



Confidence in a connected world.



# Symantec Security Information Manager User Group Discussion

Houston / Symantec User Group

May 19, 2009

# Agenda



1 (Roadmap Removed)

2 SSIM Tricks

3 Roundtable


# SSIM 4.7 – Agent (released)



- Enable or disable encryption
  - Improved performance
- Agent Failure Notification and Automated restart in Windows
- Event Queue size configurable
- Agent Data Bandwidth Management
  - Throttling schedule
  - example: “On Tuesday, Friday, Thursday between the time 15:30 and 19:30, the agent can use 2K/sec(2048 bytes/sec) of bandwidth”


2

## SSIM Tricks



Symantec Security Information Manager - Admin

File View Tasks **Tools** Help

 Symantec™

Search Notes... F3

Change Password ...

Preferences...



# Magic Web Portal



Symantec Security Information Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address [https://\[redacted\]/imr/config/index.jsp](https://[redacted]/imr/config/index.jsp) Go

Symantec™ Security Information Manager [Log Out](#)

**Incident List**

Find:

Displaying 1..15 of 197 (0.904 seconds)

[+ Details](#) [Ticket](#) [Export](#) [Merge](#) [Close](#)

Priority	Severity	Rule Name	Created	State	Assignee	Team	Reference #
2	2	パスワード推測攻撃	Thu Apr 30 13:44:15 JST 2009	New	Unassigned	Unassigned	0000000234
4	2	パスワード推測攻撃	Thu Apr 30 13:43:47 JST 2009	New	Unassigned	Unassigned	0000000233
1	1	Merged Incident	Thu Apr 30 13:26:13 JST 2009	In-Work	Takaya	Unassigned	0000000232
2	3	System Agent Malfunction	Thu Apr 30 04:58:56 JST 2009	New	Unassigned	Unassigned	0000000231
2	3	System Agent Malfunction	Tue Apr 28 17:31:17 JST 2009	New	Unassigned	Unassigned	0000000230
5	3	退職者のアクセスを検知	Thu Apr 23 16:28:35 JST 2009	New	Unassigned	Unassigned	0000000228
4	2	パスワード推測攻撃	Thu Apr 23 15:33:52 JST 2009	New	Unassigned	Unassigned	0000000227

**Left Sidebar:**

- SP Incidents
- Incidents
- Events
- Tickets
- Assets
- Queries
- Dashboard
- Intelligence
- Health
- User Settings
- Sync Incidents

