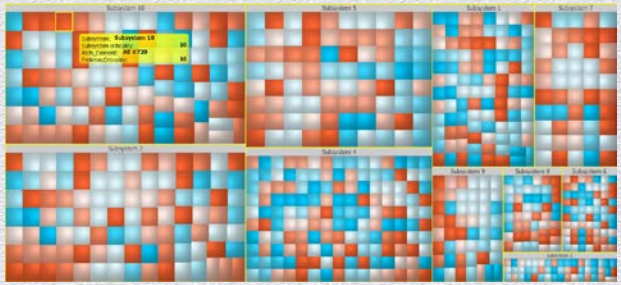
Provider

- Conduct CA by identifying components that are most critical to ongoing operation.
  - Preserve Customer Confidentiality, Integrity and Availability (CIA)
- Examine Suppliers who contribute the most critical components
- Identify Best Practices of Suppliers
- Share via Representational Assurance

Process: Step 1

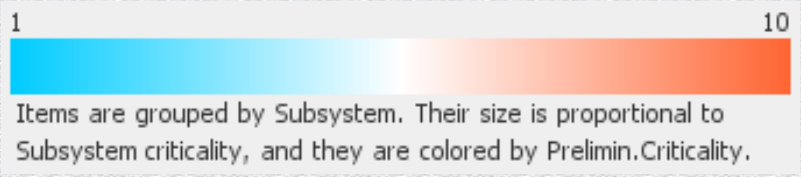
Acquirer decomposes planned system Into Subsystems & Architectural Elements

