McRoberts SECURITY TECHNOLOGIES SINCE 1876

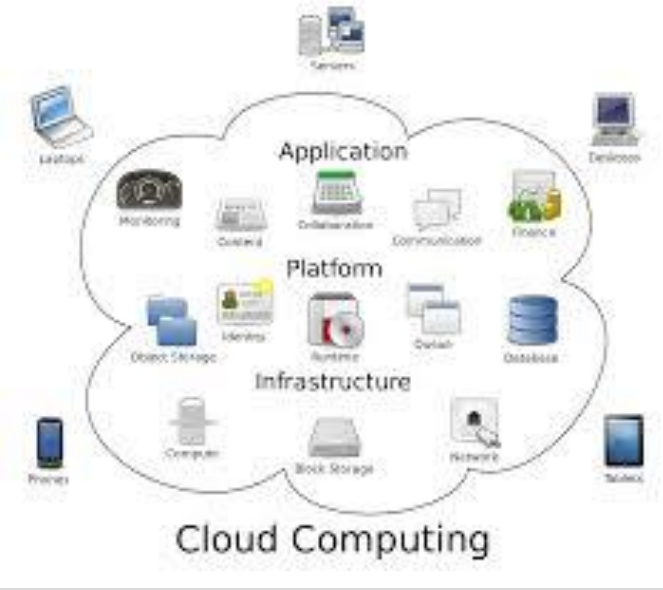
The Latest IT Trends
AAPA Cybersecurity seminar
March 12, 2015

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 Computi**
  - **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

