Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

December 7, 2011

Virginia Information Technologies Agency

ISOAG December 2011 Agenda

I.	Welcome & Opening Remarks	Michael Watson, VITA
II.	Cloud Security and Compliance	Jim Brigham, RSA
III.	Virtualizing Security Firewalls	Eric Taylor, NG
IV.	CSRM Panel Discussion	Benny Ambler, Bob Baskette, Michael Watson, VITA
V.	2011 Commonwealth Security Annual Report	Michael Watson, VITA
VI.	Upcoming Events & Other Business	Michael Watson, VITA
VII.	Partnership Update	Bob Baskette, VITA Michael Clark, NG

RSA

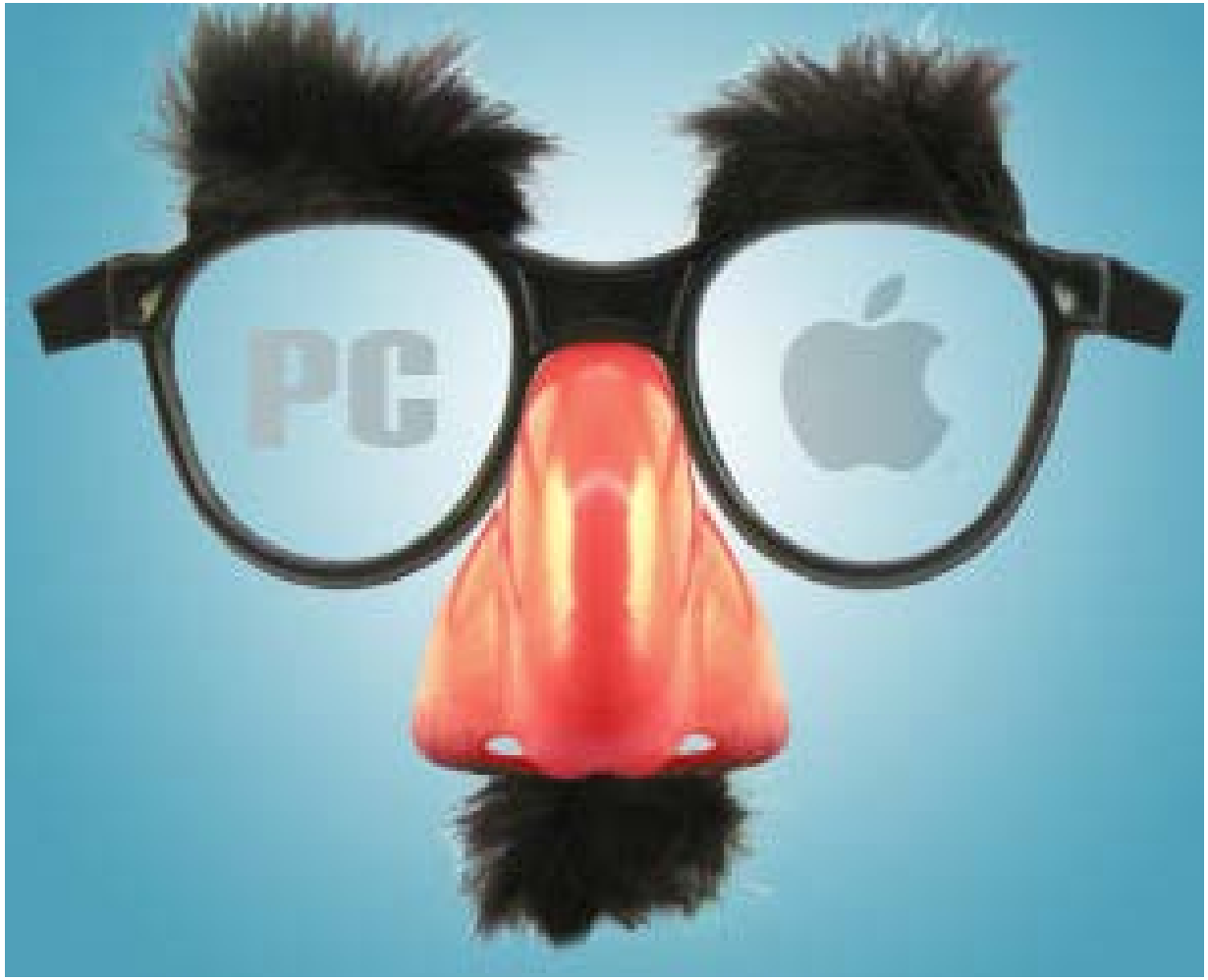
The Security Division of EMC

Cloud Security and Compliance

Jim Brigham, CISSP
Sr. vSpecialist
RSA Technical Evangelist
james.brigham@emc.com

