Security Standards in the Private sector

Aharon Chernin

Who am I?

- Aharon Chernin
- I work in the Financial Industry
  - Security Automation Program Manager
  - Vulnerability Management Program Manager
- Don't know of any other security automation programs outside of the federal government
- Fan of automation and standards (of course)
- I thrive on doing what people say cant be done
- Number two submitter to the Mitre OVAL repository – 2,339 OVAL definitions – Also on the OVAL board
- I enjoy spicy food

We've got some problems

- The private sector is not mandated to adopt standards
- The private sector may not have the vision required to see what security automation can provide
- The private sector just wants stuff "to work"
- The private sector may not care about SCAP validation
- Tool vendors may not fully entrench themselves into the automation standards unless there demand outside of the federal government
- Tool vendors are implementing government use cases for the standards

I've got some solutions

- The private sector problems can be resolved
  - Business cases
  - Education
  - Marketing
  - A "community"
- The private sector would then influence the tool vendors
  - Resistance is futile

- I ran into all these problems while attempting to implement in the private sector

Building the business case

- Move patching out of information security
- Move away from manual processes and spreadsheets
- Building a consolidated view of exposure
- CVSS Base scoring not created by the InfoSec department – less discussion with IT about how the score was derived
- See how and why a vulnerability was detected
- Stop ignoring false positives – Take ownership of the data
- Buy versus build options

- We must make the business case for standards and automation! Without one there will be no private sector demand, and limited vendor adoption.
- Without a business case *YOU* wont be adopting as well

Creating the standards vision

- If products used CPE
  - Software discovery tools could talk to vendor management/license compliance tools, vulnerability management tools, etc
  - Support teams could be assigned by CPE within the organization
- If products used OVAL
  - We could build/contract in house OVAL inventory definitions that could detect our custom applications and use them in any discovery tool
  - We could modify vulnerability definitions for our environment and use them in any vulnerability management tool
  - We could purchase feeds from vendor x and scan with vendor y
- If products used XCCDF
  - We could move from compliance tool to compliance tool without paying for professional services to "re-tool" our policy into the next tool
  - If we changed compliance tools, the findings would stay the same – saving remediation $$$$$
  - We could store baseline policy in XCCDF format for immediate consumption by tools, auditors, and policy management software

Why start a security automation program outside of the federal space?

- In-house standards evangelists
- We go out looking for manual processes to eliminate
- Our goal is objective security
- We write standards based information security policy
- Some projects –
  - Application security CWE/CWSS reporting
  - GEOIP Reporting
  - Interfacing IS products with IT products
  - Automated creation of threat indicator signatures
  - Automating the creation of vulnerability signatures
  - Information Security portals/dashboards/work flows
  - Skunkworks

Prerequisites

- Executive buy-in
  - Your business case
- Standards based (I wish) – Asset Management
  - Automation data without asset management data is not information
  - You should have at a minimum device support team and CIA risk ratings
- Standards based – Vulnerability remediation policy
- Standards based – Scanning solution
- Standards based – End user management solution