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

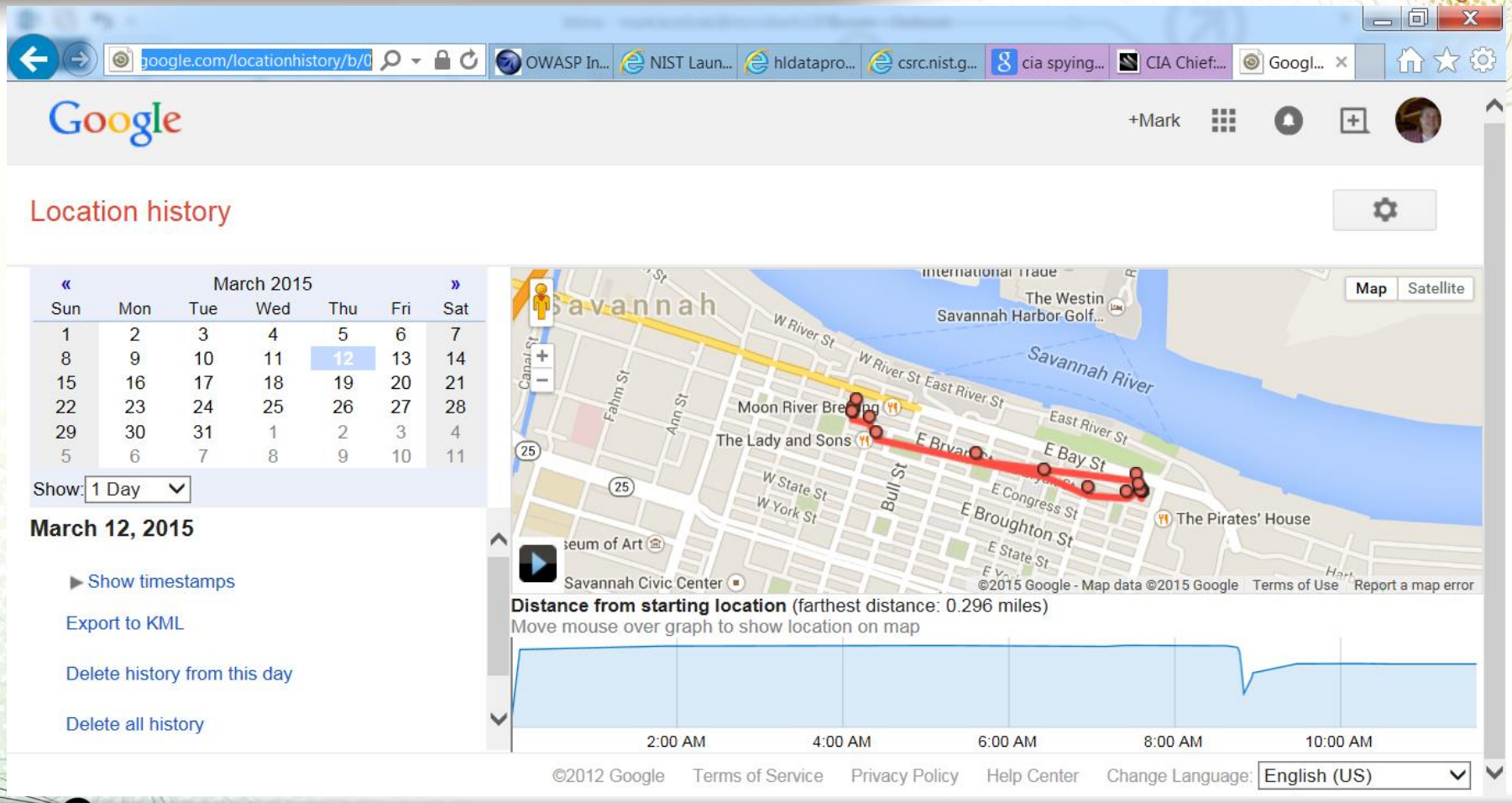
Security Implications

- 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

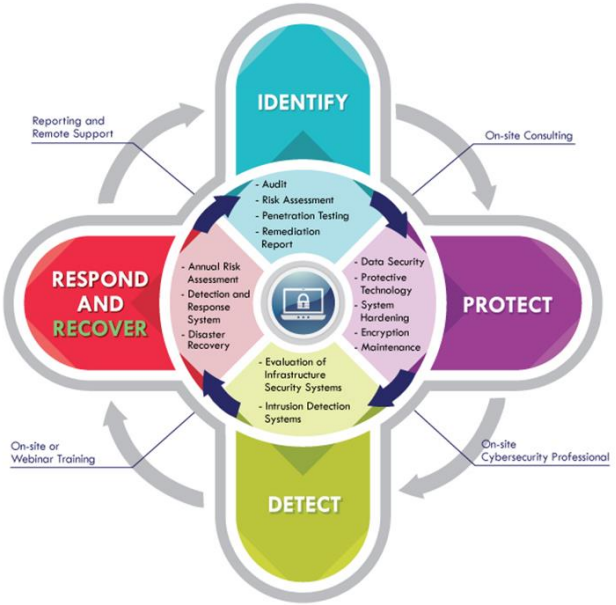
- Huawei Defends Equipment Security- 2013
  - Largest Telecom in the world
- U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts
  - Mapped the Iranian network
- How the NSA can 'turn on' your phone remotely (well not really)
- iRobot's latest Roomba robot is designed for hackers

