Windows Server 2012

What’s New about Security and Hypervisor

Prinya Hom-anek

CGEIT, CRISC, CISSP, CSSLP, CISA, CISM, CBCI, CFE, SSCP,
ITIL Expert V3, SANS GIAC GCFW, IAPP CIPP Foundation
IRCA: ISMS Lead Auditor, BCMS Auditor

(ISC)2 Asian Advisory Board;
ISACA - Bangkok Chapter Committee, ITSMF Thailand Board,
Thailand Information Security Association (TISA) Committee,
ACIS Professional Center Co., Ltd. , President and Founder
The Microsoft Hybrid Cloud
Easy to switch

Server Core

Minimal Server Interface

GUI

Desktop Experience

Add/remove Feature

Graphical Management Tools and Infrastructure

Server Graphical Shell

Desktop Experience

PowerShell

Install-WindowsFeature

Server-Gui-Mgmt-Infra

Server-Gui-Shell

Desktop-Experience

Uninstall-WindowsFeature
Windows Server 2012 DirectAccess – Simple?

• When a DirectAccess client connects to the Internet it is automatically connected to the corporate intranet
  • No user action required

It’s a truly great user experience  - But...
Tunnelling technologies for the Internet and intranet to support IPv6 over IPv4
Internet tunnelling selection based on client location – Internet, NAT, firewall
Encryption/authentication of Internet traffic (end-to-edge/end-to-end)
PKI required
Client location detection: Internet or corporate intranet
Certificates require PKI
“Building your own cloud just got a lot easier with Windows Server 2012”.
Did you know?

• 9.9 billion messages a day via Windows Live Messenger
• 600 million unique users every month on Windows Live & MSN
• 500 million active Windows Live IDs
• 40M paid MS Online Services (BPOS, CRM online, etc.) in 36 Countries
Did you know?

- 5 petabytes of content served by Xbox Live during Christmas week
- 1 Petabyte+ of updates served every month by Windows Update to millions of servers and hundreds of millions of PCs worldwide
- Tens of thousands of Windows Azure customers
- 5M LiveMeeting conference minutes per year
- Forefront for Exchange filters 1B emails per month
Cloud Considerations

• Mission Critical, Scale Up Workloads
• Storage
  - Costs
  - Complexity
  - Security
• Continuous Availability
• VM Mobility
• Networking
  - Multi-Tenancy, Security
  - IP Address Management
  - QoS
• Automation/Manageability
Security is the Major Issue

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

- Security: 74.6%
- Performance: 63.1%
- Availability: 63.1%
- Hard to integrate with in-house IT: 61.1%
- Not enough ability to customize: 55.8%
- Worried on-demand will cost more: 50.4%
- Bringing back in-house may be difficult: 50.0%
- Regulatory requirements prohibit cloud: 49.2%
- Not enough major suppliers yet: 44.3%

Source: IDC Enterprise Panel, August 2008  n=244
Cloud Security Alliance identifies fifteen areas of concern.
Main Page

Security Guidance for Critical Areas of Focus in Cloud Computing

- Introduction
- Foreword
- Letter from the Editors
- An Editorial Note on Risk
- Section I. Cloud Architecture
  - Domain 1: Cloud Computing Architectural Framework
- Section II. Governing in the Cloud
  - Domain 2: Governance and Enterprise Risk Management
  - Domain 3: Legal and Electronic Discovery
  - Domain 4: Compliance and Audit
  - Domain 5: Information Lifecycle Management
  - Domain 6: Portability and Interoperability
- Section III. Operating in the Cloud
  - Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
  - Domain 8: Data Center Operations
  - Domain 9: Incident Response, Notification, and Remediation
  - Domain 10: Application Security
  - Domain 11: Encryption and Key Management
  - Domain 12: Identity and Access Management
  - Domain 13: Virtualization
- References
Threat #1: Abuse and Nefarious Use of Cloud Computing
Threat #2: Insecure Interfaces and APIs
Threat #3: Malicious Insiders
Threat #4: Shared Technology Issues
Threat #5: Data Loss or Leakage
Threat #6: Account or Service Hijacking
Threat #7: Unknown Risk Profile

Source: Cloud Security Alliance
So You’re a Building a Cloud...