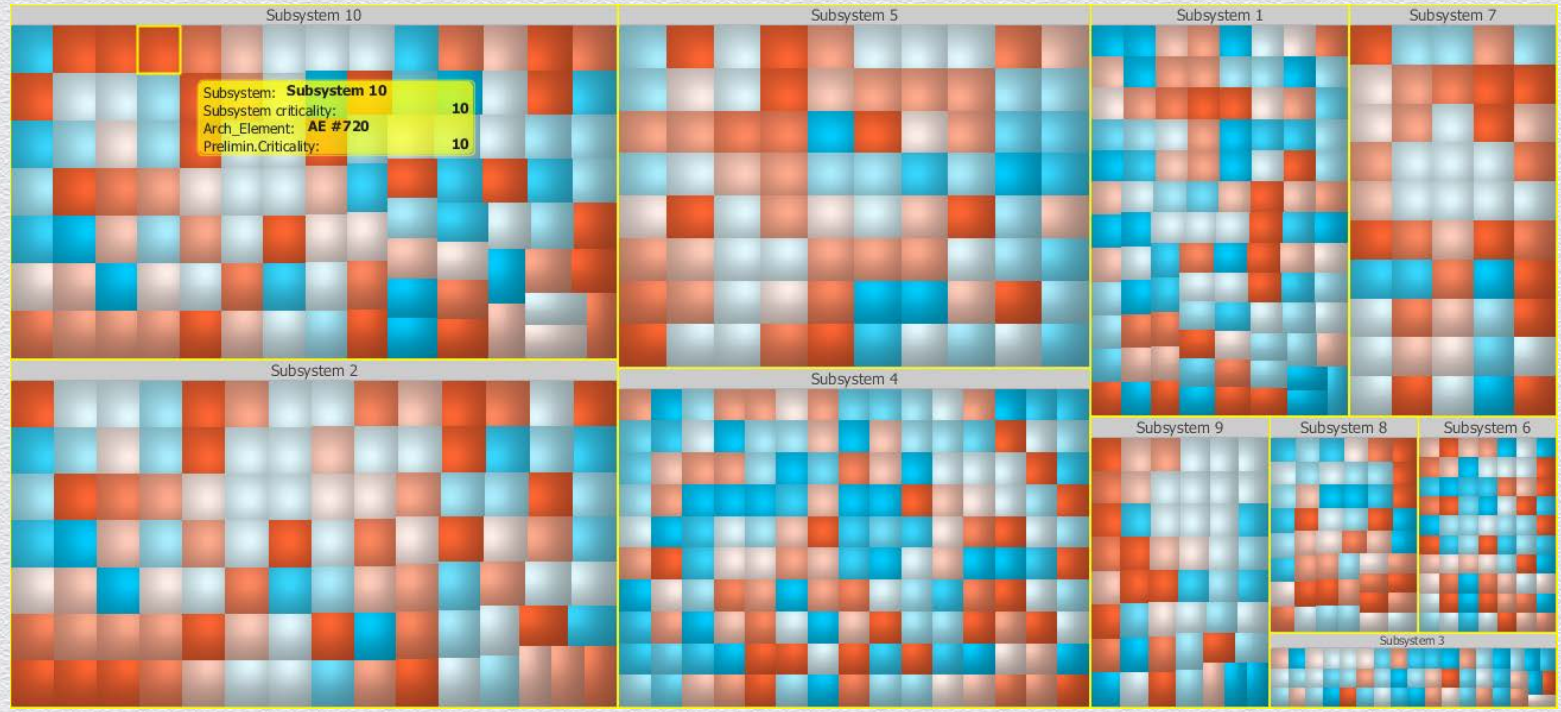
The “Before” view…



Treemap Output

Acquirer independently produces initial analysis of system.
Shows what is most critical at Subsystem & Element level.





First Architectural View of System by Builder

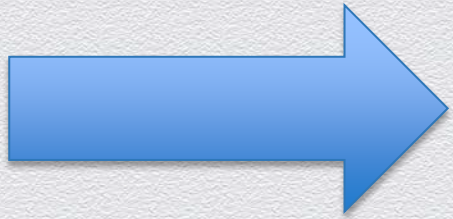
Note: Initial *perceived* risk to Subsystems and Architectural Elements

1 10

Items are grouped by Subsystem. Their size is proportional to Subsystem criticality, and they are colored by Prelimin.Criticality.

Process: Step 2

Acquirer issues Request For Information (RFI) to tech providers



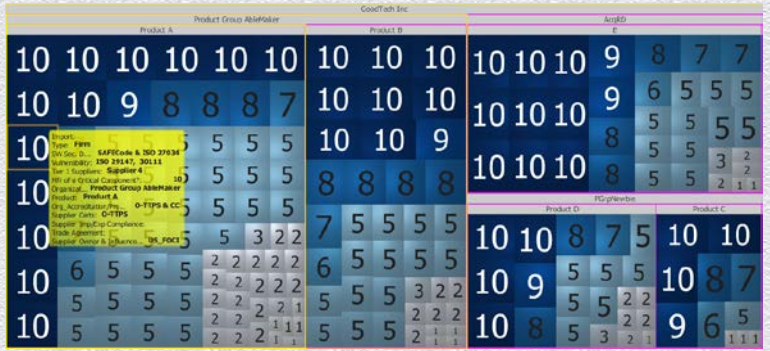
Request for Information:

1. List products with this functionality
2. Decompose products by criticality
3. Show supplier practices for each component
4. Share “representational assurance” data

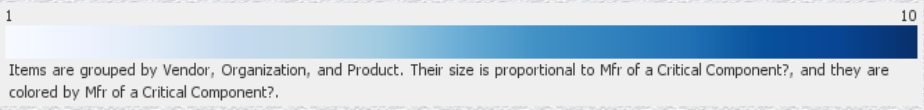
- Capture meaningful info without undue disclosure

