FIRST.Org, Inc

Incident Response Framework Journeys

Peter Allor
Education Advisory Board, Chair
FIRST.Org, Inc.
Education and Training

- It started with an idea.....it became a journey
- Then a Framework
- Then another
- Once upon a time CERT/CC
Program Timeline

- **SUMMIT I**
  - Oct 2014
  - Develop Draft Framework
  - Private Sector Input on Framework

- **SUMMIT II**
  - Feb – May 2015
  - Community Inputs on Framework
  - Service Module Development & Critical Review
  - Preliminary Framework
  - Initiate PSIRT Review

- **SUMMIT III**
  - Jun – July 2015
  - Framework v1.0
  - Review / Improve Version 1.0 Framework and Initial Modules

- **SUMMIT IV**
  - Aug – Sept 2015
  - Phase I
  - Develop Draft Framework
  - Draft Framework

- **SUMMIT V**
  - Oct - Dec 2015
  - Phase II
  - Service Module Development & Critical Review
  - Framework v1.0

- **SUMMIT V**
  - Jan – Feb 2016
  - Phase III
  - Review / Improve Version 1.0 Framework and Initial Modules

- **SUMMIT V**
  - Dec 2016
  - Phase IV
  - Initiate Training
  - Develop New Materials
Framework – hierarchical approach

• Service Area
  • Service
    • Function
      • Sub-Function
        • Task
          • Sub-Task
            • Action
Simplified Definitions

• **Capability** – Can you do it?

• **Maturity** – How well can you do it?

• **Capacity** – How much can you do?
<table>
<thead>
<tr>
<th>CSIRT Framework 2.0</th>
<th>NIST Cybersecurity Framework</th>
<th>PSRT Services Framework 1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Assurance (Service Area 3)</strong></td>
<td><strong>Identify (ID)</strong></td>
<td><strong>Stakeholder Ecosystem Management (Service Area 1)</strong></td>
</tr>
<tr>
<td>Risk Management</td>
<td>Asset Management</td>
<td>Internal Management</td>
</tr>
<tr>
<td>Compliance Management</td>
<td>Business Environment</td>
<td>Finder Management</td>
</tr>
<tr>
<td>Operating Policies Support</td>
<td>Government</td>
<td>Community Engagement</td>
</tr>
<tr>
<td>BCP/IDR Planning Support</td>
<td>Risk Assessment</td>
<td>Downstream Management</td>
</tr>
<tr>
<td>Technical Security Support</td>
<td></td>
<td>Incident Coordination</td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
<td>Recognition</td>
</tr>
</tbody>
</table>

| **Situational Awareness (Service Area 4)** | **Detect (DE)** | **Vulnerability Discovery (Service Area 2)** |
| Artifact Analysis | Anomalies & Events | Vulner. reporting |
| Media Analysis | Security Continuous Monitoring | Unreported Vulns |
| Vulner./Exploit Analysis | Detection Processes | Monitor Vulns |

| **Outreach/Communications (Service Area 5)** | **Respond (RS)** | **Vulnerability Triage (Service Area 3)** |
| Artifact Analysis | Response Planning | Qualification |
| Media Analysis | Communications | Established Finders |
| Vulner./Exploit Analysis | Analyst | Reproduction |

| **Incident Management (Service Area 1)** | **Recovery (RC)** | **Remediation (Service Area 4)** |
| Incident Handling | Recovery Planning | Release Mgmt Plan |
| Incident Analysis | Improvements | Remediation |
| Incident Mitigation & Recovery | Communications | Incident Handling |

| **Analysis (Service Area 2)** | **Vulnerability Disclosure (Service Area 5)** | **Training the PSRT Team** |
| Artifact Analysis | Notification | |