I have good processes in place, but what other safeguards can I use to protect my data?
Server Hard Disks Appear on eBay
Real Case: A US Power Company

• The Company *had processes in place* to either physically destroy drives or scrub them to U.S. DOD standards
  - Degaussing
  - Overwriting the data with a minimum of three specified patterns

• Data on drives used in servers, contained:
  - Proprietary company information such as memos, correspondence
  - Customers data (460,000+) & Confidential employee information

According to Gartner about 1/3 companies use outside firms to dispose of PCs & Servers
BitLocker ensures your data stays secure, even when your Hyper-V hosts, clusters, and storage reside in less-physically-secure locations.

<table>
<thead>
<tr>
<th></th>
<th>Local Disk</th>
<th>Traditional Cluster Disk</th>
<th>CSV 2.0</th>
</tr>
</thead>
</table>

**Physical Security**
Critical Safeguard for the Cloud
Encrypted cluster volumes

- BitLocker encrypted cluster disks
  - Support for traditional failover disks
  - Support for Cluster Shared Volumes
- Cluster Name Object (CNO) identity used to lock and unlock Clustered volumes
- Enables physical security for deployments outside of secure datacenters
  - Branch office deployments
- Volume level encryption for compliance requirements
- Negligible (<1%) performance impact
What’s New In Windows Server 2012 Hyper-V

- Scale Up Workloads
- Platform Resiliency
- Storage
- Automation/Manageability
- Networking
- Clustering
- VM Mobility
- Linux as a Guest
Network Considerations

• How do I ensure network multi-tenancy?
• IP Address Management (IPAM) is a pain.
• What if VMs are competing for bandwidth?

• Fully Leverage Network Fabric
• How do I integrate with existing fabric?
• Network Metering?
• Can I dedicate a NIC to a workload?
Hybrid Clouds

Windows Server 2012 is optimized for Hybrid Clouds to host multi-tenant workloads

Tenant 1: Multiple VM Workloads
- SQL
- IIS

Tenant 2: Multiple VM Workloads
- SQL
- IIS
Security

In a multi-tenant environment ...

... customers want security and isolation
Reliability

Even when hardware fails ...
... customers want continuous availability
Predictability

Even when multiple VMs are competing for bandwidth ...

... customers want predictability
Scalability

Cloud admins want scalability ...
... and customers want performance
Customers want specialized functionality with lots of choice ... ... for firewalls, monitoring and physical fabric integration.
Multi-Tenant Network Requirements

- Tenant wants to easily move VMs to/from the cloud
- Hoster wants to place VMs anywhere in the data center
- Both want: Easy Onboarding, Flexibility & Isolation
Introducing Hyper-V Network Virtualization

Hyper-V Machine Virtualization
• Run multiple virtual servers on a physical server
• Each VM has illusion it is running as a physical server

Hyper-V Network Virtualization
• Run multiple virtual networks on a physical network
• Each virtual network has illusion it is running as a physical fabric
One Solution: PVLAN (Private VLAN)

- **Isolation Scenario**
  - Hoster wants to isolate all VMs from each other and allow internet connectivity
  - #1 Customer Ask from hosts

- **Community Scenario**
  - Hoster wants tenant VMs to interact with each other but not with other tenant VMs
  - Requires a VLAN ID for each “community” (limited scalability, only 4095 VLAN IDs)
Microsoft expects deployment of Internet Protocol security (IPsec) to increase significantly in the coming years. The large demands placed on the CPU by the IPsec integrity and encryption algorithms can reduce the performance of your network connections. IPsec Task Offload is a technology built into the Windows operating system that moves this workload from the main computer's CPU to a dedicated processor on the network adapter.

SR-IOV is a specification that allows a PCIe device to appear to be multiple separate physical PCIe devices. The SR-IOV specification was created and is maintained by the PCI SIG, with the idea that a standard specification will help promote interoperability. SR-IOV works by introducing the idea of physical functions (PFs) and virtual functions (VFs). Physical functions (PFs) are full-featured PCIe functions; virtual functions (VFs) are "lightweight" functions that lack configuration resources.

