How to Grow and Transform your Security Program into the Cloud

Wolfgang Kandek

Qualys, Inc.

Session ID: SPO-207

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

Agenda

- Introduction
- Fundamentals of Vulnerability Management
- Differences in Cloud Computing
- Scanning in the Public Cloud IaaS
- Looking Ahead
- Questions

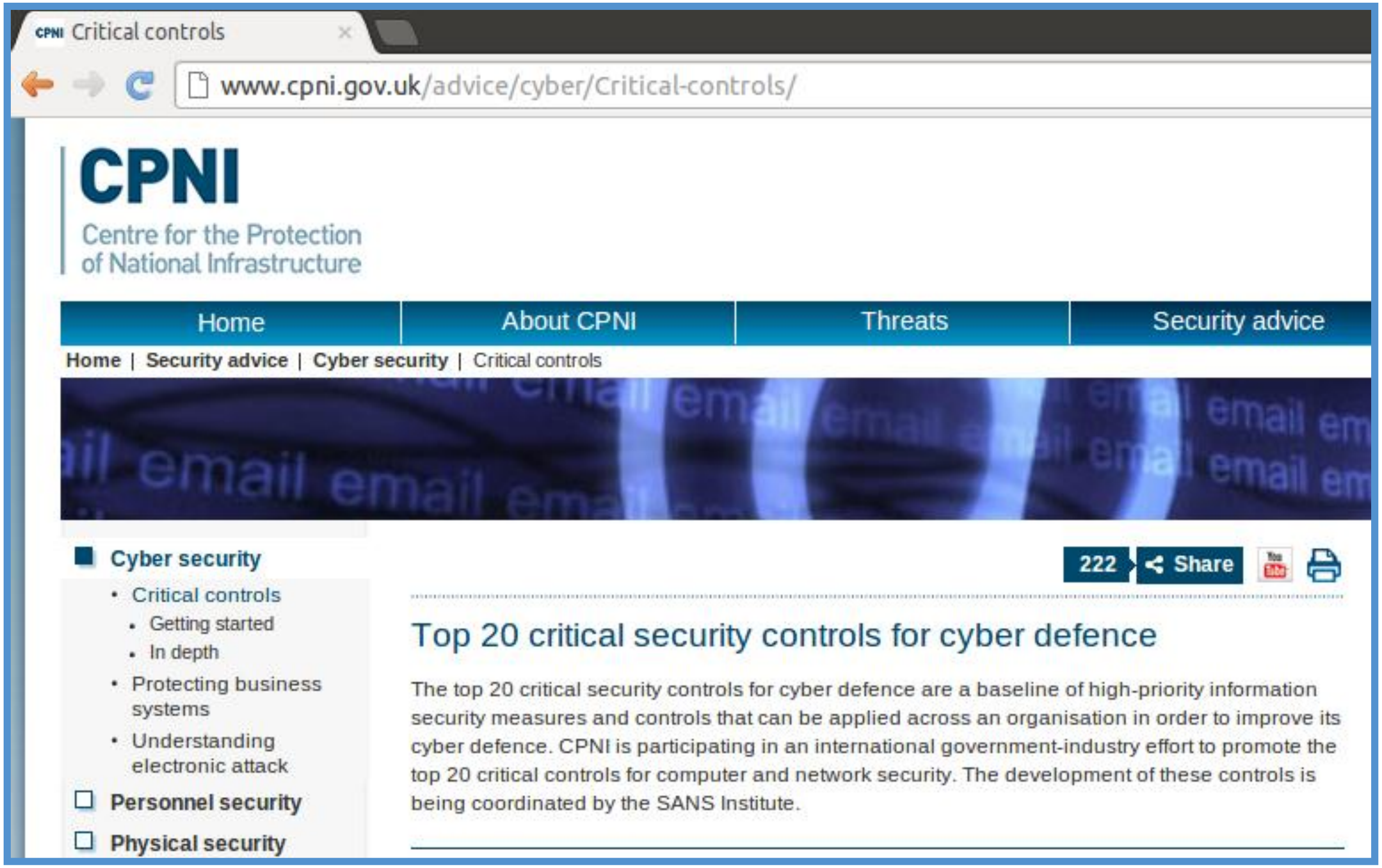
Security Program

- Vulnerability Management Impact on Security Program
  - Asset Discovery
  - Software Inventory
  - Secure Configurations
  - Continuous Assessment and Remediation

Security Program

- Vulnerability Management Impact on Security Program
  - Asset Discovery
  - Software Inventory
  - Secure Configurations
  - Continuous Assessment and Remediation

Security Program

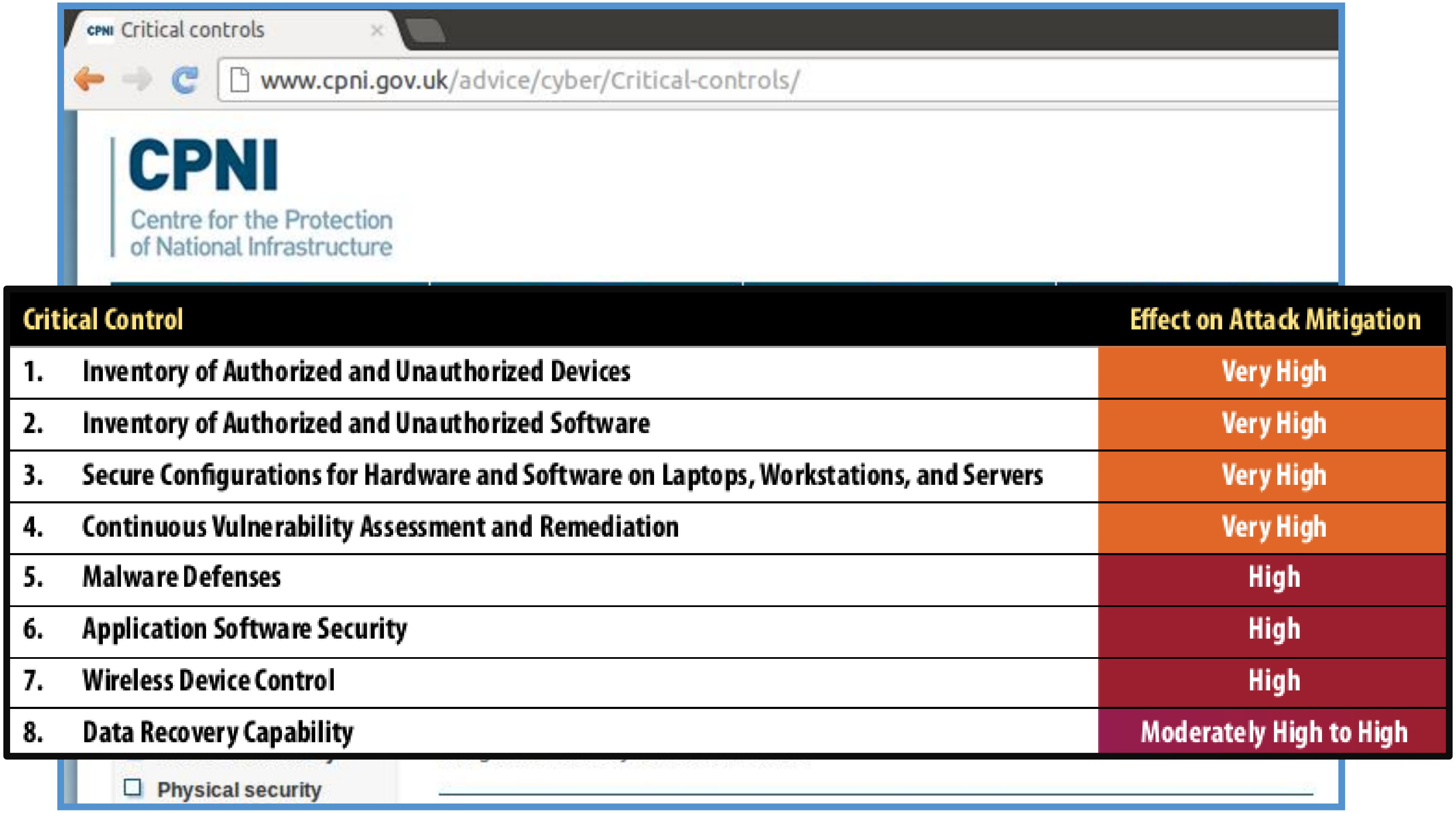


CPNI Critical controls
www.cpni.gov.uk/advice/cyber/Critical-controls/
CPNI
Centre for the Protection of National Infrastructure
Home
About CPNI
Threats
Security advice
Home | Security advice | Cyber security | Critical controls
■ Cyber security
• Critical controls
• Getting started
• In depth
• Protecting business systems
• Understanding electronic attack
□ Personnel security
□ Physical security
222
Share

Top 20 critical security controls for cyber defence

The top 20 critical security controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence. CPNI is participating in an international government-industry effort to promote the top 20 critical controls for computer and network security. The development of these controls is being coordinated by the SANS Institute.

