



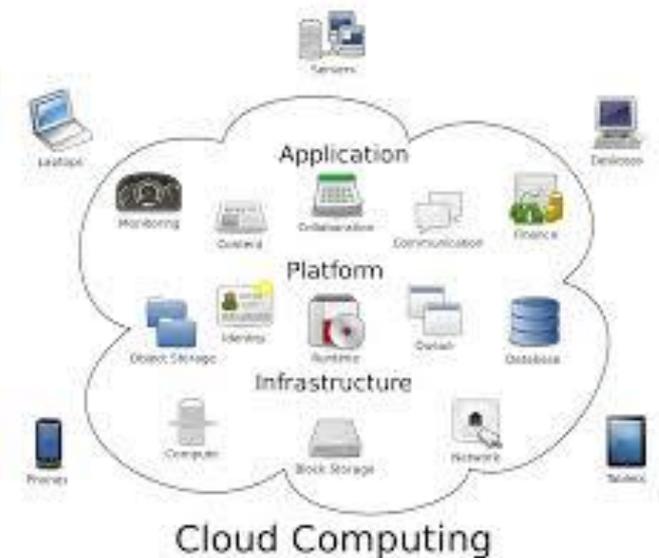
**The Latest IT Trends**  
**AAPA Cybersecurity seminar**  
**March 12, 2015**

# Trending Technologies

- Cloud-computing
- Internet of Things
- Managed Services

# Cloud Computing

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
  - The NIST Definition of Cloud Computing
  - [NIST Special Publication 800-145](#)
- Advantages
  - Availability
  - Access
  - Provisioning
  - Auto-Recover



# Security Implications

- Shared Platform
- Enterprise Id
- Privacy
- Pooling exploits
  - APIs
  - Mngt Interface
  - Resource Hoard

## Victims of Recent DDoS Attacks

Check Point  
SECURITY TECHNOLOGIES

Sony "didn't notice the security breaches that compromised 101 million user accounts because it was distracted by distributed denial of service attacks..." — *Sony in a letter to US Congress 2011*



"Amazon.com claims its widely publicized DDoS attack resulted in a loss of \$500,000 during the 10 hours it was down..." — *Amazon.com*

**POLICE**  
"While Yahoo was down, it suffered a loss of e-commerce and advertising revenue of about \$500,000..." — *According to analysts*

InfoSecMedia

©2011 Check Point Software Technologies Ltd.

# Internet of Things

- The *Internet of Things* (IoT) is the network of objects or "*things*" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

-*Wikipedia*

- Examples of Port Automation
  - Intelligent buildings
  - Automated equipment
    - Robots, cars, and cranes
  - Refrigeration Monitoring
  - Automated Ports
    - Port of Hamburg, Germany
    - Rotterdam, Netherlands



# Security Implications

- FTC Warns of the Huge Security Risks in the Internet of Things
- Cyber-Physical System (CPS)
  - [NIST Preliminary Draft](#)
- Manufacturers Security
  - Security is not the primary goal
  - Embedded systems lack standards/framework
  - Globalization

# Security Implications

- Huawei Defends Equipment Security- 2013
  - Largest Telecom in the world
- U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts
  - Mapped the Iranian network
- How the NSA can 'turn on' your phone remotely (well not really)
- iRobot's latest Roomba robot is designed for hackers

# Security Implications

Location history

« March 2015 »

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Show: 1 Day

**March 12, 2015**

- Show timestamps
- Export to KML
- Delete history from this day
- Delete all history

**Savannah**

Distance from starting location (farthest distance: 0.296 miles)