Dynamic Virtual Machine Queue (VMQ) is a feature available to computers running Windows Server 2008 R2 with the Hyper-V server role installed, that have VMQ-capable network hardware. VMQ uses hardware packet filtering to deliver packet data from an external virtual machine network directly to virtual machines, which reduces the overhead of routing packets and copying them from the management operating system to the virtual machine.
Advanced Network Security

DHCP Guard, Router Guard, Monitor Port

- **DHCP Guard** is a security feature that drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
- **Router Guard** is a security feature that drops Router Advertisement and Redirection messages from unauthorized virtual machines pretending to be routers.
- **Monitor Mode** duplicates all egress and ingress traffic to/from one or more switch ports (being monitored) to another switch port (performing monitoring).
Manage to a Service Level Agreement
Network Bandwidth & QoS

- **Bandwidth Management** allows you to easily reserve minimum or set maximums to provide QoS controls to manage to a service level agreement.
## Windows Server 2012 Networking: It’s All There

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC Teaming</td>
<td>Yes, via partners</td>
<td>Yes, via partners</td>
<td>Windows NIC Teaming in box.</td>
</tr>
<tr>
<td>VLAN Tagging</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MAC Spoofing Protection</td>
<td>No</td>
<td>Yes, with R2 SP1</td>
<td>Yes</td>
</tr>
<tr>
<td>ARP Spoofing Protection</td>
<td>No</td>
<td>Yes, with R2 SP1</td>
<td>Yes</td>
</tr>
<tr>
<td>SR-IOV Networking</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Network QoS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Metering</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Monitor Modes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IPsec Task Offload</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VM Trunk Mode</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Multitenant security and isolation: Secure separation of resources in the data center as needed per host

Hyper-V Network Virtualization: Scale beyond VLANs by moving workloads without changing network configurations or reconfiguring physical networks

Extensible Switch: Inspect, forward or report on traffic in the virtual environment based on needs

Quality of Service: Guarantee minimum services bandwidth while maximizing network throughput

Delivering a fully isolated, multitenant environment that includes tools to guarantee SLAs, enable chargebacks, and support self-service delivery
Complete Virtualization Platform

Scale beyond VLANs with Hyper-V Network Virtualization

Run multiple virtual networks on a single physical network. Each virtual network believes it is running on its own physical fabric.
Hyper-V Extensible Switch

Augmented Hyper-V Virtual Switch capabilities, offering monitoring, traffic filtering & shaping, and forwarding algorithms

Diagram:
- Virtual Machine
- Root Partition
- Virtual Machine
- Hyper-V Switch
  - Capture Extensions
  - WFP Extensions
  - Filtering Extensions
  - Forwarding Extension
- Physical NIC
- Host NIC
- VM NIC

Beyond Virtualization
## Hyper-V Extensible Switch

<table>
<thead>
<tr>
<th>PVLANS</th>
<th>ARP/ND Poisoning Protection</th>
<th>DHCP Guard Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Port ACLs</td>
<td>Trunk Mode to Virtual Machines</td>
<td>Monitoring &amp; Port Mirroring</td>
</tr>
</tbody>
</table>

Windows PowerShell & WMI Management

The Hyper-V Extensible Switch allows a **deeper integration** with customers’ existing network infrastructure, monitoring and security tools.
Hyper-V Extensible Switch is an open platform that lets multiple vendors provide extensions that are written to standard Windows API frameworks.
Hyper-V Extensible Switch

- Virtual Machine
  - VM NIC
- Host Partition
  - Host NIC
- Virtual Machine
  - VM NIC

Hyper-V Switch
- Extension Protocol
- Capture Extensions
- WFP Extensions
- Filtering Extensions
- Forwarding Extension
- Extension Miniport

Certified Extensions

Physical NIC
Partners and Their Extensions

- sFlow traffic (capture)
- Virtual Firewall v3.0 (filtering)
- Nexus 1000V (forwarding)
- UCS (forwarding w/SR-IOV)
- OpenFlow (forwarding)
## Networking Performance

<table>
<thead>
<tr>
<th>Dynamic VMq</th>
<th>Dynamically span multiple CPUs when processing virtual machine network traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Task Offload</td>
<td>Offload IPsec processing from within virtual machine, to physical network adaptor, enhancing performance</td>
</tr>
<tr>
<td>SR-IOV Support</td>
<td>Map virtual function of an SR-IOV capable physical network adaptor, directly to a virtual machine</td>
</tr>
</tbody>
</table>

The Hyper-V Extensible Switch takes advantage of hardware innovation to drive the highest levels of networking performance within virtual machines.
Network Virtualization

**Secure Isolation**
Isolate network traffic from different business units or customers on a shared infrastructure without VLANs

**Flexible Migrations**
Move VMs as needed within your virtual infrastructure while preserving their virtual network assignments

