

Introducing Laketec Proactive Monitoring.

Make the right Decisions.



Focus On Your *Business* – We Focus on your *IT!*

At Laketec Communications, we know you can't manage what you can't measure. Our 24 x 7 monitoring, alerting and reporting service provides the information, data, network performance trending analysis and security vulnerability information critical to service, plan and manage your IT environment.

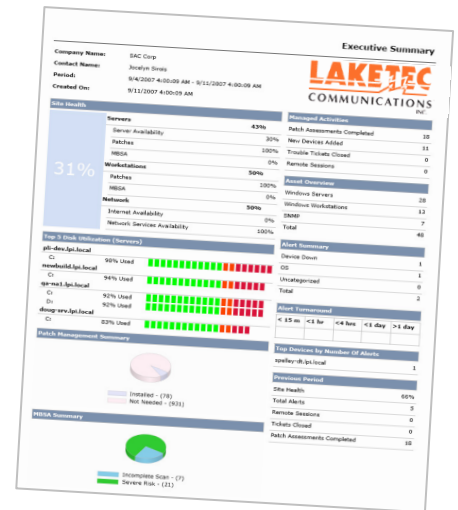
You have invested in your IT infrastructure and rely on its performance, security and reliability. Laketec's services not only ensure that you have a qualified team ready to service this critical asset but also the real time data to ensure its being done on time, when needed, using the most advanced network asset tracking and performance monitoring.

Monitoring and Reporting

- ✓ Our proactive monitoring and alerting identifies, tracks and reports on issues effecting the security, performance and reliability of your IT.
- ✓ By analyzing network device alerts, pre-failure indicators, performance benchmarks and security issues, preventative maintenance opportunities are identified.

Maximize Your Return on IT Spending

- ✓ Our service includes a complete asset inventory and regular health, security, and performance analysis reporting so that you can see what you have and how well those IT assets are working for you.
- ✓ Our improvement recommendations will help you lower your total cost of IT, including the hidden cost of downtime, substandard performance, and lost productivity due to incompatible or out-of-date software.



Features & Benefits

Security Assurance

The screenshot shows the Microsoft Baseline Security Analyzer (MBSA) interface. It displays a list of security updates, administrative weaknesses, and system information. The 'Security Updates' section shows several updates that are missing or not installed. The 'Administrative Weaknesses' section lists several issues, such as 'More than 2 Administrators were found on the computer' and 'Some user accounts (2 of 6) have long passwords'. The 'System Information' section provides details about the computer name, IP address, and operating system.

The screenshot shows the 'Patch Management - Events' report. It includes a 'Software Assets' section, a 'Patches by Status' pie chart, and a 'Device Security (MBSA - Patch Management - Events)' table. The table lists details for a device named 'lapt02r1.local', including its manufacturer, operating system, model, and IP address. A 'Scan Summary' section shows a pie chart indicating the status of the scan: 'Incomplete Scan - (1)' and 'Server Risk - (1)'.

**MBSA Reports
Site Alerts
Site Security**

Microsoft Baseline Security Analyzer Report

Reduced Risk

- Baseline security scanning to detect security holes
- Continuous monitoring for viruses, worms, spam ware, and other malware.
- Automated verification of data backup completion and identification of any failed backups

Preventative Maintenance

The screenshot shows the 'Managed Workplace Service Center' interface. It displays a list of devices with columns for 'Device Name/Alias', 'IP Address', 'Description', 'Up/Dn (hrs.)', 'WMI', 'SNMP', and 'Alerts'. The list includes various devices such as 'lapt016.destiny.local', 'lapt003.destiny.local', and 'lapt014.destiny.local'. The interface also shows navigation options like 'Status', 'Central Dashboard', and 'Patch Management'.

The screenshot shows a detailed server health report. It includes an 'Executive Summary' section with a '31%' indicator, a 'Patch Management' section, and an 'Asset Inventory' table. The report provides a comprehensive overview of the server's health, including patch status, asset inventory, and system performance metrics.

**Patch Status Detail
Server Health Report**

Preventative Maintenance

- Automated delivery of two preventative services.
- Up-to-date security patches for your desktops and servers and identification of failed or missing patches
- Comprehensive server health reports for all servers

Quarterly Business Review

Our network service program includes a Quarterly Business Review with your organization.

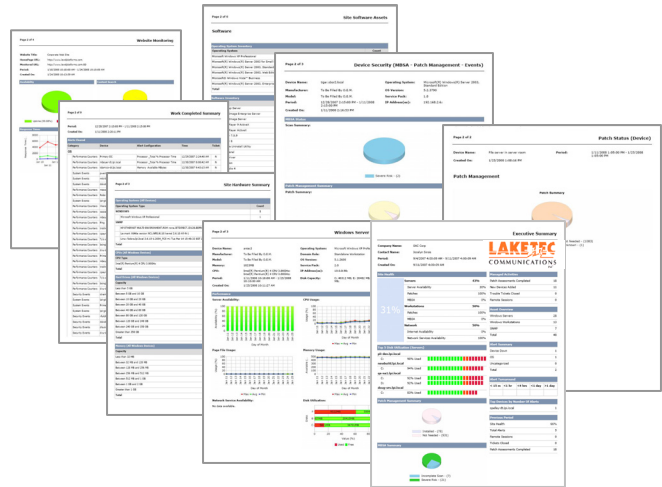
Prior to each QBR Laketec will audit all alerts and reports generated over the preceding 90 days and prepare a comprehensive analysis of our findings as well as demonstrate areas of cost savings, increased performance, any security vulnerabilities and over all health assessment of your network..