Security Program



www.cpni.gov.uk/advice/cyber/Critical-controls/

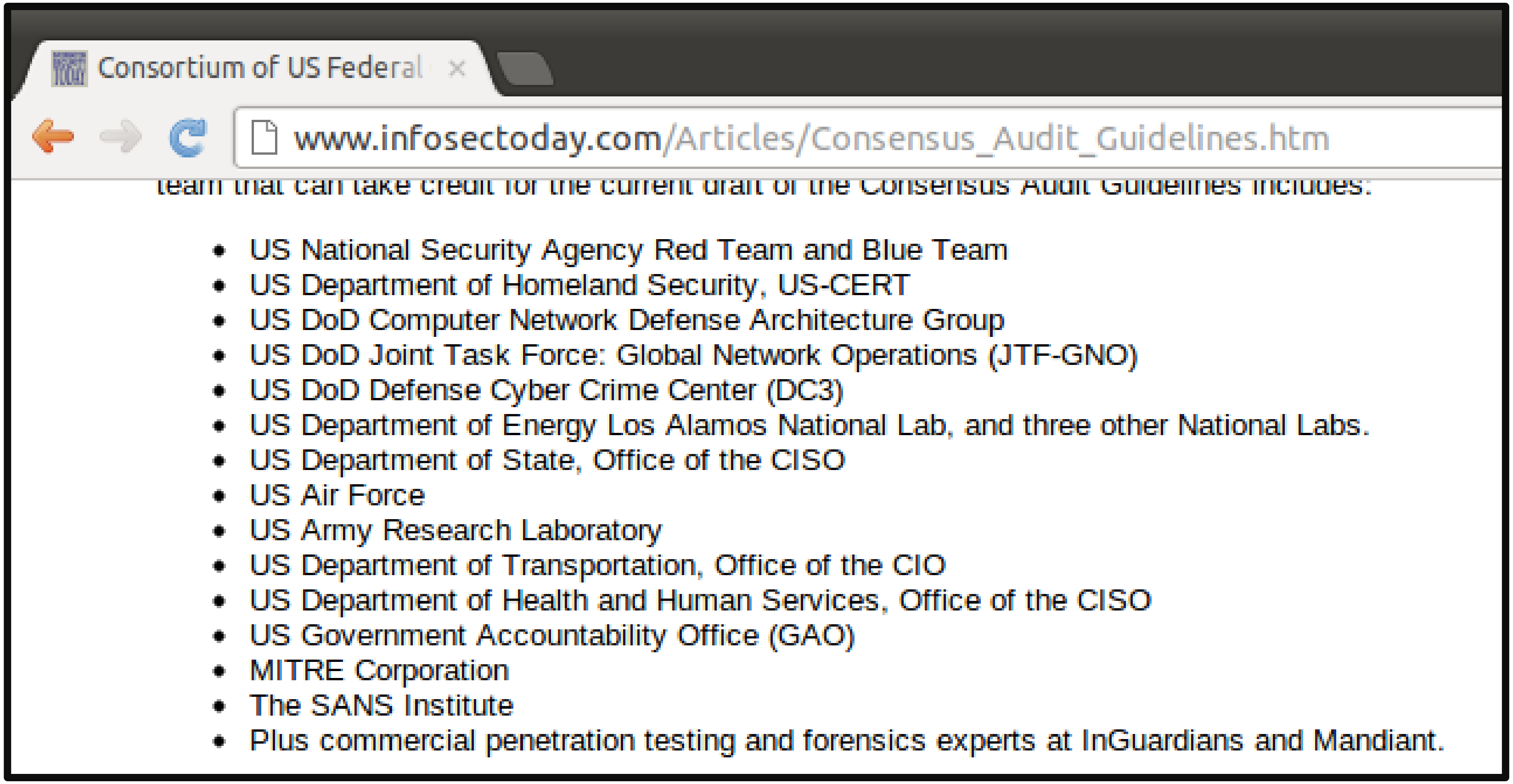
CPNI

Centre for the Protection
of National Infrastructure

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High

□ Physical security

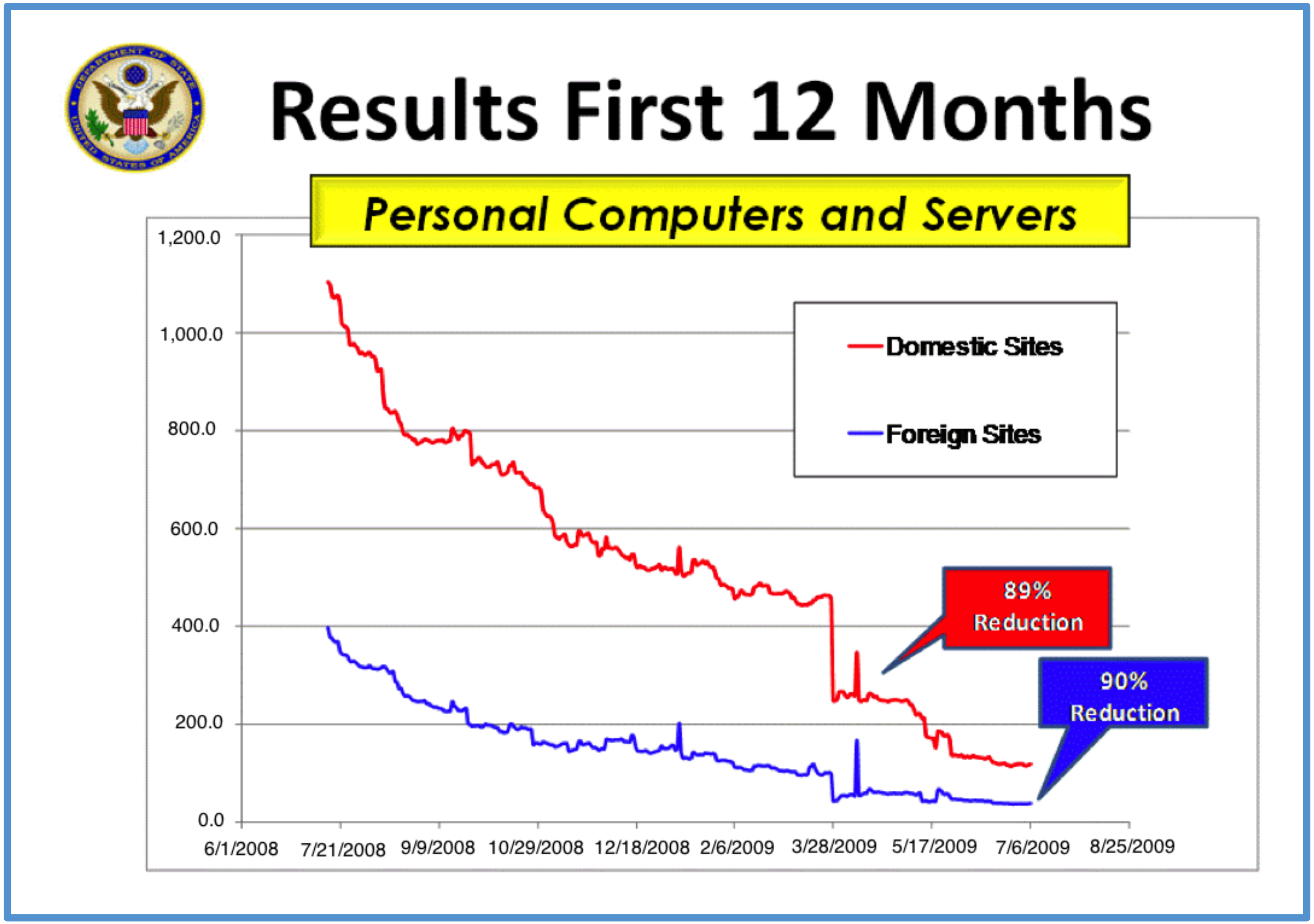
Security Program


Consortium of US Federal
www.infosectoday.com/Articles/Consensus_Audit_Guidelines.htm

team that can take credit for the current draft of the Consensus Audit Guidelines includes:

- US National Security Agency Red Team and Blue Team
- US Department of Homeland Security, US-CERT
- US DoD Computer Network Defense Architecture Group
- US DoD Joint Task Force: Global Network Operations (JTF-GNO)
- US DoD Defense Cyber Crime Center (DC3)
- US Department of Energy Los Alamos National Lab, and three other National Labs.
- US Department of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Department of Transportation, Office of the CIO
- US Department of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE Corporation
- The SANS Institute
- Plus commercial penetration testing and forensics experts at InGuardians and Mandiant.