Think Of Us As Your Sweet Tooth Fairy
DESSERTS

RSA®
The Security Division of EMC



RSA®
The Security Division of EMC

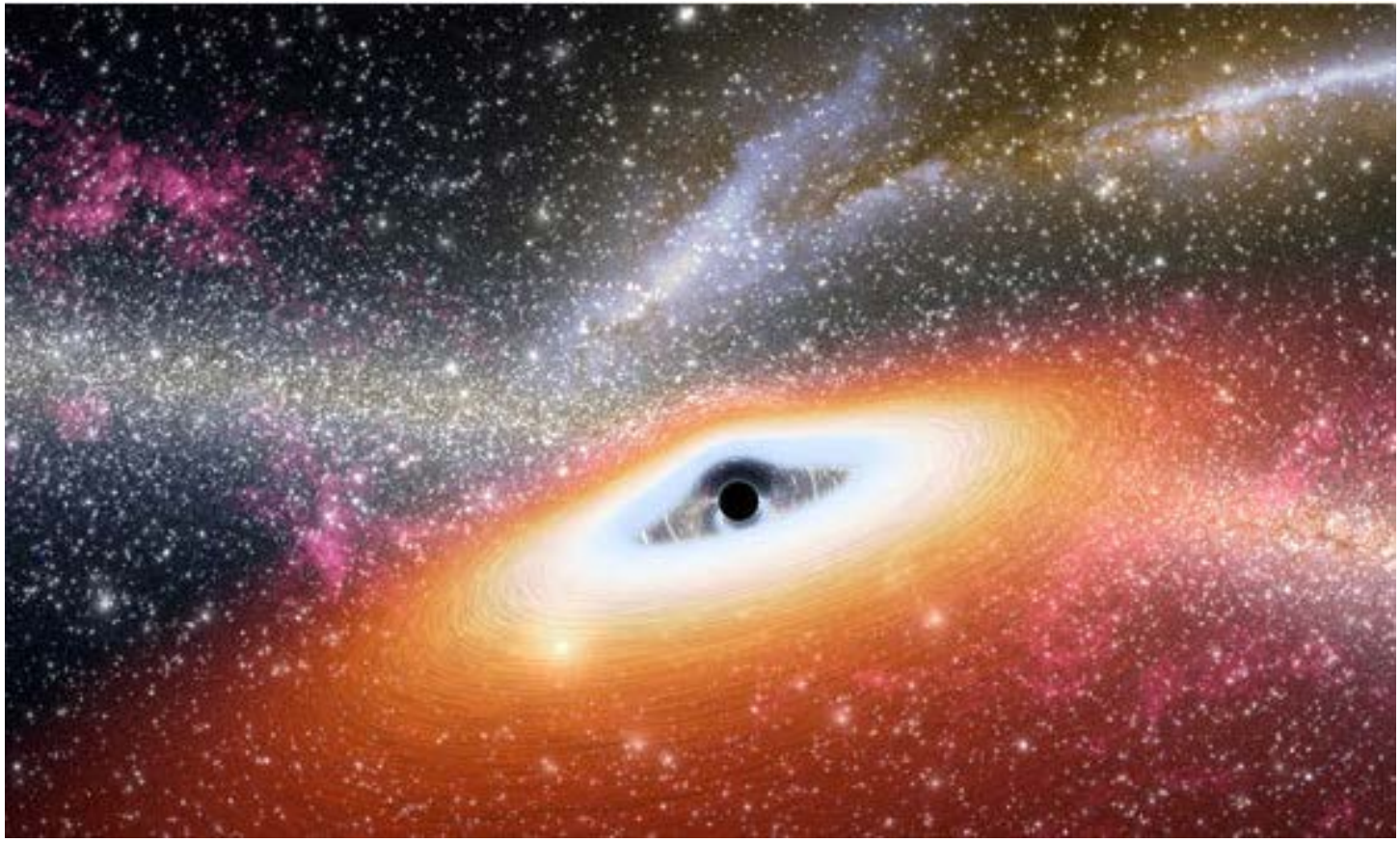
= Rain Thing

Good Rain Things

Bad Rain Things

What can make a good Rain Thing a BAD Rain Thing

A Black Hole aka Virtual Infrastructure



RSA
The Security Division of EMC

RSA
The Security Division of EMC

RSA®
The Security Division of EMC

RSA

The Security Division of EMC

vAdmin Goes Wild

Ex-vAdmin Goes Off the Deep End

On Feb 3, 2011 Biomed company Shionogi was shut down after a disgruntled ex-employee went to a McDonalds and using vCenter client on his laptop and using the free wifi from McDonalds, logged in remotely to vSphere and deleted 88 VM's running the company's email, order tracking, accounting and fulfillment, customer databases.

How this could be prevented

- Using a SIEM solution to monitor and alert for machines NOT sending logs, fire off an alert to security admin in real time
- Also using a SIEM to create an ex-admin's watchlist and when ex-employee attempted to connect via VPN, security admin could have been notified in real time and shut down the VPN
- RSA SecurID to force strong 2 factor authentication for accessing VPN and internal resources
- Appropriate MONITORED policies for suspending or deleting of credentials of ex-employee's using RSA Archer eGRC
- RSA Archer to map events to company policies and see that ex-employee's credentials were NOT terminated in timely fashion

- After The **Hack**, Should I Still Trust Google & The **Cloud** With My Data?
  searchengineland.com/after-the-google**hack**-33508

  by Danny Sullivan - In 50,810 circles
  Jan 14, 2010 – Over the past year, I've moved more and more of my data over to the **cloud** -- in particular, to being stored with Google. I'm rethinking that, in the **...**

Treasury Dept. has **cloud hacked** | Government Security News
www.gsnmagazine.com/article/.../treasury_dept_has_**cloud_hacked**
May 10, 2010 – Treasury Dept. has **cloud hacked ...** The Treasury Department was **hacked** last week, leaving the Web site for its Bureau of Engraving and **...**

LastPass Possibly **Hacked**, **Cloud** Security Concerns on the Rise **...**
www.**cloud**tweaks.com/.../lastpass-possibly-**hacked-cloud**-security-co...
May 5, 2011 – LastPass Possibly **Hacked**, **Cloud** Security Concerns on the Rise Conspiracy theory admirers will be happy to hear the news that today, **...**

Cloud 9 **Hacked** | ArcadePreHacks.com
www.arcadepre**hacks**.com/game/14565/**Cloud**-9.html
2 days ago – Hackbar: Press [1] Toggle Invincible - [2] Toggle Fall Safety - [3] Double Jump - [4] Wings - [5] Slowfall.