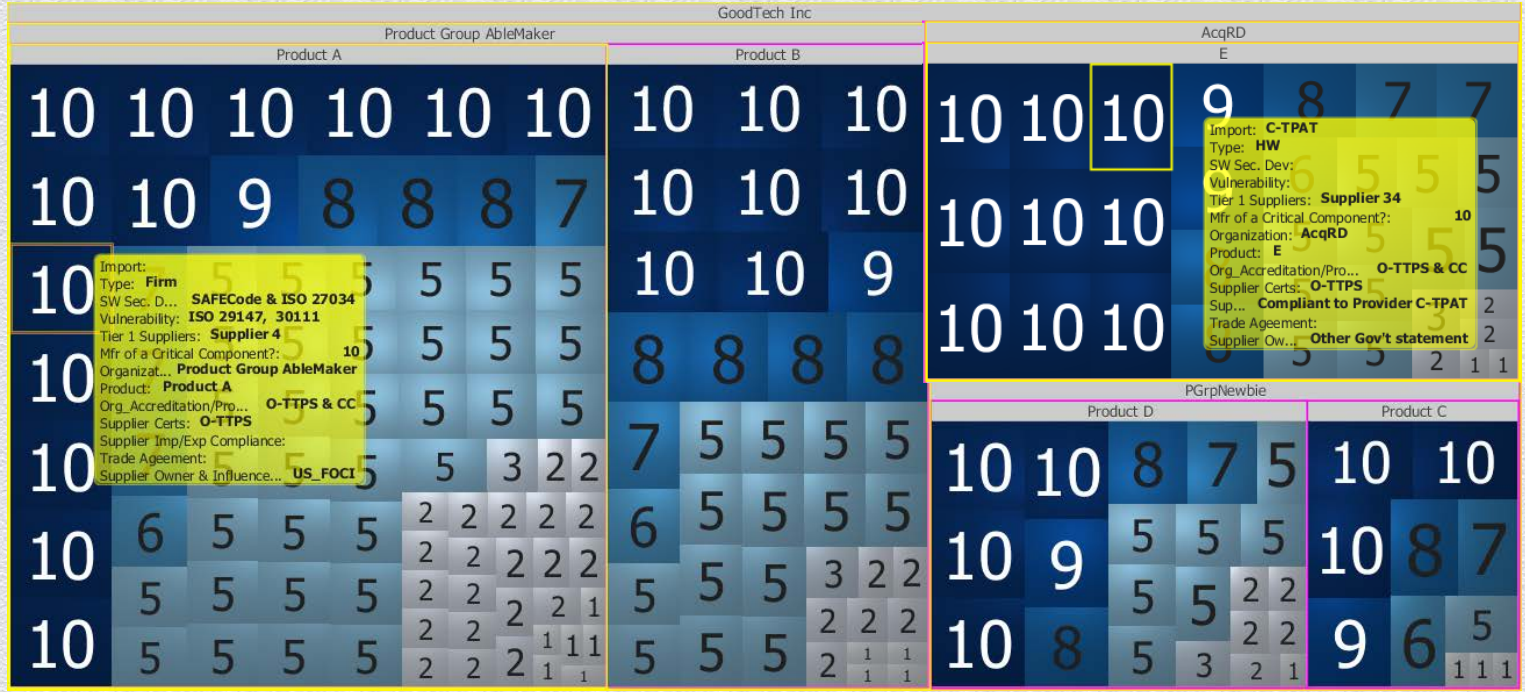
Process: Step 3

" Good Tech" does internal analysis of product set & researches the supplier security practices of each component to prep for SCRM



Provider rates each component in each product by how critical it is (10 scale)
Tracks each product organization's Certs & Accreditations
Tracks Certs & Accreditations of each supplier of each component





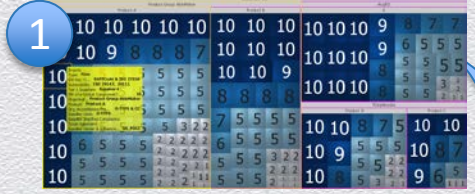
Provider's Internal View

Here are my product teams, their 3rd party accreditations, certs etc. and what I know of the suppliers and their security practices of most critical components in products.

1 10

Items are grouped by Vendor, Organization, and Product. Their size is proportional to Mfr of a Critical Component?, and they are colored by Mfr of a Critical Component?.

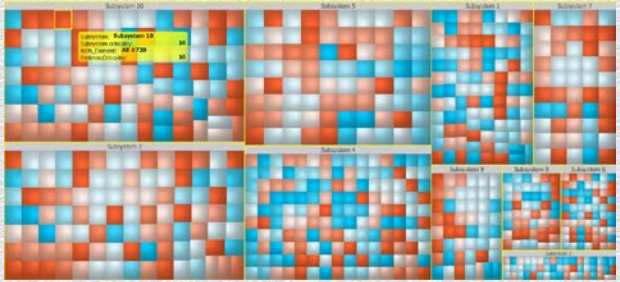
Process: Step 4



2 3 4 5 6 n

Critical components and supplier practices SCRM data from all bidders

Acquirer aggregates data from all bidders. Updates Architectural View with new Product View