Security Program



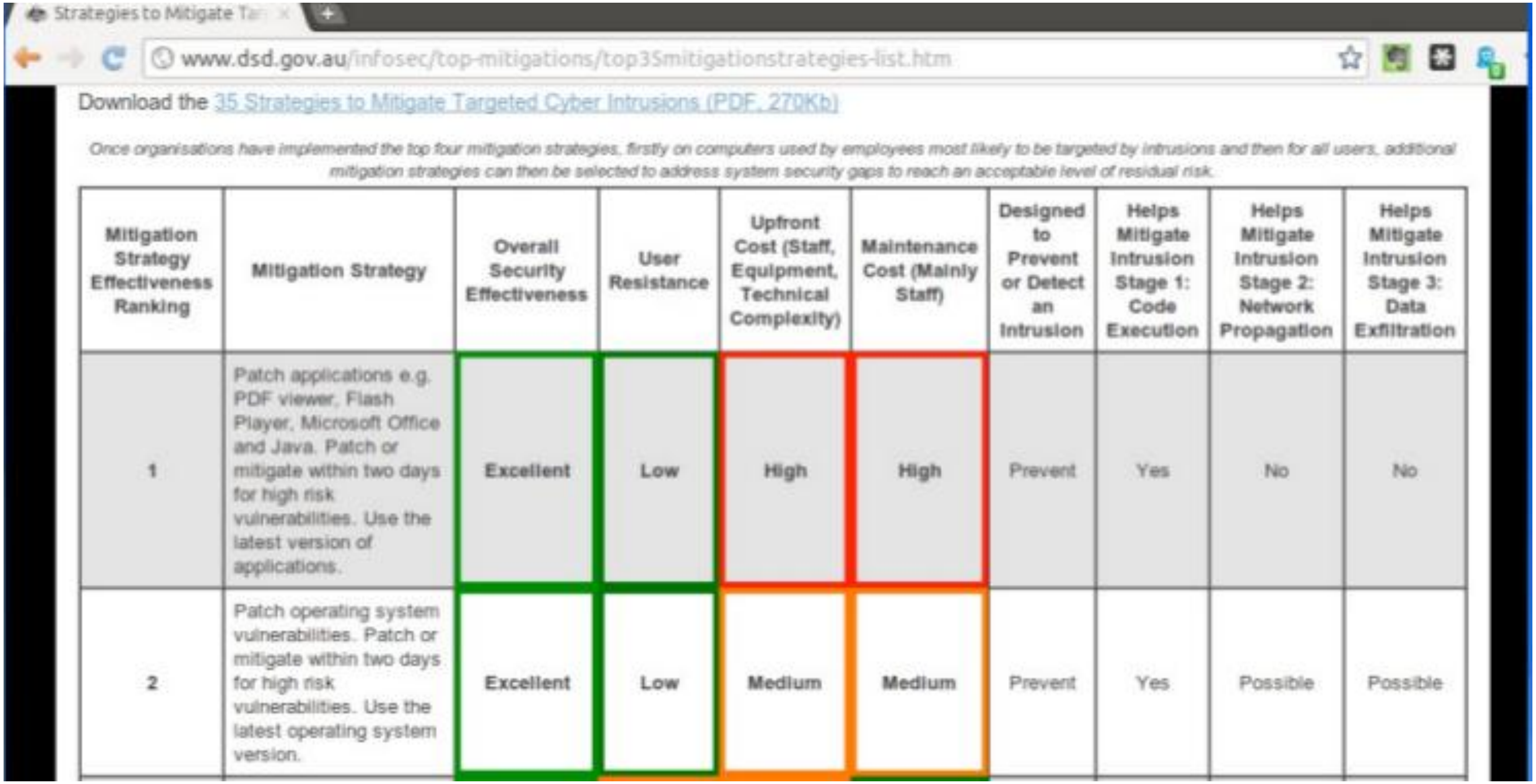
Results First 12 Months

Personal Computers and Servers

89% Reduction

90% Reduction

Security Program


Strategies to Mitigate Ta
www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

Download the 35 Strategies to Mitigate Targeted Cyber Intrusions (PDF, 270Kb)

Once organisations have implemented the top four mitigation strategies, firstly on computers used by employees most likely to be targeted by intrusions and then for all users, additional mitigation strategies can then be selected to address system security gaps to reach an acceptable level of residual risk.

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.	Excellent	Low	High	High	Prevent	Yes	No	No
2	Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.	Excellent	Low	Medium	Medium	Prevent	Yes	Possible	Possible

Security Program

- Dsd.gov.au: 85 % of Incidents prevented
- Application Patching
- Operating System Patching
- Non-Admin for Users
- Whitelisting

Fundamentals of Vulnerability Management

Terminology

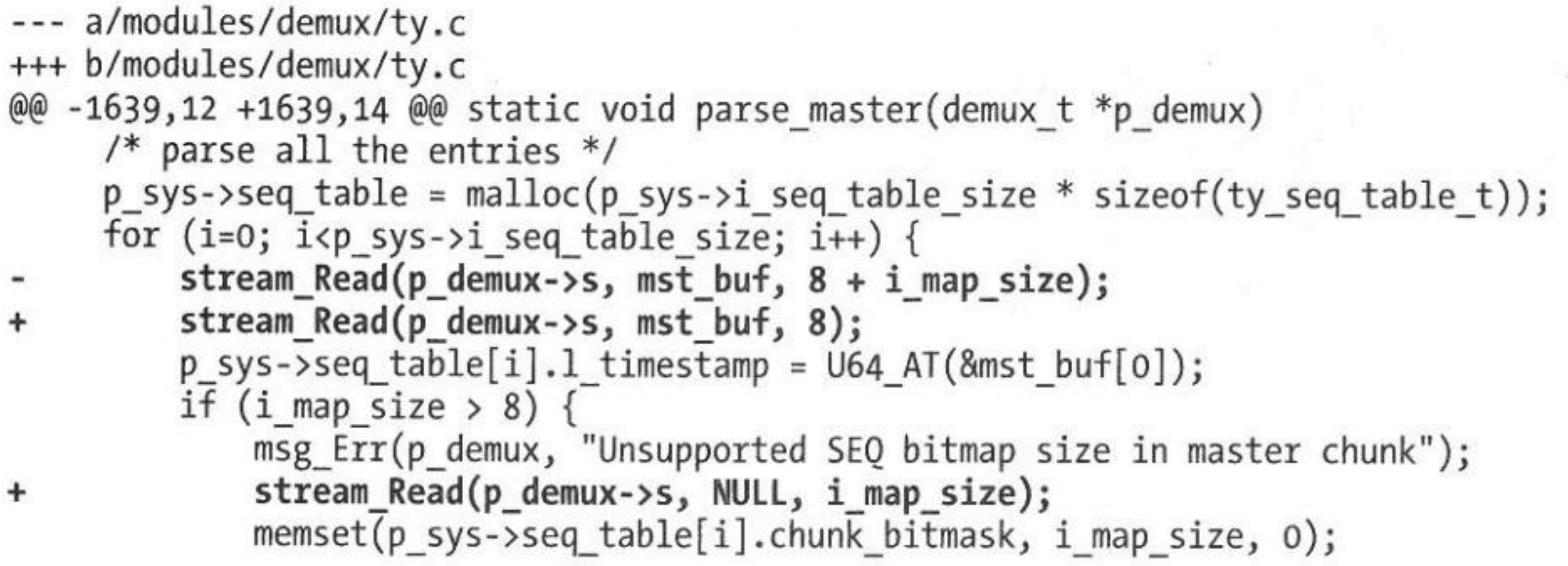
- **Vulnerability**
  - Inability to withstand the effects of a hostile environment
  - Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer system.
- **Threat:** Any circumstance or event, deliberate or unintentional, with the potential to cause harm to a system.
- **Exploit:** Code that takes advantage of a vulnerability to gain greater access or privileges on a computer system.
- **Risk:** The probability that a particular threat will exploit a particular vulnerability.