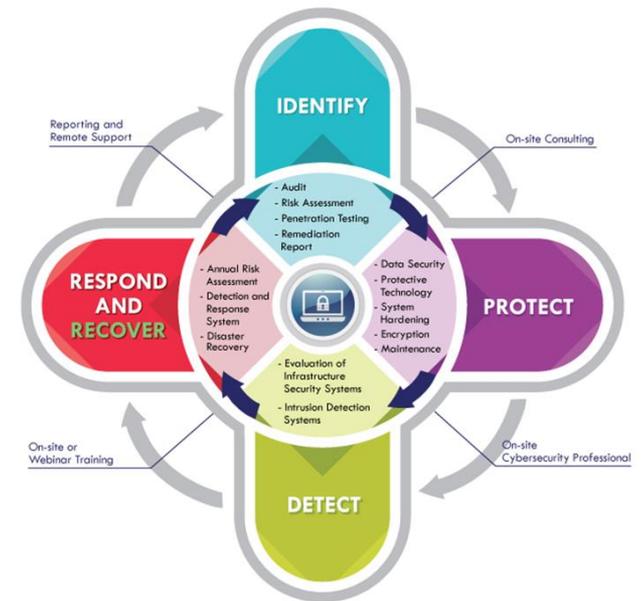
Move mouse over graph to show location on map

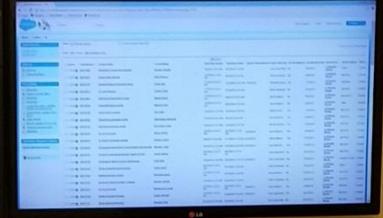
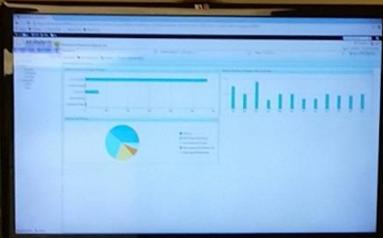
2:00 AM 4:00 AM 6:00 AM 8:00 AM 10:00 AM

©2012 Google Terms of Service Privacy Policy Help Center Change Language: English (US)

# Managed Services

- Limited Resources
  - Budget
  - Personnel
  - Utilities/Tools
- Scalable
- Industry Compliance
  - Identify
  - Protect
  - Detect
  - Respond/Recover





# Identify

- Audit
- Risk Assessment
- Penetration Testing
- Remediation Report

**IDENTIFY**

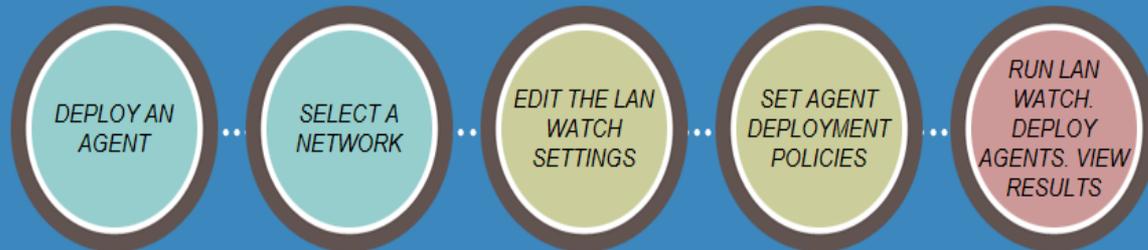
# Identify



## LAN WATCH

Discover Network Devices & Deploy Agents

 [View the Discovery Quick Start Guide](#)  
 [View the Discovery Training Video](#)



*To discover devices on a network, deploy at least one Agent to a computer on that network.*

*Under 'LAN Watch', a list of discoverable networks is presented based on the agents that are deployed. Choose a network from the list, or manually create a new network.*

*- Associate the Network with an Organization  
- Select a probe machine  
- Tailor the IP Scan Range  
- Enable SNMP Discovery  
- Enable vPro Discovery  
- Enable Alerting  
- Configure Asset Tracking*

*Set policies to automatically deploy agents to discovered computers. Select an agent deployment package, and specify credentials.*

*Run a Scan now, or schedule it on a recurring basis. View the summary page to monitor scan progress. View a list of all discovered devices and drill in to see details about each device. If deployment policies are set, the LAN Watch Scan will deploy agents to discovered devices.*

# Identify

Summary Software Hardware Agent Patch Status Remote Control

New Custom Field Rename Custom Field Delete Custom Field

System Information Collected: 2:34:37 pm 13-Sep-13

Next Collection:

**OS** Name/OS Information

Computer Name:	MSTbridge
Operating System:	2008
Version:	R2 Server Standard x64 Edition Service

