Log Management SIMetry

A Step by Step Guide to Selecting the Correct Solution

Jim Beechey
April, 2008

Objective

- Selecting a SIM can be a daunting task in today's crowded and complex marketplace. This presentation guides you through key elements of the selection process and offers suggestions for selecting the correct solution.

  The full paper is available at: http://www.giac.org/certified_professionals/practicals/GSEC/05330.php

Introduction

- SIM - A tool capable of centrally collecting logs from a variety of sources, analyzing logs for security events and reporting based upon the data.
- SIM Marketplace – Gartner
  - "organizations may need to evaluate offerings from vendors in all quadrants, depending on their requirements. Product selection decisions should be driven by organization-specific requirements" (Nicolette & Kavanagh, 2007)
- SIM Selection Steps

1. Determine Organizational Requirements
2. Calculate System Size Needs
3. Research Available Options
4. System Evaluations
5. System Selection

Determine Requirements

- What is the primary driver for SIM?
  Compliance, Log Aggregation, Security Monitoring/Alerting

- Appliance vs. Server/Database Model
  Can your organization/area support a system which requires backend database knowledge or is an appliance required?

- What log generating devices, operating systems and applications are there on the network?

Note: See Appendix B of paper for template to help list requirements

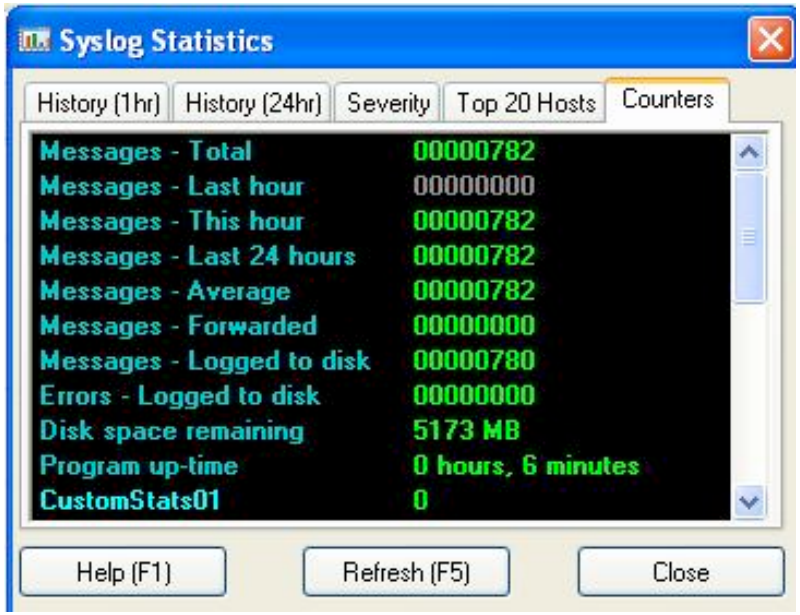
System Sizing

- Vendors will use a variety, often combination. of methods for licensing their solution. Most use some combination of number of devices sending logs and number of events per second. Some will license an entire appliance or build to your specifications.

- Calculating an estimate of events per second is usually the key metric.

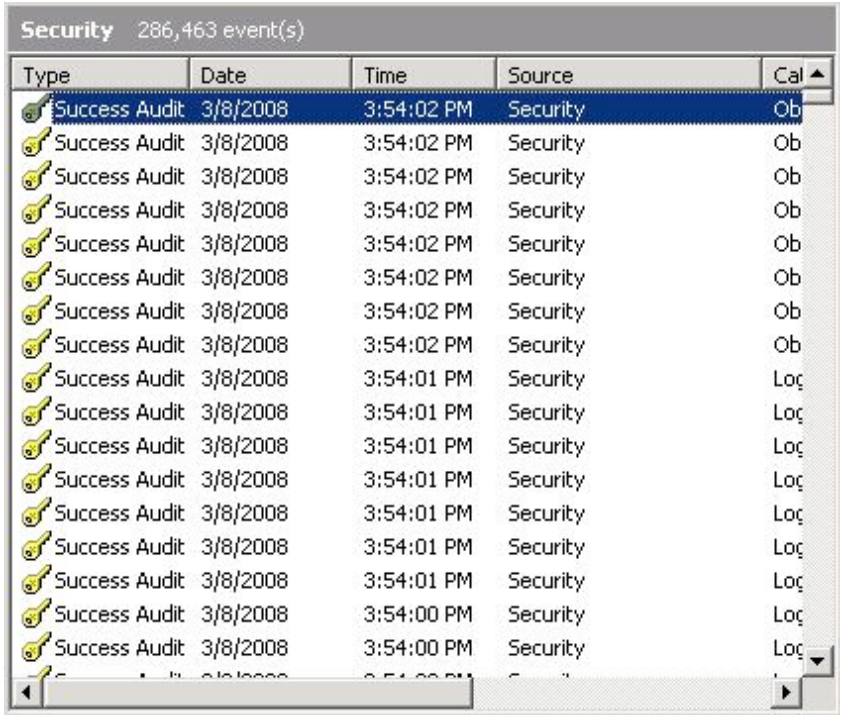
Calculate Syslog Events per Second

- Setup syslog server such as Kiwi on Windows or Syslog-NG on Linux to collect logs for a period of time



Calculate Windows Events per Second

- Use Windows Event Viewer
- 286,463 events in a 4 hours = 19.89 per second



Security 286,463 event(s)

Type	Date	Time	Source	Cal
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:02 PM	Security	Ob
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:01 PM	Security	Log
Success Audit	3/8/2008	3:54:00 PM	Security	Log
Success Audit	3/8/2008	3:54:00 PM	Security	Log

Security 286,463 event(s)

Type	Date	Time	Source	Cal
Success Audit	3/8/2008	11:54:20 ...	Security	Log
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Log
Success Audit	3/8/2008	11:54:20 ...	Security	Log
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Log
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob
Success Audit	3/8/2008	11:54:20 ...	Security	Ob

Key Issues/Differentiators

There are many options and features to consider when evaluating a SIM. Below are four that I believe to be key.