Origin of Vulnerabilities

- Programming mistakes
  - 5-20 bugs per 1,000 lines of code
  - note: not all "bugs" result in vulnerabilities.

Origin of Vulnerabilities

- Programming mistake example
- VLC - CVE-2008-4654 – Stack overflow



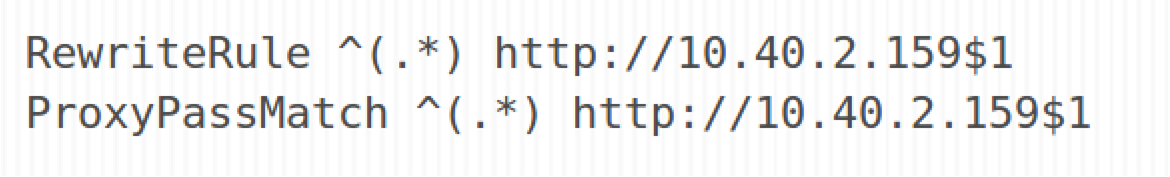
```
--- a/modules/demux/ty.c
+++ b/modules/demux/ty.c
@@ -1639,12 +1639,14 @@ static void parse_master(demux_t *p_demux)
     /* parse all the entries */
     p_sys->seq_table = malloc(p_sys->i_seq_table_size * sizeof(ty_seq_table_t));
     for (i=0; i<p_sys->i_seq_table_size; i++) {
-        stream_Read(p_demux->s, mst_buf, 8 + i_map_size);
+        stream_Read(p_demux->s, mst_buf, 8);
         p_sys->seq_table[i].l_timestamp = U64_AT(&mst_buf[0]);
         if (i_map_size > 8) {
             msg_Err(p_demux, "Unsupported SEQ bitmap size in master chunk");
+            stream_Read(p_demux->s, NULL, i_map_size);
             memset(p_sys->seq_table[i].chunk_bitmask, i_map_size, 0);
```

Origin of Vulnerabilities

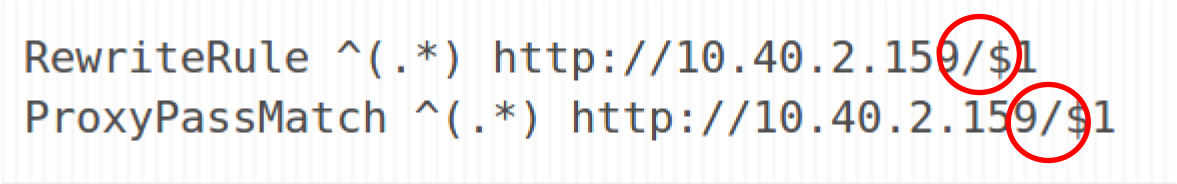
- Programming mistakes
  - 5-20 bugs per 1,000 lines of code
  - note: not all “bugs” result in vulnerabilities.
- Configuration errors
  - Default passwords
  - Sample program
  - Configuration directives

Origin of Vulnerabilities

- Configuration error example
- Apache mod_proxy - CVE-2011-4317
  missing trailing slash – information disclosure



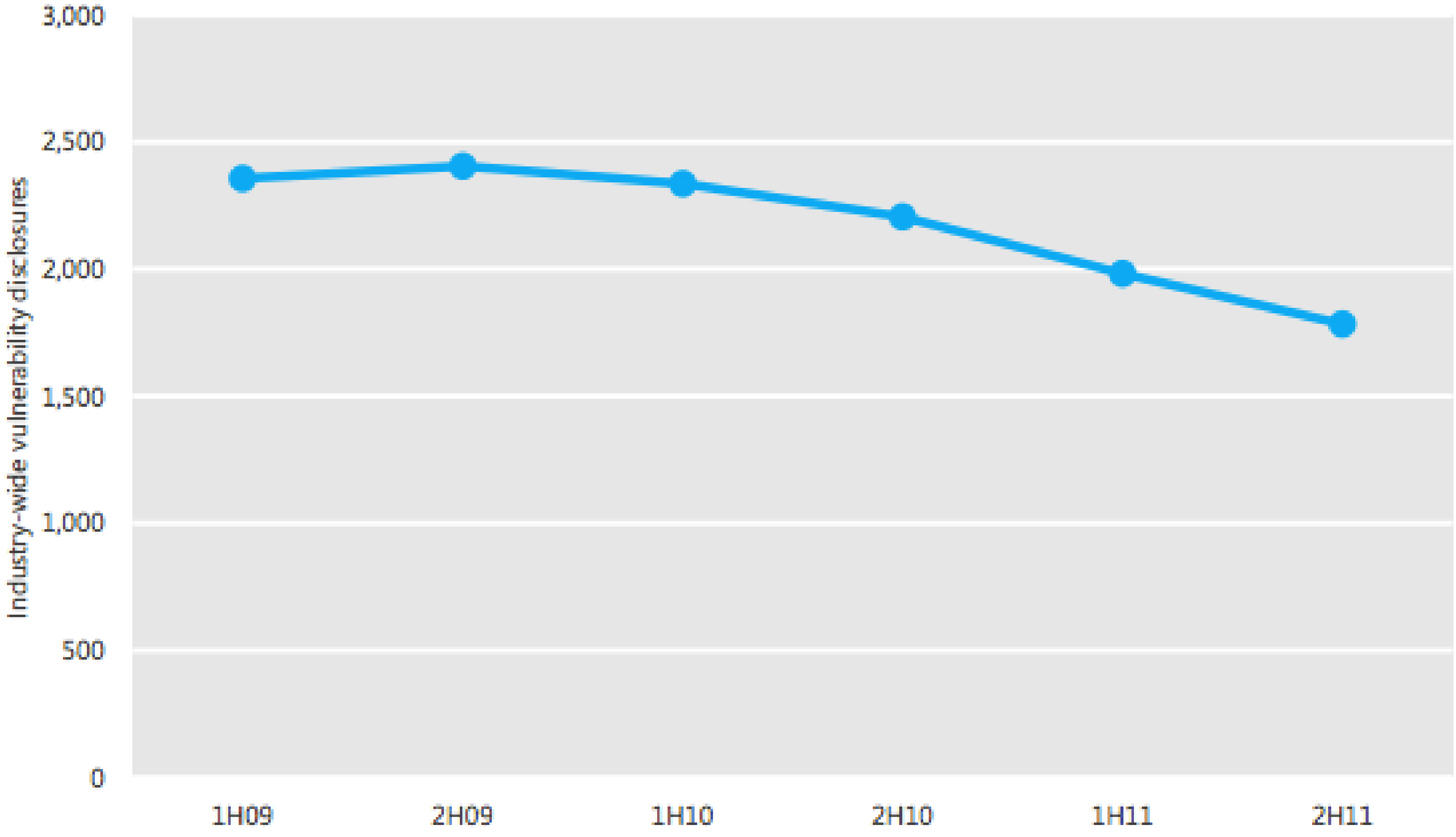
```
RewriteRule ^(.*) http://10.40.2.159$1
ProxyPassMatch ^(.*) http://10.40.2.159$1
```



```
RewriteRule ^(.*) http://10.40.2.159/$1
ProxyPassMatch ^(.*) http://10.40.2.159/$1
```

How Many Vulnerabilities?