**\*** System Information

Manufacturer:	HP
Product Name:	ProLiant DL360p Gen8
System Version:	(none)
System Serial Number:	MXQ3250BPS

**CPU** CPU/RAM Information

Processor Manufacturer:	Intel
Processor Family:	Intel Xeon
Processor Version:	Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz
CPU Max Speed:	4800 MHz
CPU Current Speed:	2400 MHz

**Network Information**

IPv4 Address:	10.20.1.132
IPv6 Address:	fe80::180e:5573:cdb6:36c6%19
Subnet Mask:	255.255.255.0
Default Gateway:	10.20.1.1
Connection Gateway:	50.73.201.57
Country:	United States
MAC Address:	D8-9D-67-1C-9C-CC
DHCP Server:	DHCP disabled
DNS Server:	208.67.220.220 - 208.67.222.222

# Protect

- Data Security
- Protective Technology
- System Hardening
- Encryption
- Maintenance

**PROTECT**

# Protect

Schedule installation of selected patches on all machines.

- Hide machines set for [Automatic Update](#)
- Hide patches denied by [Patch Approval](#)

Click **Machines...** buttons to alter schedule or to ignore patch for individual machines.

Schedule

Cancel

**WARNING: Scheduling patch installations from this screen will override all Patch Approval Policies!**

**NOTE:** Machines that are being processed by Initial Update are excluded from this page until Initial Update completes.

**NOTE:** Patches that are currently being processed cannot be cancelled.

 indicates the patch status for one or more machines should be checked before installing this patch. Click on Machines... and review the Status column.

<a href="#">Select All</a>	<a href="#">KB Article</a>			<a href="#">Product</a>	<input checked="" type="checkbox"/> Show Details
<a href="#">Unselect All</a>	(Security Bulletin)	Missing	Ignore		<a href="#">Update Classification</a>
<input type="checkbox"/>	<a href="#">Machines...</a> <a href="#">KB2636927</a>	1	0	Silverlight	Feature Packs (Optional - Software)
	Microsoft Silverlight (KB2636927)				
<input type="checkbox"/>	<a href="#">Machines...</a> <a href="#">KB2841134</a>	1	0	Windows Server 2008 R2	Update Rollups (High Priority)
	Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems				
<input type="checkbox"/>	<a href="#">Machines...</a> <a href="#">KB2858725</a>	1	0	Windows Server 2008 R2	Feature Packs (Optional - Software)
	Microsoft .NET Framework 4.5.1 for Windows Server 2008 R2 x64-based Systems (KB2858725)				

# Detect

- Evaluation of Infrastructure Security Systems
- Intrusion Detection Systems

**DETECT**

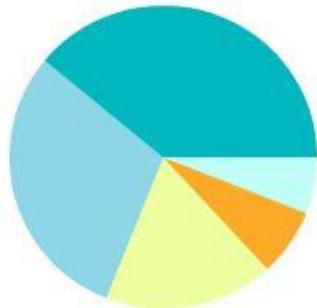
# Detect

Details Add Exclusion Delete Restore Hide Filter

Machine Name	Name	Path	Time	Status	Type
mst03132013.mst.internal	Tullio	szRestorePath	12-Mar-15 09:22	Quarantined	Unknown
mst11242014.mst.internal	RssControlZ.exe	C:\Users\rfrey\AppData\Local\Temp\SLinkSW...	12-Mar-15 08:41	Quarantined	Unknown
mst03132013.mst.internal	Tullio	szRestorePath	12-Mar-15 08:23	Quarantined	Unknown
mst09112013b.mstwatch-test.mst.i...	autorun.inf	G:\autorun.inf	12-Mar-15 06:51	Quarantined	Unknown
mst09112013b.mstwatch-test.mst.i...	c_payment_details_credit.htm	D:\Prasad\CEI Projects\NCO Doc\customer_ui...	12-Mar-15 06:51	Quarantined	Unknown