**Seamless Integration**
Transparently integrate these private networks into a preexisting infrastructure on another site
Hyper-V Scalability Improvements

<table>
<thead>
<tr>
<th>System</th>
<th>Resource</th>
<th>Windows Server 2008 R2 Hyper-V</th>
<th>Windows Server 2012 Hyper-V</th>
<th>Improvement Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Logical Processors</td>
<td>64</td>
<td>320</td>
<td>5x</td>
</tr>
<tr>
<td></td>
<td>Physical Memory</td>
<td>1TB</td>
<td>4TB</td>
<td>4x</td>
</tr>
<tr>
<td></td>
<td>Virtual CPUs per Host</td>
<td>512</td>
<td>2,048</td>
<td>4x</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual CPUs per VM</td>
<td>4</td>
<td>64</td>
<td>16x</td>
</tr>
<tr>
<td></td>
<td>Memory per VM</td>
<td>64GB</td>
<td>1TB</td>
<td>16x</td>
</tr>
<tr>
<td></td>
<td>Active VMs per Host</td>
<td>384</td>
<td>1,024</td>
<td>2.7x</td>
</tr>
<tr>
<td></td>
<td>Guest NUMA</td>
<td>No</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Cluster</td>
<td>Maximum Nodes</td>
<td>16</td>
<td>64</td>
<td>4x</td>
</tr>
<tr>
<td></td>
<td>Maximum VMs</td>
<td>1,000</td>
<td>4,000</td>
<td>4x</td>
</tr>
</tbody>
</table>

“Nothing from Microsoft, and I mean literally **nothing** has ever been this ambitious”

— Jason Perlow, ZDNet
<table>
<thead>
<tr>
<th>Capability</th>
<th>Windows Server 2012 Hyper-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensible vSwitch</td>
<td>Yes</td>
</tr>
<tr>
<td>Confirmed Partner Extensions</td>
<td>4</td>
</tr>
<tr>
<td>Private Virtual LAN (PVLAN)</td>
<td>Yes</td>
</tr>
<tr>
<td>ARP Spoofing Protection</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Snooping Protection</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Port ACLs</td>
<td>Yes</td>
</tr>
<tr>
<td>Trunk Mode to Virtual Machines</td>
<td>Yes</td>
</tr>
<tr>
<td>Port Monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Port Mirroring</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Secure Multitenancy
Management Efficiency

Broader automation of common management tasks and a path toward full lights-out automation

- **Multi-server management with Server Manager:** Simplify the processes of configuring new servers, deploying roles and features to Windows Server and managing multiple-server environments.

- **Resilient and simple automation with PowerShell:** Expanded cmdlet scope, simplified usage, automation and workflow to manage every aspect of your data center.

- **Volume License Activation:** Machines can seamlessly activate when joined to the domain with no additional deployment or configuration requirements.

The Availability of Many Servers, The Simplicity of One
PowerShell 3.0

- **Integration for all roles:** New support for SMB, NIC Teaming and Hyper-V management and configuration
- **RunAs Flexibility:** commands may be executed using delegated credentials, allowing limited permission users to run critical jobs
- **Constrained Mode “sandboxes”:** PowerShell cmdlets can restrict access and execution of commands with security implications

2,400+ commandlets along with workflows and...
Simplified scripting through Windows PowerShell ISE 3.0

Show-Command pane lets users find and run cmdlets in a dialog box

IntelliSense provides context-sensitive command completion for cmdlet and script names, parameter names and enumerated values, and property and method names.
Make sure PowerShell is your best friend

- PowerShell 3.0 with over 2000 cmdlets
  - Allows creation scripts with workflow
  - AD PowerShell history helps you get started
  - Newest help files download on demand – *Update-Help*
Dynamic Footprint

- **Dynamic remotely managed Servers**: All Servers can be remotely managed and deployed as Server Core with all critical roles as well as on-demand feature management.
- **Flexibility at all times**: Choose between Server Core (the default) or Full Server or run without the shell with no re-install.
- **Features on Demand**: Use and install exactly the capabilities you need, nothing more.
- **Reduced disk size**: Install from a remote repository on your network and not in every image.