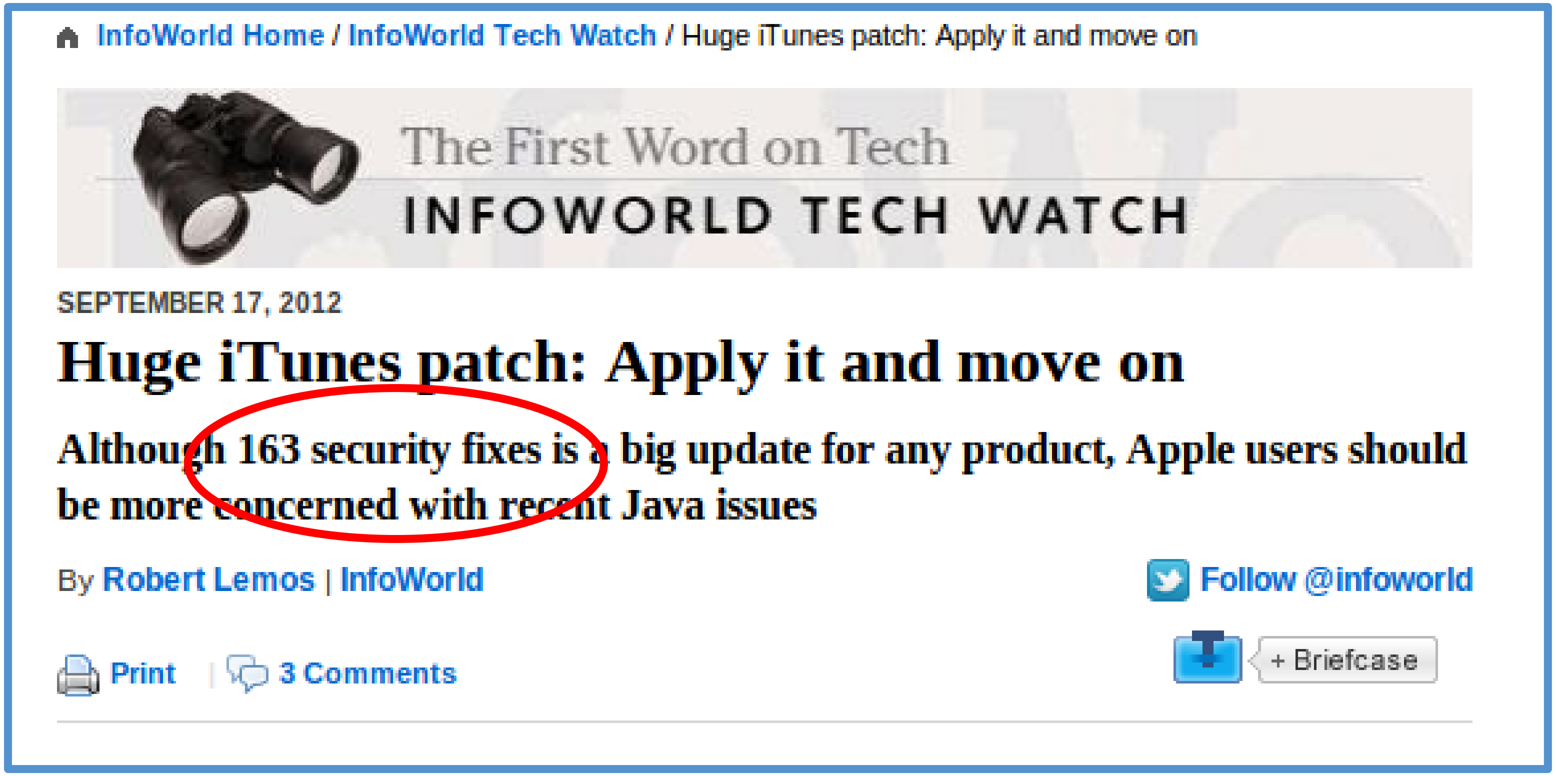
Figure 8. Industry-wide vulnerability disclosures, 1H09–2H11



Volume 12, July – December, 2011

How many Vulnerabilities?

- 1000s of CVEs every 6 months
- Many CVEs are bundled in 1 Patch



InfoWorld Home / InfoWorld Tech Watch / Huge iTunes patch: Apply it and move on

SEPTEMBER 17, 2012

Huge iTunes patch: Apply it and move on

Although 163 security fixes is a big update for any product, Apple users should be more concerned with recent Java issues

By Robert Lemos | InfoWorld

How many Vulnerabilities?

- 1000s of CVEs every 6 months
- Many CVEs are bundled in 1 Patch
- Microsoft – 50 / 6 months
- Oracle – 70 / 6 months
- Apple – 15 / 6 months
- Wordpress – 10 / 6 months

Vulnerability Management Basics

- Track inventory and categorize assets
- Scan systems for vulnerabilities
- Verify vulnerabilities against inventory
- Classify and rank risks
- Identify patches, fixes and workarounds
- Apply patches, fixes and workarounds
- Rescan to validate remediation

Scanning and Asset Inventory

- Vulnerability scanners validate asset management inventory systems through network discovery scans.
- Discovery scans use IP network blocks to discover assets.
- Administrators use the results of discovery scans to group and classify assets for detailed vulnerability scans.

External vs. Internal Scanning

- External Scanning:
  - Also known as “Perimeter Scanning”.
  - Vulnerability scanning from the Internet.
  - Scans must pass though perimeter firewalls and security appliances
  - Used to identify vulnerabilities on perimeter systems.
- Internal Scanning:
  - Vulnerability scanning from inside the Enterprise (behind the Firewall)
  - Used to identify vulnerabilities on internal systems and to discover detailed system information.

Trusted Scanning

- Trusted scanning uses credentials to log into the Target System
  - Increased Accuracy
  - Detailed Software Inventory
  - Client Side Vulnerabilities
    - Browsers, PDF Readers, Databases
- Eliminates the requirement for permanent resident software agents on every system.
- Maintains Ease of Installation

Differences in Cloud Computing

Cloud Computing

- SaaS – Software as a Service
  - E-mail: Gmail, Exchange Online
  - Productivity: Google Apps, Office365
  - Business: Salesforce, Netsuite
- PaaS – Platform as a Service
  - Google App Engine – Java, Python
  - Microsoft Azure – C# and SQL DB
- IaaS – Infrastructure as a Service
  - Amazon AWS EC2
  - Rackspace

Differences with the Cloud - IaaS

- Very Dynamic
- Usage Based Price Model
- Instances
- Machine Images
- IP Address variable
- Asset Discovery
- Access Control (Firewalling)
- Permission to Scan (AUP)
- Management
- Introspection

Cloud IaaS is Dynamic

- Instances can be created, and torn down, very rapidly.
  - Impact: Asset management systems may not be accurate. Is IT part of the process, or are they excluded?
- Instances may not be always powered on because of the cost model (usage based).
  - Impact: Potentially challenging to scan all systems.

Usage Based Cost Model

Varies by IaaS provider but:

- You pay for each hour/fraction thereof the instance is “powered on”.
  - Different instance types have different rates.
- You pay for Internet data transfer.
  - Typically transfer rates are measured in GB/month.
  - Some providers don’t charge for inbound (from Internet) traffic.
- You pay for Storage
  - Typically storage rates are measured in GB/month AND million I/O requests

Instance

- An individual system in a cloud IaaS is known as an “instance”.
- Instances can be “powered on” or “powered off”.

Machine Images

- Systems in a Cloud IaaS environment are typically built from predefined software “Images”.
- IaaS subscribers can use publicly available images, or build and upload their own images.
- Possible advantage of scanning images before deployment into production, allowing for more secure images.
- Some IaaS providers allow for the import and export of images to/from a variety of formats.

Cloud IaaS IP Addressing

Varies somewhat with IaaS provider however:

- Typically, instances have a private internal address, and a public address. NAT is used to map public address to private addresses.
- Addresses are typically assigned by the IaaS provider; networks and contiguous addresses are not typically provided.
- Both private and public addresses are released when an instance is stopped or terminated.

Discovery in a Cloud

- Discovery scanning is typically not possible in public IaaS cloud environments due to the IP Addressing assignment method.

- However, Cloud IaaS APIs typically provide a mechanism to “discover” detailed information about all instances in a given account, even those that are powered off.

Access Control for IaaS

- Public Cloud IaaS provide access control to permit/deny packets from reaching an instance.
- Implemented in the form of “Security Groups”
- Instances are members of one or more Security Groups
- No ability to filter outbound traffic.

Permission to Scan/AUP

- Currently, the Acceptable Use Policies for most public IaaS do not permit vulnerability scanning without prior approval.
  - Impact: Extra step in your vulnerability management program. You must request permission/schedule vulnerability management scans in advance.
  - http://aws.amazon.com/security/penetration-testing/

Cloud Management

- IaaS Cloud providers have extensive management consoles
- Functions are are often accessible via APIs.
- API access allows for automation of many Cloud management tasks.
- APIs also allow for tight integration with other tools, including vulnerability management tools.
- Asset discovery can be automated through the API.