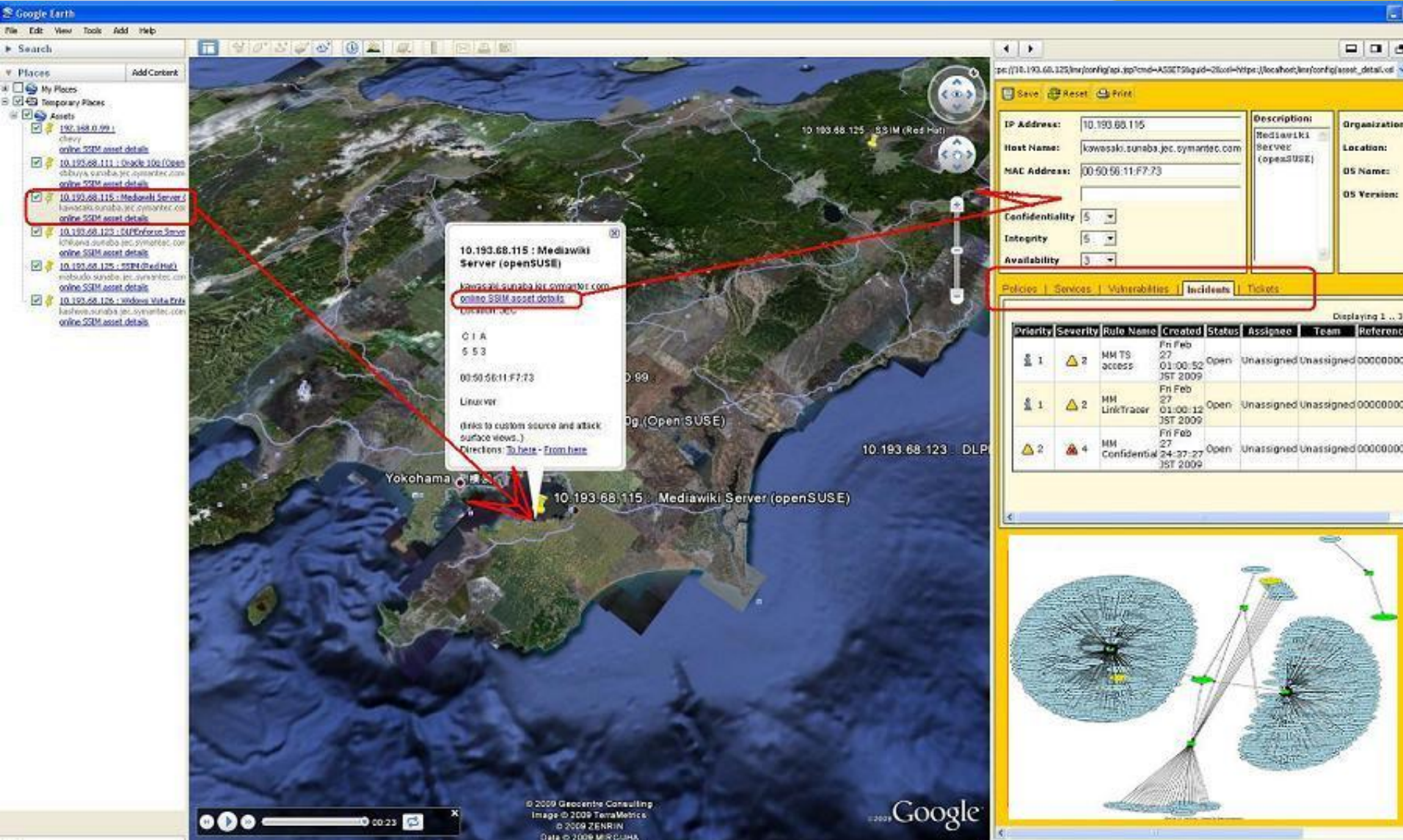
**Annotations:**

- Red circle around the sidebar menu with an arrow pointing to it.
- Text box: **Click There**
- Text box: **Type: portal**

Done Internet



# SSIM (xml) + XSLT = Google Earth (kml)



10.193.68.115 : Mediawiki Server (openSUSE)

kowasaki.sunaba.joc.symantec.com  
online SSIM asset details  
Location: JOC

C I A  
5 5 3  
00:50:56:11:F7:73  
Linux/ver  
(links to custom source and attack surface views.)  
Directions: [To here](#) - [From here](#)

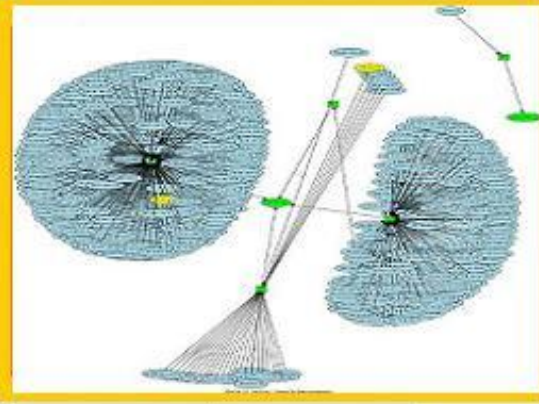
10.193.68.115 : Mediawiki Server (openSUSE)

IP Address: 10.193.68.115  
Host Name: kowasaki.sunaba.joc.symantec.com  
MAC Address: 00:50:56:11:F7:73  
Confidentiality: 5  
Integrity: 5  
Availability: 3

Mediawiki Server (openSUSE)  
Organization: Symantec  
Location: JOC  
OS Name: Linux  
OS Version: 2.6.18-028.el5