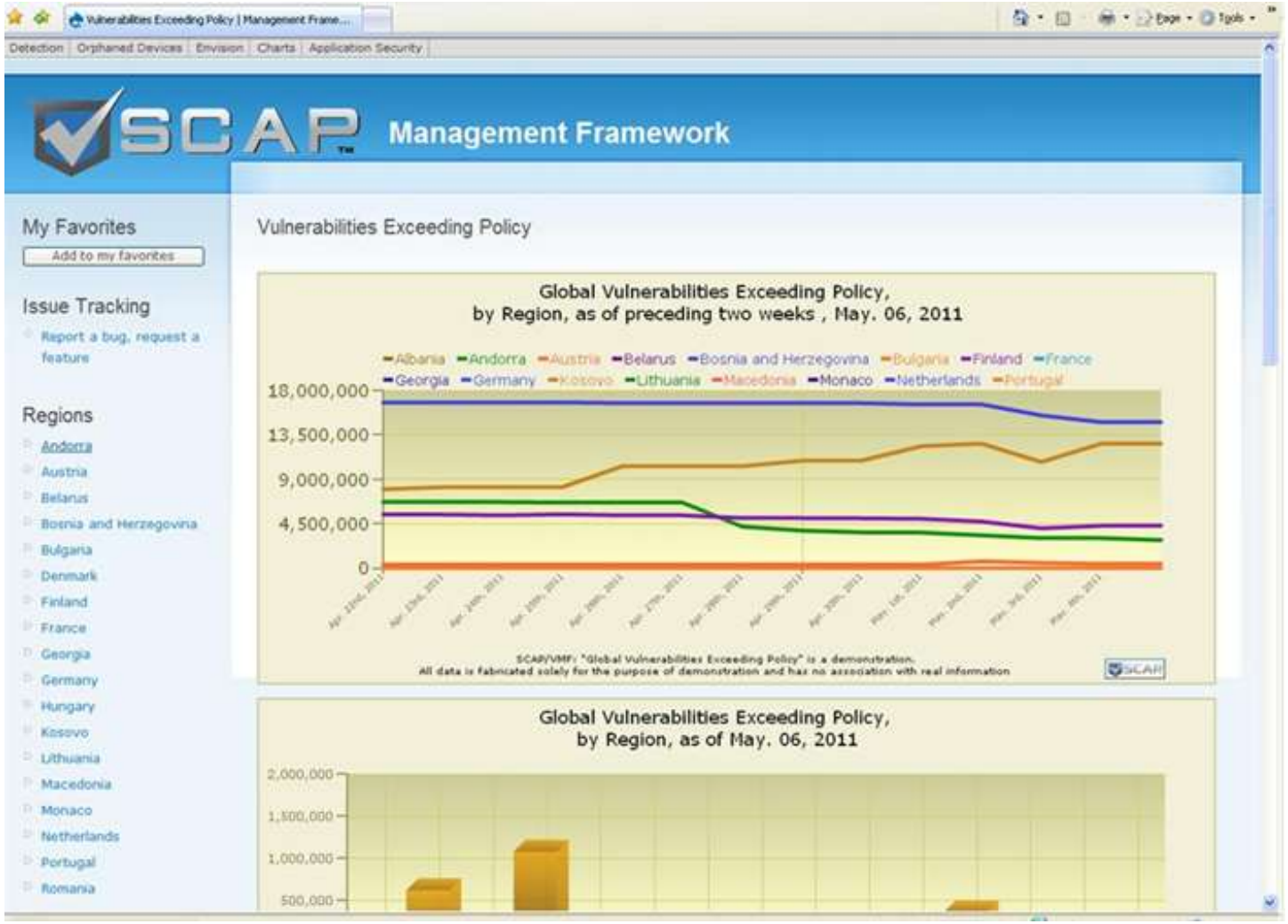
So how did I do it?

- Get IS out of IT
  - You cant measure device exposure by missing patch
  - Let the business manage their own patch policies
- Align vulnerability remediation policy
  - You can measure device exposure by vulnerability
  - High severity vulnerabilities should have faster remediation time frames than low severity (the obvious)
  - *All vulnerabilities should be remediated*
- Development of Exposure versus Performance concept
  - Performance is compliance to Vulnerability Remediation policy
  - Exposure is aggregated CVSS scoring without the lens of policy
- Risk view keeps the exposure footprint small and Performance view drives remediation of high severity exposures first
- Development of Detection versus Notification concept
  - Just because I cant detect it doesn't mean I shouldn't track it

