Taking SCAP Beyond Compliance: Use cases to gaining better situational awareness

Tiffany Jones
Director, Public Sector Strategy and Programs
Symantec Corporation

Agenda

1. Threat Landscape & Situational Awareness Challenge
2. SCAP Trends
3. How SCAP Can “Change the Game”
4. Use Cases

Threat Landscape

- According to Symantec's latest Internet Security Threat Report, 70% of malicious code is designed to steal personal & confidential information. These threats log keystrokes, grab passwords, take account information, and send the information from your computer to a remote attacker.
- In 2008 Symantec created more than 1.6 million new malicious code signatures (more than Symantec has created in the last 17 years, combined.)
- On average we blocked almost 250 million attacks each month in 2008
- Threats are much more targeted and stealth

Situational Awareness Challenge

- Increasingly sophisticated and dangerous threats
- Given the sheer amount of data being produced to defend networks and systems, automation must play a critical role in the vulnerability, compliance and risk management lifecycle decision support process.
- However, in the process of quickly dealing with all these changes to our internal and external environments, enterprises have built silos and created piecemeal approaches that don’t allow visibility into the entire infrastructure or inform each other of
- Need to shift the focus of security from the infrastructure or devices to the information or data itself.

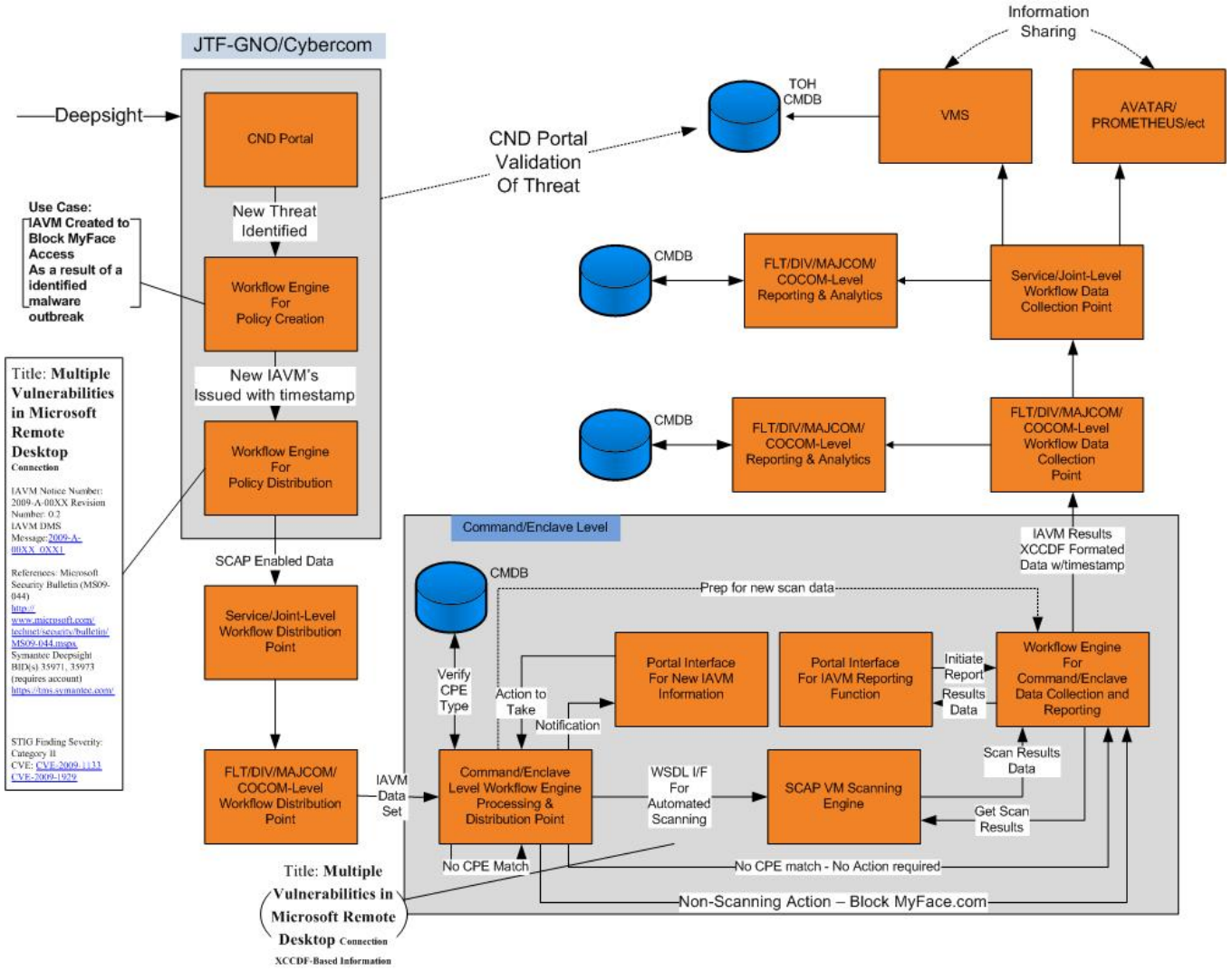
How SCAP Can "Change the Game"

- In order for organizations to develop true "Situational Awareness", the threat intelligence data received, the methodology by which systems are measured, scored and data created by those processes organizations must adopt process automation in order to have a comprehensive view of actions to achieve a "state of readiness" assessment for their enterprise.
- Common use of standardized enumerations makes it easier to use security tools, share information, develop situational awareness and issue guidance to address security issues.
- Evolve from **static verification** of a checklist to **real-time validation** of operational readiness. The current ideas and implementations for extending SCAP functionality to assist in this shift are working to improve and/or integrate the following theme activities: Vulnerability Risk, Baseline Health, Secure Operations, and Threat Risk. One can inform the others.
- Bottom line: Drive to real-time, automated, contextual, machine-to-machine action with continuous feedback loop

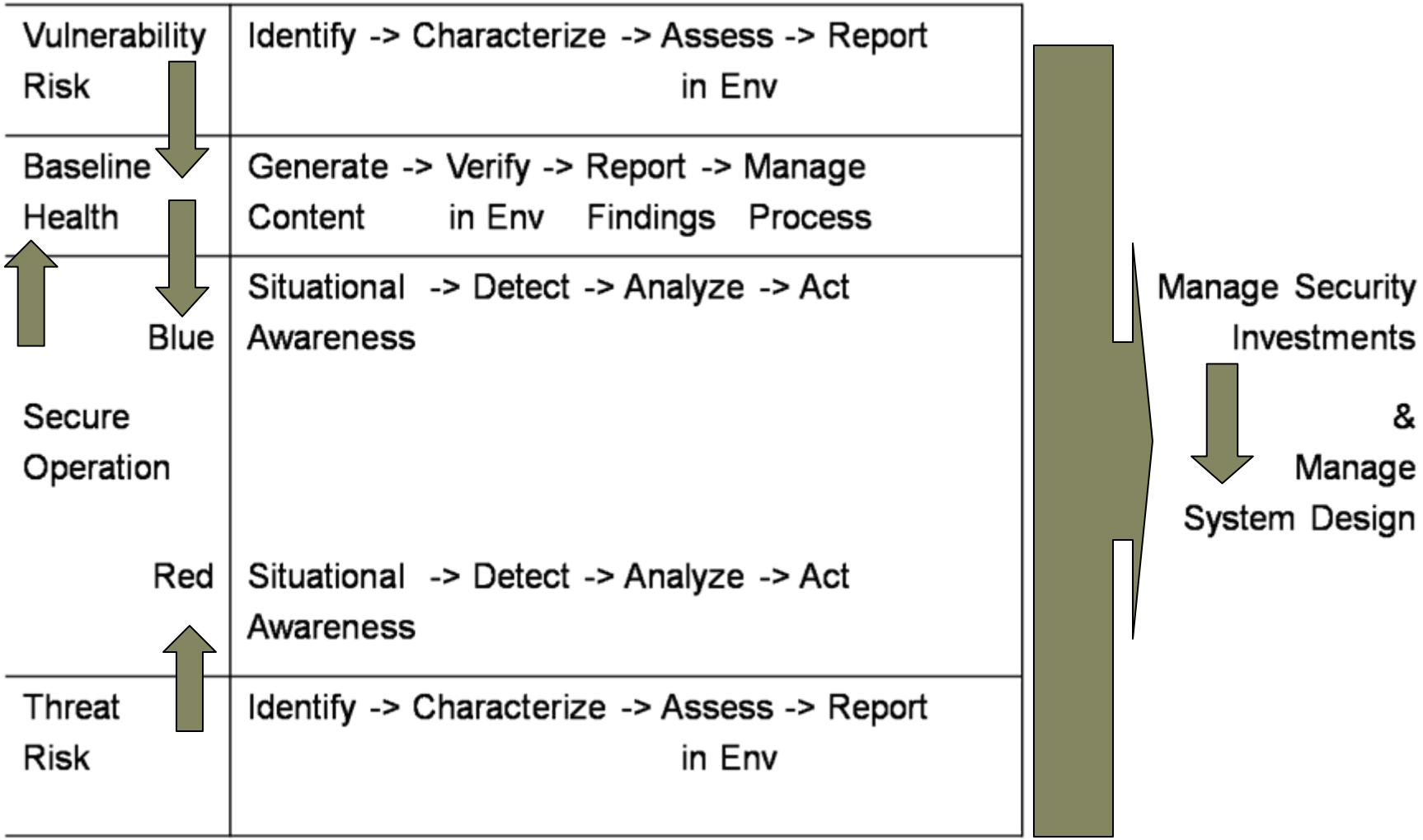
SCAP Trends

- FDCC
- Government requirement for SCAP in Compliance products and technologies
- Government requirements for SCAP in other products and technologies soon to follow
- “Operationalize Security”: a model that is risk-based, information centric, responsive and workflow driven.

Use Case: Automation of Security with Compliance



Use Case: Threat Risk Informs Secure Ops



Questions?

Tiffany Jones

Director, Public Sector Strategy and Programs

Symantec Corporation

Tiffany_jones@symantec.com

703-668-8853

Questions?