Security Implications



Managed Services

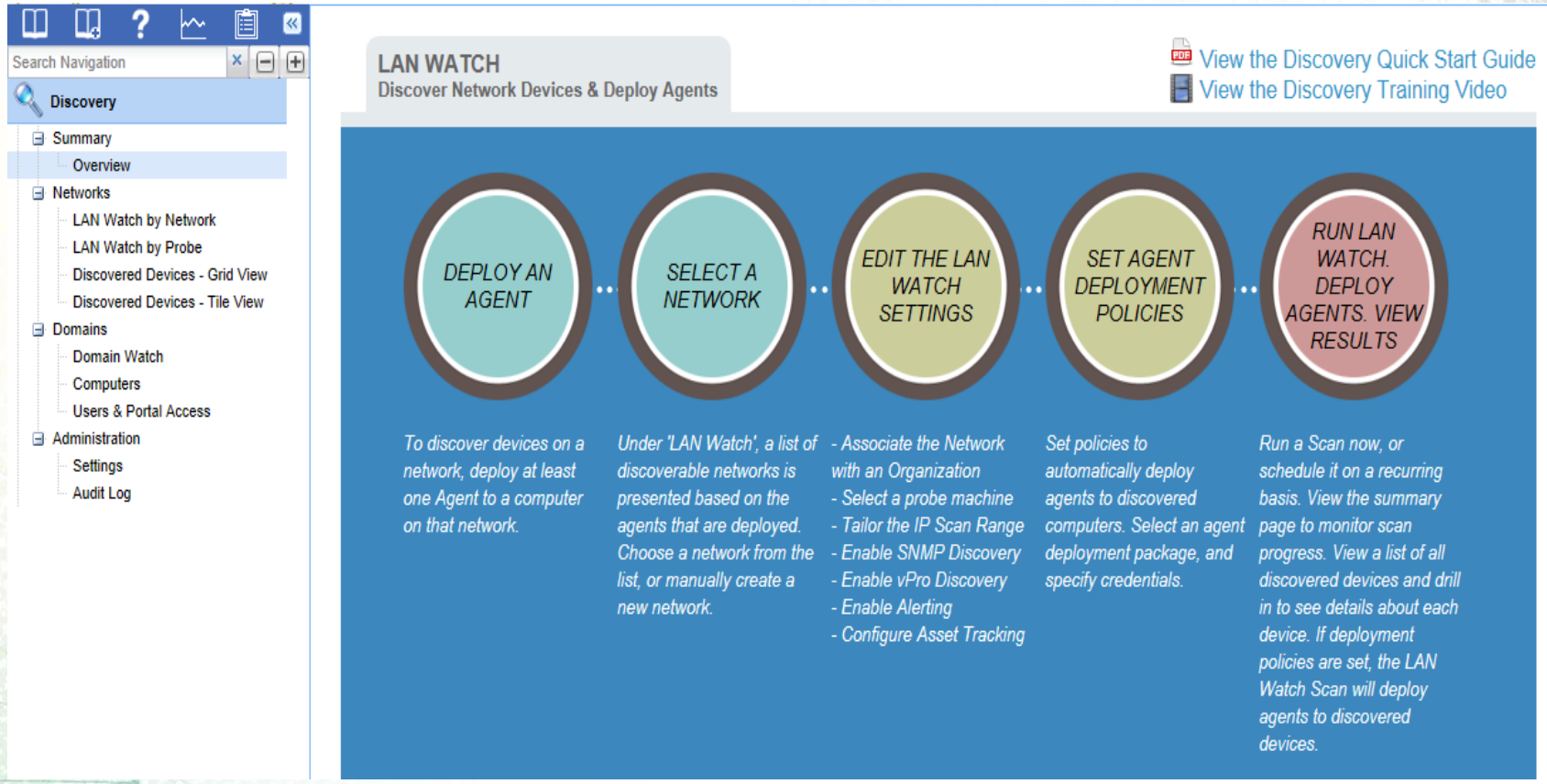
- Limited Resources
  - Budget
  - Personnel
  - Utilities/Tools
- Scalable
- Industry Compliance
  - Identify
  - Protect
  - Detect
  - Respond/Recover