RSA
The Security Division of EMC

How Do We Make a Good Rain Thing?

The Journey To Your Rain Thing

Three-phases to delivering IT-as-a-service

Phase I	Phase II	Phase III
IT Production *Efficiency*	**Business Production** *Quality of Service*	**IT-as-a-Service** *Agility*
IT-owned applications	**Mission-critical applications**	**Run business**

Secure hybrid clouds(trusted multitenancy, chain of trust

Security compliance, information-centric security, risk-driven policies, IT and security operations alignment

Visibility into virtualization infrastructure, privileged user monitoring, access management, network security

RSA
The Security Division of EMC

Our Customer Are Asking Themselves

- Can I ensure my virtualized business critical applications are running in a secure and compliant environment?
- How do I centrally manage compliance across mixed VMware and physical IT environments?
- Can I respond more quickly to security events in my virtual environment?
- How do I begin to assess hybrid and public cloud service providers?

Implications of Challenges

CISOs need to manage security and compliance across virtual and physical IT

Security and compliance concerns stall the adoption of virtualization

Missing opportunity for "better than physical" security

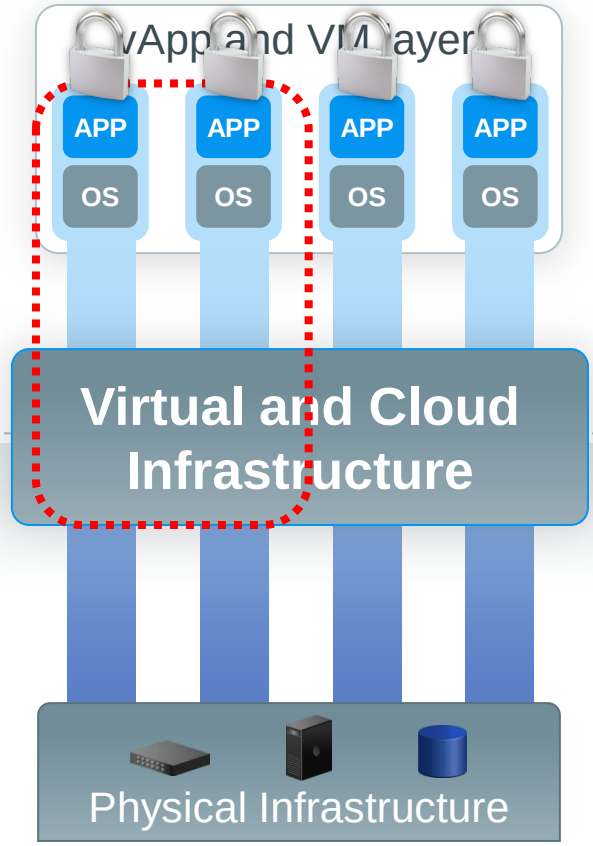
Opportunity for More Effective Security by Pushing Enforcement Down the Stack

Today most security is enforced by the OS and application stack. This is:

- Ineffective
- Inconsistent
- Complex

Building in information security enforcement in the infrastructure layer ensures:

- Consistency
- Simplified security management
- Enables customers to surpass the levels of security possible in today's physical infrastructures



RSA
The Security Division of EMC

RSA®

The Security Division of EMC

www.rsa.com/securecloud

Thank you!

Virtualizing Security Firewalls

IT Infrastructure Partnership Team

Eric Taylor

Senior Cyber Architect

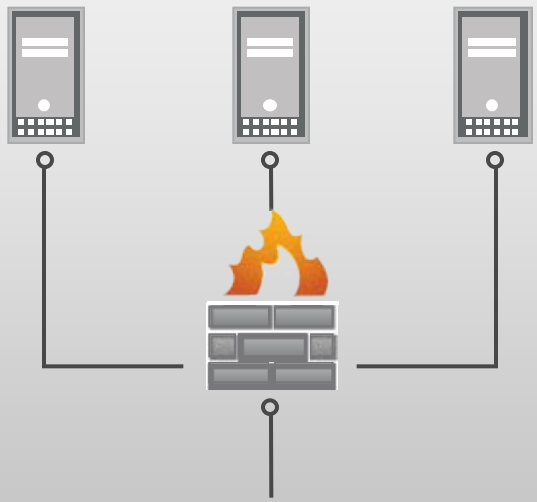
December 7, 2011

Business Case for Virtual Security

- Virtualization technology has enabled IT to consolidate compute resources on fewer servers while improving the utilization as well as providing flexibility and agility in the deployment of virtual resources.
  - Firewall Choke Point and Unscalable Architecture
  - Visibility
  - VLAN Issues
  - Firewall Rule Sprawl and Management Concerns
  - Rigid Infrastructure and Fixed-Capacity Physical Devices