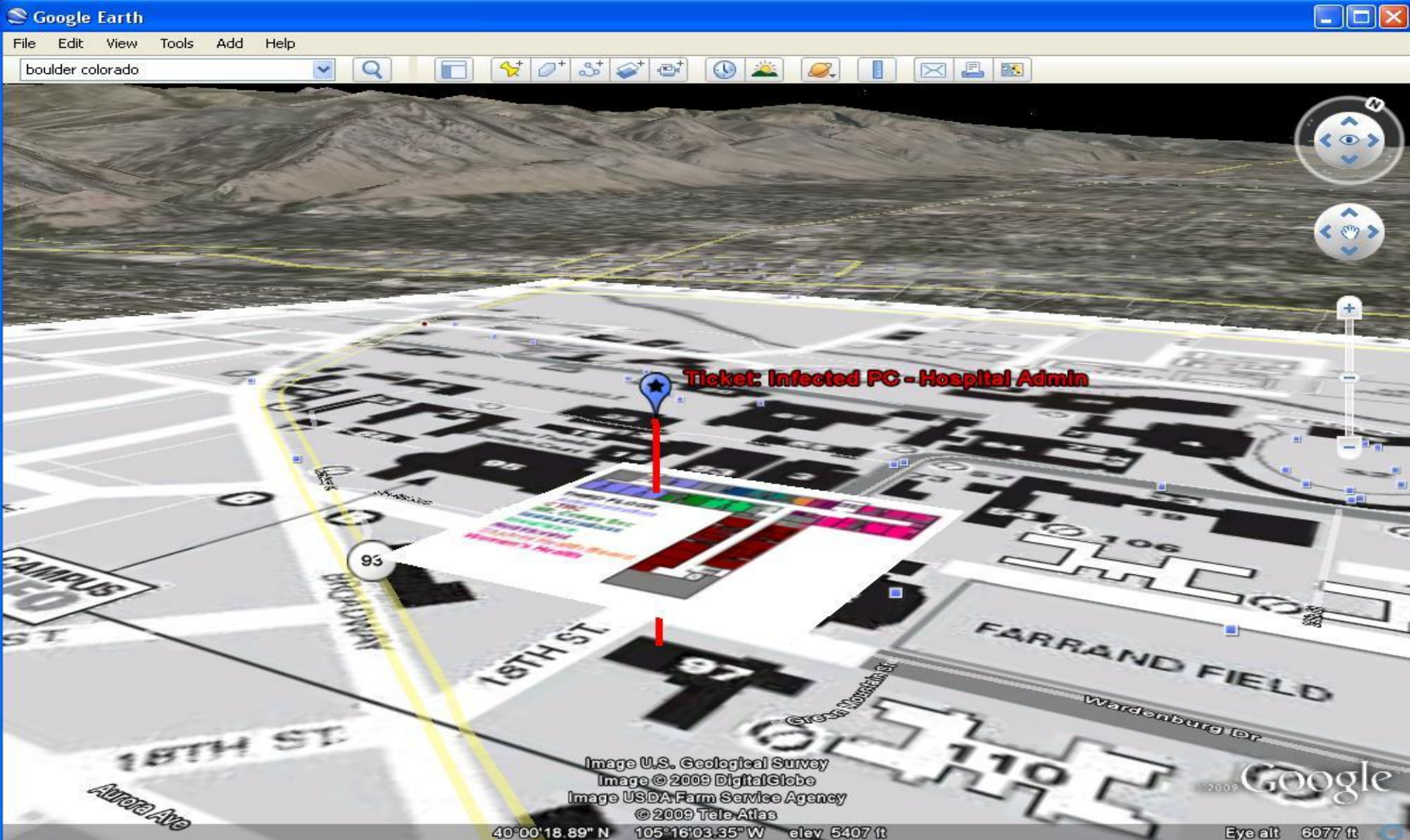
Priority	Severity	Rule Name	Created	Status	Assignee	Team	Reference
1	2	MM TS access	Feb 27 01:00:52 JST 2009	Open	Unassigned	Unassigned	00000000
1	2	MM LinkTracer	Feb 27 01:00:12 JST 2009	Open	Unassigned	Unassigned	00000000
2	4	MM Confidential	Feb 27 24:37:27 JST 2009	Open	Unassigned	Unassigned	00000000

Displaying 1..3





# Ticket Response via iPhone?





# NetBackup / SSIM – Use Case



- Monitoring the failure/success of NBU jobs.
- Related OS events that might have caused problems
  - (drivers not loaded, etc.)

- Backup\_Start
- Backup\_Cancel
- Backup\_Suspended
- Backup\_Resume
- Backup\_Complete

- Restore
- Restore\_Start
- Restore\_Paused
- Restore\_Complete

- Media\_Device
- Size of the media or size of the copied data
- Name of tape, drive
- Name of session

- Verification
- Verification\_Start
- Verification\_Success

## 3 Roundtable Discussion

# Why Did You Buy SSIM?



- Continue Symantec relationship
- GIN/DeepSight real time feed of security information
- Compliance controls and reporting
- Solution TCO/ROI
- Capability (which one)?
- Inherited solution

# Roundtable Discussion Topics

- Metrics for executive focused dashboards
  - What information is most relevant?
  - Data Sources
  - Format: dashboard or reports
  - SANS, NIST, common framework, internal company metrics
- Current usage scenarios
  - Log aggregation, Threat detection, Compliance
  - Unexpected benefits?
- Biggest threats to organization
  - Insider
  - Perimeter





Confidence in a connected world.

# Thank You!

**Copyright © 2008 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.