Introspection

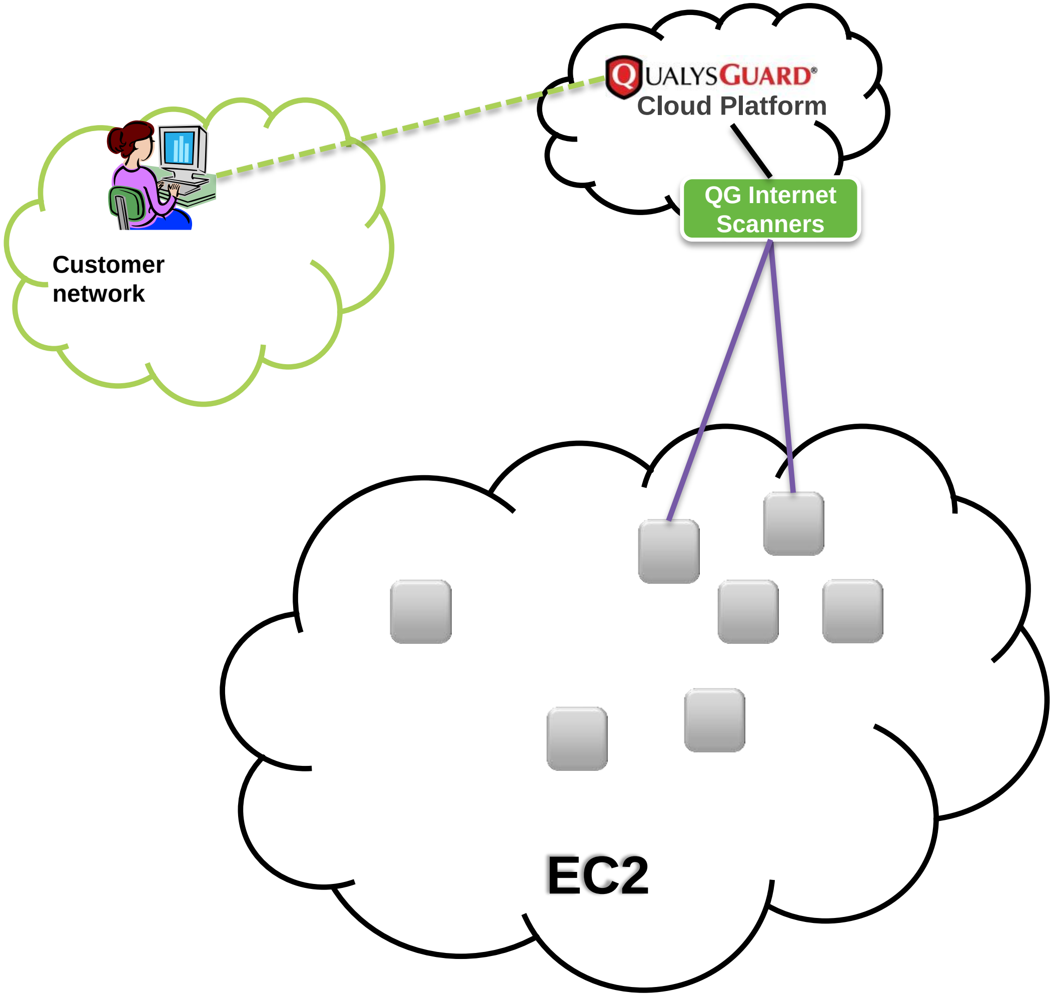
- Visibility into the memory of a particular system provided through the hypervisor
  - System under examination can be powered off
- Vulnerability assessment can be done entirely through introspection
  - performance impact to the hypervisor
- Introspection in a public IaaS Cloud could be problematic due to Multi Tenancy

Scanning in the Public Cloud IaaS

Scanning Public IaaS Instances

- External Scanning from the Internet
- Internal Scanning through VPN tunnels.
- Internal Scanning from inside the IaaS.

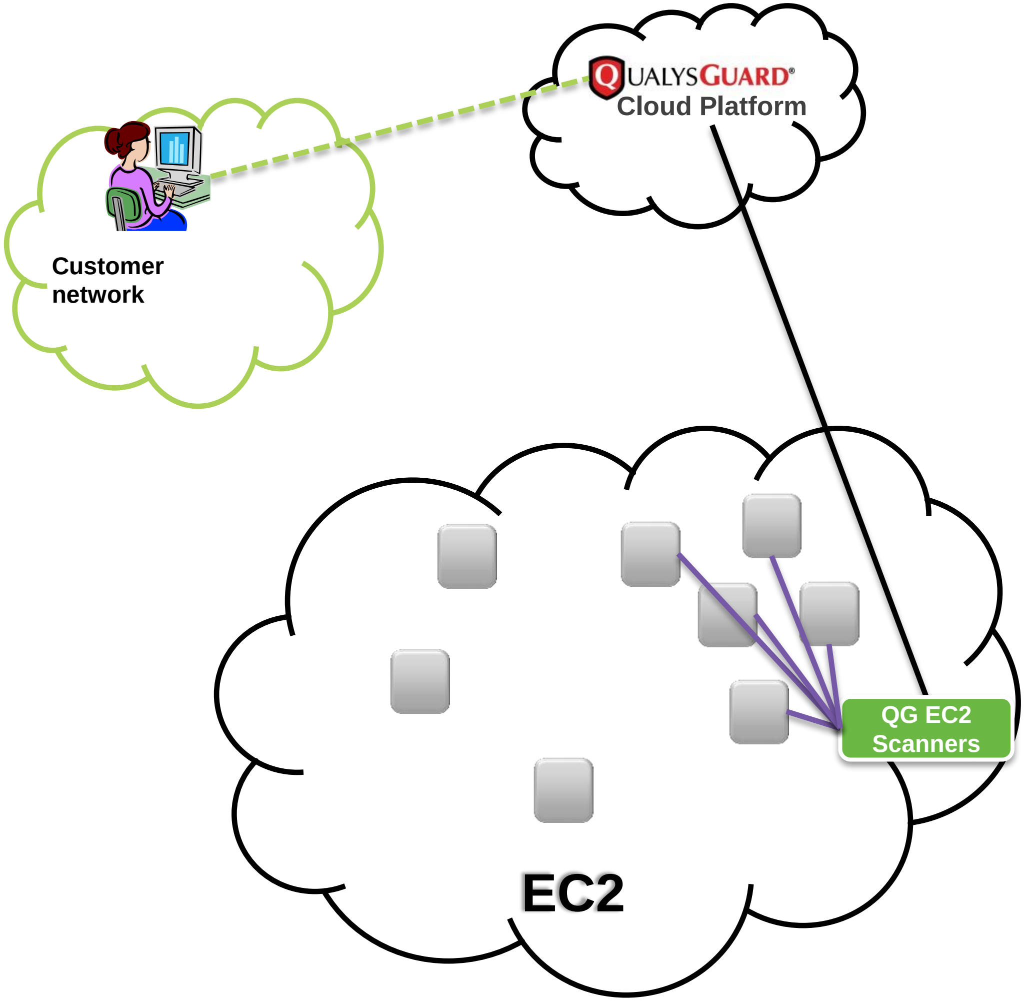
External Public IaaS Scanning



External Public IaaS Scanning

- Instance(s) must have a public IP address.
- Scan individual IaaS instance public IP address.
- Obtain permission to scan from IaaS provider.
- Modify security groups for scanner IP address.
- Network charge for scanning traffic.