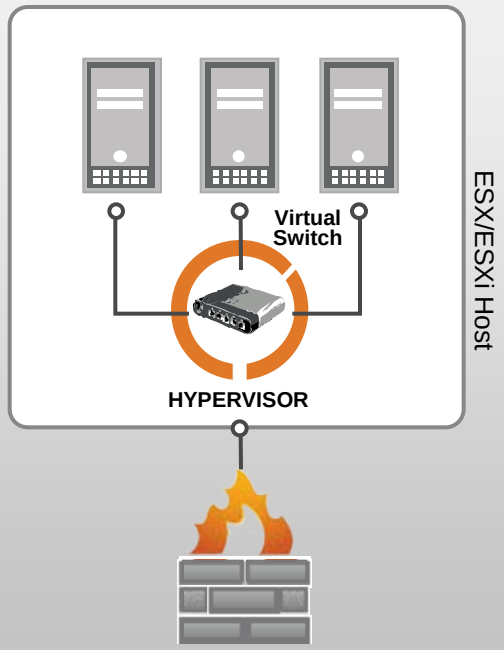
Security Implication of Virtualization

Physical Network



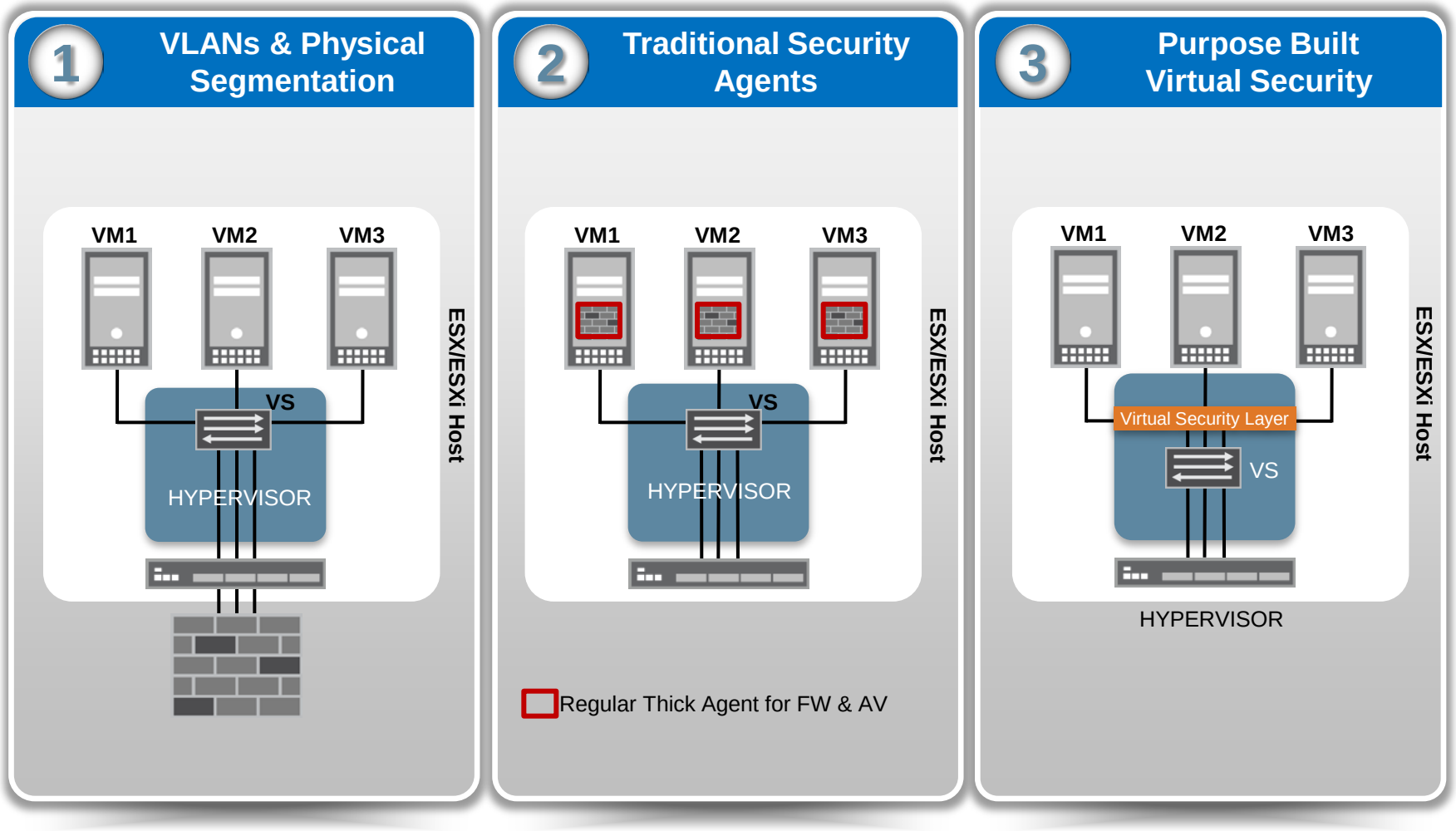
Firewall/IDS Sees/Protects All Traffic between Servers