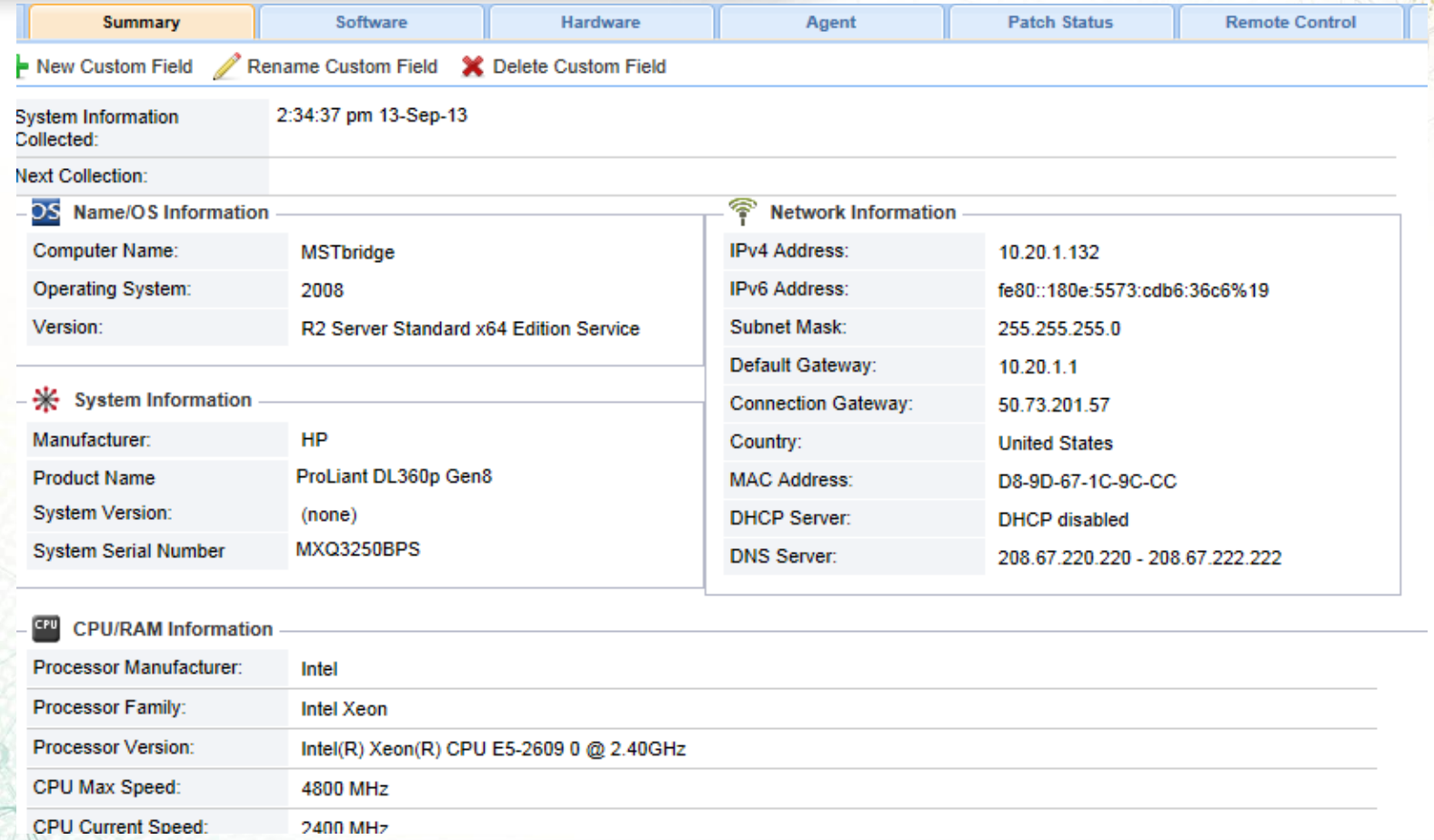
Identify


- Audit
- Risk Assessment
- Penetration Testing
- Remediation
Report
IDENTIFY

Identify



Identify



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.*

Select All / Unselect All

	KB Article (Security Bulletin)	Missing	Ignore	Product	☑ Show Details: Update Classification
☐ Machines...	KB2636927	1	0	Silverlight	Feature Packs (Optional - Software)
Microsoft Silverlight (KB2636927)					
☐ Machines...	KB2841134	1	0	Windows Server 2008 R2	Update Rollups (High Priority)
Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems					
☐ Machines...	KB2858725	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