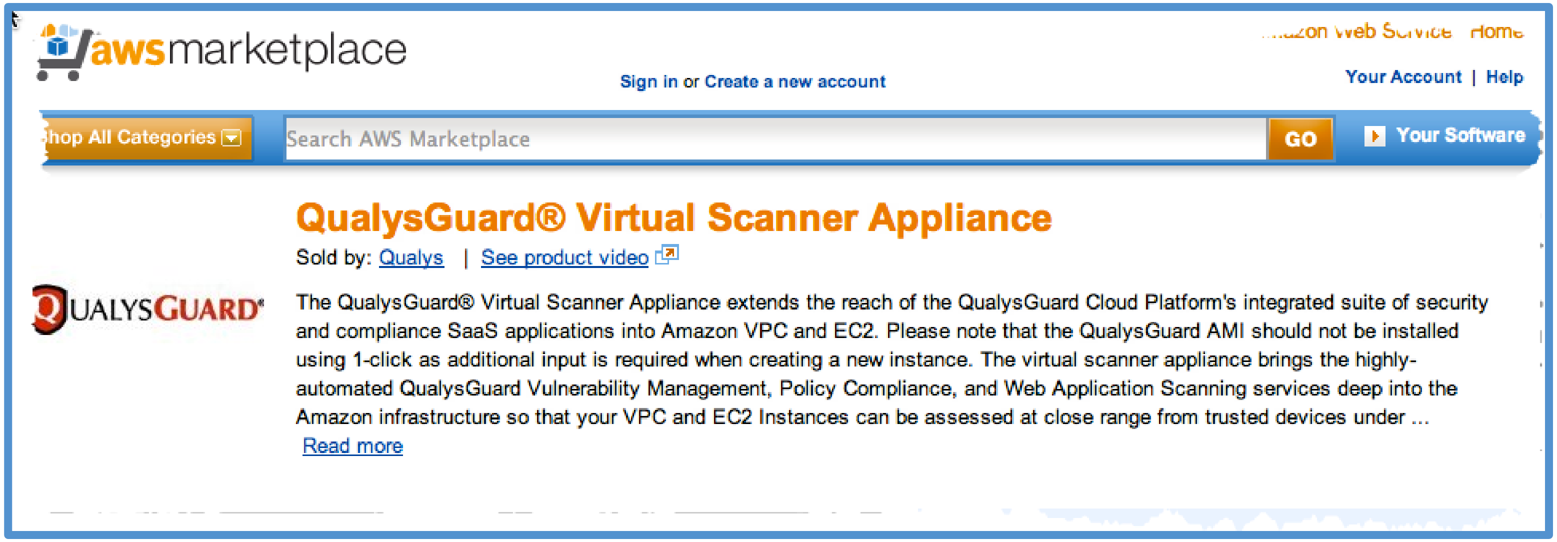
Internal Scanning from inside IaaS



Internal Scanning from inside IaaS

- Deploy a scanning system into the IaaS environment.
- Can scan individual IaaS instance private IP addresses.
- Obtain permission to scan from IaaS provider.
- Security Group for scanner instance.
- Authenticated scans are possible and recommended.
- Network charges for data transfer.
- Instance charges for vulnerability scanner(s).

QualysGuard Virtual Scanner Appliance



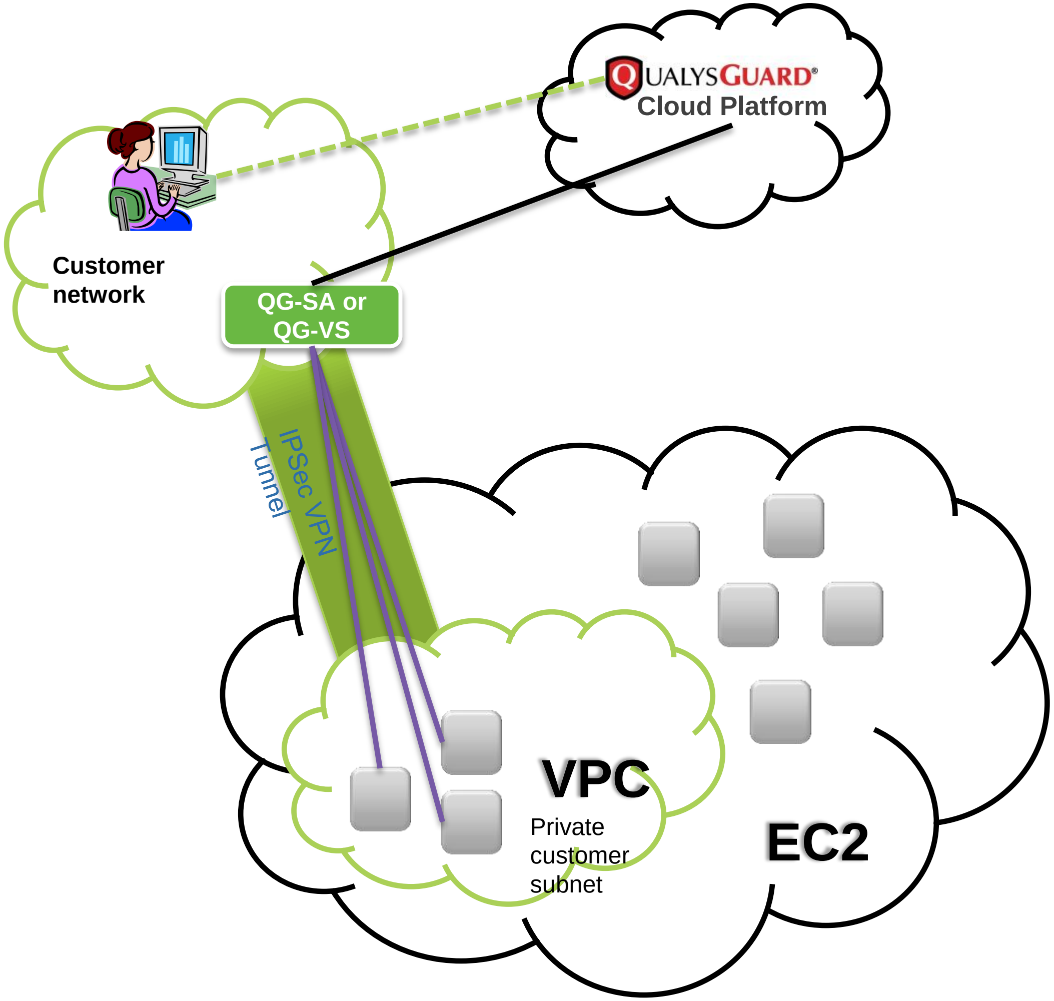
QualysGuard® Virtual Scanner Appliance

Sold by: Qualys | See product video

The QualysGuard® Virtual Scanner Appliance extends the reach of the QualysGuard Cloud Platform's integrated suite of security and compliance SaaS applications into Amazon VPC and EC2. Please note that the QualysGuard AMI should not be installed using 1-click as additional input is required when creating a new instance. The virtual scanner appliance brings the highly-automated QualysGuard Vulnerability Management, Policy Compliance, and Web Application Scanning services deep into the Amazon infrastructure so that your VPC and EC2 Instances can be assessed at close range from trusted devices under ...