Virtual Network



Physical Security Is “Blind” to Traffic between Virtual Machines

Approaches to Securing Virtual Networks



Key Elements

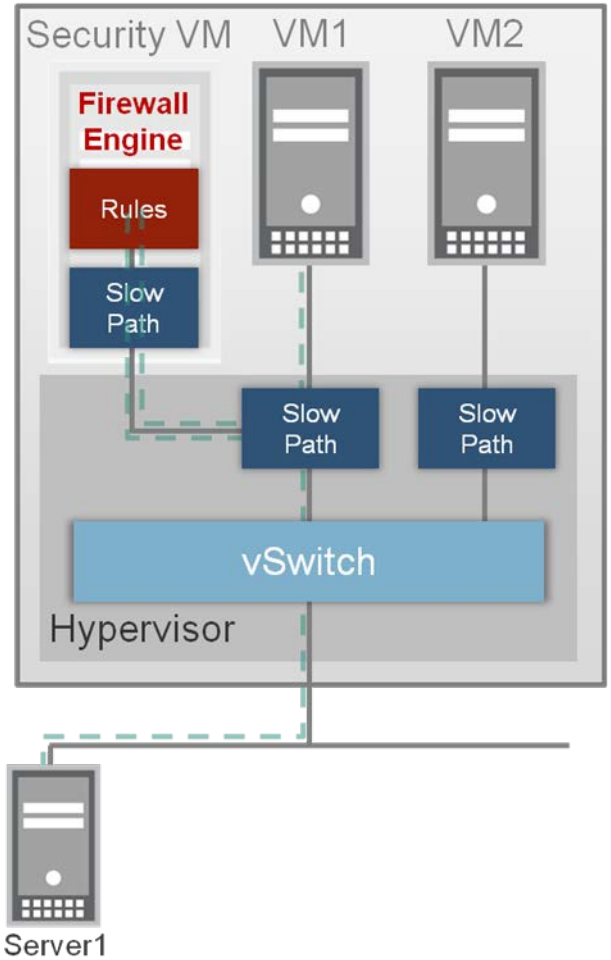
- Solution Scalability
- Policy Mobility
- Performance
- Traffic Monitoring and Visibility
- Automated Security
- VMsafe Implementation
- Management Scalability
- High Availability
- Physical Security and Networking Integration
- VMware Endpoint Security **(EPSEC)**
- Compliance (PCI, etc)

Partner ecosystem program delivered by Vmware [1]

- vCompute (CPU and Memory) API
  - Inspect memory access and CPU states before any code is actually executed.
- VDDK API (for disk block inspection)
  - Capability for creating applications to manage virtual storage
  - Think anti-virus security products, compliance checking, file integrity and change control monitoring
- vNetwork Appliance (DVFilter) API
  - Protect network packet streams
  - Network packet filter is inserted between the vNIC and virtual switch (vSwitch).
  - Two possible agents that can be used. These agents are referred to as the **fast-path** agent and **slow-path** agent, which make up the "filter"

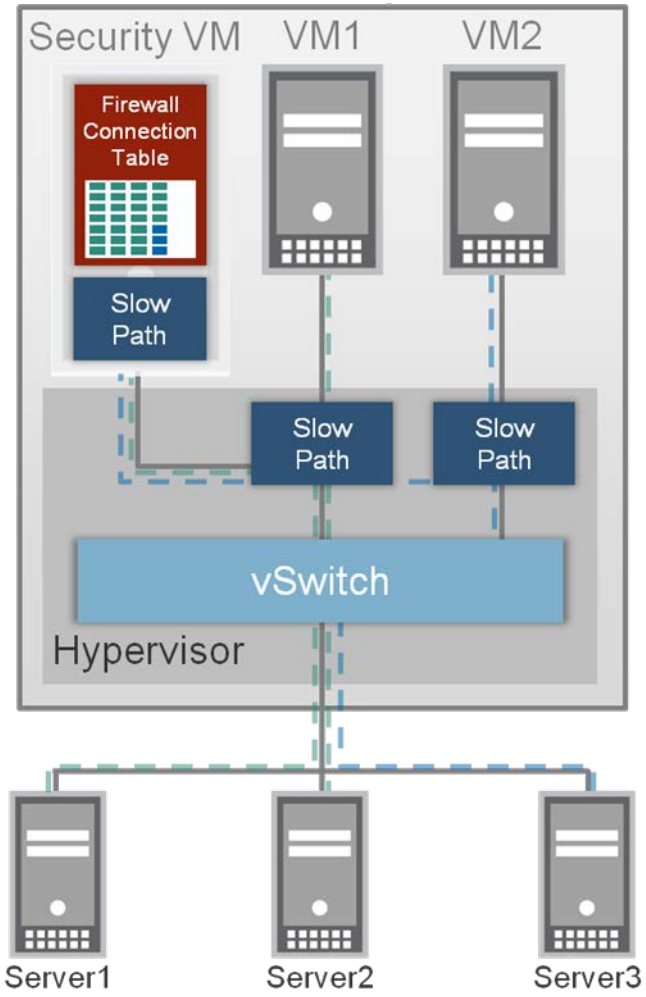
VMware Slow Path Hybrid Model

- Forward packets to a VM in order to do all or part of the processing
- Introduces performance penalty in the transfer of the packets into the Security VM
- Could also introduce of failure points in your architecture for traffic processing
- Many times this requires single monolithic rule base