- Device/OS/Application Support
- Log View and Search Capabilities
- Network Behavior Analysis Integration
- Reporting

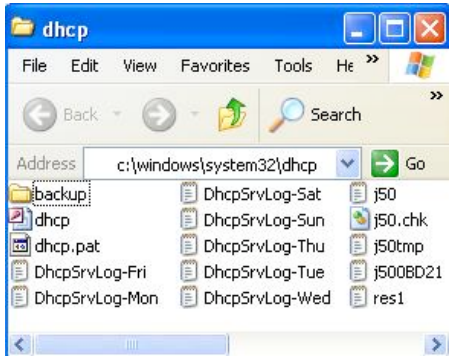
Device and Unix/Linux Support

- Check for support based upon manufacturer, device and version
- Example from our evaluation
  - Vendor - “We support Juniper products”
  - Reality – They supported Netscreen firewalls, but not any other Juniper products.
- Most vendors support “syslog from Unix/Linux”, but what kind of events can be correlated?

Windows Support

Windows Server 2003 and prior do not support syslog natively in the event log. Three key question to ask about Windows are:

1. How do you collect Windows logs?
2. Which agent do you use if required?
3. Can the agent be centrally managed?
4. Can you collect logs not in the event viewer?
   (DHCP and MS-SQL for instance)



Log View/Search Options

- Raw logs may be required for forensic purposes and may allow for better search and reporting.
- Example of normalized and raw logs (data altered)

Event Name	Device	Event Count	Time	Category	Source IP	Source Port	Destination IP	Destination Port	Username
Account Logon Failed	SERVER1	1	18:16	Auth Server Login Failed	192.168.1.1	0	192.168.2.2	0	testuser

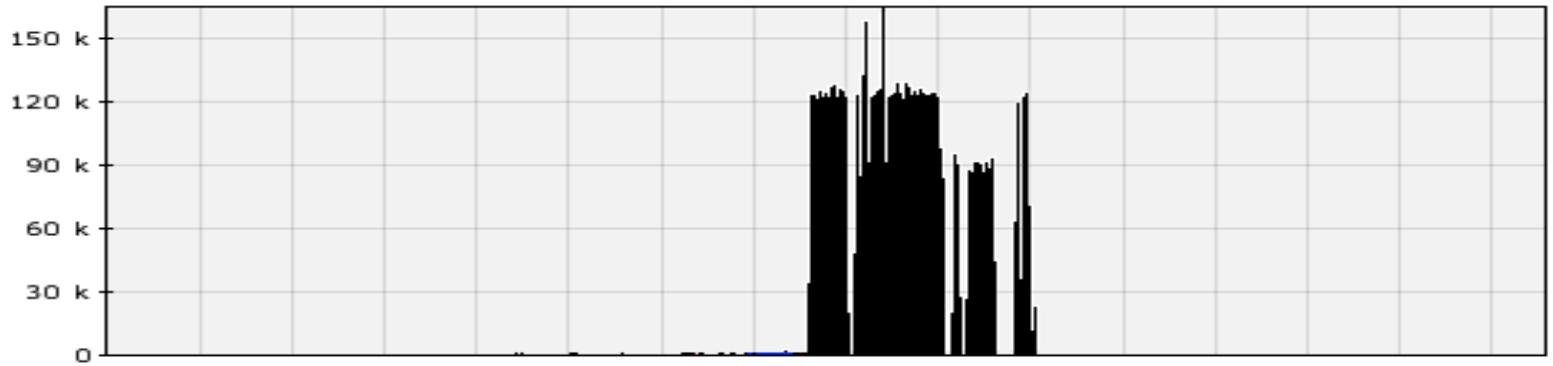
<13>Mar 08 18:16:45 192.168.1.1 AgentDevice=WindowsLog.AgentLogFile=Security.Source=Security. Computer=SERVER1.User=SYSTEM.Domain=.EventID680.EventIDCode =680.EventType=16.EventCategory=9.RecordNumber=546602486. TimeGenerated=1205018206.TimeWritten=1205018206.Message=Logon attempt by:MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: testuserSource Workstation:TEST Error Code: 0xC00006A

Network Behavior Analysis

- The integration of network flow data with system logs can increase the visibility of a SIM
- Some SIM vendors provide flow collection and analysis included in their solution while others integrate with third party NBA solutions.
- The following examples show the advantage adding flow data to your solution

NBA Examples

- Call comes in about Internet connectivity issues. Firewall CPU is high. SIM shows the following:
  - Packets/sec from DNS server are through the roof (see graph)
  - Because the flows are capturing some content we are able to search the flows and see DNS traffic to zen.spamhaus.org
  - Able to quickly identify the problem server and service



Reporting

- Most systems offer compliance reports
  - If compliance is a driver, you might consider taking sample reports to management for review

- Ensure that device level reporting is available.
  A daily PCI report counting failed logins is ok, but a report showing those counts by device with accounts and IP addresses is much more useful for identifying issues.

Summary

SIM can be a very powerful tool in your organization's overall security program. SIM can help to address many issues on both the security and operations side of IT. Selecting the correct SIM boils down to determining your organizational requirements and evaluating solutions based upon those needs. In the end, your solution should help create a more efficient and effective security organization. Good Luck!!

Good luck!!