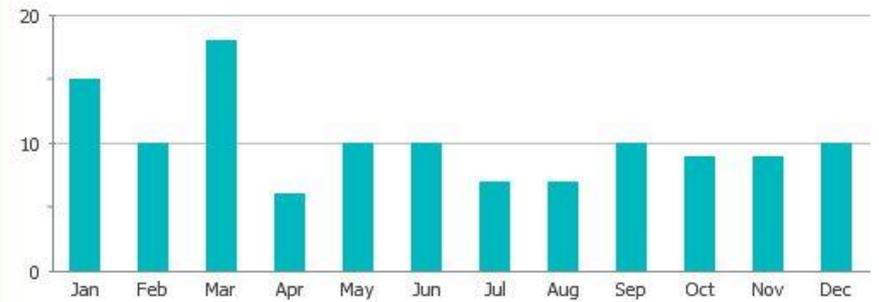
## Antivirus Detection History

### Antivirus Top Threats



- Unknown
- HEUR:Trojan.Win32.Generic
- Worm.Win32.Vobfus.bgdq
- Trojan-Ransom.Win32.Blocker.fain
- Trojan-Spy.Win32.Zbot.tms0

### Antivirus Number of Machines With Detections



# Respond and Recover

- Annual Risk Assessment
- Detection and Response System
- Disaster Recovery

**RESPOND  
AND  
RECOVER**

# Respond and Recover

## Assign monitoring on selected Machine IDs

Create Alarm  
 Create Ticket  
 Run Script [select agent procedure](#) on [this machine ID](#)  
 Email Recipients (Comma separate multiple addresses)

Apply  
Clear  
Clear All

Add to current list  Replace list

Auto Learn

Add Monitor Set  Replace Monitor Set(s)

[Select All](#)  
[Unselect All](#)

Machine.Group ID      Monitor Set

<input type="checkbox"/>	11southpeds-hp.stony_brook_university_hospital-ny.mc5.customer
<input type="checkbox"/>	1570halo1.brownwd_medctr-tx.customer
<input type="checkbox"/>	1570halo2.brownwd_medctr-tx.customer
<input type="checkbox"/>	1730wc03.northwest_medical-az.customer

https://k.mcroberts1876.com/?scriptPick=true - Se...

- Wake Up
- Sample Procedures\Managed Services\System Mgmt\Renew IP
- Sample Procedures\Managed Services\System Mgmt\Set Agent Naming
- Sample Procedures\Managed Services\System Mgmt\Shutdown
- Sample Procedures\Managed Services\Workstation Management\Default IE Page
- Sample Procedures\Managed Services\Workstation Management\Lock Workstation
- Sample Procedures\Managed Services\Workstation Management\Send Message if Logged On
- Sample Procedures\Managed Services\1 - Computer Cleanup
- Sample Procedures\Managed Services\2 - Server Maintenance

# Respond and Recover

Machine Name

- miami-dc.core.internal
- miamidispatchlt.core.internal

### Agent Procedure Status

Refresh

1 of 1 | 100 Selected: 1 | Viewing: 1-61 of 61

Procedure Name	Time	Status	Admin
K-VNC 4.x Uninstall	11:31:27 am 05/03/2013	Success THEN	mmartone
Execute Patch Scan	10:44:51 am 05/03/2013	Success THEN	mmartone
WUA Patch Scan 1	10:44:51 am 05/03/2013	Success THEN	mmartone
WUA Patch Scan 2	10:44:51 am 05/03/2013	Success THEN	mmartone
WUA Patch Scan Check	10:41:11 am 05/03/2013	Success THEN	mmartone
WUA Patch Scan PreReq2	10:41:11 am 05/03/2013	Success ELSE	mmartone
WUA Patch Scan PreReq1	10:41:11 am 05/03/2013	Success ELSE	mmartone
Patch Scan	10:40:34 am 05/03/2013	Success THEN	mmartone
Patch Required Services Check	10:40:34 am 05/03/2013	Success THEN	mmartone
Patch Post-Services Check Action	10:40:34 am 05/03/2013	Success THEN	mmartone
Reset Password 478843453985133	12:09:52 pm 12/21/2012	Success THEN	*kDefault*
vncInstall	12:09:51 pm 12/21/2012	Success THEN	*kDefault*
Update Lists By Scan	12:09:48 pm 12/21/2012	Success THEN	*kDefault*
System Info	12:09:06 pm 12/21/2012	Success THEN	*kDefault*