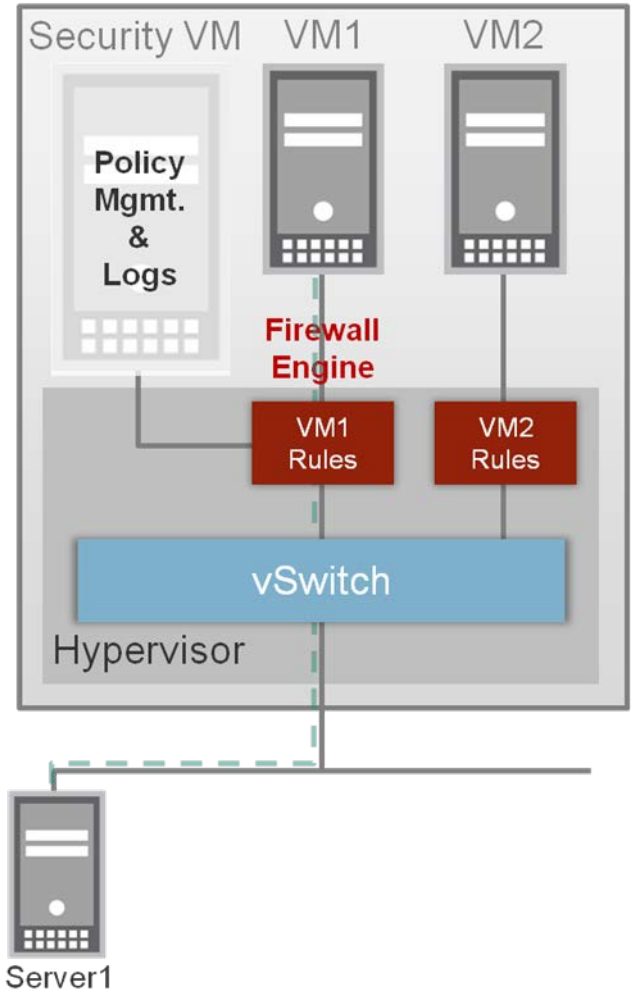
Shared Connection Table in Slow Path Products

- A single connection table that holds information about all the communication between systems (sessions)
- Single table is it can get very large
- Sessions and rules become CPU bound on the “Security VM”
- A handful of systems with high session rates can impact the firewall performance for all systems being protected.



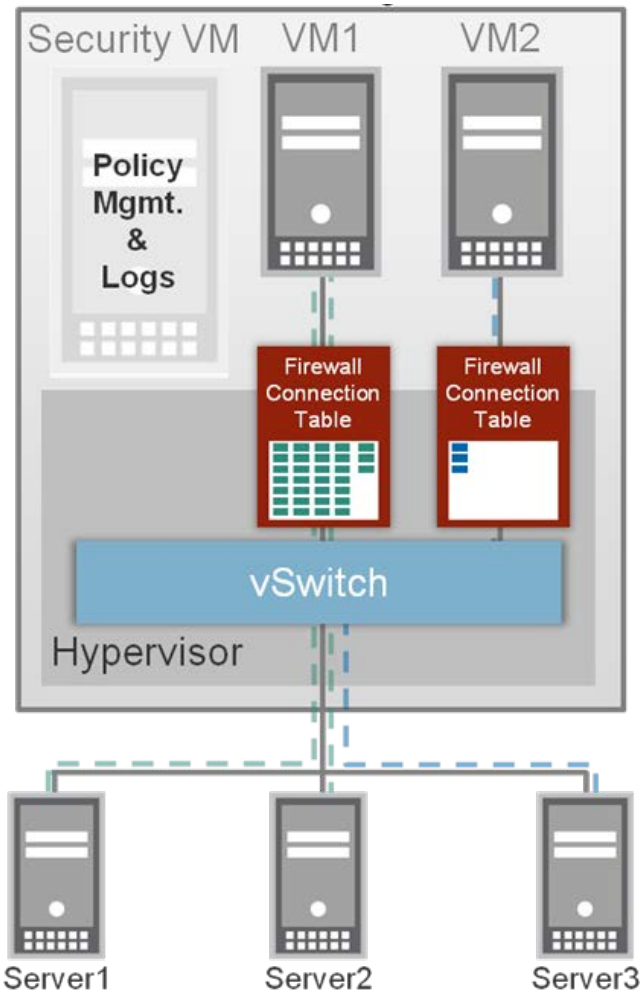
VMware Fast Path Model

- Using the Fast Path approach provides the best possible performance because packets don't have to be forwarded into a "Security VM" for processing.
- Rules processing does not become CPU bound on the "Security VM"
- A firewall engine built completely in the hypervisor as a kernel module
- Allows for relevant rules for each VM



Separate Connection Tables and Firewall Engines

- Fast Path mode avoids forwarding packets up to a VM for processing
- Allows for firewall connection tables to be distributed
- The connection table enables the start of a session to be validated instead of doing intensive analysis on every single packet.
- Isolation of the connection table is key to high-performance firewall processing.
- In the hypervisor, the connection table size is not a limiting factor



Other Considerations

- Service Provider & Enterprise Grade
  - Three Tiered Model
  - VMware Certified (signed binaries!)
  - Fault-tolerant architecture (i.e., HA)
- Policy Mobility
  - Virtualization-aware
  - “Secure VMotion”
  - Rules Follow VM
- Automated Security
  - “Auto Secure” detects/protects new VMs
  - VDDK API to inspection VM for automation of rule