Minimizing size and security attack surfaces at all times.
Secure Remote Management

Standards based protocol and capabilities for management and workflows

- **Robust Sessions**: PowerShell remote sessions can be re-established and managed by users on multiple machines

- **Integrated DoS protection**: WinRM provides a fixed-limit queue for access requests, prior to their authentication

- **Trusted connections**: Once an administrator has successfully connected their address details are stored to ensure successful connections when attacks occur

Windows Remote Management (WinRM) is on by default
Cluster Based Availability

Cluster-Aware Updating and Integrated Encryption

- **Automatic updates**: Patch every node in a cluster with no application downtime
- **Integrated cluster automation**: Transparently takes each node offline by pausing, draining and fallback to apply all updates
- **BitLocker enabled clusters**: AD Cryptography Next Generation used to enable encrypted Cluster Shared Volumes for physical security

Minimized downtime and maximum uptime
Enhanced Data Security and Compliance

Offers granular access to data and corporate resources based on strong identity and device security status, as well as simplified configuration and administration for remote access.

- **Central access policies and authorization**: Define who can access what information within the organization based on claims and dynamic policies.

- **Active Directory Federation Services**: Integrates Active Directory claims with AD FS allowing the claims from Kerberos tickets to be transformed into SAML tokens for use with claims aware applications both inside the corporate network and across federated trusts.

- **Audit policies for compliance reporting**: Identify who accessed highly sensitive information.
Finer-grain Security Controls

Allows administrators to more easily and accurately express their intentions around password-policy and delegation of the right to act on behalf of other users in n-tier application scenarios

- **Fine-Grained Password Policy**: Active Directory Administrative Center simplifies the creation and administration of fine-grained password-policies (policies that can be configured to impose different constraints and assigned more granularly than their domain-policy counterparts)

- **Kerberos Constrained Delegation (KCD)**: Extends KCD functionality to cross-domain and cross-forest scenarios while also shifting this important administrative decision to the resource owners rather than the domain administrator
Simplified Identity Management

Active Directory provides simplicity and flexibility for the hybrid environment.

- **Virtualizing Active Directory**: Domain controller cloning provides elastic-deployment while virtualization safeguards ensure service continuity.
- **Simplified Management**: Integrated object-deletion recovery and automatic PowerShell script-generation simplify disaster recovery and automation of important identity management tasks.
- **Group Managed Service Accounts**: Windows services running across multiple machines share a single user account with automatic password management.
Active Directory Rights Management Services provides enhanced deployment flexibility in Windows 8, with more cryptographic options, remote deployment, support for Server Core, enhanced remote management and more.
Windows 2012 enhances DNS Security (DNSSEC) with dynamic updates, improved encryption and integrated key management with AD

- **Supports the latest DNS Security standards:** NSEC3 plus RSA/SHA-2 encryption
- **DNS Dynamic Updates:** DNS zone can be signed online, with DNS dynamic updates now enabled
- **AD Integration:** Uses Active Directory to store and distribute keys used for DNS record signing, with automatic rollover support

Protect your Infrastructure
Information Protection Scenarios

Windows 2012 enhances existing information protection scenarios and supports new ones.

- **Simple delegation**: Support employees that need to delegate email management to an assistant.

- **Enhanced File Classification integration**: Active Directory Rights Management Services now integrates with file servers out of the box to automatically detect, classify and protect documents based on content and context.
Active Directory Certificate Services now supports TPM-protected keys, enhanced key management, more flexible deployment and configuration tools and a powerful template management user interface.

Take control of your PKI
Enhanced Certificate Management

- **Certificate Lifecycle Notifications**: Flexible notification types based on policy to reduce errors and outages
- **Key Based Auto-Renewal**: Support for offline enrollment and subsequent automatic renewal
- **Group Protected PFX**: The password included in the PFX is limited to a set of SIDs using new data protection APIs

Take control of your PKI
• **Simple deployment**: End-to-end encryption of SMB data in flight with no new infrastructure or specialized hardware

• **Flexible configuration**: Defined on a per share basis or for the entire server

• **Secure multi-tenancy**: Enables a variety of scenarios where data traverses untrusted networks or WANs
Scalable and Elastic Web Platform

Improves web site density, elasticity, and efficiency, while enabling service providers to better build, provision, and manage a hosting environment.

- **Scalability and Management**: Scale up using next-generation hardware, NUMA support and CPU Throttling for maximum performance.

- **Centralized SSL Certificate Support**: Rapidly add servers to a web farm without manually configuring SSL; centrally share and manage SSL certificates.