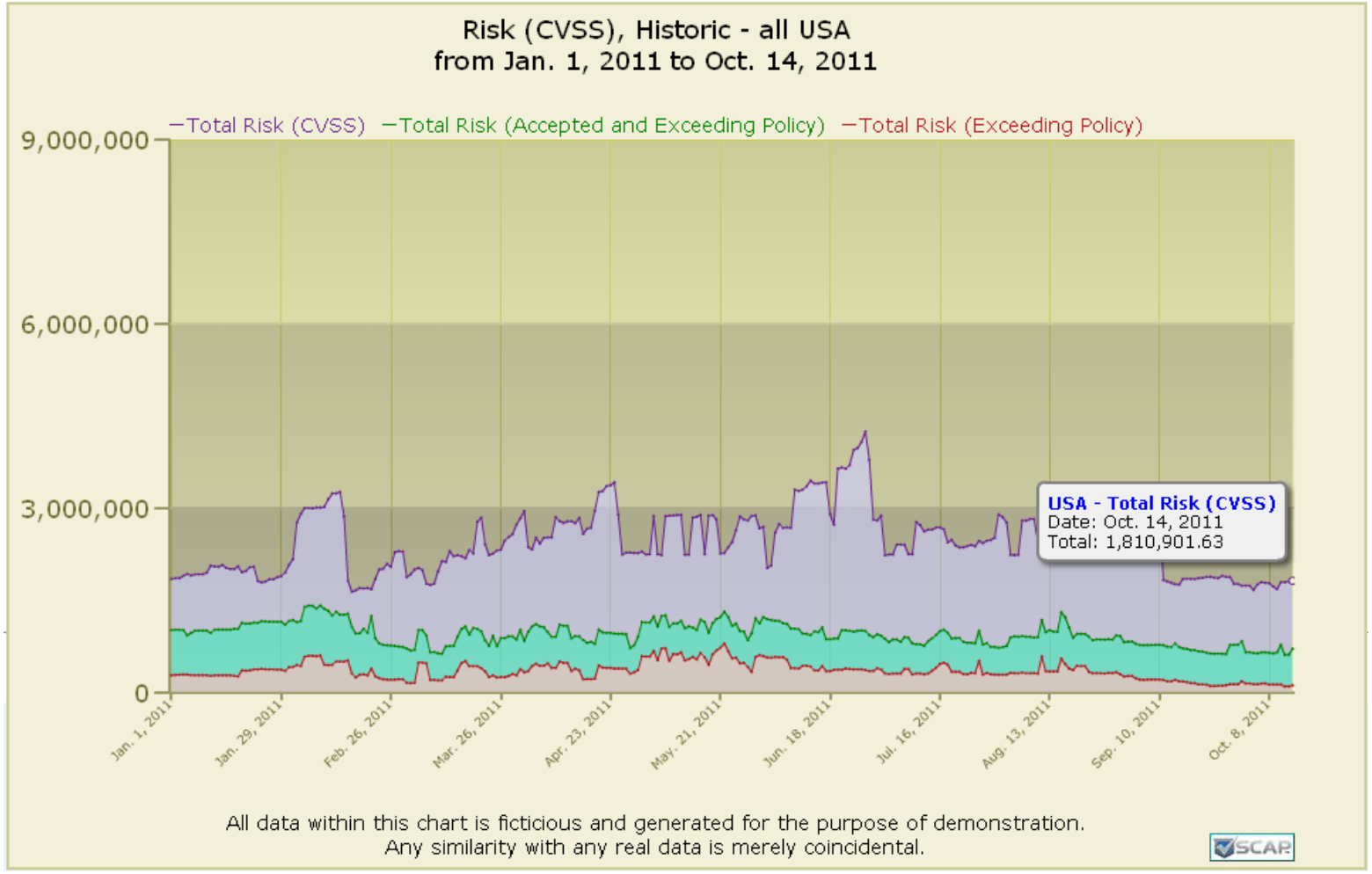
So how did I do it?

- Deploy OVAL interpreters to all platforms
- Integrate with Mitre OVAL repository and third party OVAL feeds
- Execute and return data
- Millions of rows of vulnerability data returned nightly
  - Made vulnerability data actionable
  - Modify a content management system into a vulnerability management system
- Vulnerability Management is now a compliance process
- Trust the process or forever be distracted