These meetings are designed to help ensure we:

- Are aligned with your IT business goals and address any changes as they occur; Present all the reports we have captured over the past quarter - ensuring you understand its overall impact to your business;

Our QBR summary and reports include:

- Executive Summary
- Website Monitoring
- Windows Server Health
- Work Completed Summary
- Site Performance
- Patch Status Detail
- Site Health
- Server Health
- MBSA and Patch Summary
- Asset Inventory
- Device Performance
- Site Performance
- Website Performance



- Review and update you on all the work completed in the last quarter and discuss project(s) in progress;
- Help identify IT solutions that will address existing and future IT requirements allowing you to ultimately make informed financial decisions.

Package Offer

- ✓ Continuous Monitoring 24x7
- ✓ Asset Management
- ✓ Security Assurance
- ✓ Preventative Maintenance
- ✓ Monthly Reports
- ✓ Quarterly Business Reviews

Company Name: CIS Corporation
 Contact Name: Jocelyn Sirois
 Period: 1/29/2008 9:50:00 AM - 2/12/2008 9:50:00 AM
 Created On: 2/12/2008 9:54:32 AM

Site Health	
39%	Servers 36%
	Server Availability 100%
	Patches 0%
	MBSA 8%
	Workstations 38%
	Patches 0%
	MBSA 75%
	Network 42%
	Internet Availability 0%
	Network Services Availability 84%

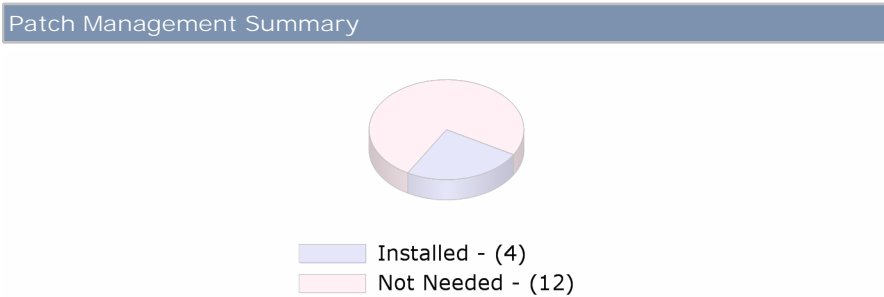
Managed Activities	
Patch Assessments Completed	75
New Devices Added	0
Trouble Tickets Closed	0
Remote Sessions	2

Asset Overview	
Windows Servers	6
Windows Workstations	2
SNMP	2
Total	10

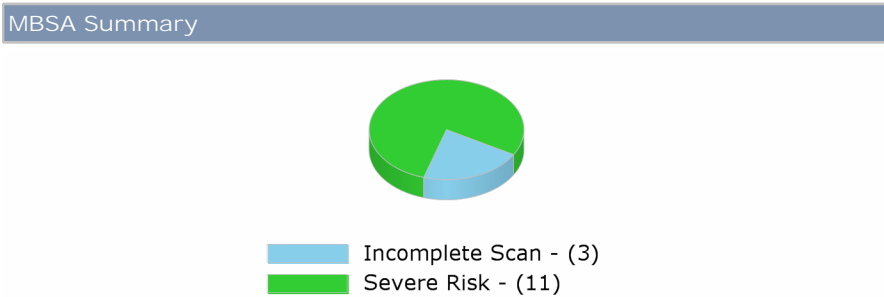
Top 5 Disk Utilization (Servers)		
webom.sbsr2.local		
C:	93% Used	
D:	53% Used	
sbs2k3r2.sbsr2.local		
C:	57% Used	
sqlwhite.sbsr2.local		
C:	45% Used	
eeom.sbsr2.local		
C:	34% Used	

Alert Summary	
Network	96
OS	51
Device Down	4
Uncategorized	0
Total	151

Alert Turnaround				
< 15 m	<1 hr	<4 hrs	<1 day	>1 day
43	1	1	0	1



Top Devices by Number Of Alerts	
sbs2k3r2.sbsr2.local	42
SBS Switch	25
sbsswitch2.sbsr2.local	23
tiger.sbsr2.local	4
sqlwhite.sbsr2.local	3



Previous Period	
Site Health	45%
Total Alerts	105
Remote Sessions	5
Tickets Closed	7
Patch Assessments Completed	30