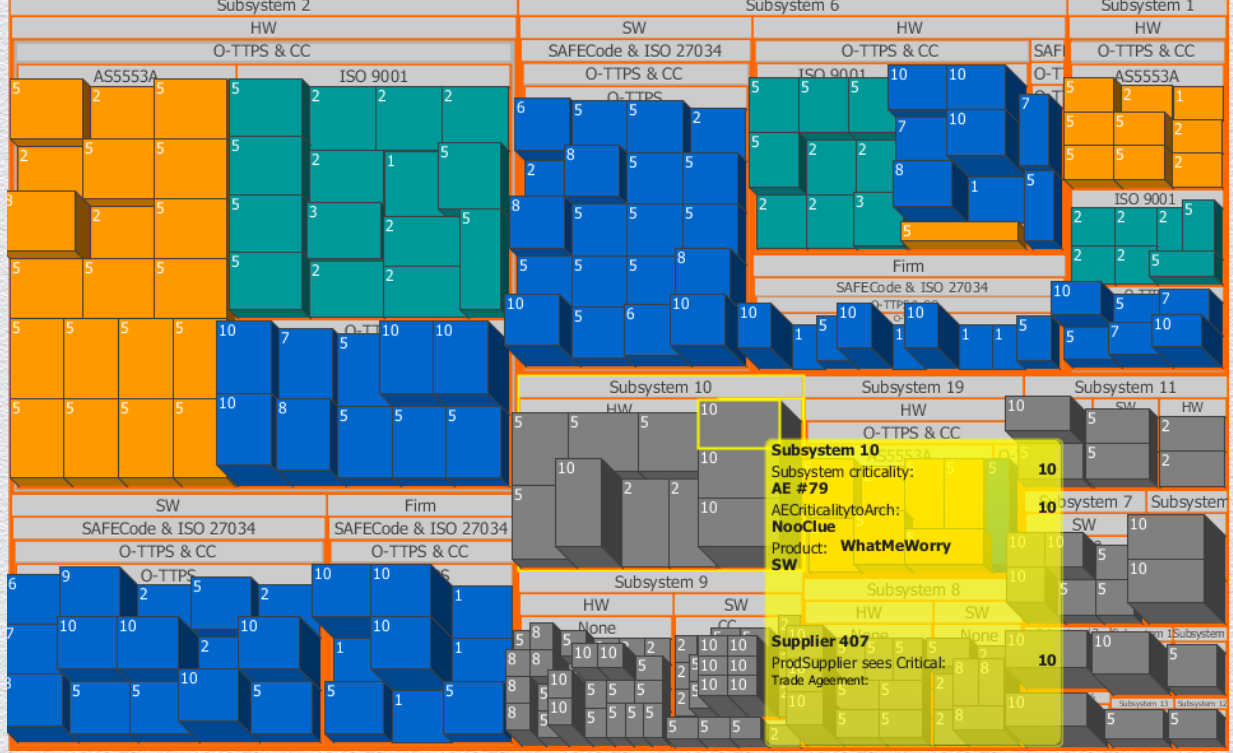


Before

After

Bring it all together.

Can now be sliced & diced for further follow-up



Process: Step 5 - Acquirer's Final Product View (after RFI)

Asserted data about SCRM from suppliers.

Consider applying mitigation controls and countermeasures.

Representational Assurance

- Provider conveys essence of security practices without detailed results
- Similar to assertion that “My product team performs static code analysis and handles the results in this manner”
- Provides actionable data without undue disclosure
- Allows criticality analysis to begin early (where it should)
- Provides meaningful dialog between Acquirer and Provider
- Better than talking past each other
  - What do *you* mean by supply chain?

Further Resources

- Failure Modes, Effects & Criticality Analysis
  - US Military Standard (Not Active) 1629
  - NASA - http://history.nasa.gov/rogersrep/v6ch3.htm
- Treemap software: Macrofocus GmbH, 2014. (www.treemap.com)
- My full article on the topic: Technovation, Special Issue: *Supply Chain Risk Management*, Spring 2014
  - http://www.journals.elsevier.com/technovation/
- LinkedIn: http://www.linkedin.com/in/danreddySCRMsme