Read more

Internal Scanning through VPN tunnel



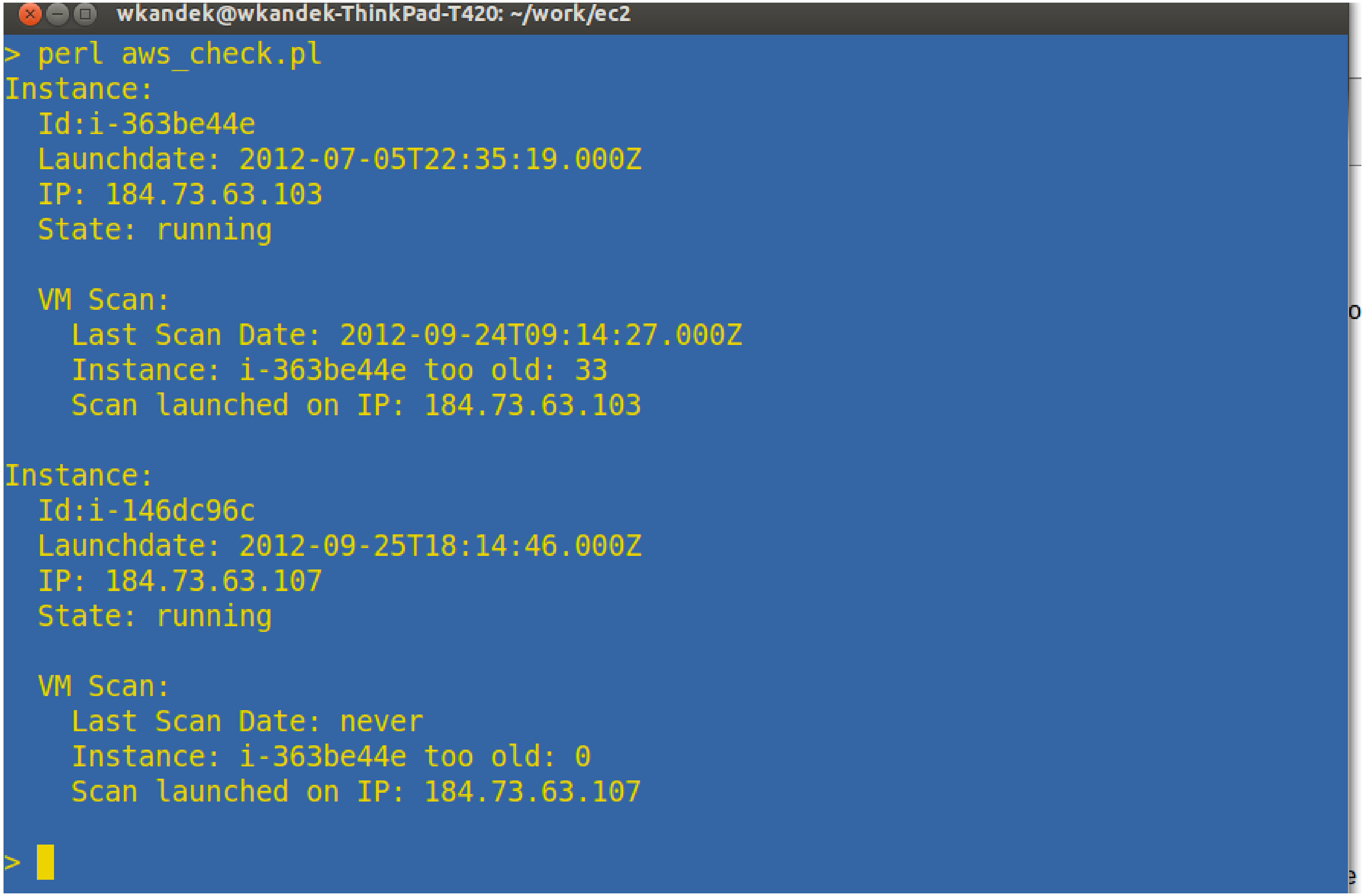
Internal Scanning through VPN

- Requires establishment of VPN tunnel between IaaS environment and Enterprise. VPN options vary.
- Can leverage scanner systems inside Enterprise .
- Can scan IaaS instance private IP addresses.
- Obtain permission to scan from IaaS provider.
- May need to modify security groups for scanner IP address.
- Authenticated scans are possible.
- Network charges for data transfer and VPN tunnel.

IaaS API Integration for Scanning

- Automatically scan new machines for vulnerabilities
  - Do not scan if we have a fresh result (24 hours)
- Strategy: Use IaaS Asset API to detect new servers
- Amazon EC2 API: rich functionality
- API can be used to query for active machines
- API results can drive new scans through Scanning APIs
- Script integration necessary for small correlation DB
- Sample run:

IaaS API Integration for Scanning



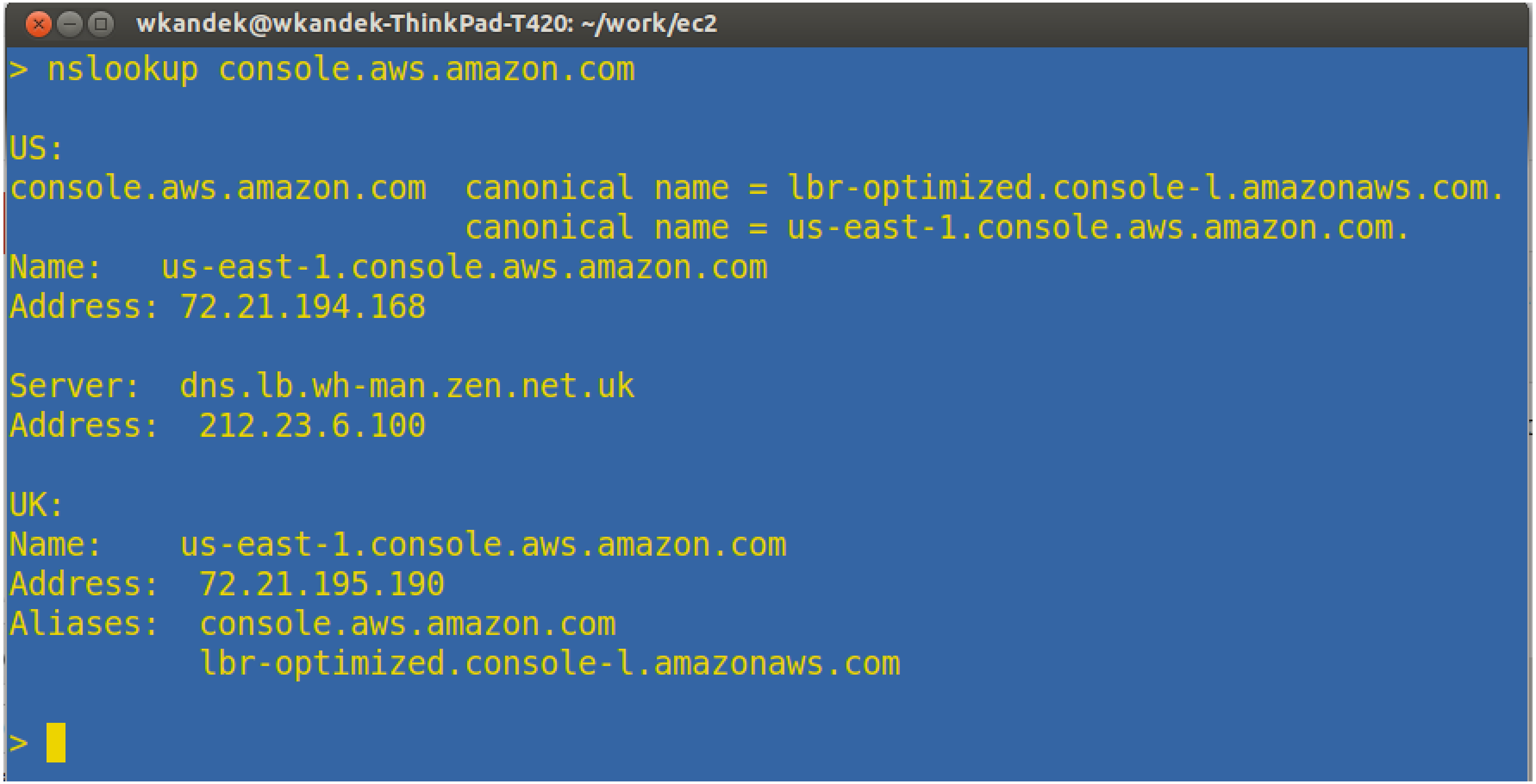
wkandek@wkandek-ThinkPad-T420: ~/work/ec2

```
> perl aws_check.pl
Instance:
  Id:i-363be44e
  Launchdate: 2012-07-05T22:35:19.000Z
  IP: 184.73.63.103
  State: running

  VM Scan:
    Last Scan Date: 2012-09-24T09:14:27.000Z
    Instance: i-363be44e too old: 33
    Scan launched on IP: 184.73.63.103

Instance:
  Id:i-146dc96c
  Launchdate: 2012-09-25T18:14:46.000Z
  IP: 184.73.63.107
  State: running

  VM Scan:
    Last Scan Date: never
    Instance: i-363be44e too old: 0
    Scan launched on IP: 184.73.63.107

> 
```

Do we use AWS already?

- Monitor for AWS use on the network level
- Firewall log rule for 71.21.194.168

Do we use AWS already?



```
> nslookup console.aws.amazon.com

US:
console.aws.amazon.com  canonical name = lbr-optimized.console-l.amazonaws.com.
                        canonical name = us-east-1.console.aws.amazon.com.
Name:   us-east-1.console.aws.amazon.com
Address: 72.21.194.168

Server:  dns.lb.wh-man.zen.net.uk
Address:  212.23.6.100

UK:
Name:    us-east-1.console.aws.amazon.com
Address:  72.21.195.190
Aliases:  console.aws.amazon.com
          lbr-optimized.console-l.amazonaws.com

> 
```

Do we use AWS already?

- Monitor for AWS use on the network level
- Firewall log rule for 71.21.194.168
  - May vary for your geo location
- DNS logs for console.aws.amazon.com
  - Or amazonaws.com
- Web proxy logs

Apply

- Investigate your vulnerability management provider to see if scanning capabilities inside the Public IaaS clouds are available
- Integrate your scanning through the IaaS management APIs.
- Use data from scanning and IaaS provider management systems through their respective APIs to improve your Asset Management.

Thank you

wkandek@qualys.com
@wkandek
http://laws.qualys.com