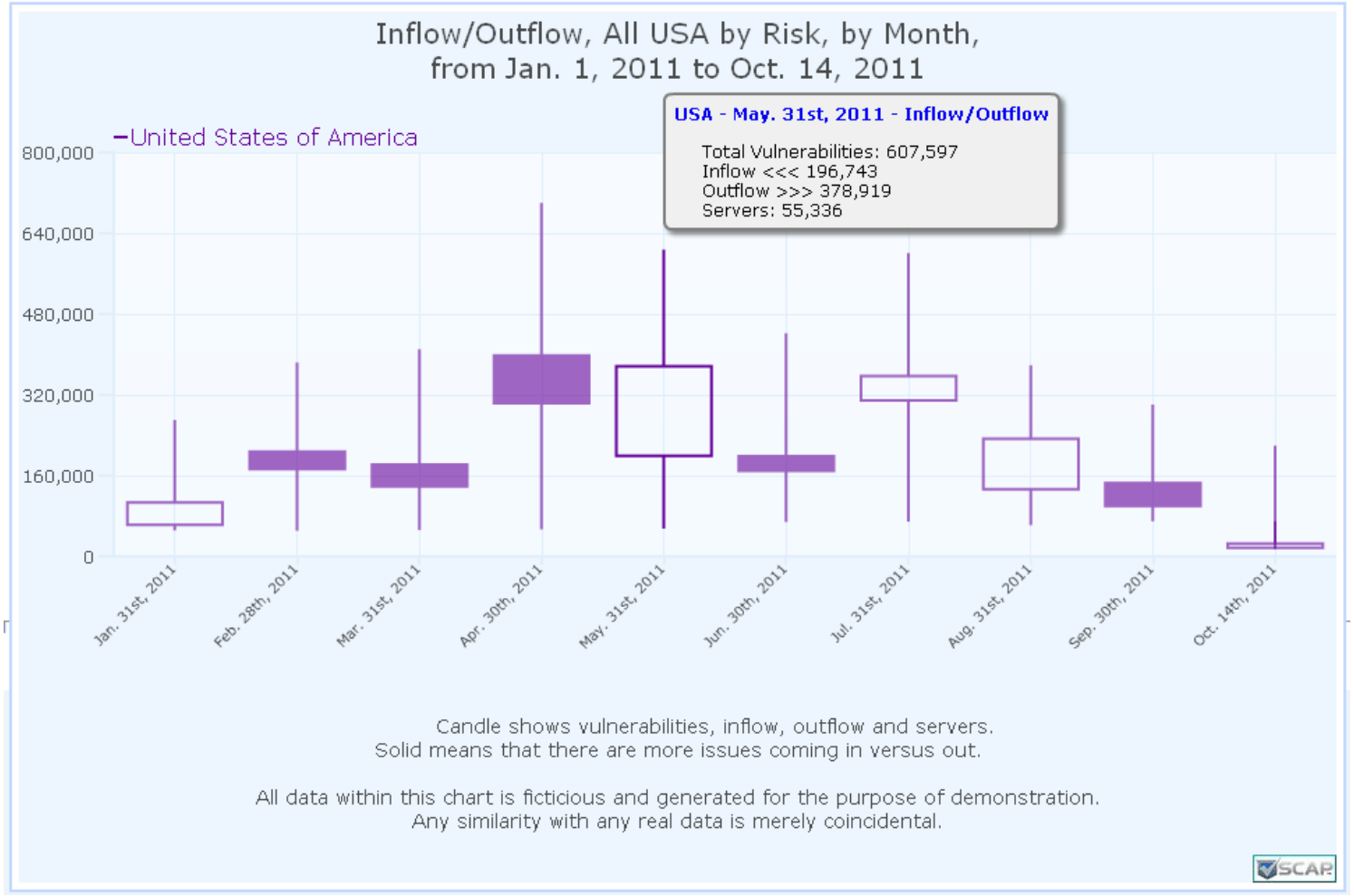
Vulnerability Management Framework



Vulnerability Management Framework



Vulnerability Management Framework



What is needed…

- Business case, marketing, and education
- Less focus on extending the standards and more focus on operationalizing the standards
  - Maybe even less standards
- Standardize the process of vulnerability management – more operationalizing!
- An unauthenticated scan OVAL schema
- A findings standard
  - How do I talk about an easily guessable password?
- **THREAT STANDARDS – Can I make this text bolder?**