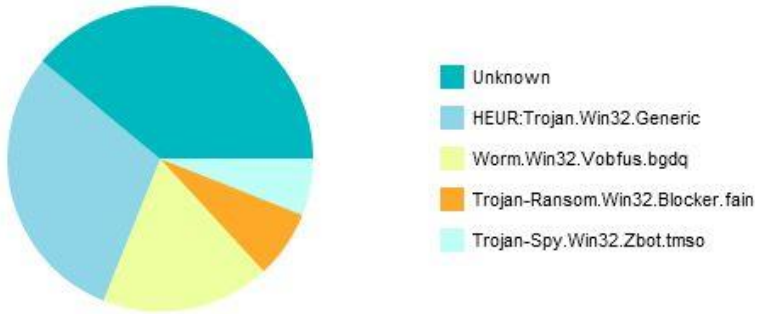
Detect

Details | Add Exclusion | Delete | Restore | Hide | Filter

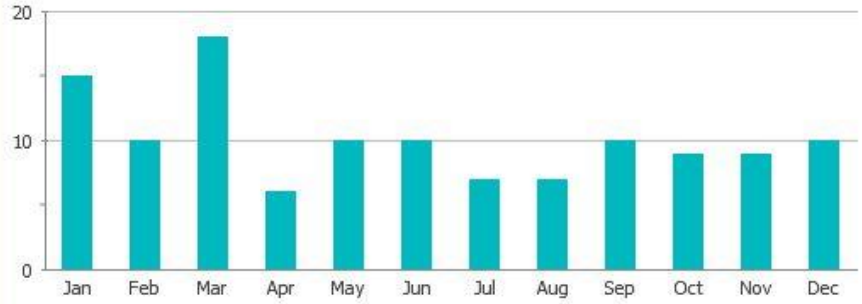
Machine Name	Name	Path	Time	Status	Type
mst03132013.mst.internal	Tullio	szRestorePath	12-Mar-15 09:22	Quarantined	Unknown
mst11242014.mst.internal	RssControlZ.exe	C:\Users\rfrey\AppData\Local\Temp\SLinkSW\...	12-Mar-15 08:41	Quarantined	Unknown
mst03132013.mst.internal	Tullio	szRestorePath	12-Mar-15 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



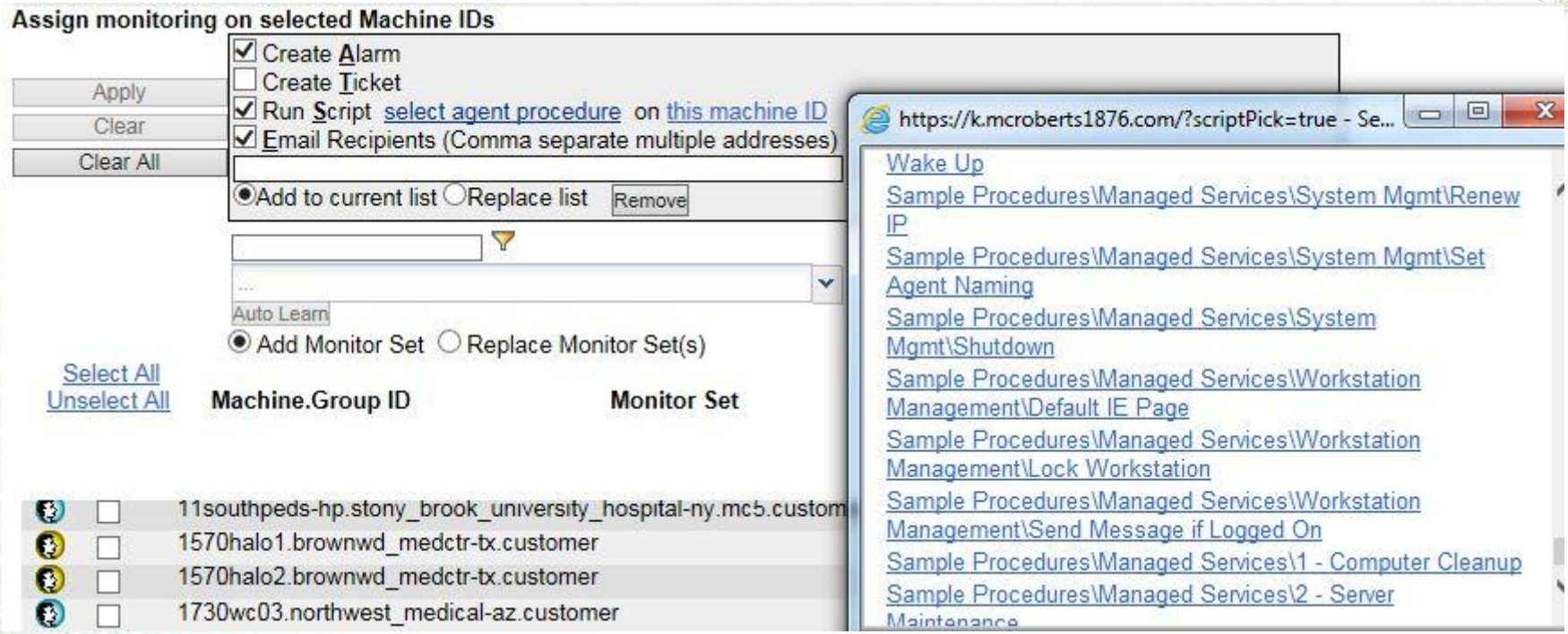
Antivirus Number of Machines With Detections



McRoberts SECURITY TECHNOLOGIES SINCE 1876

Respond and Recover

Respond and Recover



Respond and Recover