- **Flexible tools and extensions**: Open source software support using common tools, languages and capabilities.
Security Development Lifecycle

Tools to support all phases of development from requirements to release

- **Holistic and comprehensive approach**: Integration with Visual Studio Team System
- **Improved threat modeling**: Design reviews and requirements validation performed early
- **More and stronger fuzzing tools**: Additional tools including FxCop, Binscope, AppVerifier and Attack Surface Analyzer
- **Public tools and guidance**: All available for download from the Microsoft SDL Portal
Disaster Recovery
Disaster Recovery Challenges

- Cost
- Complexity
- Inflexibility
- Initial Replication
- Distance Requirements
Hyper-V Replica Unlimited Replication

- Disaster Recovery Scenarios:
  - Planned, Unplanned and Test Failover
  - Pre-configuration for IP settings for primary/remote location

- Key Features:
  - RPO/RTO in minutes
  - Seamless integration with Hyper-V and Clustering
  - Automatically handles all VM mobility scenarios (e.g. Live migration)
  - Supports heterogeneous storage between primary and recovery
  - Integrates with Volume Shadow Services (VSS)
## Hyper-V Replica

*Complements Array Based Replication*

<table>
<thead>
<tr>
<th>Replication Provider</th>
<th>Cost</th>
<th>Management</th>
<th>Performance</th>
</tr>
</thead>
</table>
| **Hyper-V Replica**           | Microsoft                         | • Flexible Storage Options Available  
• Unlimited VM Replication included                                                                 | • 5 minutes RPOs  
• Application Level Consistency  
• File Level Consistency         |
| **Storage Based Replication** | NetApp, HP, Fujitsu, IBM, Hitachi, FalconStor, 3Par, EMC, LSI, Compellent, EqualLogic and more... | • High end replicating storage  
• Additional replication software Adam                                              | • Synchronous Replication  
• High Data Volumes
References

- Windows Server 2012 site:
  - [http://www.microsoft.com/windowsserver](http://www.microsoft.com/windowsserver)
  - Including the Windows Server 2012 Datasheet

- Microsoft Security Development Lifecycle Portal:
โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 12

CDIC 2013 Key Highlights

CDIC for Management

CDIC for IT Professional

CDIC for Amateur

CDIC Conference Workshop

Advanced Mobile Application Attack and Defense

Mobile Application Vulnerability (SSLstrip and OWASP Top 10)

Mobile App Exploit (Mercury)

Cloud Forensics

- Cloud Application Forensics Computer Platform
- Cloud Application Forensics Smartphone Platform
- Free Mail Forensic - Cloud Storage Forensics

CDIC 2013 Live Show !!

- Wireless WPA2 PEAP
- WPS Brute-Force
- Wifi Pineapple- HotSpot Pen-Testing
- Evilgrade - Blindly Exploitation
- Firefox XPI Exploit
- HTML5 Hacking
- HiperText Access Exploit
- Pivot and Forward Tunnel
- Mobile App Malware
- FlashBack Trojan for Mac User
CDIC 2013 Key Highlights

- Update Top Ten Threats and Trends on IT & Information Security in 2013 and Beyond
- Int’l Conference, IIA, RSA 2012-1023 Highlights
- National Cybersecurity Master Plan and Strategies vs. ASEAN ICT Master Plan and Strategies
- Business - Organizational Resilience - the Next Step Forward for Business Continuity
- Evaluating and Managing Cyber Risks & Security Impacting an Organization
- Actions on Threat Horizon 2013
- Security Insights on Threat Horizon 2014
- How to Upgrade COBIT 4.1 with new COBIT 5
- How to Upgrade New ISO/IEC 27001
- GRC Security Approaches and Roadmap
- Unified Compliance and Security Standards
- IT Consumerization and BYOD Policy
- How to Secure Online and Internet Banking from Reforming Man-in-the-Middle Attacks
- Online Privacy Threats & Behavioral Social Networking Security
- Lessons Learned and Truths about Cloud Security and Services
- Mobile Malware Transformation
- Advanced Botnet-based Distributed Denial of Service (DDoS)
- Real Case Studies from the Professionals and Experts
- In-depth Live Show Demonstration on New Advanced Cybercrime and Ethical Hacking Techniques
www.cdicconference.com

CDIC 2013 conference,
27-28 February @Central World
Bangkok, Thailand
Email: prinya@acisonline.net
Facebook: www.facebook.com/prinyah
Twitter: www.twitter.com/prinyaACIS
Thank You 😊