Other Considerations

- Granular, Tiered Defense
  - Stateful firewall, integrated IDS, and AV
  - Flexible Policy Enforcement – zone, VM group, VM, individual vNIC
- High Availability
  - Security VM
  - Management VM
- Traffic Monitoring and Visibility
  - PCAP
  - SPAN Port
  - NetFlow / sFlow
- Compliance
  - Inspection
  - Reporting

Reference

- [1] - What actually is VMsafe and the VMsafe API?
  - http://blogs.vmware.com/vcloud/2010/04/what-actually-is-vmsafe-and-the-vmsafe-api.html
- The Technology Foundations of VMware® vShield
  - http://www.vmware.com/files/pdf/techpaper/vShield-Tech-Foundations-WP.pdf

Questions

Virginia Information Technologies Agency

CSRM Panel Discussion

Benny Ambler, Sr Mgr Security Governance

Bob Baskette, Sr Mgr Security Operations & Architecture

Michael Watson, Acting Chief Information Security Officer and Sr Mgr IT Risk Management

Virginia Information Technologies Agency

2011
Commonwealth Security Annual Report
as of
December 5, 2011

Michael Watson
Acting Chief Information Security Officer

§ 2.2-2009

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.

Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011 - Percentage of CAPs Received	2011 - Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

Acronyms:

ISO: Information Security Officer
IS: Information Security
CAP: Corrective Action Plan
CISO: Chief Information Security Officer of the Commonwealth

ISO Designated: The Agency Head has

Yes - designated an ISO with the agency within the past two years
No – not designated an ISO for the agency since 2006
Expired –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

Attended IS Orientation:

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

Security Audit Plan Received: The Agency Head has

Current - submitted a Security Audit Plan for the period of fiscal year (FY) *2011-2013 or 2012-2014* for systems classified as sensitive based on confidentiality, integrity or availability *(Note: after July 1, 2011, Audit Plans submitted shall reflect FY 2012-2014)*

No - not submitted a Security Audit Plan since 2006

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

Expired –submitted a Security Audit Plan on file that does not contain the current three year period FY *FY 2011-2013 or FY 2012-2014*

Pending –submitted a Security Audit Plan that is currently under review

2011 - Percentage of CAPs Received: The Agency Head or designee has

% – submitted % of CAPs for planned audits listed on submitted Audit Plan

N/A - not had Security Audits scheduled to be completed

Pending –submitted a Corrective Action Plan that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

2011 - Percentage of Quarterly Updates Received: The Agency Head or designee has
% – submitted % of quarterly status updates received for corrective actions resulting from Security Audits previously conducted by or on behalf of the agency
N/A - no open Security Audit findings
Pending - submitted quarterly status update that is currently under review

Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- Percentage of CAPs Received	2011- Percentage of Quarterly Updates Received	3 year - Percentage of Audit Obligation Completed
XYZ	Yes	5	Current	90%	75%	100%

3 year - Percentage of Audit Obligation Completed:

Percent of sensitive systems reported by 2008 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *"At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years."*

Agencies that did not submit an IT Security Audit Plan by 2008 were not in compliance and therefore there is no data to report on for 2011.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

N/C – agency not in compliance by 2008, agency did not submit an IT Security Audit Plan by 2008

Pending – currently under review

Exception – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

FAQ!

What should an agency do if they conduct a Security Audit that results in no findings?

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?

December 31, 2011

Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CB	Yes	0	Expired	0	N/A	0
DGS	Yes	0	Current	N/A	N/A	0
DHRM	Yes	0	Current	0	N/A	100
DMBE	Yes	1	Expired	N/A	N/A	0
EDR	Yes	1	Current	100	100	100
HRC	Yes	1	Current	N/A	N/A	100
SBE	Yes	1	Expired	N/A	0	50

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOF	Yes	1	Current	100	N/A	100
VDACS	Yes	1	Current	100	100	100

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
BOA	Yes	1	Current	N/A	N/A	0
DBA	Yes	0	Expired	N/A	N/A	0
DHCD	Yes	0	Current	100	100	33
DMME	Yes	5	Current	50	0	57
DOLI	Yes	0	Expired	0	N/A	0
DPOR	Yes	1	Expired	N/A	0	100
TIC	Yes	0	Expired	0	N/A	0
VEC	Yes	0	Expired	25	50	11.11
VEDP	Yes	0	Expired	0	N/A	0
VRA	No	0	Expired	N/A	N/A	N/C
VRC	Yes	1	Current	100	N/A	100

* VEDP includes VTA and VNDIA

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
CNU	Yes	1	Current	0	N/A	0
DOE	Yes	1	Current	100	25	76.12
FCMV	Yes	0	Expired	N/A	N/A	100
GH	Yes	1	Expired	N/A	N/A	0
JYF	Yes	0	Current	N/A	100	100
LVA	Yes	0	Expired	0	N/A	100
NSU	Yes	4	Expired	N/A	N/A	0
RBC	Yes	1	Current	50	N/A	100
SCHEV	Yes	0	Expired	0	N/A	0
SMV	Yes	0	Expired	0	N/A	0
SVHEC	No	0	Expired	N/A	N/A	N/C
UMW	Yes	1	Current	50	33.33	80
VCA	Yes	0	Expired	N/A	N/A	100
VMFA	Yes	2	Expired	N/A	0	50
VSDB	Yes	0	Current	0	N/A	0
VSU	Yes	0	Expired	100	36.36	77.78

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CS&RM .

Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DOA	Yes	1	Current	0	0	25
DPB	Yes	0	Expired	N/A	0	100
TAX	Yes	0	Current	Pending	Pending	Pending
TD	Yes	0	Current	Pending	N/A	Pending

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
*DBHDS	Yes	1	Current	N/A	0	100
DHP	Yes	2	Current	0	N/A	0
DMAS	Yes	2	Current	N/A	N/A	0
*DRS	Yes	2	Current	60	48.15	45
DSS	Yes	5	Current	0	50	22
VDH	Yes	0	Current	N/A	58.33	21
VFHY	Yes	0	Current	N/A	N/A	100

* DBHDS includes VCBR
* DRS includes DBVI, VDA, VDDHH,VBPD and WWRC

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DCR	Yes	0	Current	100	75	67
DEQ	Yes	2	Current	0	N/A	100
DGIF	Yes	3	Current	0	N/A	0
DHR	Yes	0	Expired	0	N/A	0
MRC	Yes	1	Current	100	50	100
VMNH	Yes	0	Expired	0	N/A	0

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Virginia Information Technologies Agency

Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
ABC	Yes	3	Current	Pending	Pending	100
CASC	Yes	0	Expired	N/A	N/A	100
DCE	Yes	2	Current	0	57.14	50
DCJS	Yes	1	Expired	0	N/A	0
DEM	Yes	2	Current	N/A	N/A	0
DFP	Yes	0	Current	N/A	100	100
DFS	Yes	0	Pending	Pending	N/A	0
DJJ	Yes	2	Current	N/A	100	66.67
DMA	Yes	0	No	N/A	N/A	N/C
*DOC	Yes	4	Expired	71.43	100	59
*DVS	Yes	1	Current	100	N/A	100
VSP	Yes	0	Current	100	100	83%

*DOC includes VPB
*DVS includes VWM

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IEIA	Yes	2	Expired	0	N/A	0
VITA	Yes	1	Current	100	100	50

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
DMV	Yes	1	Current	0	0	100
DOAV	Yes	2	Expired	0	N/A	0
DRPT	Yes	0	Expired	N/A	N/A	0
MVDB	Yes	0	Expired	N/A	N/A	100
VDOT	Yes	2	Current	Pending	Pending	Pending
VPA	No	0	No	N/A	N/A	N/C

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
IDC	Yes	4	Current	N/A	80	100
SCC	Yes	2	Current	66.67	50	50
SLD	Yes	2	Expired	0	N/A	0
VCSP	Yes	1	Current	N/A	N/A	100
VOPA	Yes	1	Current	0	N/A	0
VRS	Yes	0	Pending	Pending	Pending	Pending
VWC	Yes	1	Current	N/A	N/A	17

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	2011- CAPs Received	2011- Quarterly Updates	3 Year Percentage of Audit Obligation Completed
GOV	Yes	0	Expired	N/A	N/A	N/A
OAG	Yes	2	Expired	N/A	N/A	N/A

NOTE: Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact CommonwealthSecurity@VITA.Virginia.Gov

Upcoming Events

General Assembly

General Assembly convenes January 11, 2012

(Even number year = regular session)

AITR Meeting

AITR Meeting:

Wednesday, December 14th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC

MS-ISAC

MS-ISAC Partnership with SANS Institute for Security Training

The MS-ISAC has a new 2012 partnership agreement to provide discounted pricing for state, local, territory and tribal governments, including government partner entities and educational institutions, during specific timeframe.

Visit MS-ISAC web for more information:

http://msisac.cisecurity.org/resources/videos/sans-training.cfm

Virginia Information Technologies Agency

MS-ISAC

National Webcast Initiative

Thursday, Dec 15

2:00 pm – 3:00 pm EDT

Topic: **Social Networking: The Latest Security Issues and How to Manage Them**

Visit MS-ISAC web for more information:

http://www.msisac.org/webcast/

Information Security System Association

ISSA

DATE: Wednesday, Dec 14, 2011

LOCATION: Maggiano's Little Italy
11800 West Broad Street, #2204, Richmond, VA 23233
TIME: 11:30 - 1:00pm. Presentation starts at 11:45.
Lunch served at 12.
COST: ISSA Members: $20 & Non-Members: $25

SPEAKER: TBD

TOPIC: TBD

Virginia Information Technologies Agency

2011 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials!

http://www.vita.virginia.gov/security/toolkit/

New materials are available at the back of today's meeting room. Please help yourself!

For printing cost estimates you can contact DMV's Damian McInerney at (804)367-0925 or email: damian.mcinerney@dmv.virginia.gov

Thank you DMV!

Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - January 4, 2011

Speaker: Patrick Gray, Principal Security Strategist at Cisco Systems

Wednesday - February 1, 2012

Speaker: Marc Gaudette, Director, IT Risk Mgmt, Dominion

Upcoming:

March – Dave Marcus, McAfee on Challenges in today's environment

April – Laurie Jarrett, VCU on Grant Writing

ISOAG will be held the 1st Wednesday of each month in 2012

Future IS Orientation Sessions

Tuesday - February 7, 2011 1:00 – 3:30p (CESC)

Email CommonwealthSecurity@VITA.virginia.gov if you are interested in attending.

IS Orientation is now available via webinar!

Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to: **CommonwealthSecurity@VITA.Virginia.Gov**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

December 7, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN