On Providing Risk Metrics Using Security Automation, Protocols, and Standards

James Park
NSA CND R&T Team

Nov 2, 2011

Agenda

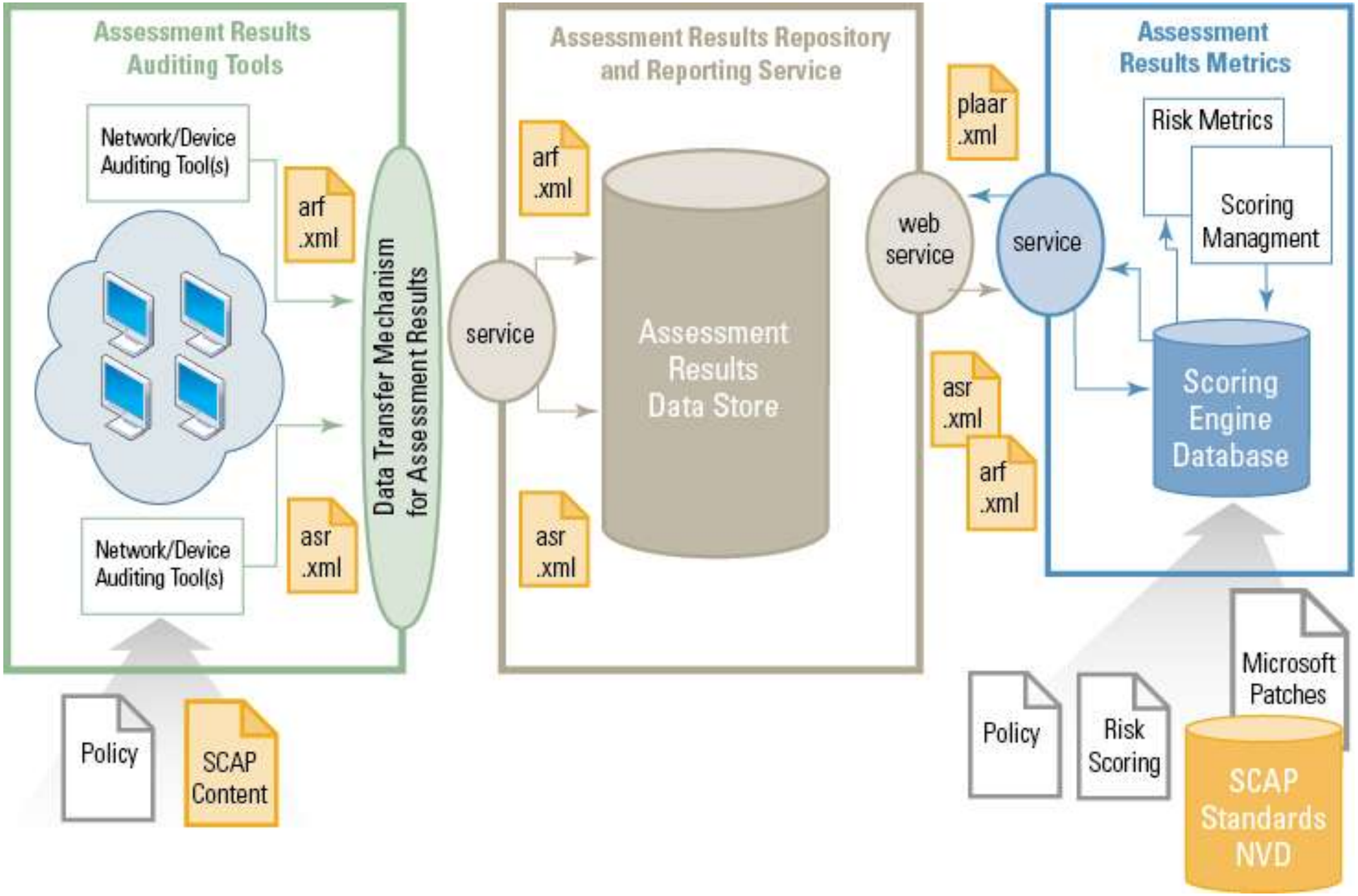
- Once upon a time….
- Maturing Architecture
- In the life of a Patch metric
- Lessons Learned
- Current Research

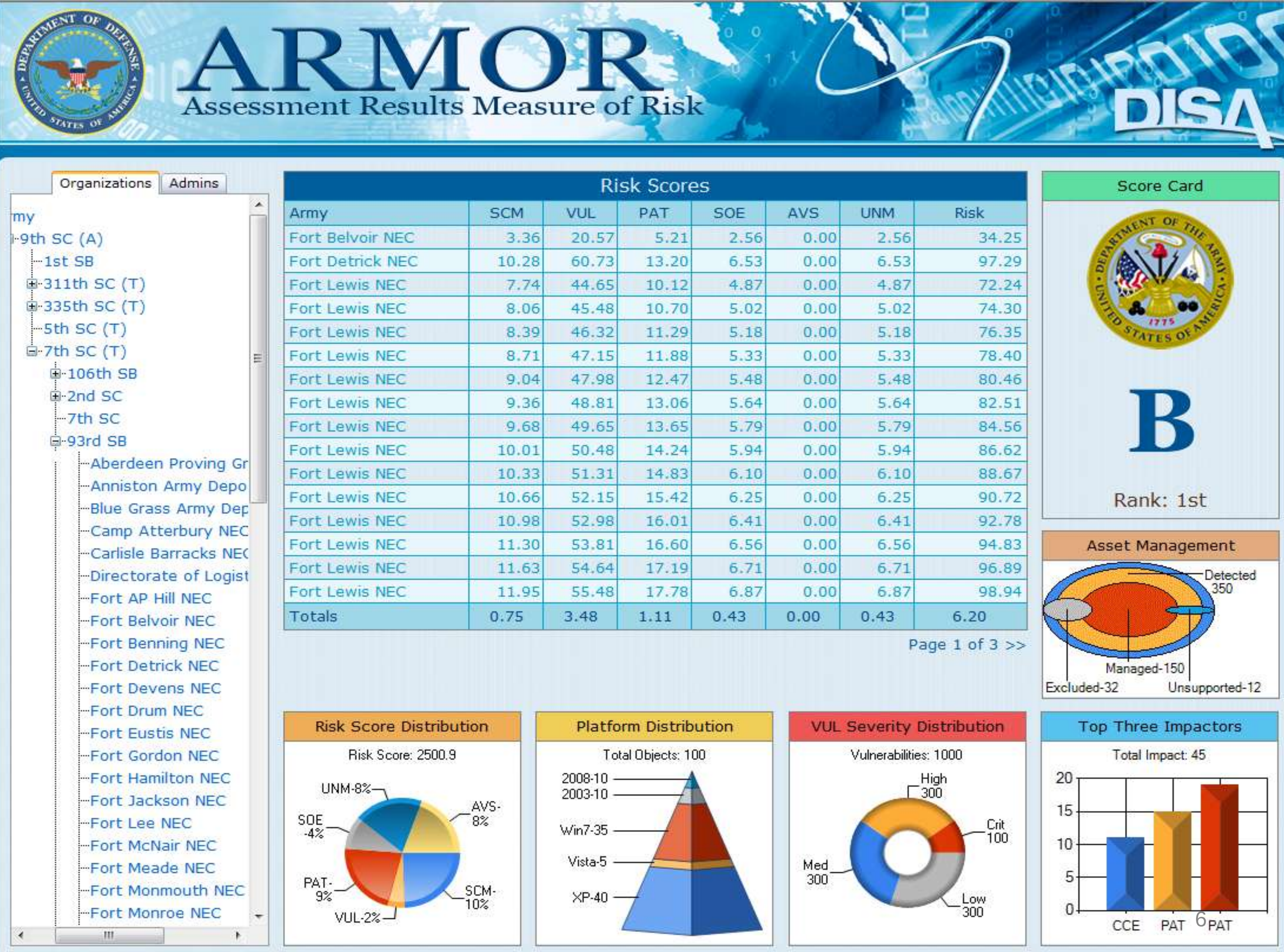
History

once upon a time….

2008	NSA proposes ARF/ASR as SCAP standards
2009	Oct: Risk Dashboard (RD) selected as one of key (GS) initiatives
	Nov: DoS iPost earns NSA Frank B. Rowlett Award
2010	Feb: Start building RD
	Mar: WH Mr. Schmidt asks when we will have iPost like capability
	RD redirected and start to integrate SCAP results into iPost
	Apr: Continuous Monitoring (CM) and Risk Scoring forum held
	Army CIO office team w/ NSA and DISA to stand up RD demo
	Jun: NSA and DISA successfully demo SCAP results populating iPost
2011	Mar: Completion of ARMOR reference implementation
	Jun: Lessons learned documented and submitted for publications
	Start to assess unstructured vs. structured data
	Aug: Initiated unstructured data project ARMOR-u

ARMOR Architecture


Assessment Results Auditing Tools
Network/Device Auditing Tool(s)
arf .xml
Network/Device Auditing Tool(s)
asr .xml
Data Transfer Mechanism for Assessment Results
Policy
SCAP Content
Assessment Results Repository and Reporting Service
service
arf .xml
Assessment Results Data Store
asr .xml
plaar .xml
web service
asr .xml
arf .xml
Assessment Results Metrics
Risk Metrics
Scoring Managment
service
Scoring Engine Database
Policy
Risk Scoring
Microsoft Patches
SCAP Standards NVD



ARMOR

Assessment Results Measure of Risk

DISA

my
- 9th SC (A)
  - 1st SB
  - 311th SC (T)
  - 335th SC (T)
  - 5th SC (T)
  - 7th SC (T)
    - 106th SB
    - 2nd SC
    - 7th SC
    - 93rd SB
      - Aberdeen Proving Gr
      - Anniston Army Depo
      - Blue Grass Army Dep
      - Camp Atterbury NEC
      - Carlisle Barracks NEC
      - Directorate of Logist
      - Fort AP Hill NEC
      - Fort Belvoir NEC
      - Fort Benning NEC
      - Fort Detrick NEC
      - Fort Devens NEC
      - Fort Drum NEC
      - Fort Eustis NEC
      - Fort Gordon NEC
      - Fort Hamilton NEC
      - Fort Jackson NEC
      - Fort Lee NEC
      - Fort McNair NEC
      - Fort Meade NEC
      - Fort Monmouth NEC
      - Fort Monroe NEC

Risk Scores

Army	SCM	VUL	PAT	SOE	AVS	UNM	Risk
Fort Belvoir NEC	3.36	20.57	5.21	2.56	0.00	2.56	34.25
Fort Detrick NEC	10.28	60.73	13.20	6.53	0.00	6.53	97.29
Fort Lewis NEC	7.74	44.65	10.12	4.87	0.00	4.87	72.24
Fort Lewis NEC	8.06	45.48	10.70	5.02	0.00	5.02	74.30
Fort Lewis NEC	8.39	46.32	11.29	5.18	0.00	5.18	76.35
Fort Lewis NEC	8.71	47.15	11.88	5.33	0.00	5.33	78.40
Fort Lewis NEC	9.04	47.98	12.47	5.48	0.00	5.48	80.46
Fort Lewis NEC	9.36	48.81	13.06	5.64	0.00	5.64	82.51
Fort Lewis NEC	9.68	49.65	13.65	5.79	0.00	5.79	84.56
Fort Lewis NEC	10.01	50.48	14.24	5.94	0.00	5.94	86.62
Fort Lewis NEC	10.33	51.31	14.83	6.10	0.00	6.10	88.67
Fort Lewis NEC	10.66	52.15	15.42	6.25	0.00	6.25	90.72
Fort Lewis NEC	10.98	52.98	16.01	6.41	0.00	6.41	92.78
Fort Lewis NEC	11.30	53.81	16.60	6.56	0.00	6.56	94.83
Fort Lewis NEC	11.63	54.64	17.19	6.71	0.00	6.71	96.89
Fort Lewis NEC	11.95	55.48	17.78	6.87	0.00	6.87	98.94
Totals	0.75	3.48	1.11	0.43	0.00	0.43	6.20

Page 1 of 3 >>

Score Card

B

Rank: 1st

Asset Management

Risk Score Distribution

Risk Score: 2500.9

Platform Distribution

Total Objects: 100

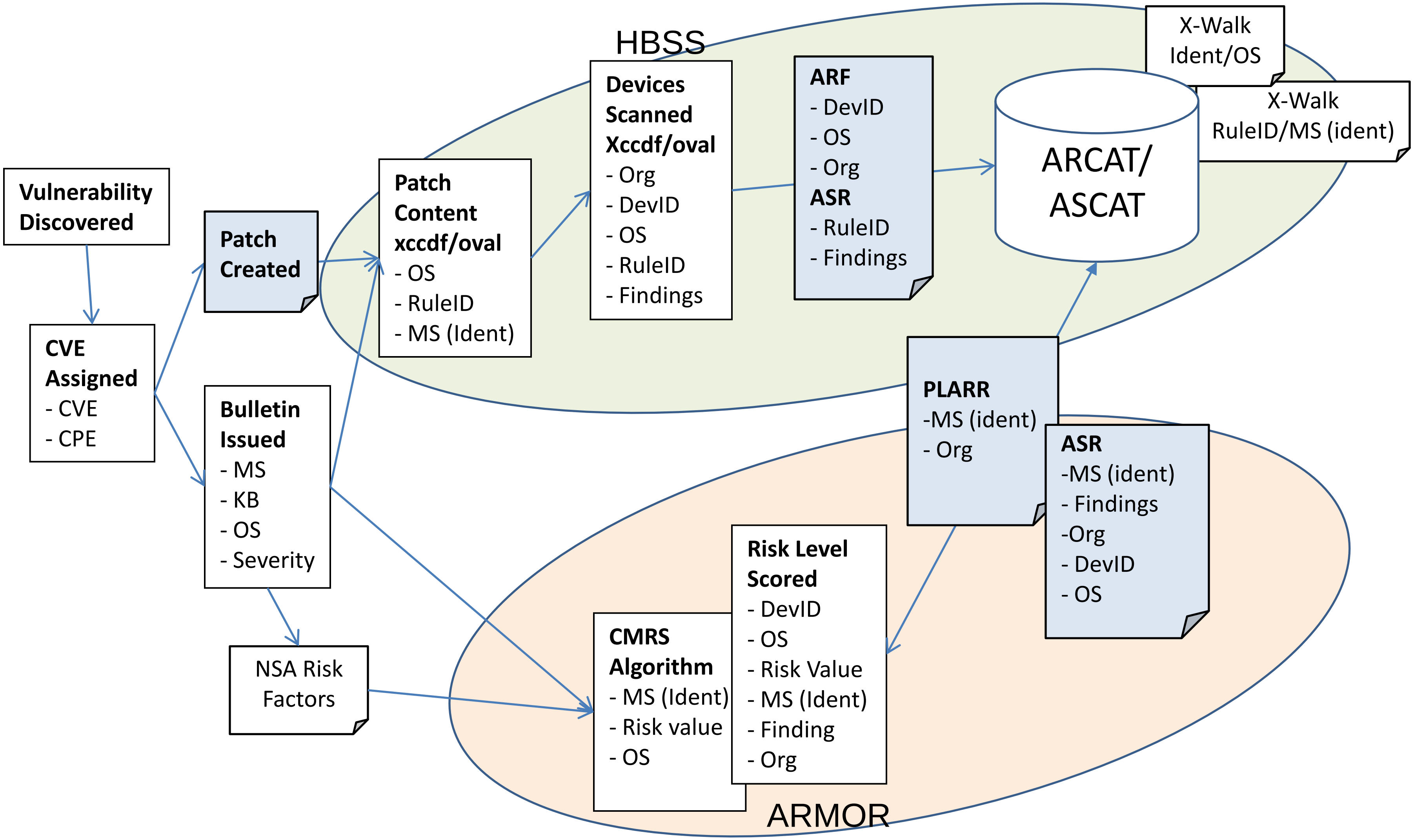
VUL Severity Distribution

Vulnerabilities: 1000

Top Three Impactors

Total Impact: 45

PAT (Patch)



Vulnerability Discovered

CVE Assigned
- CVE
- CPE

Patch Created

Bulletin Issued
- MS
- KB
- OS
- Severity

NSA Risk Factors

HBSS

Patch Content xccdf/oval
- OS
- RuleID
- MS (Ident)

Devices Scanned Xccdf/oval
- Org
- DevID
- OS
- RuleID
- Findings

ARF
- DevID
- OS
- Org

ASR
- RuleID
- Findings

ARCAT/ ASCAT

X-Walk Ident/OS

X-Walk RuleID/MS (ident)

PLARR
-MS (ident)
- Org

ASR
-MS (ident)
- Findings
-Org
- DevID
- OS

Risk Level Scored
- DevID
- OS
- Risk Value
- MS (Ident)
- Finding
- Org

CMRS Algorithm
- MS (Ident)
- Risk value
- OS

ARMOR

Lessons Learned

- **XCCDF/OVAL Content is Complex and Demanding**
  - Lacks rigid style guide and validation
  - Requires very specialized skill set
- **Enumerations Enable Risk Scoring**
  - Naming standards improve interoperability and reduce ambiguity
- **Data Exchange Standards Have Benefits and Drawbacks**
  - ARF/ASR allowed for ease of ingestion, but resource intensive

Lessons Learned

- **Metrics Enhance Situational Awareness and Improve Effective Mitigation**
  - Well engineered metrics drive desirable behaviors
- **Asset Visibility is Key**
  - Unknown device risk far outweigh risk of managed device
  - All other metrics depend on reliable asset inventory
- **Other Un-Assessable Device Attributes and Organizational Structure Gaps Inhibit Rollup**
  - Large organizations unable to delineate who owns vs. who manages devices

Current Research

- **Unstructured + Non-Relational Data Business Model**
  - Alleviate collection challenges through unstructured data collection
  - Alleviate structured databases overhead for large data continuous feeds
  - Produce more responsive/real-time displays
- **Further research into network device risk metrics**
- **Continuing development of risk scores (CCSS, SW)**
- **CAESARS Continuous Monitoring Reference Architecture**

Contact

James Park

NSA, CND R&T Team, Program Manager

410-854-8264

Dayna Harris

NSA, CND R&T Team, Software Engineer

410-854-2003